Security and Privacy Threats Posed by IoT Devices Used by Students on College Campuses

Hala Strohmier
Computer Science, Engineering and Mathematics
University of South Carolina Aiken
Aiken SC USA
hala.strohmier@usca.edu

James R. Lowe Jr.
Computer Science, Engineering and Mathematics
University of South Carolina Aiken
Aiken SC USA
jrlowe@usca.edu

Angel G. Rodriguez
Computer Science, Engineering and Mathematics
University of South Carolina Aiken
Aiken SC USA
angelgr@usca.edu

Miles M. Trammell
Computer Science, Engineering and Mathematics
University of South Carolina Aiken
Aiken SC USA
mmt6@usca.edu

2024 12th International Symposium on Digital Forensics and Security (ISDFS) | 979-8-3503-3036-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISDFS60797.2024.10527253

***Abstract*—The increasing use of Internet of Things (IoT) devices on college campuses has significantly changed how students go about their daily lives. This surge of IoT brings potential security and privacy risks. This research focuses on understanding the IoT landscapes at the University of South Carolina Aiken (USCA), investigating vulnerabilities, and determining the need for improved security awareness. By combining survey data, network live scanning data, network monitoring, and simulated attacks, our analysis revealed a wide range of devices on the campus, suggesting possible security risks. Using the tool PRET exposes vulnerabilities in common devices, showing the need for direct security measures. Additionally, we explored wireless network vulnerabilities through capturing and decrypting WPA handshakes. The study showed common issues in IoT security, such as default credentials and network vulnerabilities. The conclusions underscore the need for a careful balance between the benefits of IoT and the need for increased security measures.**

***Keywords*—Cybersecurity, Network Security, IoT, WPA Handshake, ARP Scan, PRET**

I. Introduction

The Internet of Things (IoT) is a transformative technology that allows physical objects to connect, communicate, and interact with each other and with humans over the internet. [1]. IoT, also known as internet-connected devices, has become an integral part of our daily lives. Since the term was first conceived, they have become commonplace in many facets of society, from manufacturing to medical and education [2]. This can be seen profoundly on college campuses. The most important attribute of IoT devices is that they are connected to each other [3]. The interoperability concepts in IoT systems and devices allow different devices to work together despite having different manufacturers or service providers [4] providing Edge Computing by processing data on the device or nearby to reduce latency, bandwidth use, and reliance on cloud services [5]. College students use connected devices, anything from involved network devices and key cards to the vast range of personal IoT devices, to make their campus experience more convenient and efficient. The scalability of IoT systems must be designed to scale efficiently as the number of devices grows into the billions [6] [7]. As stated by Quy in the article Wireless Communication, IoT development has created an interconnected ecosystem where everything is accessible through the internet [8], which creates concerns over security and privacy. Schiller references a study conducted by Hewlett-Packard that found 70 percent of IoT devices had some level of basic security risk [9]. The rapidly growing attacks, these devices also bring a host of security threats that many are untrained to handle. Data gathered by Statista in 2023 as shown in figure 1 shows an estimated 6:1 devices when compared to the world population [10].

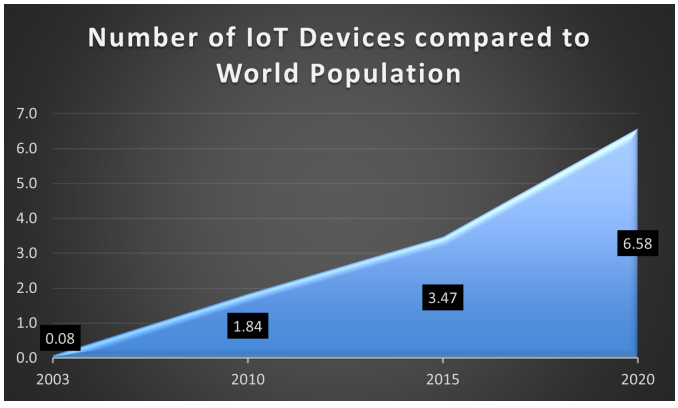

Fig. 1. Number of IoT devices per Population [3]

Security concerns are critical due to the vast amount of personal and sensitive data collected and transmitted by IoT devices. Robust security measures are essential to protect against unauthorized access and cyberattacks while privacy with devices collecting detailed information about users' lives, ensuring data is used ethically and with consent is paramount

[11]. IoT development has created an interconnected ecosystem where everything is accessible through the internet [8].

Our goal for this research is to contribute to the growing analysis of IoT devices and offer insights into their use in academic institutions. This research aims to shed light on the threats posed by IoT devices used by students on college campuses, focusing on whether there is a need for additional training on their proper usage. To address these concerns, we employ various research methods to provide insights into the landscape of IoT usage on campuses.

II. Methodology

This research investigates college students' understanding of the Internet of Things (IoT). Assesses IoT security threats on college campuses by creating and analyzing data sets from live scanning of network traffic at the University of South Carolina Aiken (USCA) campus. The study not only aims to assess the general knowledge possessed by college students regarding IoT and IoT security but also references general thoughts from a recent survey, "The Benefits of IoT in the Workplace." Network monitoring tools are used to gather Address Resolution Protocol (ARP) data from three locations on the USCA campus. Primarily focusing on the Media Access Control (MAC) addresses to identify individual devices on the network. This approach allows us to create a dataset from our campus, which will be crucial to examine, analyze, cross-reference, and analyze the similarity and other characteristics in devices across the campus environment. As we progress, we will perform vulnerability testing and exploit selected devices to understand their vulnerabilities and explore their potential implications on the security posture of the campus network. This methodology ensures a well-rounded examination of the campus's IoT landscape, allowing for informed decisions. Based on the findings, we will address some potential security issues by discussing a potential exploit on a commonly used device.

A. Survey on IoT in the Workplace

To understand the IoT device landscape on college campuses, we analyzed a survey among students [12] conducted at USCA in 2023 . This survey provided valuable insights into the prevalence of IoT devices in the workplace and potential knowledge gaps among students. The survey collected over one hundred and twenty responses, with students responding to two question prompts. The first question asked, "How do you keep the bad guys out if you enable the IoT for your personal and professional life?". The general response from students suggested that to garner the full benefit of IoT technology, it is first important to solve the lapses in security. This risk is even more present in large organizations as they must make significant investments in the number and cost of many devices. The second question asked, "Do you think the benefits of IoT devices in the workplace outweigh the security risks? Why or why not?". While several respondents acknowledge the economic benefit the IoT market has created on a global scale, one respondent rightly mentioned "IoTs are practically inseparable from our lives". In architectural practices, it is standard for a strong foundation to be laid before the frame is built. This practice has not been used when it comes to the deployment of IoT devices. As it currently stands, there are a number of devices that have become critical for businesses and citizens to interact, and removal would cause great social harm.

B. Network Live Scan for Devices:

On November 8th, we conducted an ARP scan at multiple locations across the USCA campus, specifically focusing on gathering data from its Wi-Fi networks to determine the presence and types of IoT devices. Utilizing Wireshark, a popular protocol analyzer, we captured and analyzed network traffic, gathering detailed information about the network's makeup. Our primary target was the MAC addresses associated with the various devices connected to the network. The scan produced a data set of over eighty thousand entries. Nine hundred of these are unique Mac addresses, showing the diversity of devices on campus as shown in Figure 2.

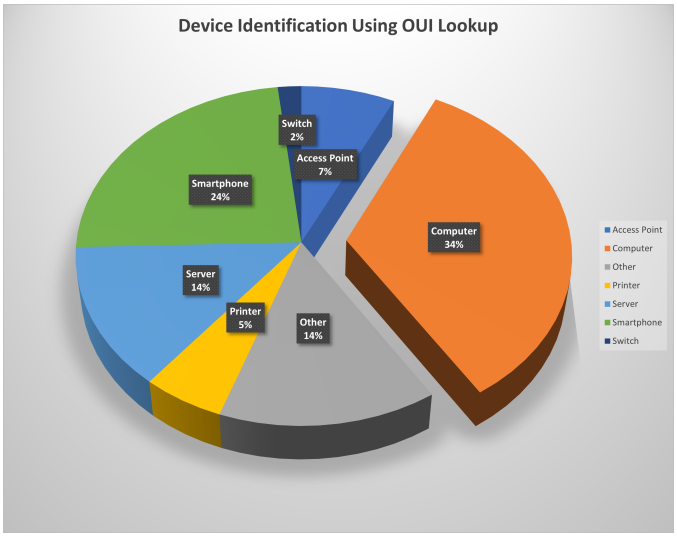

Fig. 2. Identified Devices at USCA - Nov 2023

We randomly selected a subset of data targets to get a more representative proportion of devices. We then employed multiple organizationally unique identifier (OUI) Lookup tools to identify unique devices, including make and model. We divided the results into Smartphones, AP, Printers, and Laptops, of which we could identify one hundred and ten. Identified targets only comprised 1.16 percent of the scan results and 11.34 percent of the identified unique results. Though this is a small fraction of the total data set gathered, the overall number of potential attack vectors is worrisome. Our gathering method was done using free tools with limited capabilities, expressing the need for a more robust and section network infrastructure on the campus.

III. Vulnerabilities and Exploits

A. PRET - Printer Exploit

On November 1st, a printer penetration test was conducted to demonstrate potential methods for hackers to infiltrate university IoT devices connected to the network. The test involved utilizing the PRET tool in Kali Linux, and the procedures were informed by the documentation provided by RUB-NDS on GitHub [13]. We show examples of the exploitation methods used in Figures 3, 4, and 5. Through the exploitation of a printer on the network, a hacker can execute various exploits, including:

Unauthorized Access: PRET may allow an attacker to gain unauthorized access to a targeted printer. This access could give the attacker control of the printer's functions, settings, and stored documents.

Information Disclosure: An attacker could use PRET to extract sensitive information stored on the printer, such as previously printed documents, configuration settings, or network-related information.

Manipulation of Print Jobs: Attackers could manipulate print jobs in progress or pending in the print queue. This could involve altering the content of documents or redirecting print jobs to unauthorized locations.

Device Manipulation: PRET might enable attackers to manipulate the physical functions of the printer, such as changing settings, updating firmware, or causing malfunctions.

Denial of Service (DoS): An attacker could use PRET to launch a Denial of Service (DoS) attack on the printer, rendering it unavailable for legitimate users.

Network Reconnaissance: PRET could be used for network reconnaissance, allowing attackers to identify other devices on the network and potentially exploit vulnerabilities in those systems.

Persistence: An attacker might use PRET to establish persistence on the compromised printer, maintaining unauthorized access for an extended period without detection.

Exploiting Printer Vulnerabilities: PRET could exploit specific vulnerabilities in the printer's firmware or software, potentially leading to remote code execution or compromise.

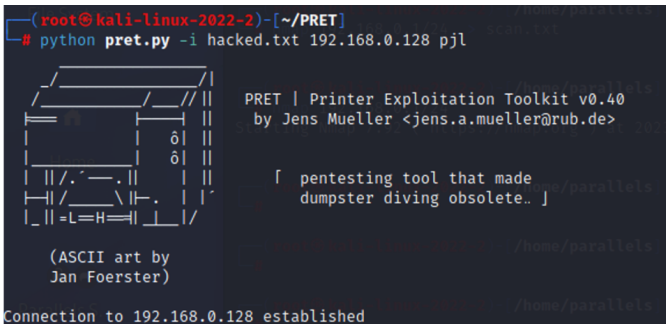

Fig. 3. Printer Remote Connection Established

How we did it:

1. Using PRET, we scanned for printers in the network.
2. Selected the printer we wanted to target.

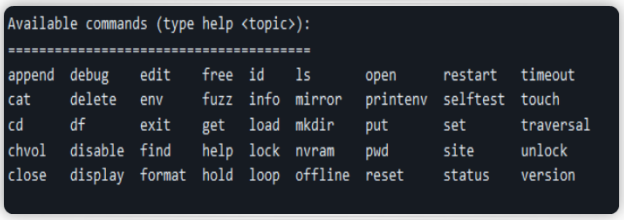

Fig. 4. PRET Menu

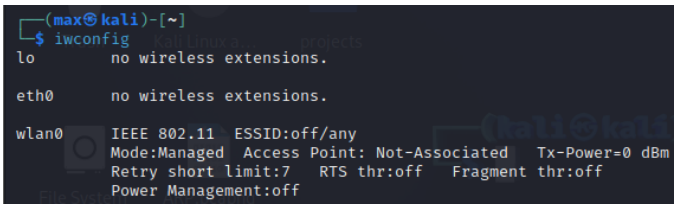

Fig. 5. Wireless Interface Configuration

3. Selected from the list given.

B. Capturing and Decrypting WPA Handshakes

In the initial stage of the operational sequence, it is imperative to ascertain the establishment of a seamless connection between the wireless interface and our computer as shown in Figure 6. This verification process is facilitated through the utilization of the Linux command, namely "iwconfig," a command that affords us insight into the wireless configuration of our interface. It is at this juncture that we observe the successful connection of our wireless interface, denoted by the nomenclature "wlan0."

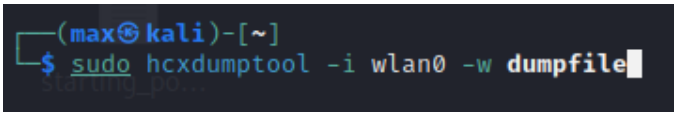

Fig. 6. Write to Capture File

Subsequently, we employ a utility titled "hcxdumptool," a tool explicitly designed for the evaluation of Wi-Fi security. This tool functions by capturing WLAN (Wireless Local Area Network) traffic, thereby extracting WPA/WPA2-PSK (Wi-Fi Protected Access/Wi-Fi Protected Access 2 - Pre-Shared Key) hashes for further analysis. The execution of this tool is characterized by the inclusion of command-line parameters, wherein the "-i" flag is employed to designate the utilization of the previously referenced "wlan0" interface from the preceding section. Notably, the "-w" flag is then invoked to name the resulting file, with the chosen identifier being "dumpfile."

The output above displays the executed hcxdumptool command as shown in Figure 7, grants crucial information integral to the reconnaissance process. This output comprehensively delineates pertinent details such as channels, MAC addresses, and ESSID (Extended Service Set Identifier) names. The

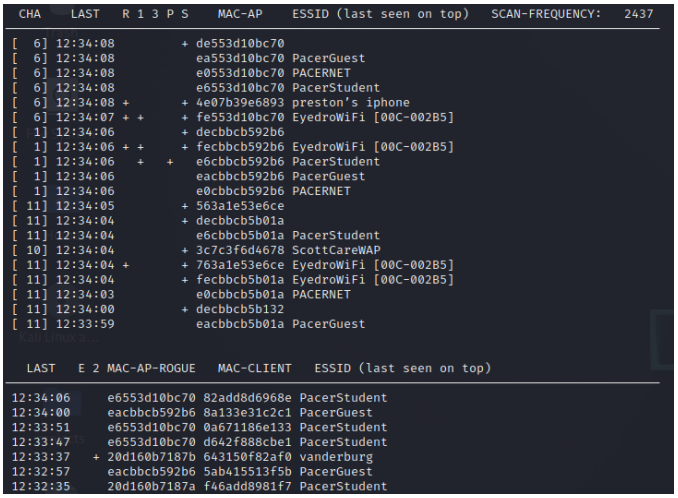

Fig. 7. Output from hcxdumptool

channels clarify the specific frequency bands utilized, the MAC addresses provide unique hardware identifiers associated with the discovered devices, and the ESSID names disclose the identifiers assigned to the individual wireless networks captured during the scanning operation. This combination of information serves as a foundational dataset for subsequent stages of analysis and evaluation within the context of the Wi-Fi security assessment.

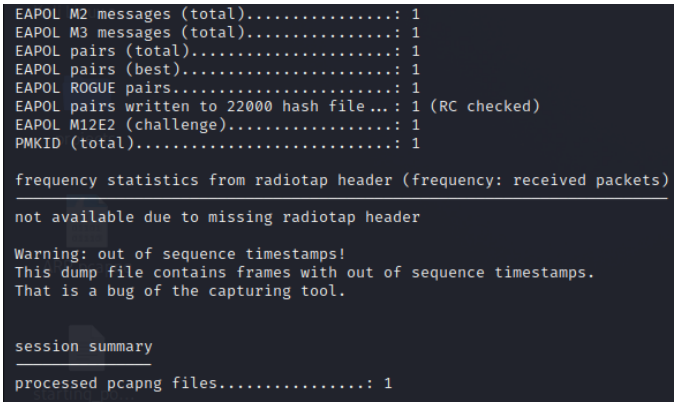

Fig. 8. Generate Hash File from Capture

A satisfactory volume of data has now been collected. Upon termination of hcxdumptool, the tool automatically generates a dump file Figure 8. Notably, by default, this dump file appears in the pcapng (Packet Capture Next Generation) file type. However, for our specific requirements, utilizing a 22000 hash file type is preferable. The transformation from the default pcapng format to the desired hash format is executed through the following command: "hcxdumptool -o hash.hc22000 -E essidlist dumpfile". In this command, the "-o" flag is employed to designate the nomenclature of the resultant file, which, in this instance, is set as "hash.hc22000." Furthermore, the "-E" flag is utilized to specify the extended service set identifier list (essidlist) to be employed in the conversion process. Following the execution of this command, hcxdumptool generates a file in the desired 22000-hash format, thereby facilitating subsequent analytical procedures [14].

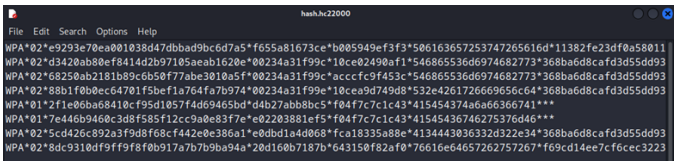

Fig. 9. Encrypted WPA Hashes

Upon inspection of the opened hc22000 file, the contents appear as seemingly arbitrary strings of characters, commonly referred to as hashes Figure 9. These hash values constitute a cryptographic representation of sensitive information, adding an additional layer of security by obviating the storage of data in plain text format, thus mitigating the risk of unauthorized access.

The significance of the earlier conversion to the hc22000 format becomes apparent in the context of the subsequent tool employed in the decryption process, namely "hashcat." Hashcat specializes in deciphering cryptographic hashes and is adept at interpreting the specific format generated by hcxdumptool. In the ensuing step, hashcat will be utilized to decrypt the captured hash, thereby revealing the underlying information encrypted within. This process is pivotal in the broader scope of network security assessment and serves as a practical demonstration of the cryptographic resilience inherent in the utilized Wi-Fi security protocols [14].

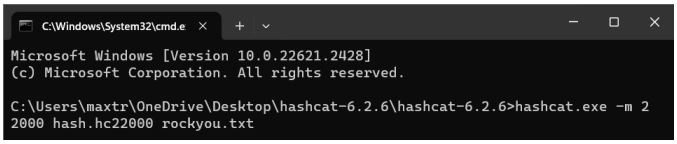

Fig. 10. Word List Approach

The first approach to cracking the hash would be to employ the use of a word list Figure 10. The rockyou.txt is one of the most well-known word lists. In this example, we tell hashcat to compare the hash that every word in the list generates to the hash we have captured. However, this approach often fails because the password of the WPA has to exist within the list for this approach to work.

Another approach we investigated was brute-force attacks Figure 11, which involve trying every possible password combination until the correct one is found. This method is particularly effective against weak passwords. Tools like Aircrack-ng facilitate this process by capturing the WPA handshake and then using powerful computational resources to try thousands or millions of possible password combinations to do that we specify what types of characters we would like for hashcat to iterate through. Assuming that we knew the password's structure and size we would enter the command, "hashcat.exe -m 22000 hash.22000 -a 3 ?u?l?l?l?l?s?l?l?l?l?l". The symbol, "?u" denotes an uppercase. The symbol , "?l"

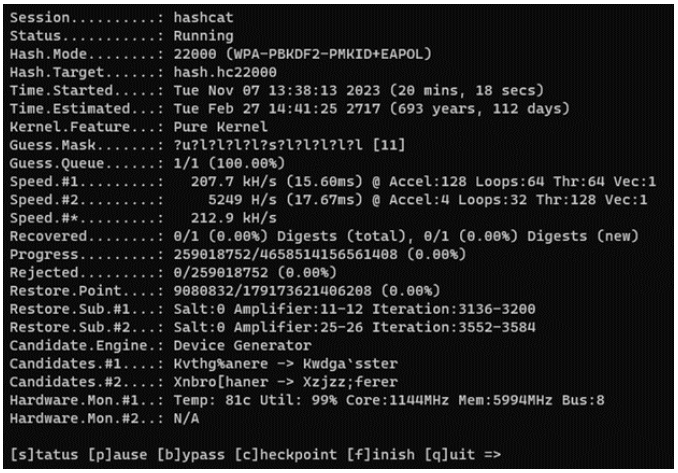

Fig. 11. Brute Force Approach

denotes lowercase, and the symbol "?s" denotes a special character. This approach fails for two reasons. Firstly, it is unlikely that we would have access to the structure of the password. Secondly, hashcat estimates that it would take over 693 years to iterate through all the generated hashes. For this example, we utilized the a NIVIDIA GeForce GTX 1660 Ti.

IV. Security Concerns in IoT

- Weak passwords IoT proliferation has introduced numerous security vulnerabilities. One prevalent concern, as shown by the student survey responses and the vulnerability scanning we performed, is the persistence of insecure default credentials. Many IoT devices are shipped with pre-configured usernames and passwords that users tend to neglect changing. This poses a severe security risk, as attackers can easily exploit these default credentials to gain unauthorized access to the device. This vulnerability highlights the importance of user awareness and the need for manufacturers to enforce more robust security practices, prompting users to change default credentials during the device's initial setup. Addressing this issue is fundamental to fortifying the overall security posture of IoT ecosystems.
- Network Vulnerability Security challenges in IoT extend to the realm of network vulnerabilities, as shown in our investigation of IoT vulnerabilities in the USCA campus network. These services have vulnerabilities and often do not implement strong authentication, making them prime targets for remote attacks.
- Insufficient privacy protection and data security IoT devices' communication channels and protocols may be exploited, potentially exposing authentication data to malicious activities such as eavesdropping or man-in-the-middle attacks. In an insecure network environment, adversaries can intercept and manipulate the data exchanged between IoT devices and their respective servers, compromising the authentication process. To counteract these vulnerabilities, robust encryption protocols and secure communication channels must be implemented. Additionally, regular security audits and updates to address emerging threats are essential to maintain the integrity of IoT networks and safeguard authentication processes.

V. Methods to remediate IoT vulnerabilities

To effectively remediate IoT vulnerabilities, organization must adopt a comprehensive approach that spans technical, organizational, and procedural aspects. Here are some of methods that can be employed to reduce the risks associated with IoT devices:

- Security awareness, USCA IT technical management realizes that student, faculty, and staff education on cybersecurity is crucial to achieving a secure environment, and in this effort, a project was created to implement security awareness across campus.
- Network segmentation and review of the network to improve segmenting of the growing network and isolate IoT devices from critical networks.
- Disable unnecessary services, as shown in the printer exploitation, it was proven that this printer was a weak link on the network as we gained access to it and were able to access the network; therefore, a continuous review of network devices and disabling unnecessary service is a good practice.
- Secure wireless communication, as technology is rapidly changing, and designing a zero-trust security model based on the principle of "never trust, always verify." The zero-trust model assumes that threats could be internal or external and that everything trying to connect to the system must be verified before access is granted, regardless of where the connection originates.
- Encryption, Encrypt sensitive data stored on the IoT devices and during transmission to protect sensitive information

VI. Conclusion

This research shows that IoT development has created an interconnected ecosystem where everything is accessible online. With combined survey data, network live scanning data, network monitoring and exploitation, and various analyses, we investigated IoT security and privacy threats at the University of South Carolina Aiken campus. We confirm that IoT poses security and privacy issues by enacting real threat simulations that show various points on the USCA campus that are vulnerable to attacks. While the potential benefits of integrating IoT devices on college campuses are considerable, they must be carefully weighed against the security risks. Similarly, the use of IoT devices in the workplace and the advantages of IoT technology can be integral. However, proactive planning and implementing comprehensive security measures to mitigate these risks and achieve a balance between the benefits of IoT and its associated security risks is ultimately the goal any institution should drive for. Failure to prioritize effective security measures will expose college campuses to cybersecurity risks and may lead to significant liabilities. It

is essential to ensure the secure integration of IoT devices into campus networks to enhance the efficiency of students' education experience and ensure appropriate security measures are in place to limit the risk of compromising the campus networks, data, and operations.

REFERENCES

[1] G. Lampropoulos, K. Siakas, and T. Anastasiadis, "Internet of things in the context of industry 4.0: An overview," *International Journal of Entrepreneurial Knowledge*, pp. 4–19, 2019.

[2] S. Madakam, V. Lake, V. Lake, V. Lake, *et al.*, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[3] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to iot," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, 2018.

[4] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future generation computer systems*, vol. 56, pp. 684–700, 2016.

[5] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," *IEEE access*, vol. 6, pp. 6900–6919, 2017.

[6] H. S. Berry, "The importance of cybersecurity in supply chain," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–5, 2023.

[7] M. Ghaleb and F. Azzedin, "Towards scalable and efficient architecture for modeling trust in iot environments," *Sensors*, vol. 21, no. 9, p. 2986, 2021.

[8] Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, "Wireless communication technologies for iot in 5g: Vision, applications, and challenges," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, 2022.

[9] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of iot security," *Computer Science Review*, vol. 44, p. 100467, 2022.

[10] S. R. Department, *Number of network connected devices per person around the world from 2003 to 2020.* PhD thesis, NA, 2016.

[11] C. Maple, "Security and privacy in the internet of things," *Journal of cyber policy*, vol. 2, no. 2, pp. 155–184, 2017.

[12] H. S. Berry, "Survey of the challenges and solutions in cybersecurity awareness among college students," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6, 2023.

[13] CheariX, S. Juraj, Martin, and R. Paul, "Ruhr university bochum - chair for network and data security - pret (printer exploitation toolkit)," *GitHub - RUB-NDS*, vol. https://github.com/RUB-NDS/PRET, no. 1, p. 10, 2023.

[14] K. E. Faraj, *Security technologies for wireless access to local area networks*. PhD thesis, Universidade do Algarve (Portugal), 2019.