ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

IoT AND CYBERSECURITY APPLICATIONS IN THE MILITARY

Anishka Rao
Euro School, Airoli
anishkarao02@gmail.com

Abstract

This paper is based on a situation where robotic soldiers and biomechanical robotic prosthetic limbs are used to fight battles and wars. This paper is based on the hypothetical, yet possible circumstance where the artificial intelligence-oriented devices are hacked mid battle, costing humans their lives, and aims to find a solution using a coordination between the Internet of Things and Cybersecurity to prevent such an issue from happening, or resolve it if it occurs. It explores the uses of IoT and Cybersecurity and how a protective software can be developed using them.

Keywords:*Internet of Things, Cybersecurity, Military, malware, Internet of Robotic Things, cyberattacks.*

Introduction

Technology is becoming a major part of everyone's lives in today's world. One part of this is the Internet of Things (IoT). The Internet of Things refers to physical devices containing sensors, software and many other technological conundrums meant for the exchange and sharing of data over a network like the Internet. IoT is very commonly used today, with its capabilities growing more and more by the day. Another important and common technology is Cybersecurity. With more devices connected over a common network – the internet – cyber threats become a rising danger. Cybersecurity is particularly important for a device part of any network to remain secure. One uncharted use of IoT and Cybersecurity is in the Military. A very recent development in the IoT industry is the Internet of Robotic Things (IoRT). This technology is being made specifically for robots using Artificial Intelligence. These robots use various kinds of sensors, metal detectors, integrated circuit systems and wireless cameras to receive and interpret data, and then carry out a certain task related to the data received. [1]We see robotic soldiers and weapons being built with A.I., but what do these ultimately require to function? The answer is IoT. Along with this, it is very important for lethal devices like these to prevent any malfunctions for the sake of the people working with them. Here is where Cybersecurity comes into play. The objective of this paper is to determine how IoT and Cybersecurity can be used together in the Military to improve efficiency of the technology being created while ensuring safety of those working with them.Interpretation of this paper will require basic knowledge in Computer Science and Information and Technology, as well as awareness about cybersecurity. [2]

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

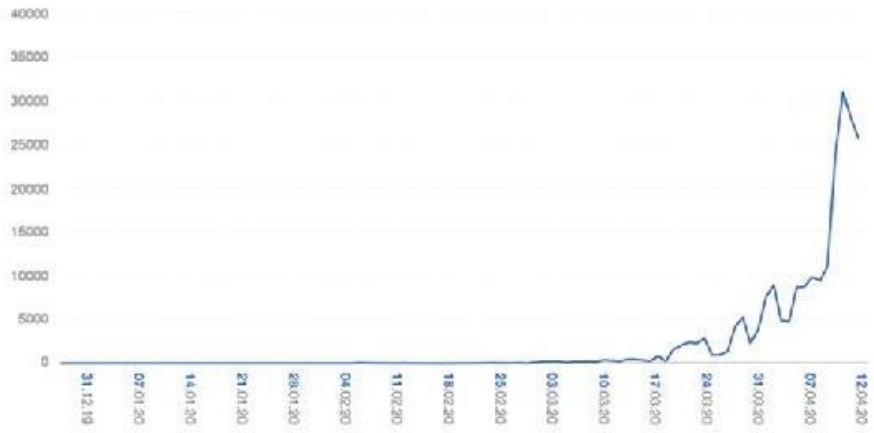
MISA
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

Theory

The Internet of Things is defined by its name. Billions of devices connect to the internet over a wireless network to share data and information, and this is IoT. IoT devices are widely used in smart homes or connected homes, but they can also be a simple wireless pet camera or a medical device implanted in your body such as a pacemaker. These devices connect to the internet. They work by using sensors, microprocessors and actuators.

The sensors in the IoT device sense and record data in the form of binary digits (1s and 0s). This data could originally have been in analogue form like sound, pressure, temperature, movement, light, moisture, humidity, and many more. Once the sensors record the data, it is transmitted to the microprocessor where it is analyzed and interpreted. Incase of alarm systems, if this data is outside the acceptable range, the microprocessor sends a signal over a network giving instructions to an actuator that performs a physical task like sounding an alarm. In case of a smart home, this microprocessor will interpret the data and send an appropriate command or instruction over the internet to perform a task such as turning on the lights. What makes IoT devices smart is their capability of machine learning, where certain algorithms help a machine remember a user's preferences or choices, and recommend options related to those. Connecting over a common network – the internet – can be resourceful, however it makes a device vulnerable to hacking and malware.[3]

Cybersecurity is the process and method of preventing cyberattacks on devices and networks, and recovering said devices and networks when these attacks happen. Cybersecurity is very important in today's world as without it, cybercriminals could use malware to steal and destroy sensitive data and files, or even extort money. Cyberattacks are a growing cause and have destroyed many businesses, reputations of people, as well as the financial lives of people. [4]



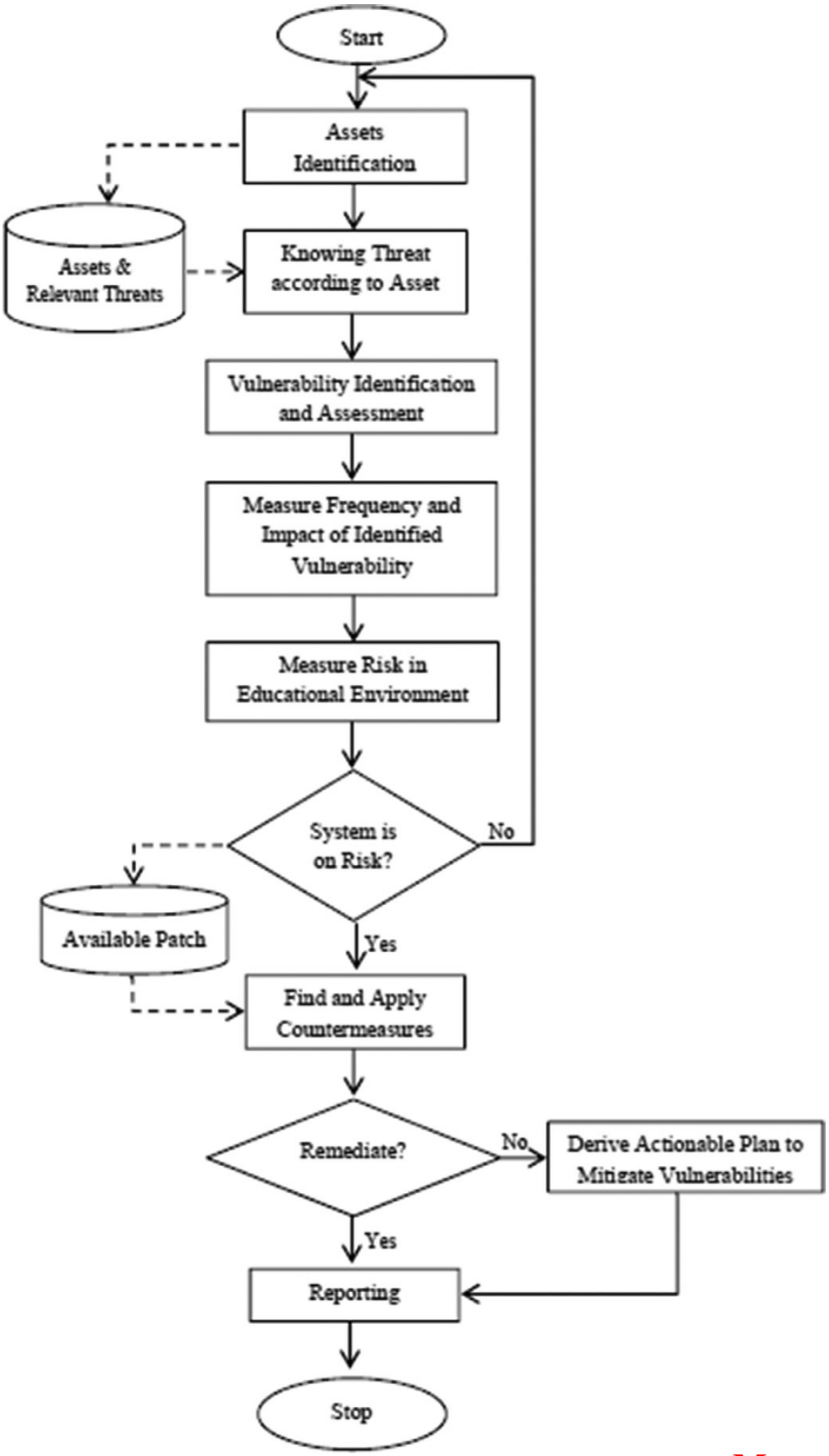
Source: Check Point Software Technologies, "Coronavirus update: as economic stimulus payments start to flow, cyber-attackers want to get their share too", Check Point Blog, https://blog.checkpoint.com/2020/04/09/coronavirus-update-as-economic-stimulus-payments-start-to-flow-cyber-attackers-want-to-get-their-share-too/

Cyberattacks are a growing cause for concern, and the recent pandemic hasn't helped a lot. Over the last few years, with the advancement of technology, cyberattacks have increased more and more in number. Even though cybersecurity software like anti-virus and anti-malware has been developed, so have various methods of penetrating software and malware. In 2016, a business fell prey to a ransomware attack every 40 seconds.According to a report by Cybersecurity Ventures, this is anticipated to increase to every 11 seconds by 2021.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal



This flowchart explains the basic logic used in a cybersecurity system. First, the suspicious files – the ones that could possibly be under attack – are identified. The threat is then acknowledged and assessed according to the file as well as in general. The impact the vulnerability has created is then measured – whether it has corrupted a file, or if it has accessed private information, or if it has extorted money – and if the system is at risk, appropriate countermeasures and counterattacks are applied. This process is repeated until the threat is fully eradicated.

The Internet of Robotic Things (IoRT) is a fairly recent technology that combines simple principles of robotics with the Internet of Things to allow robots to sense and analyze

their surroundings using IoT technologies like sensors and microprocessors to connect to the internet and perform tasks on their own using machine learning. These robots can decide courses of action based on the conditions in their environment by manipulating and controlling objects in the physical world. The main difference between IoT and IoRT is that IoT is designed to handle and perform specific tasks while IoRT is designed to help robots react to unexpected conditions. [5]

IoT and cybersecurity must work together to ensure efficient and safe use of the devices. The same logic, as mentioned in the flowchart above, is used to do so. There are different measures that can be taken to protect a device from malware and ransomware. This is done using anti-malware and anti-virus software, along with firewalls. This helps protect and secure the network the IoT is a part of, thereby securing and protecting all devices on the network. Another way of protecting data is through physical authentication and verification systems like biometric sign-ins on computers. These would ensure data doesn't fall into the wrong hands. The Public Key Infrastructure strategy uses cryptographic public and private key pairs to ensure secure forms of communication, data exchange and money exchange. This is sometimes referred to as encryption.[6]

IoRT is used in the recent military robotics projects in which robots are being developed for the military with the capabilities of a soldier. Even biomechanical prosthetic limbs that perform the task the user thinks of uses IoRT. Sensors in the robot's surroundings pick up information that is transmitted to the microprocessor, and a task is performed by the actuator. However, when it comes to these devices, getting hacked can endanger the lives of the people wearing the prosthetic limb, or the soldiers fighting alongside the robot. This is the reason a reassuring cybersecurity system must be installed.

The logic of the cybersecurity system is to detect a threat, analyze how dangerous it is, and then repair it with a counterattack. To interlink cybersecurity with IoT, we would have to use the principles of IoT and IoRT technology; sensors and microprocessors. The following hypothetical situation can be used to explain the concept. During a battle, there are two sides. The side opposing the robot soldier or the soldiers with prosthetic limbs is likely to cause a cyberattack. There are three ways this cyberattack could be detected:

1. The cyberattack uses malware that causes the robot to malfunction
   This would cause parts of the robot to fire in the wrong direction, fire at itself, stop moving, move in the direction of civilians, fire the wrong weapons, or go into a "stealth mode". The sensors used to detect these would be motion sensors, temperature sensors, pressure sensors and optical sensors. Since these robots use machine learning, the sensors and microprocessors could detect these attacks by looking for anomalies in movement patterns of the robot, looking for a sudden change in direction (coordinate system) or if there is damage to any part of its exoskeleton. They could also analyze the input data and look for the use of the wrong weapons, or extreme use of unauthorized weapons. To analyze if the robot is movingin the direction of the civilians, facial recognition could be used to see whether the people it is moving towards are wearing uniforms.
2. The cyberattack causes intentional friendly fire

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

This would cause the robot to fire at its fellow soldiers. This could be detected using sensors and microprocessors. The data will be input using optical sensors and image sensors, and will be sent to the microprocessor. The microprocessor will then run this data through facial recognition software which will determine the identities of the soldiers the robot is firing at. If the data matches the robot's fellow soldiers, it will be identified as intentional friendly fire.

3. The cyberattack deactivates the robot
   This would cause the robot to stop moving and functioning completely. This could either be detected using a possible back up system in the robot, or would require visual assessment from the fellow soldiers. If a backup system is available, it can be used to counterattack and reactivate the robot's system. If a backup system is not available, the cyberattack can only be prevented.

For all of these situations, if the data is out of the acceptable range, and if malware or a cyberattack is detected, a counterattack will be administered by a protective software. This will follow an algorithm where if a check for firewall comes back negative, a check for malicious software possibilities comes back positive, and any abnormal data or code apart from the original is detected, a counterattack will be ordered. The countermeasure will include a new firewall being put up, a thorough reboot of the robot's system being performed, and an anti-virus or anti-malware code being used to destroy the malware along with the hacker being tracked and identified.

Methodology

Aprotective software can be created to respond to these threats and prevent them. The algorithm for this is shown in the following flowchart. Before the flowchart begins, data from the microprocessor will be input into the cyberattack detection software. This data will then be analyzed to see if it is in the acceptable range. If it is outside the acceptable range, a threat has been detected. Next, the software will check if the firewall has been penetrated. If it has, the software will then review if any abnormal code has been detected. This could be malicious software that is causing damage to the robot. To rule out any known bugs, the software will check if the code is from an unidentified source. If this is true, the level of danger of the threat will be evaluated. If the threat turns out to be dangerous, and if it is the cause of the malfunctioning of the robot, countermeasures will be taken. A new firewall is created and an anti-malware or anti-virus software or code is administered. A signal is then sent to track the IP Address of the source of the threat and its location is found. The hacker is identified and added to a list of offenders to be found later. Lastly, a thorough reboot of the robot's system is performed to repair internal damage, and the robot is fully functional again. This protective software system will also prevent a cyberattack from happening as machine learning could also help the microprocessor analyze and predict if a threat is possible. If it is, a stronger firewall will be installed.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

Conclusion

This algorithm will not only prevent a cyberattack from occurring, but it will also neutralize the threat that has appeared in the robot's system. This can be used in any IoRT device to protect it in a way that uses IoT along with cybersecurity and not just the latter. After this algorithm, once the robot has rebooted, the offender will be tracked and retaliatory actions will be taken. The machine learning in the robot's system will allow it to analyze the threat and create a stronger security system to prevent attacks of the same kind. This is how IoT and Cybersecurity can be used together to create a protective software.

References

1. "The Internet of Robotic Things (IoRT): definition, market and examples." I-scoop.eu. https://www.i-scoop.eu/internet-of-things-guide/internet-robotic-things-iort/ (Accessed Jul. 4, 2021).
2. "What Is IoT?." Oracle.com. https://www.oracle.com/in/internet-of-things/what-is-iot/ (Accessed Jul. 4, 2021).
3. K. Chivers. "What is the Internet of Things? How the IoT works, and more." Norton.com. https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html (Accessed Jul. 11, 2021).
4. A. Johansen. "What is cyber security? What you need to know." Norton.com. https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html (Accessed Jul. 11, 2021).
5. K. Matthews. "The Internet of Robotic Things: How IoT and Robotics Tech Are Evolving Together." Iot.eetimes.com. https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/ (Accessed Jul. 11, 2021).
6. N. Agarwal. "How to Ensure Cybersecurity in the Age of IoT." Appinventive.com. https://appinventiv.com/blog/how-to-ensure-cybersecurity-in-iot/ (Accessed Jul. 11, 2021).