ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 4 (2024)
https://doi.org/ 10.62019/abbdm.v4i4.261

Analysis of the Effects of Cyber Attacks on Battery-Powered Internet of Things Devices

Iqra Javed, Arshad Mehmood, Ahthasham Sajid*, Mahtab Khalid, Muhammad Khurram Ameer, Wajid Ali, Ishu Sharma

Chronicle

Article history
Received: 1st December, 2024
Received in the revised format: 12th December, 2024
Accepted: 30th December, 2024
Available online: 31st December, 2024

Iqra Javed, Arshad Mehmood, Ahthasham Sajid* and Mahtab Khalid are currently affiliated with the Department of Information Security and Data Science, Riphah International University Islamabad, Pakistan.
Email: haniakiani123@gmail.com
Email:arshad.mehmood1@riphah.edu.pk
Email:ahthasham.sajid@riphah.edu.pk
Email: maazimahtab1162@gmail.com

Muhammad Khurram Ameeris currently affiliated with the Comsats University Lahore Campus, Lahore, Pakistan.
Email: khurram_chohan@live.com

Wajid Ali is currently affiliated with the Bahria University Lahore Campus Computer Science, Lahore Pakistan.
Email: 4750526@gmail.com

Ishu Sharma is currently affiliated with the Chandigarh Group of Colleges, Jhanjeri, Mohali, India.
Email: ishu.sharma001@gmail.com

Corresponding Author*

Abstract

A New Paradigm: IoT The Internet of Things (IoT) has changed our living and work style by connecting day-to-day devices to the internet. But along with this increased connectivity comes an increased risk of cyber-attacks. This is especially true for IoT devices powered by batteries, which have a finite amount of resources at their disposal. This is an abstract that focuses on studying the impact on battery-operated Internet of Things devices through cyberattacks and identifying difficulties in securing those kinds of devices. The fundamental consequence of cyber-attacks on battery powered IoT devices is that they may potentially cease to function, temporarily or permanently. This can happen if the attack damages the device, or if the device drains its battery trying to defend itself against the attack. As they go through the Installation add the library it may work fine but in other words, will lead to inoperability and loss of functionality to the user. If that wasn't bad enough, right after the initial infection, the first thing that is going be run is a backdoor, which means an attacker can get access to the device (or to the network where the device is located). Data breaches, robbery of sensitive data, and other safety violations can follow. Also, a cyber-attack against a battery-powered IoT device may result in the device consuming more energy than usual. Which can cause the device to discharge faster, or the device can get heat up and even get damaged. There are a number of difficulties that arise in securing battery-powered IoT devices. The devices need to operate on reduced power resources, thus making it complicated to enforce security measures. Considering the battery-operated IoTs that are designed to operate at low power, it becomes challenging to implement advanced security features. Moreover, a lot of these devices are purpose built, and won't have the required hardware or software to run robust security features. Overall, cyber-attacks on battery-driven IoT devices may pose a fatal threat to the device itself and the existing data network. These types of devices should be protected from cyber attacks with stringent security measures. However, as these devices generally operate on low-power and have unique design considerations, securing them presents a variety of challenges. More research should focus on providing solutions for these challenges, and on protecting the security in battery-powered Internet-of-Things devices.

Keywords: IOT, Cyber Security, DDOS

© 2024 EuoAsian Academy of Global Learning and Education Ltd. All rights reserved

INTRODUCTION

Cyberattacks against battery-powered IoT devices can pose a risk to life and health as battery-powered IoT devices are widely used in critical infrastructure and, if compromised or malfunction, have the potential to threaten the health and safety of humans. The cybersecurity risk of a cyberattack affecting an Internet of Things battery powered device could be a reduced remaining battery life. If an attacker is successful in accessing the device and can continuously execute programmes or commands on the device, the battery of the device will get drained before it can be recharged and the device will no longer be functional as mentioned by (Arkorful & Abaidoo, 2015,Winzer et al., 2018,Banica, Burtescu, & Enescu, 2017,GoP, 2018,Abbasy & Quesada, 2017,Turcu & Turcu, 2018) . This might be particularly worrying if the equipment is used for matters of safety or emergency, such as a smoke detector or a medical device. Outcome No. 6: The Functions Or Data Of An Internet Of Things Device That Runs On A Battery Or A Cyberattack3. An attacker, for example, could tamper with the controls of a smart lock or have an impact on the readings or output of a smart thermostat. This may cause the device to either stop working, or to provide incorrect information, both of which can have life-threatening consequences based on the type of device and its use case.

In the grand scheme of things, cyberattacks on battery-powered Internet of Things (IoT) devices can have the potential to cause adverse consequences that surpass the immediate impact on the device. A cyberattack on a technology used as a critical part of an infrastructure, like a power grid or transportation system, could for example lead to a disruption or outage with far-reaching effects on many people. Overall, it should be ensured that battery-powered Internet of things device is safe from cyber attack and consequences thereof. This could mean protection through strong passwords and regularly updating the device software to seal any possible weaknesses. Hackers could also launch cyberattacks against battery-powered Internet of Things devices, which could have economic consequences. If the device is vulnerable, it might also need to be replaced, which can be pricey. Moreover, in case of an attack on an Internet of Things device that disrupt an essential infrastructure or will generate problems that would be widespread, it could lead to massive financial loss for corporations and other institutions Anandaraj & Indumathi, 2020,Osanaiye, Choo, & Dlodlo, 2016,Salemi et al., 2021.

Companies whose Internet of Things devices powered by batteries are hacked in a cyberattack could also experience reputational repercussions from the event. If the attack affects the people or the society as a whole, then it can harm its reputation, and as a result, the company may tend to lose clients. In some cases, cyberattacks on battery-powered Internet of Things devices may have even legal consequences. Both an instance of some physical phenomenon (such as dangerous for humans or destruction of property) and a business responsible for the device could be responsible for the attack consequences(Aysa, Ibrahim, & Mohammed, 2020,Kambourakis et al., 2007,Tekleselassie, 2021,Ali et al., 2022,Mishra & Pandya, 2021,Van Rijswijk-Deij, Sperotto, & Pras, 2014). They should be aware that they can be the target of cyberattacks that affect the battery-based Internet of Things devices they own, leading to severe consequences. This might involve keying security measures such as robust passwords and regular software updates, as well as teaching personnel on how to spot and avoid such threats (Cvitic et al., 2022,Perez-diaz & Cantoral-ceballos, 2022,Doshi, Apthorpe, & Feamster, 2018,Aytaç, Aydın, & Zaim, 2020).

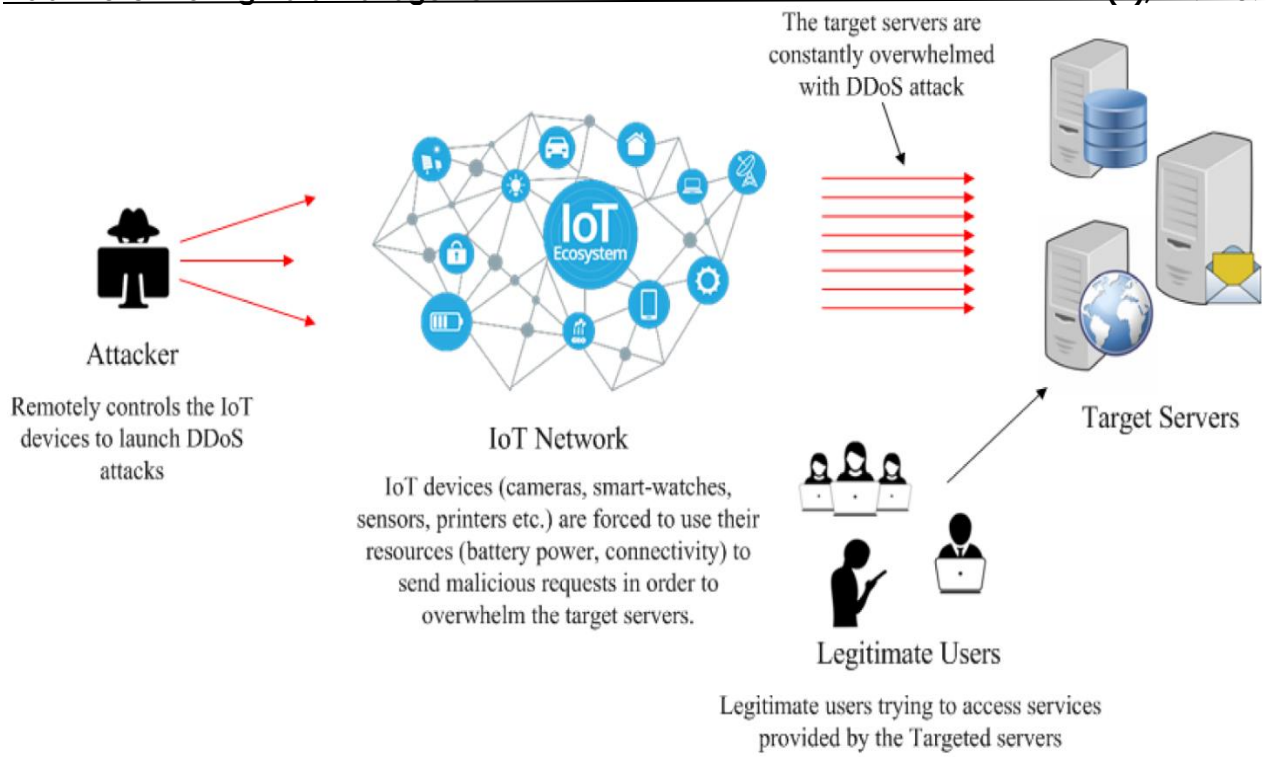

Figure 1:
Cyber Attacks and IoT

IoT gadgets are user-friendly and convenient in many ways, including being small, having wireless connectivity, and being simple to set up and operate. Temperature, humidity, and sound level sensors are common components of these gadgets, and their inclusion in a network makes it possible to operate them from a smartphone or personal computer. Examples of first-generation wireless sensor network devices include the Zolertia Z1, Sky Mote, and Tmote. These gadgets' next-gen counterparts, known collectively as Internet of Things (IoT) gadgets, come prepackaged as consumer-friendly, plug-and-play smart home essentials. Companies like Amazon have implemented these IoT devices into their dash buttons Arkorful & Abaidoo, 2015. Compact and allowing for user management via readily available mobile devices, these devices find utility in a wide range of settings, from health monitoring systems and home automation to the battlefield(Al-Hadhrami & Hussain, 2020),Kambourakis et al.,2008,Aslam et al., 2022,Alghazzawi et al., 2021).

Some studies, however, have found that as many as 70% of these devices contain numerous security flawsWinzer et al., 2018. To ensure that our experiment is representative of the latest generation of IoT devices, we are employing a Zolertia Z1. Due to the network's reliance on these devices, which are often underpowered and incapable of complex computations, any kind of attack, like as a wormhole or a flood, might have catastrophic consequences. A low-power intrusion detection system is needed to thwart these assaults (IDS). Intruder detection systems are able to keep a constant eye on the entire network, looking for any signs of intrusion-related harm. An IDS can take the form of supplementary hardware or a software programme. There is a potential for an increase in the IoT network's power consumption if IDS is implemented in hardware. Massive distributed denial of service (DDoS) attacks Banica, Burtescu, & Enescu, 2017 have been

documented recently, often using millions of Internet of Things (IoT) devices. In the situation in question, millions of IoT devices were utilised to make queries to a Domain Name System (DNS) provider called Dyn, disrupting services of providers including Netflix, CNN, and Twitter GoP, 2018. As a result, it is safe to assume that manufacturers have been too preoccupied with speeding up the production, marketing, and distribution of their products to worry much about the safety of their Internet of Things gadgets. The protection of businesses and individuals utilising IoT devices for smart homes needs the creation of a secure communication protocol that can be implemented on any such device, regardless of its manufacturer. Given these constraints and prerequisites, a resource-efficient method that guarantees safety is essential. Such low-powered devices require the development of a secure message-passing technique in addition to cyber-attack detection. Clearly, the implementation of multiple secure cryptographic protocols on these devices will raise the use of resources on these IoT devices.

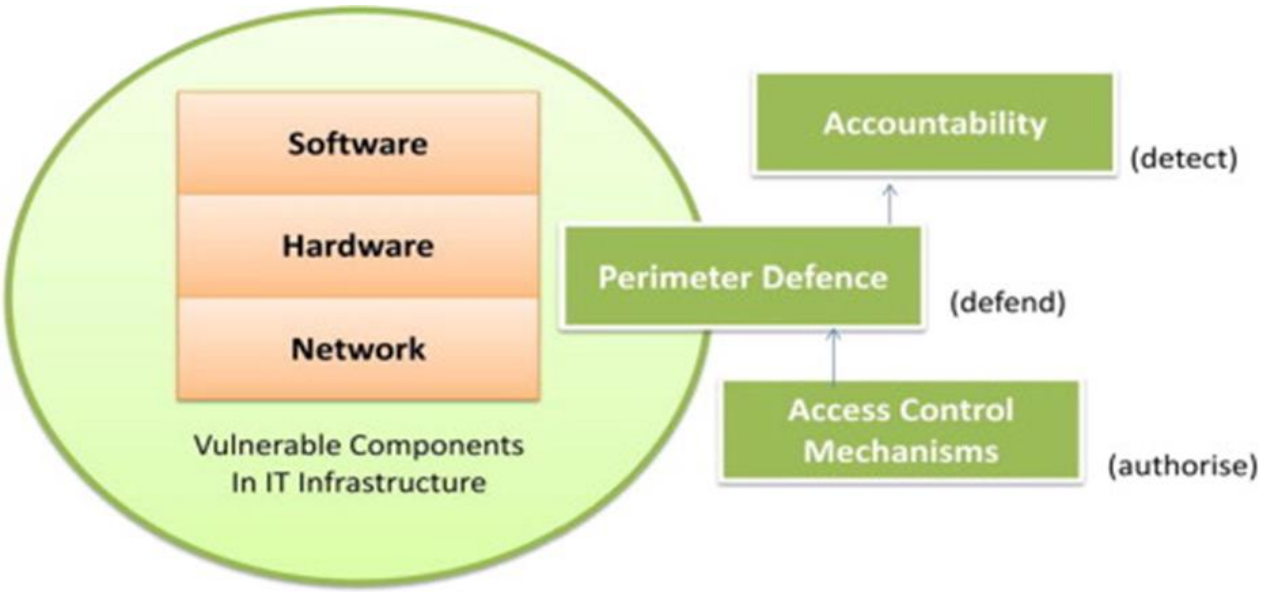

Figure 2:
Dependency of Attacks on Differed Components

Since the Zolertia Z1 motes operate on the same principle as the newer generation of IoT devices, this study offers a novel algorithm that is applied within Zolertia Z1 motes to test the efficacy of the algorithm in terms of improving security and decreasing power consumption. Once we've verified the findings, we can apply the same technique to additional common IoT gadgets. The compromise of sensitive data or information is yet another consequence that could result from a cyberattack on a battery-powered Internet of Things device. There are many Internet of Things devices that are connected to networks that collect and send data. If an adversary is successful in gaining access to the device, they may be able to access and steal this data. This might be especially worrisome for devices used in healthcare or financial settings, as these are typically the environments in which sensitive personal or financial information is collected and communicated. Cyberattacks on battery-powered Internet of Things devices can have consequences for national security in addition to the potential effects they could have on persons and organisations. An assault on a device might possibly have greater repercussions for a country's security and stability as these devices become increasingly prominent in key infrastructure. It is essential for individuals as well as companies to not

only be aware of the possible dangers and repercussions of cyberattacks on battery-powered Internet of Things devices, but also to take precautions to defend themselves from such attacks. This may require putting in place stringent security measures and routinely upgrading the software on the device in order to patch any flaws. It could also mean keeping an eye out for strange goings-on or conduct that seems fishy, and then reporting any potential dangers to the authorities that are in charge of that area.

PROPOSED INFRASTRUCTURE

In this article, we propose a new method for protecting networks of IoT devices from cyberattacks. Cyberattacks and the implementation of the IDS algorithm on the network of IoT devices are both taken into account in the analysis. Earlier work gave a comparison of energy use and estimated battery life for similar IoT devices Abbasy & Quesada, 2017. In this study, we use the same style of experiments to verify our algorithm. However, the effectiveness of the proposed security algorithm is explored in this work, and a comparison of the outcomes of the same experiment conducted in a controlled laboratory environment with and without IDS during a live cyber-attack is offered. Most energy usage studies that account for current attacks and actively deployed IDS make use of simulation rather than real-world motes. However, in a study including real-world tests, a Z1 and Open motes are used. Instead, this work does not focus on security or examine how motes react when a security mechanism is put into place. One such work focuses on security, but since it relies on simulation, its analysis is limited Anandaraj & Indumathi, 2020. Constraints on available energy sources will continue to be an essential consideration when thinking about Internet of Things devices.

After Elliptical curve cryptography was implemented, an investigation was conducted using MICAz and TelosB sensors to analyses performance Osanaiye, Choo, & Dlodlo, 2016, energy usage, and computational perspective. Although a comparable study was conducted taking into account all Mica wireless sensor network devices and TelosB sensors Salemi et al., 2021 , these devices have greater computing features compared to the Zolertia Z1, which is a very low powered device comprising of very limited. Lightweight encryption for Internet of Things devices is also proposed in one of the research. When applied to healthcare application systems like Wireless body area network, Aysa, Ibrahim, & Mohammed, 2020, there are several security concerns that arise. Kambourakis et al., 2007 If we think about how much energy these IoT gadgets use, we find a plethora of research, including a survey of wireless sensor network energy use, but all of it was done in a simulated setting. Tekleselassie, 2021 However, the effectiveness of the proposed security algorithm is explored in this work, and a comparison of the outcomes of the same experiment conducted in a controlled laboratory environment with and without IDS during a live cyber-attack is offered. The vast majority of published research in this field is focused on analysing energy use in the context of current attacks. Following this, we shall describe in depth the technological methods we employed to carry out the experiments.

Mittiagtion of Attacks: We are utilising Zolertia Z1 motes as a testing platform to examine the effects of cyber attacks and the ways in which these attacks can be prevented on low-power Internet of Things devices.

Hardware: The MSP430 is a low-power, 16-bit MCU that is used in these devices. It operates at 16 MHz. The microUSB port is used for charging and debugging purposes. The CC2420 transceiver, which is compatible with IEEE 802.15.4, 6LowPAN, and ZigBee protocols, is also included. Additionally, it has a digital temperature sensor (TMP102) with an accuracy of 0.5oC and a digital accelerometer (ADXL345) that measures acceleration from 0 to 16 g. There is a trade-off between voltage (these devices can run on anywhere from 0.3 to 3.6V; in fact, two 1.5V AA batteries will do the trick) and code size (these IoT gadgets have very little storage space). This operating system is C-programmable and features a kernel, libraries, a programme loader, and a group of processes Ali et al., 2022. Varying operating circumstances, such as a basketball court, auditorium, open parking lot, and working lab area, as well as different lighting conditions, are being tested to determine the impact of a cyber-attack and the proposed IDS. Simulating the system, we used the same topology—eight motes in a 15 by 5 foot grid—and followed the same approach, with the exception of switching the operating environment. However, there is little help available on the Cooja platform for running simulations in a non-default setting Mishra & Pandya, 2021.

METHODOLOGY AND EQUIPMENT FOR THE EXPERIMENT

In order to conduct our experiments, we built a testbed consisting of nine motes and used eight of them to construct a 15 by 5 foot grid on which to test our broadcast and one-to-one communication software. Using the power trace algorithm, the ninth mote gathered data on power consumption under varying operational and illumination settings Abbasy & Quesada, 2017, Van Rijswijk-Deij, Sperotto, & Pras, 2014 . This method was used to examine the network's natural state, prior to an assault. Then, we repeated the process by making one of the motes in the grid into the attacker, and we used the identical approach once more by installing our proposed IDS in one of the eight motes. Topology employed in actual mole investigations is shown in Figure 1. We also conduct a Cooja-based simulation analysis to verify the experimental results with real-world motes.

Programs

As we saw in the preceding section, we gave some thought to using Contiki OS to distribute drivers for the Zolertia Z1. An excellent example of a device that would benefit from Contiki OS is the Z1 mote, Sky mote, etc. You need a kernel, libraries, a software loader, and a process set Van Rijswijk-Deij, Sperotto, & Pras, 2014 to get the most out of Contiki OS. This OS can operate platforms like MSP430 Mishra & Pandya, 2021, Cvitic et al., 2022 and it is compatible with the C programming language. It's possible to implement any network architecture in Contiki OS. Based on the topology we've implemented, the hub node is the attacker node. The efficiency of the suggested method was demonstrated by comparing its results to those of other algorithms. Our IDS's power analysis, for instance, shows that while its actual power consumption is higher than its simulated one, the algorithm still consumes less power than the targeted system. Figure 5 shows a comparison of energy usage before and after an attack was simulated and then carried out on real-world motes that had an IDS in place. Our primary goal in designing the lab was to provide a functional setting for conducting experiments. As the number of nodes grows, it becomes evident that energy usage also rises. In contrast to before IDS was installed, energy usage has not gone up noticeably.

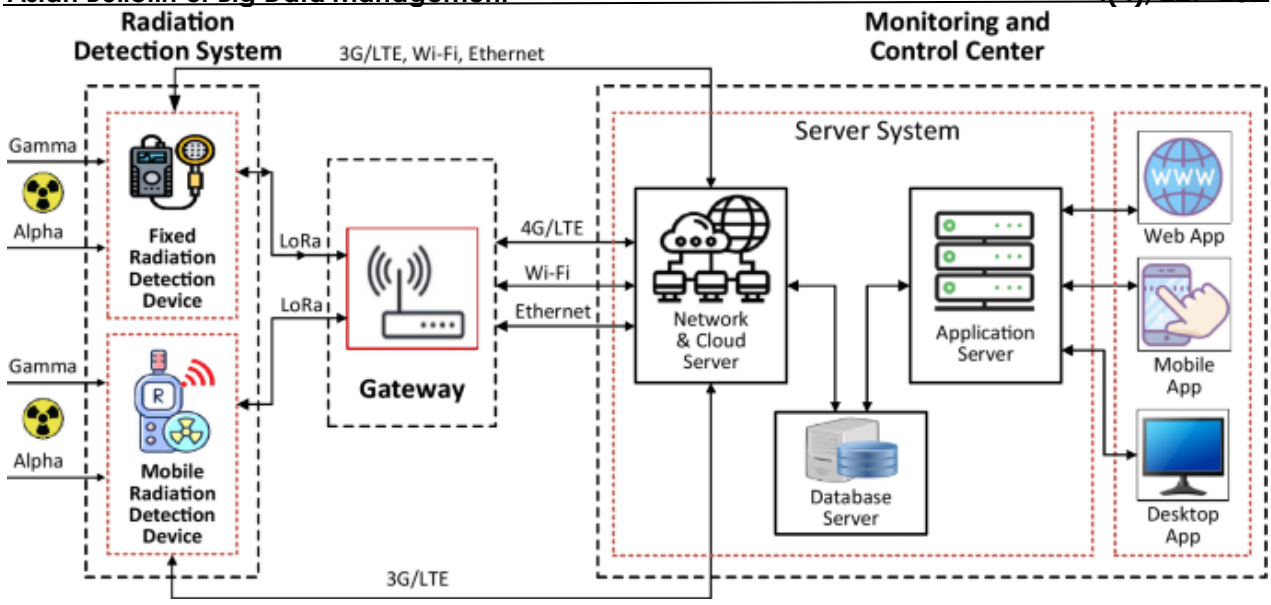

Figure 3:
IoT Battery Robust Consumption for Cyber Attack analysis

It is the responsibility of a nation's important infrastructure to provide many of the basic services that are relied on by its citizens, such as electronic communications, power, banking and finance, essential public services, transportation, water management, and so on. Each nation takes a unique approach to the development of its most vital infrastructures, and that strategy differs from country to country depending on the specifics of the business. As a result of the development of solutions based on IoT, formerly disconnected critical infrastructures have gained access to networks and the internet. Given that these significant systems are parts of a wider information network, it should come as no surprise that they are open to the possibility of being attacked through the use of cyberspace. It is vital to be aware of the different guises that cyberattacks can adopt, to work on designing defenses against those It is important to be aware of the different forms that cyberattacks can take. Today, taking preventative measures to prevent cyberattacks on these systems is more critical than ever. The focus of this article is an exploration of attacks against some form of critical infrastructure, specifically those which have most frequently occurred over the last years.

We also explore some of the preventive actions that can be used to reduce the level of impact caused by an IP-centric invasion, as well as how to protect ourselves from it. Battery-powered Internet of Things (IoT) devices can be vulnerable to cyberattacks, which can have severe consequences, as battery-powered IoT devices are often deployed in critical infrastructure and their compromise can pose threats to human health and safety if they were compromised or failed. The batt ery powered IoT devices are often part of critical infrastructure, so cyberattacks could have grave consequences. But battery-powered Internet of Things devices are widely used throughout critical infrastructure, making cyberattacks on this infrastructure potentially high-impact. One potential result of a cyberattack on a device run on batteries, such as one that is part of the Internet of Things, could be a reduction in the amount of battery life still available for

a device. If an adversary has access to the device and can continuously run programs or commands on it the battery on the device can run out of power before it has the chance to recharge, rendering the device worthless. If this happens this only proves the attacker has successfully gained access to the device. This could be especially concerning if the equipment is used for safety or emergency-related purposes, such as a smoke detector or a medical device, both of which things could be adversely impacted by this, as this is an example of something that could adversely affect these things, as this is an example of something that could adversely impact these things. Another potential effect of a cyberattack on an Internet of Things device is that, if it runs on battery power, it can also have the side effect of making changing the functionality of the device or the information it holds possible. A rogue actor, for example, can jam the controls of a smart lock or change the readings or output of a smart thermostat. Smart locks and smart thermostats can also be manipulated. The second explanation is that readings on a smart lock may be compromised. This may cause the device to malfunction or generate erroneous information that, depending on the actual device and the intended use to which it was originally designed, could have disastrous consequences. Depending on the actual device as well as the intended purpose in the first place.

The relevance of the impact would be directly related to the type of device involved. Cyberattacks involving battery powered Internet of Things (IoT) devices may have effects that can ripple out of the initial damage they inflict on the device itself in the immediate aftermath of the attack. But these repercussions could reverberate much wider. We're defining it broadly: A cyberattack against a technology that has the potential to cause a disruption or an outage in something critical that people use — like a power grid or a transportation system — that affects a large number of people. This could be the case even if the attack itself is unsuccessful. Because of this, it is possible that a sizeable number of individuals will be unable to use the technology that is being affected. It is vital to make sure that battery-powered Internet of Things devices are safe in order to prevent cyberattacks and the potential ramifications that can emerge from them. This is because cyberattacks can have serious consequences. This is due to the fact that cyberattacks can have a diverse variety of repercussions. In the context of this discussion, "this can imply implementing strong passwords and routinely upgrading the software on the device in order to remedy any vulnerabilities that may present." (Cybersecurity & Infrastructure Security Agency [CISA], n.d.)

CONCLUSION

The vital infrastructure of a nation is responsible for providing many essential services, including electronic communications, power, banking and finance, key public services, transportation, water management, and so on. Depending on the particulars of the industry, each nation takes a distinctive approach toward the development of its most important infrastructures. The development of IoT-based solutions has led to the establishment of networks and Internet access in previously disconnected critical infrastructures. Given that these important systems are components of a larger information network, they are naturally susceptible to being attacked via cyberspace. It is essential to be aware of the various guises that cyberattacks can adopt, to work on devising defenses against those guises, and to take any and all precautions that are required. And it's more important than ever to take steps to prevent cyberattacks on

these vital systems. Focus: Attacks on Critical Infrastructure (Overview and Most Common Attacks in Recent Years) We also discuss the various precautionary measures that can be adopted to mitigate the damage caused by IP-based intrusions and secure ourselves from them. Battery-powered Internet of Things (IoT) devices are vulnerable to cyberattacks which have critical implications, and battery-powered IoT devices are often deployed in the critical infrastructure and can put at risk people health and safety if compromised. This is a problem because battery-powered IoT devices are often used in critical infrastructure, and cyberattacks can have grave consequences (Page 7 of 9 - AI Writing Submission ID trn:oid:::1:3123329434 Page 7 of 9 - AI Writing Submission ID trn:oid:::1:3123329434 6). One example of what could happen as a result of a gigabyte attack on a battery powered device, such as an IoT device, is to affect the amount of remaining battery level of the attacked device. If an enemy gains access and can continuously run programs or commands on the device, the device will run out of power from its battery and become useless until recharged. If this happens, then the attacker has broken into the device.

This can be of particular concern if the apparatus is employed for safety or emergency-related purposes, like with a smoke alarm or a medical device, as those are both examples of things that could suffer from this. The second possible manipulation resulting from a cyberattack is when a device that is powered by a battery can be reprogrammed to change its functionality or its data. An attacker might, for example, alter the controls of a smart lock (opens in new tab) or change the readings or output of a smart thermostat. https://www.securitymagazine.com/articles/97789 control-the-controls-and-the-access Moreover, the reads of a smart lock can be tampered. The device would then be unable to work as intended, returning faulty information, both of which could lead to disastrous outcomes depending on what the device is and was meant to do. This can have dire consequences depending on the device. Such cyberattacks may have consequences way beyond what the attacks do to the battery-powered Internet of Things devices themselves. These repercussions can also resonate on a greater scale. A cyberattack on a technology used in critical infrastructure, such as a power grid or transportation system, could cause a disruption or outage that impacts thousands of people. This may cause thousands of people not to be able to access the technology in question. It is necessary to make assured that battery-powered Internet of Things devices are safe in order to prevent cyberattacks and the potential ramifications that can emerge from them. This is because cyberattacks can have a wide range of consequences. In this context, "this can mean implementing strong passwords and periodically upgrading the software on the device in order to fix any vulnerabilities that may present."

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Arkorful, V., & Abaidoo, N. (2015). The role of e-learning, advantages and disadvantages of its adoption in higher education. International Journal of Instructional Technology and Distance Learning, 12(1), 29–42.

Winzer, R., Lindberg, L., Guldbrandsson, K., & Sidorchuk, A. (2018). Effects of mental health interventions for students in higher education are sustainable over time: A systematic review and meta-analysis of randomized controlled trials. PeerJ, 6, e4598. https://doi.org/10.7717/peerj.4598

Banica, L., Burtescu, E., & Enescu, F. (2017). The impact of Internet-of-Things in higher education. Scientific Bulletin: Economic Sciences, 16(1), 53–59.

Government of Pakistan. (2018). Academy of Educational Planning and Management.

Abbasy, M. B., & Quesada, E. V. (2017). Predictable influence of IoT (Internet of Things) in higher education. International Journal of Information and Education Technology, 7(12), 914–920. https://doi.org/10.18178/ijiet.2017.7.12.995

Turcu, C. O., & Turcu, C. E. (2018). Industrial internet of things as a challenge for higher education. International Journal of Advanced Computer Science and Applications, 9(11), 55–60. https://doi.org/10.14569/IJACSA.2018.091108

Anandaraj, A. P. S., & Indumathi, G. (2020). Enhanced fuzzy particle swarm optimization load distribution (EFPSO-LD) for DDoS attacks detection and prevention in healthcare cloud systems. Journal of Internet Technology, 21(2), 435–445. https://doi.org/10.3966/160792642020032102012

Osanaiye, O., Choo, K.-K. R., & Dlodlo, M. (2016). Analysing feature selection and classification techniques for DDoS detection in cloud. Southern Africa Telecommunications Networks and Applications Conference 2016, 198–203.

Salemi, H., Rostami, H., Talatian-Azad, S., & Khosravi, M. R. (2021). LEAESN: Predicting DDoS attack in healthcare systems based on Lyapunov exponent analysis and echo state neural networks. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-020-10179-y

Aysa, M. H., Ibrahim, A. A., & Mohammed, A. H. (2020). IoT DDoS attack detection using machine learning. 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020. https://doi.org/10.1109/ISMSIT50672.2020.9254703

Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2007). A fair solution to DNS amplification attacks. 2nd International Annual Workshop on Digital Forensics and Incident Analysis (WDFIA), 38–47. https://doi.org/10.1109/WDFIA.2007.4299371

Tekleselassie, H. (2021). DDoS detection on Internet of Things using unsupervised algorithms. E3S Web of Conferences, 297, 01005. https://doi.org/10.1051/e3sconf/202129701005

Ali, M. H., et al. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT). Electronics, 11(3), 494. https://doi.org/10.3390/electronics11030494

Mishra, N., & Pandya, S. (2021). Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408

Van Rijswijk-Deij, R., Sperotto, A., & Pras, A. (2014). DNSSEC and its potential for DDoS attacks: A comprehensive measurement study. Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC), 449–460. https://doi.org/10.1145/2663716.2663731

Cvitic, I., Perakovic, D., Gupta, B. B., & Choo, K. K. R. (2022). Boosting-based DDoS detection in Internet of Things systems. IEEE Internet of Things Journal, 9(3), 2109–2123. https://doi.org/10.1109/JIOT.2021.3090909

Perez-Diaz, J. A., & Cantoral-Ceballos, J. A. (2022). Transport and application layer DDoS attacks detection in IoT.

Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. 2018 IEEE Symposium on Security and Privacy Workshops (SPW), 29–35. https://doi.org/10.1109/SPW.2018.00013

Aytaç, T., Aydın, M. A., & Zaim, A. H. (2020). Detection of DDoS attacks using machine learning methods. Electrica, 20(2), 159–167. https://doi.org/10.5152/electrica.2020.20049

Al-Hadhrami, Y. S., & Hussain, F. K. (2020). Intelligent machine learning architecture for detecting DDoS attacks in IoT networks.

Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2008). Detecting DNS amplification attacks. Lecture Notes in Computer Science, 5141, 185–196. https://doi.org/10.1007/978-3-540-89173-4_16

Aslam, M., et al. (2022). Adaptive machine learning-based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. Sensors, 22(7), 2697. https://doi.org/10.3390/s22072697

Alghazzawi, D., Bamasaq, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Applied Sciences, 11(24). https://doi.org/10.3390/app112411634

Roopak, M. (2021). Intrusion detection system for IoT networks for detection of DDoS attacks.

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). Cybersecurity tips and best practices. https://www.cisa.gov.

2024 by the authors; EuoAsian Academy of Global Learning and Education Ltd. Pakistan. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).