ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #35698

Introducing and Facilitating Internet of Medical Things (IoMT) Research for Undergraduate Students and High School Teachers

Ms. Paige Janae Harvey, Morgan State University

Paige J. Harvey received her B.S. degree in electrical and computer engineering from Morgan State University, Baltimore, MD, in 2018. She is currently a Ph.D student at Morgan, in the Department of Electrical and Computer Engineering, and affiliated with the Center for Reverse Engineering and Assured Microelectronics (CREAM) Research Lab as well as the Cybersecurity Assurance and Policy (CAP) Center, under the direction Dr. Kevin T. Kornegay. Her research focus is security and privacy of the Internet of Medical Things (IoMT).

Ms. Otily Toutsop, Morgan State University

Otily Toutsop is a Ph.D. student with a concentration on secure embedded systems in the Electrical and Computer Engineering department at Morgan State University. She is also affiliated with the Cybersecurity Assurance and Policy (CAP) center. She received her bachelor's degree in Computer Science. Her research interests focus on IoT Security, machine learning, artificial intelligence, cyber-physical system, software security, home automation systems, and networking security. Her work has been published in several conferences, including the IEEE Computer Science, IEEE Applied Imagery Pattern Recognition Workshop (AIPR), IEEE International Conference on Internet of Things: Systems, Management and Security (IoTSMS), IEEE Future Internet of Things and Cloud (FiCloud), IEEE International Conference on Smart Innovations (SCI).

Prof. kevin kornegay, Morgan State University

Kevin T. Kornegay received the B.S. degree in electrical engineering from Pratt Institute, Brooklyn, NY, in 1985 and the M.S. and Ph.D. degrees in electrical engineering from the University of California at Berkeley in 1990 and 1992, respectively. He is currently the IoT Security Professor and Director of the Cybersecurity Assurance and Policy (CAP) Center for Academic Excellence in the Electrical and Computer Engineering Department at Morgan State University in Baltimore, MD. His research interests include hardware assurance, reverse engineering, secure embedded systems, and smart home/building security. Dr. Kornegay serves or has served on the technical program committees of several international conferences, including the IEEE Symposium on Hardware Oriented Security and Trust (HOST), IEEE Secure Development Conference (SECDEV), USENIX Security 2020, the IEEE Physical Assurance and Inspection of Electronics (PAINE), and the ACM Great Lakes Symposium on VLSI (GLSVLSI). He serves on the State of Maryland Cybersecurity Council and the National Academy of Sciences Intelligence Community Science Board Cybersecurity Committee. He is the recipient of numerous awards, including He is the recipient of multiple awards, including the NSF CAREER Award, IBM Faculty Partnership Award, National Semiconductor Faculty Development Award, and the General Motors Faculty Fellowship Award. He is currently a senior member of the IEEE and a member of Eta Kappa Nu and Tau Beta Pi engineering honor societies.

Introducing and Facilitating Internet of Medical Things (IoMT) Research for Undergraduate Students and High School Teachers

Abstract

The Internet of Medical Things (**IoMT**) is a rapidly growing community of intelligent medical technologies dedicated to sensing, monitoring, and reporting patient vitals, often with the intent of communicating findings with healthcare professionals (**HCPs**). For the past two summers, 2020 and 2021, four undergraduate electrical/computer engineering and computer science students, and two high school STEM teachers, worked with two graduate student mentors to explore various IoMT use cases via their participation in a Research Experiences for Undergraduates (**REU**) and Teachers (**RET**) program. During both summers, the REU/RET program was conducted remotely over nine weeks, not including pre-summer engagement activities. These pre-summer activities were designed to promote and encourage healthy mentor-mentee interactions while also providing an additional opportunity for participants to acclimate to their research projects before the program start.

Throughout this work, participants were able to gain or further develop skills in some of the following areas: Ethical Hacking, Data Science, Intrusion Detection Systems, Linux, Machine Learning, Networking, and Python, as well as interact with a designated smart device and testing environment. In the first summer, participants were assigned a smart glucose meter and tasked with 1) exploiting the potential threats associated with installing smart devices onto unsecured network configurations via address resolution protocol (**ARP**) poisoning, and 2) exploring social engineering tactics through cloning the device user application. Additionally, in the following summer, participants became acquainted with an existing IoMT dataset, developing an intrusion detection system (**IDS**) to accurately distinguish between normal and abnormal network packets due to a deployed Man-in-the-Middle (**MitM**) attack. The outputs of this work include: both sets of participants preparing verbal presentations, including demonstrations, and written papers outlining their results and experiences. After the project, participants should understand and implement a set of guidelines for utilizing IoMT devices more securely and with added privacy.

Introduction

The medical things that can transfer data over a network without human-to-human or human-to-computer interaction are called Internet of Medical Things [1]. IoT, in healthcare, offers several benefits such as enabling doctors and hospital staff to do their work more precisely and actively with less effort and intelligence [2]. However, this trade-off does not come without its challenges. The main challenge in the IoMT domain is preserving patient's privacy without degrading the security level [4]; as cybercriminals are targeting electronically protected health information (**ePHI**) to benefit from fraudulent insurance, medication, or financial schemes and even generate a profit from sales on the dark web [5]. This paper will further detail the projects: their activities and objectives, outcomes, and future work. Also included in this paper are the obstacles faced while facilitating research under virtual circumstances and possible areas of improvement for the following summers.

REU/RET Research Projects

Soon, the integration of smart medical technologies into smart home ecosystems may become more desirable for consumers relying on both technologies. Throughout this research, a variety of and heterogenous intelligent medical devices are considered to determine the potential threats that may arise from overlapping the two areas (**i.e.,** IoMT and smart homes) and provide solutions to uphold both security and privacy standards [6]. Tables **I** and **II** showcase the proposed REU/RET schedules and the projects are briefly described in the following paragraphs.

Project 1a aimed to explore *ethical hacking* through exploiting a smart glucose meter. By gaining access to the end user's home network, the participant was then tasked with identifying the smart medical device, located on an isolated wireless access point (**WAP**), and attacking the Bluetooth protocol.

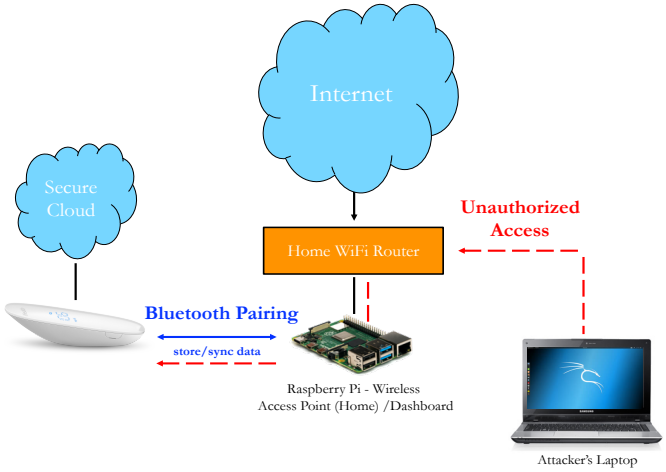


Figure 1. Summer 2020 Remote Attack Scenario 1a

Project 1b, once again, aimed to exploit a smart glucose meter; this time however, focusing on *social engineering* tactics. By providing users with a false sense of security, attackers can easily gain sensitive user credentials and even be granted access to view or modify unauthorized information. Arm with this knowledge, participants were tasked with exploring that exact scenario by targeting the user application instead of the device itself.

Following successful attack attempts for both projects, students were also tasked with developing a countermeasure(s) to defend their assigned system architecture.

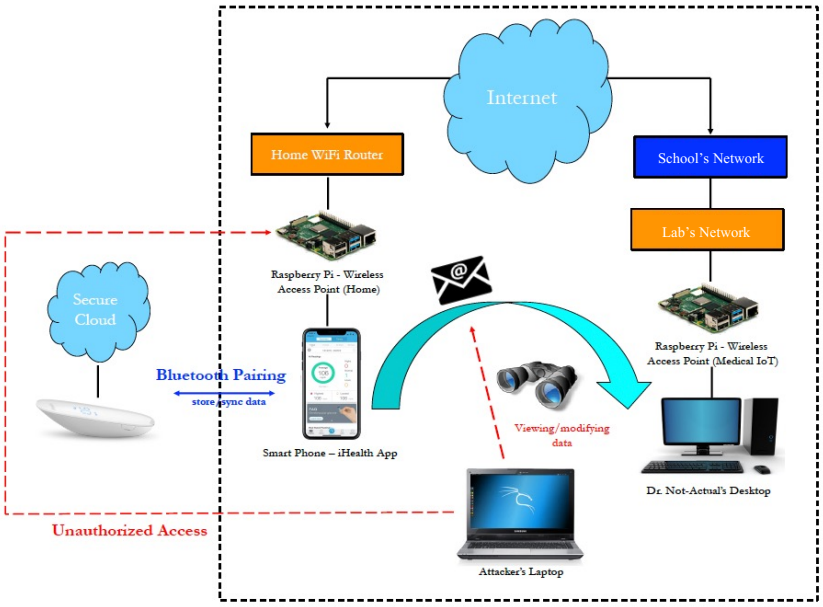


Figure 2. Summer 2020 Remote Attack Scenario 1b

Project 2 aimed to introduce the concept of *cyber resilience*, which suggests that a device's functionality will not be affected in the presence of a cyber-related event, through hands-on-experience executing and defending against a cyber security attack(s). The target for this attack scenario was a continuous positive airway pressure (**CPAP**) machine, located on a networked-raspberry pi, serving as an access point, with a display screen, for data visualization. Students were tasked with utilizing Wireshark to monitor the network traffic in this configuration, discovering the CPAP machine's IP address, deploying a cyber-attack aimed at the device, and assessing the attack's impact on the system. Additionally, participants were tasked with developing and implementing a mitigation strategy, of their choice, for accurately detecting the cyber-attack(s) and triggering an alarm to alert end users in the event a similar threat is detected in the future.

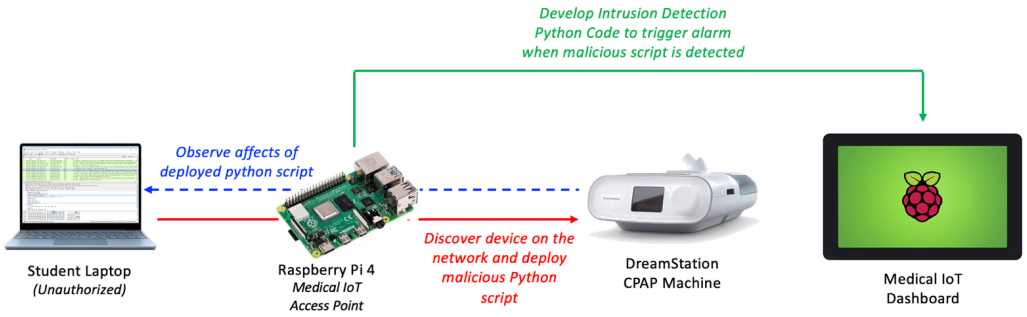


Figure 3. Summer 2021 Remote Attack Scenario

Table I – Schedules for the 2020 Summer Research Program

Week	*Activities*		*Description of Group Activities*
Pre-Summer	Reviewing Key Competencies and Resource Material		Introducing the project and current research problems
1 - 2	Linux Tutorials OSI Model Review	Network Security & Basics Wireshark Tutorials	Preliminary training
3	• Set-Up the Raspberry Pi as a Wireless Access Point & Dongle • Set-Up Kali Linux Virtual Machine		Initial System Set-Up
	Review the Bluetooth Chapters in Hacking Exposed Wireless **(Project 1a)**	Create a user profile and enter 'dummy' data into the user application **(Project 1b)**	
4	• Research Cybersecurity Terminology & Attacks • Literature Reviews		Introducing the correlations between cybersecurity and IoMT
5 - 6	Preform a Cyber Attack(s) & Investigate the System Affects		Offense Measures **(Attack Phase Demo)**
7 - 8	Propose and Implement a Security Countermeasure		Defense Measures **(Defense Phase Demo)**
9	Final Presentations and Paper Submission		Final REU/RET-wide program completion; virtual presentation and final write-up submission

Table II – Schedule for the 2021 Summer Research Program

Week	*Activities*		*Description of Group Activities*
Pre-Summer	Reviewing Key Competencies and Resource Material		Introducing the project and current research problems
1 - 2	Linux Tutorials OSI Model Review	Network Security & Basics Wireshark Tutorials	Preliminary training and understanding the literature
	IoMT Literature Searches and Reviews		
3 - 4	• Discover the CPAP machine on the network • Write Malicious Python Script & Observe the System Affects		Offensive Measures
5 - 6	• Develop an Intrusion Detection System that will Trigger an Alarm Once the Malicious Script and/or Affects Are Detected		Defensive Measures
7 - 8	Testing, Demos, and Refinement		Demo(s) and system evaluation and improvements
9	Final Presentations and Paper Submission		Final REU/RET-wide program completion; virtual presentation and final write-up submission

Results

Summer 2020

Project 1a.

Man-in-the-Middle **(MitM)** attacks are a form of eavesdropping in which malicious individuals intrude upon an existing conversation or data transmission. In this scenario, the participant sniffed the network traffic, using the *netdiscover* tool, to discover the glucose meter's IP address and performed ARP Poisoning, using the *arpspoof* tool, to impersonate the home router; successfully retrieving the information intended for the WAP and the glucose meter.

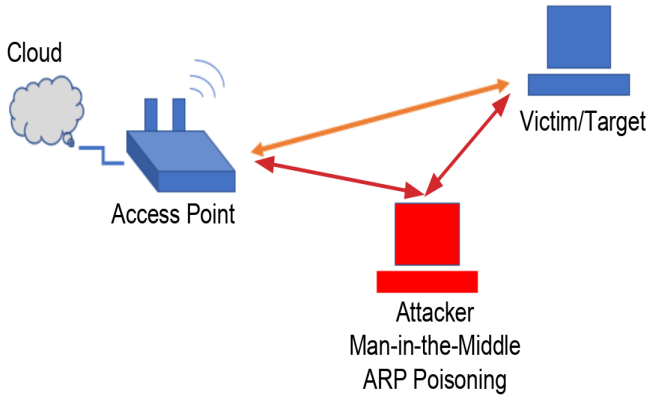


Figure 4. Man-in-the-Middle **(MitM)** Attack Showcase

Project 1b.

Phishing attacks are a type of social engineering tactic that leverages seemingly innocent appearing messages or emails that are actually malicious in origin and designed for data theft or malware deployment. Clone phishing, in particular, is the term coined for phishing attacks that aim to mimic an existing website or application that victims often frequent. In this approach, participants utilized the Social Engineering toolkit for cloning the smart glucose meter application. Additionally, with the help of the Ettercap DNS Spoofing tool, victims were then re-directed to the hacker's IP address to capture user credentials.

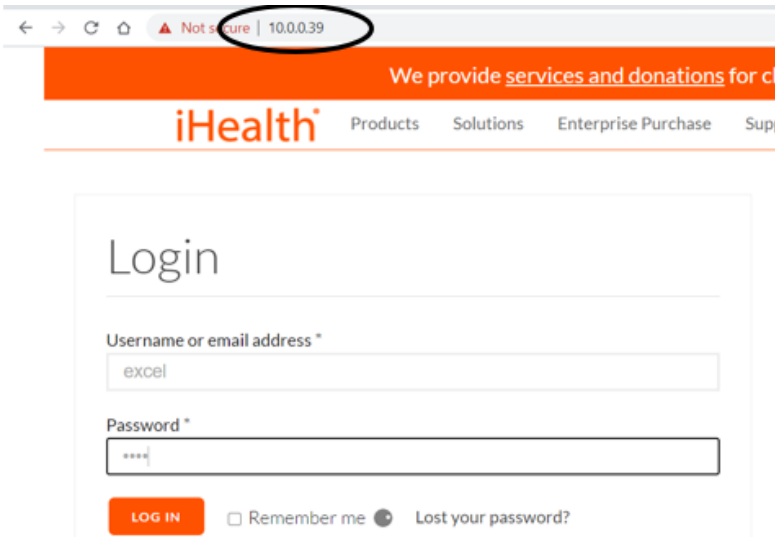


Figure 5. Cloned User Application from Attacker's IP Address

Although, the participants were unable to devise a countermeasure(s) to protect the smart glucose meter for their respective attack scenarios; they were, however, able to perform a case study, providing further insight into organizations can better secure smart medical technologies [7]. These recommendations include, but are not limited to:

1. Categorizing existing devices based on risk
2. Implementing a clinical management framework
3. Ensuring that their organizations follow basic security hygiene
4. Including security requirements in new proposals and contact languages
5. Applying a zero-trust networking architecture

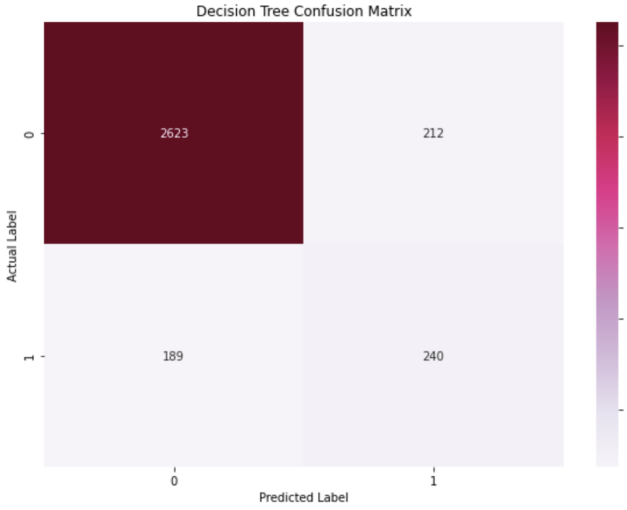
Additionally, the participants found that social engineering training could potentially help mitigate phishing attempts [8].

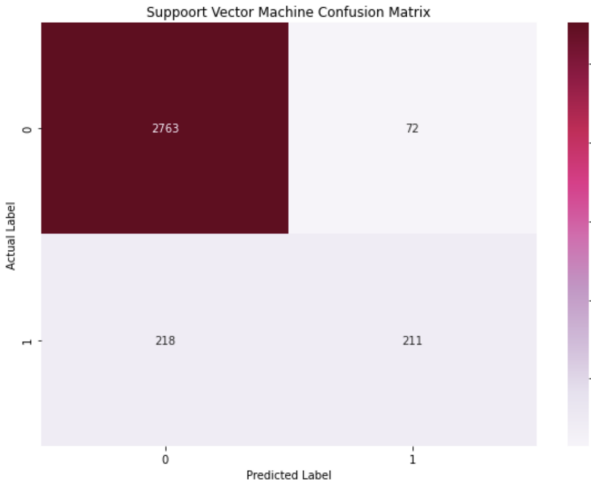
Summer 2021

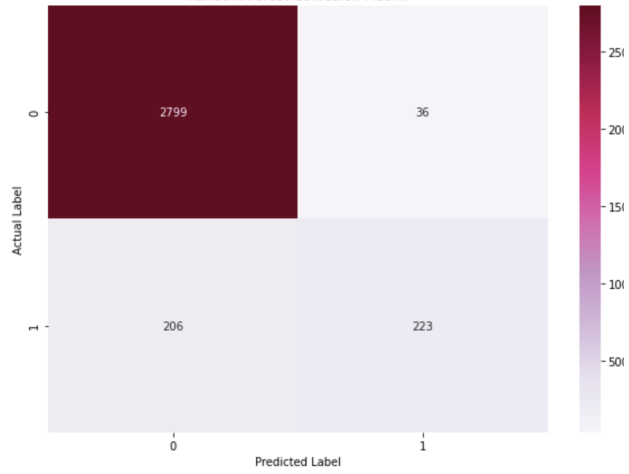
Throughout this summer, numerous challenges were presented when accessing and communicating with the testing environment. We provide the challenges in the next section. Thus, the project's direction shifted focus to the mitigation strategy first, hoping to collect data at a later point. The mitigation strategy determined for this scenario was a network-based intrusion detection system (**IDS**). An IDS is a device or software dedicated to monitoring, detecting, and reporting system security risks. In this case, participants utilized an existing IoMT dataset in which an Enhanced Healthcare Monitoring System (**EHMS**) was developed and monitored in the presence of a MitM attack(s), resulting in both normal and abnormal packets being captured [3]. This dataset also consisted of both network and biometric data points; however, we were only concerned with the network-related data for this work.

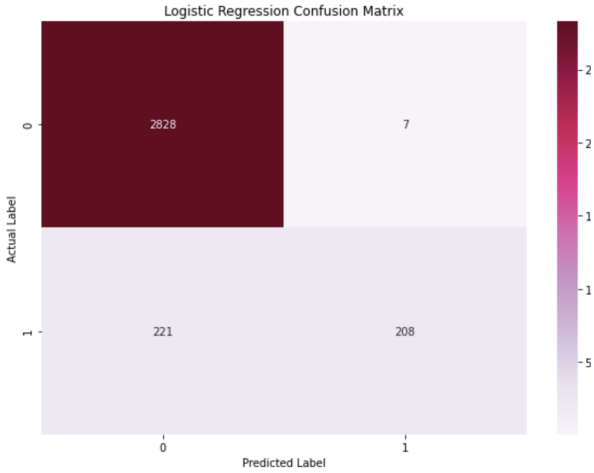
Once participants pre-processed the data, they were able to apply various machine learning algorithms including: Decision Tree, Random Forest, Logistic Regression, Gaussian Naïve Bayes, Support Vector Machines, Gradient Descent, and K-Nearest Neighbors for training and testing the dataset to evaluate how accurately the system was able to detect malicious activity. Confusion matrices then depicted the relationships between the system's predictions and actual labels for the data. Lastly, students were able to draw conclusions based on the testing time, and each algorithm's accuracy score, see formula (1), further suggesting that Logistic Regression may yield higher accuracy over a shorter amount of time than the other approaches.

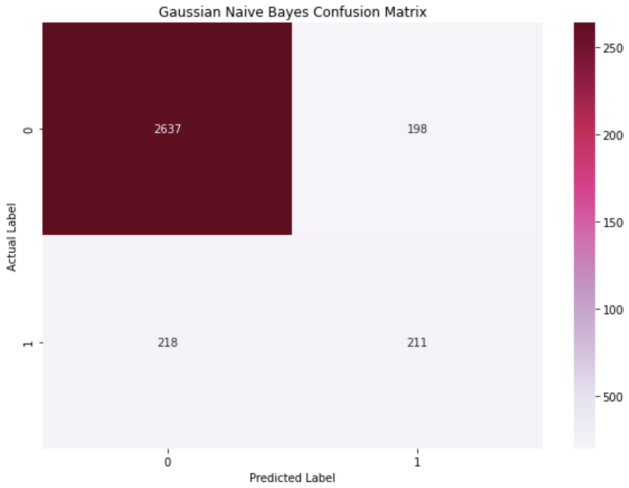
$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

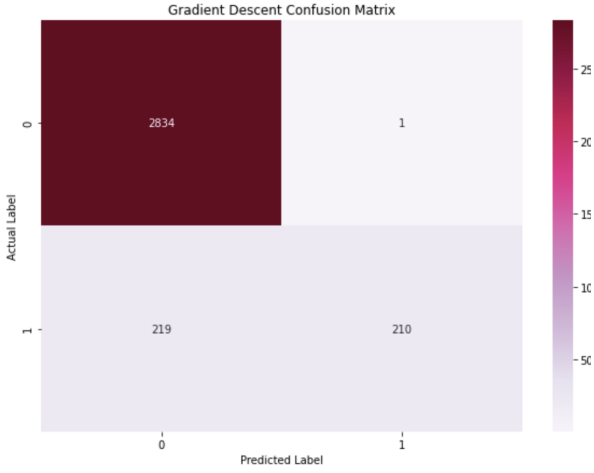

Decision Tree Confusion Matrix
2623
212
189
240
Actual Label
Predicted Label
0
1

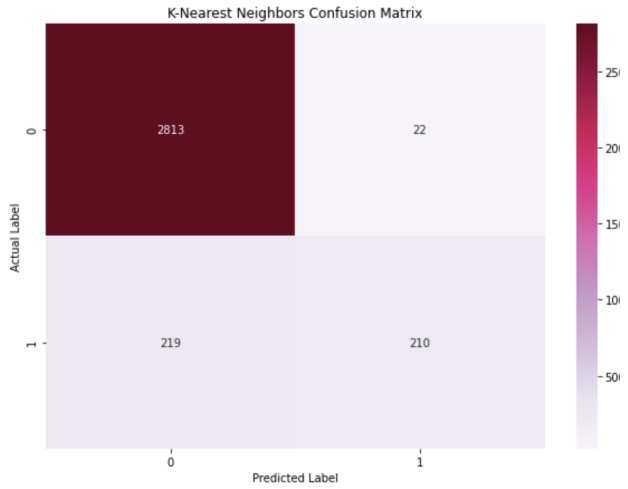

Suppoort Vector Machine Confusion Matrix
2763
72
218
211
Actual Label
Predicted Label
0
1


Random Forest Confusion Matrix
2799
36
206
223
Actual Label
Predicted Label
0
1


Logistic Regression Confusion Matrix
2828
7
221
208
Actual Label
Predicted Label
0
1


Gaussian Naive Bayes Confusion Matrix
2637
198
218
211
Actual Label
Predicted Label
0
1


Gradient Descent Confusion Matrix
2834
1
219
210
Actual Label
Predicted Label
0
1



Legend:
0 – normal network activity
1 – abnormal network activity

***Quadrant I** – True Negative (TN) events*
***Quadrant II** – False Positive (FP) events*
***Quadrant III** – False Positive (FP) event*
***Quadrant IV** – True Positive (TP) events*

Figure 6. Algorithm Confusion Matrices

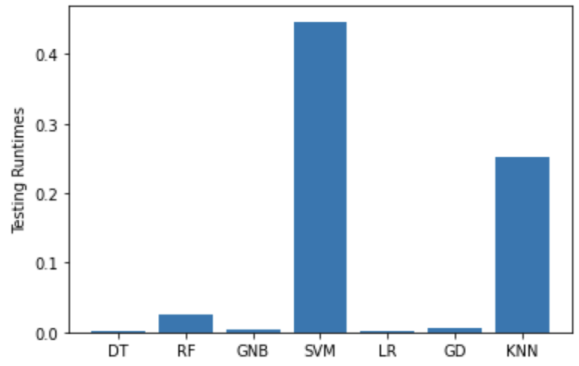


Figure 7. Algorithm Runtimes

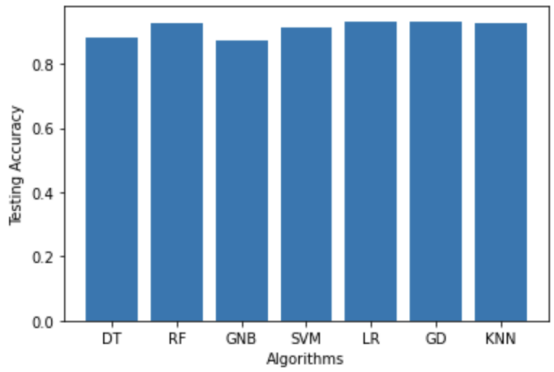


Figure 8. Algorithm Testing Accuracy

Challenges and Areas for Improvement

"Apart from the technical issues that prevented us from doing the hacking portion, [which] I was looking forward to, it was a great project."

As mentioned in the previous section, we faced many challenges during the summer 2021 project; troubleshooting the testing environment's issues under virtual circumstances proved to be overwhelming, effectively resulting in the project's direction changing to a data science project. The schedule was slightly adjusted for the participants to focus on defensive measures first to allow time for networking issues to be resolved and real-time data to be collected and fed in for system evaluation. However, this was not the case; instead, participants were allowed to explore machine learning concepts in further detail throughout this summer. Furthermore, participants were invited back to observe offensive measures post-summer.

Since the REU/RET was hosted under virtual constraints, one area of improvement would be to evaluate the testing scenarios before the program starts. Therefore, mentors could better assist or provide more detailed instructions when facing issues. Additionally, since a final paper is one of the critical deliverables for completing the REU/RET program, designing more creative ways to

encourage participants to develop actively and receive feedback on components of the paper might alleviate some of the stress towards the end of the program.

Closing Remarks and Future Work

When it comes to security, although IoMT devices are very similar in structure and implementation to non-medical-related IoT devices, they diverge where privacy is concerned. While there might be a wealth of knowledge available for the various cyber-attacks, mitigations, and recommendations mentioned in this paper, these devices and systems remain vulnerable. Additionally, IoMT systems pose much higher risks to consumers when under attack, as damage to the network, devices, and even data leakage could result in catastrophic consequences ranging from finances to injury or loss of life. For the subsequent phases of this research, we aim to troubleshoot the testing environment and simulate device-to-device communication patterns, using automated scripts, for real-time data collection and *vulnerability assessment*.

Acknowledgments

We would like to thank the faculty, staff, and students from the Center for Reverse Engineering and Assured Microelectronics (**CREAM**) Research Laboratory, Cybersecurity Assurance and Policy (**CAP**) Center, as well as the Smart Cities Research Experience for Undergraduates and Teachers (**SCR2**) for their support.

References

[1] S. Vishnu, S. R. J. Ramson and R. Jegan, "Internet of Medical Things (IoMT) - An overview," 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), 2020, pp. 101-104, doi: 10.1109/ICDCS48716.2020.243558.

[2] Joyia, Gulraiz & Liaqat, Rao & Farooq, Aftab & Rehman, Saad. (2017). Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain. Journal of Communications. 12. 240-247. 10.12720/jcm.12.4.240-247.

[3] A. A. Hady, A. Ghubaish, T. Salman, D. Unal and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," in IEEE Access, vol. 8, pp. 106576-106584, 2020, doi: 10.1109/ACCESS.2020.3000421.

[4] Jean-Paul A. Yaacoub, Mohamad Noura, Hassan N. Noura, Ola Salman, Elias Yaacoub, Raphaël Couturier, Ali Chehab, "Securing internet of medical things systems: Limitations, issues and 0167-739X, https://doi.org/10.1016/j.future.2019.12.028.

[5] "White Paper: The Internet of Medical Things (IOMT)," 1Call., McFarland, WI, USA, [Online]. Available: https://1call.com/sites/default/files/resources/white-papers/1Call-White-Paper-The-Internet-of-Medical-Thin.pdf

[6] P. Harvey, O. Toutsop, K. Kornegay, E. Alale and D. Reaves, "Security and Privacy of Medical Internet of Things Devices for Smart Homes," 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2020, pp. 1-6, doi: 10.1109/IOTSMS52051.2020.9340231.

[7] "5 steps to cybersecurity for Internet of Things medical devices ...". [Online]. Available: https://www.healthcareitnews.com/news/5-steps-cybersecurity-internet-things-medical-devices

[8] K. Greene, M. Steves and M. Theofanos, "No Phishing beyond This Point," in Computer, vol. 51, no. 6, pp. 86-89, June 2018, doi: 10.1109/MC.2018.2701632.