The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #41850

Integrating Cybersecurity in BSCS/BSIT Senior Design Capstone Projects: A Case Study

Dr. Radana Dvorak,

Radana Dvorak has worked as a researcher, professor, dean, consultant, and program architect. Her Ph.D. CS-AI and MSc-AI from the UK, and BA from the University of Michigan. She has worked in the UK, US and the Cayman Islands. Radana spent time in the software industry, headed a VC funded company bringing her PhD work to market, served on government, university strategic planning committees, international fellowships; she was one of the key architects of the Microsoft Software System Academy - partnership between the DoD, Microsoft, and Universities. Radana is currently an associate professor and a Chair of the CS Dept. at Saint Martin's University.

Mr. John L. Whiteman, Saint Martin's University

John L. Whiteman is a Senior Security Engineer for Lam Research in Oregon and a part-time adjunct cybersecurity instructor at Saint Martin's University. John received a Master of Science in Computer Science from Georgia Tech University. John holds multiple security certifications, including CISSP and CCSP.

Integrating Cybersecurity in BSCS & BSIT Senior Design Capstone Projects: A Case Study

John Whiteman M.S. & Radana Dvorak Ph.D.

Abstract

ABET mandates the incorporation of cybersecurity concepts in CS programs. Specifically, the BSIT's ABET outcome six emphasizes: “Using systemic approaches to select, develop, apply, integrate, and administer secure computing technologies to achieve user objectives.”

At Saint Martin’s University, BSIT and BSCS students collaborate in a two-semester Senior Capstone Project course. These projects necessitate an external client, with students working in small groups to design, develop and deliver a product, presentation, and demonstration. While cybersecurity forms an integral part of all projects, this paper highlights a distinctive project centered on developing an IoT device that uses various sensors to continuously monitor for hidden cameras, microphones, and GPS trackers in a room even while humans are away. The unique aspect of the project is that it sends the sensor telemetry data to a cloud application the students build, using microservices, storage, and data models to identify invasive devices. Optionally, if an invasive device is confirmed, its telemetry data is cryptographically packaged as forensic evidence for law enforcement.

Furthermore, the project resonates with modern software engineering practices, notably the employment of cloud microservices to collect and model data used to protect personal privacy. Our presentation is bifurcated into two segments:

> (1) Project Overview: This section expounds on the concepts covered, details the project’s structure, highlights its relevance to industry trends and employment opportunities, and pedagogical strategies for student engagement.
>
> (2) Beyond Technical Design: We discuss the broader aspects, including giving students firsthand experience in formulating a lean business plan, navigating patent applications, and effectively presenting to potential investors.

The paper outlines the modules, learning outcomes, and student experiences in both product development and investor pitching.

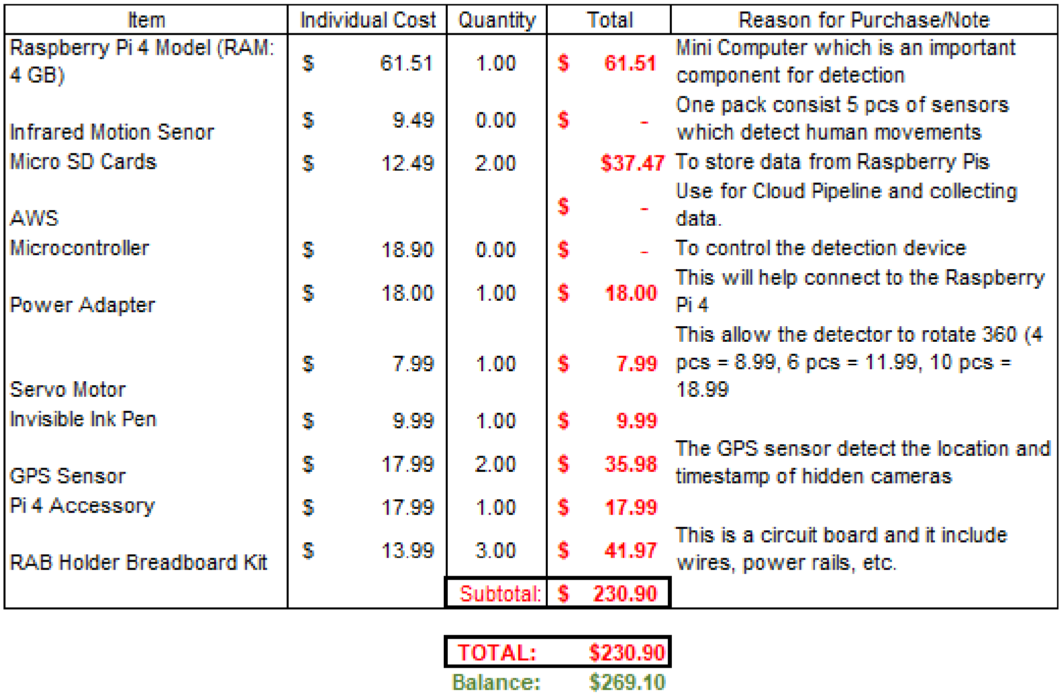
Introduction

The prevalence of privacy invasions is escalating with the widespread availability of inexpensive surveillance equipment, such as miniature wireless cameras. [11][14]. Despite the irony that major online retailers offer both spy gadgets and their countermeasures, consumers are drawn to spy detector devices. [6]. Spy detectors typically have a common set of features, including RF detection for wireless cameras and microphones, magnetic field detection for GPS trackers, and flashing LED infrared lights that capture camera lens reflections [1][2]. The more expensive devices come with sounds and haptic vibrations to alert for possible detection. Unscrupulous sellers make inaccurate claims that devices prevent camera spying when, in reality, the devices only provide detection, giving their customers the false impression that a camera is no longer capable of spying on them.

This paper presents a project by a senior capstone team of four students who aimed to develop an advanced spy camera detection device. Their objective was to create a reliable tool that could not only detect hidden surveillance equipment but also aid in legal actions against privacy violators, subject to local laws [9][12]. The project, named the Smart IoT Hidden Detection Device (SIHDD), seeks to offer a more effective solution in the fight against unauthorized surveillance.

Budget

Every capstone team received a $500 budget from the university. The students focused on keeping the cost of their device comparative, if not cheaper, than the devices sold online. They wanted to build a better 'mousetrap' without breaking the bank, but before moving forward, the team had to learn how to make the original mousetrap first. They purchased Raspberry Pis[1], various sensors, wires, breadboards, and tools to assemble comparable devices. No one on the team except one had experience with hardware IoT devices. After some technical tradeoffs, including using less powerful, older versions of Raspberry Pis, the students stayed within budget.



Item	Individual Cost	Quantity	Total	Reason for Purchase/Note
Raspberry Pi 4 Model (RAM: 4 GB)	$ 61.51	1.00	$ 61.51	Mini Computer which is an important component for detection
Infrared Motion Senor	$ 9.49	0.00	$ -	One pack consist 5 pcs of sensors which detect human movements
Micro SD Cards	$ 12.49	2.00	$37.47	To store data from Raspberry Pis
AWS			$ -	Use for Cloud Pipeline and collecting data.
Microcontroller	$ 18.90	0.00	$ -	To control the detection device
Power Adapter	$ 18.00	1.00	$ 18.00	This will help connect to the Raspberry Pi 4
Servo Motor	$ 7.99	1.00	$ 7.99	This allow the detector to rotate 360 (4 pcs = 8.99, 6 pcs = 11.99, 10 pcs = 18.99
Invisible Ink Pen	$ 9.99	1.00	$ 9.99	
GPS Sensor	$ 17.99	2.00	$ 35.98	The GPS sensor detect the location and timestamp of hidden cameras
Pi 4 Accessory	$ 17.99	1.00	$ 17.99	
RAB Holder Breadboard Kit	$ 13.99	3.00	$ 41.97	This is a circuit board and it include wires, power rails, etc.
		Subtotal:	$ 230.90	

TOTAL:	$230.90
Balance:	$269.10

Diagram 1: Project's Budget

[1] The team also received two donated Raspberry Pis from Saint Martin's University

Requirements and Features

The project consisted of two major parts: first, a hardware IoT device that collects, aggregates, and sends sensor telemetry data to a cloud application, and second, the cloud application itself.

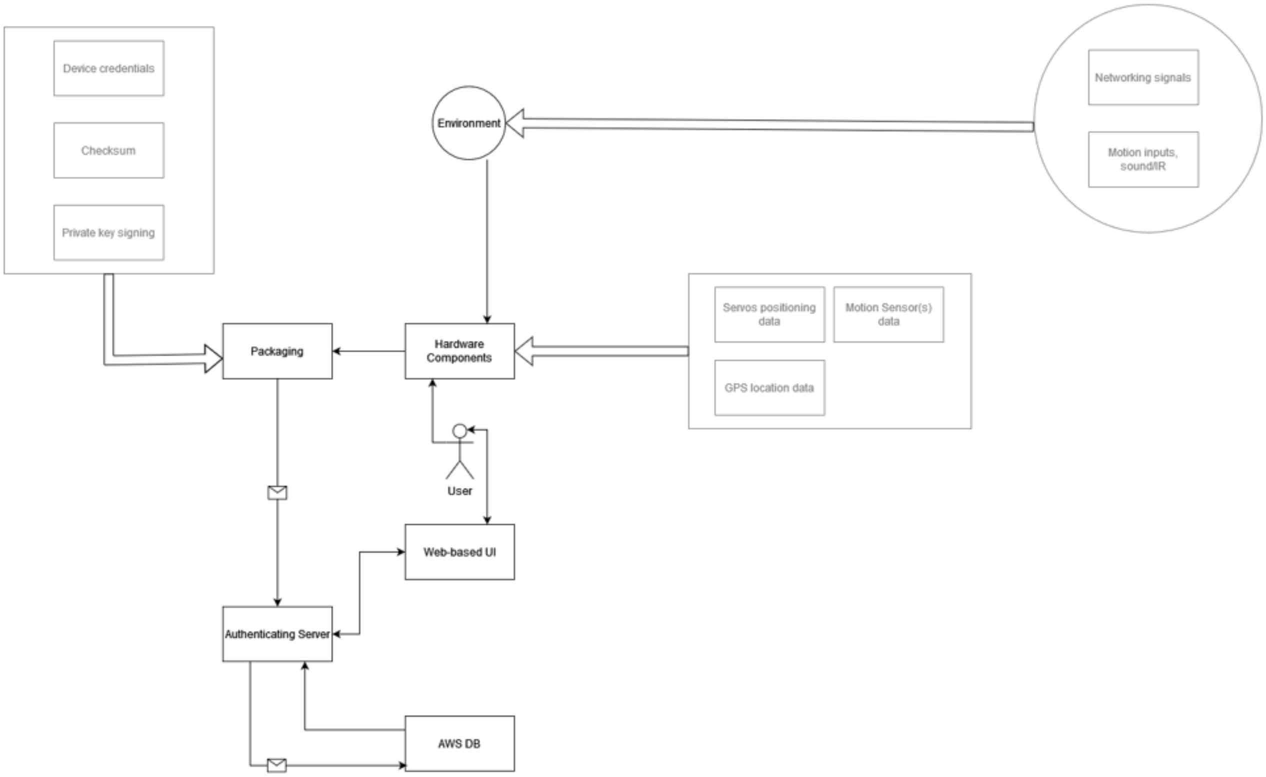


Diagram 2: Project's Architecture

Much like the hardware IoT device, only one student on the team had a background working with cloud technologies, a critical skill for students to have in the competitive job market. Besides supporting the existing capabilities that the other detection devices offered, the client provided the team with three new requirements:

Continuous Unattended Omnidirectional Monitoring

Most wireless spy cameras can be deactivated remotely by its owner. A savvy perpetrator might wait until an unsuspecting victim completes a sweep of a space. While a wireless camera might still broadcast a heartbeat packet, its detection is less likely than if it was actively sending streams of video packets. Once a victim completes a bug sweep and no spy device is detected, the victim will likely not perform another sweep for the rest of the stay. The perpetrator who has access to space, owner or employee, could enter the premises while the victim is away and install a new spy camera. Like a radar, the SIHDD can continuously rotate its sensors from a fixed location in the center of a room, sending its telemetry data back to the cloud application via a wireless connection. The owner of the device does not have to hold it. SIHDD can always be left on, even while the owner is away. The owner could receive alerts if a device is discovered.

Advanced Spy Camera Detection Capabilities

One challenge with typical detection devices is filtering out all legitimate wireless traffic in a room, especially in a hotel. Processing the wireless traffic data is resource-intensive, especially if the IoT device runs on a battery. The cloud application handles the processing using statistical models based on existing data collected from other spy cameras to identify possible threats [15].

A Cryptographic Forensics Evidence Packager

What happens when a spy camera is detected? If the owner of the spy camera is alerted, the owner can turn it off and claim it was never on. Owners can argue that the camera is only used when the place is vacant. Without evidence, police cannot make any arrests. The project novel addition is the forensics evidence packager exists in the cloud application. It can take the same sensor telemetry data used to identify the spy camera and package it as a cryptographically signed evidence package for law enforcement[2]. This work is expected to continue in the late spring. The sensor data includes:

- GPS's latitude and longitude coordinates
- Synchronized timestamps between the IoT device and the cloud application using the cloud vendor's clock
- The camera's unique media access control (MAC) address extracted from the wireless headers found in the network traffic logs [3][10]

No Cameras or Microphones

Another project requirement prohibits the use of a camera or microphone on SIHDD since the client did not want criminals to engineer it into a smart spy device.

3D Printed Protective Form Factor

Although not an original requirement, one student created a protective form factor for the IoT board using a 3D printer. The student learned how to create CAD files using Autodesk Fusion.

[2] The public certificate must come from a third-party such as the cloud vendor.

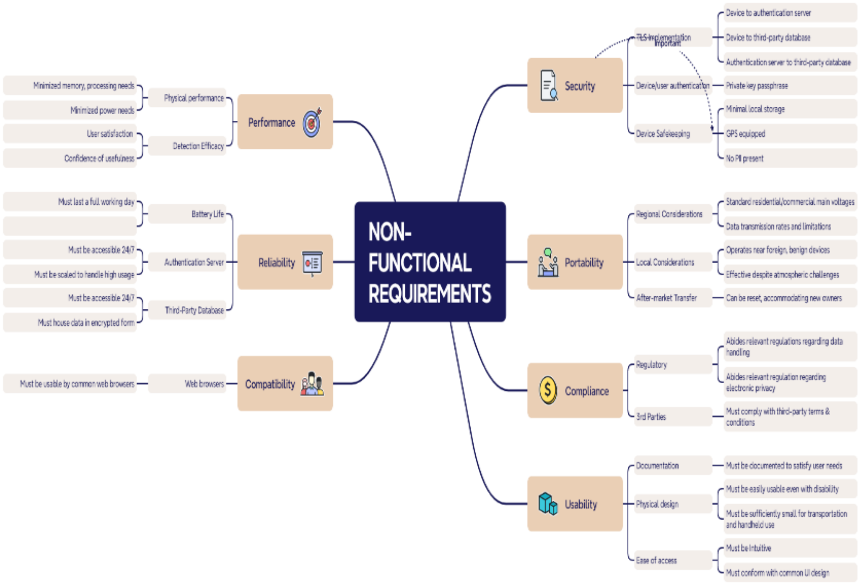

NON-FUNCTIONAL REQUIREMENTS
Performance
Physical performance
Minimized memory, processing needs
Minimized power needs
Detection Efficacy
User satisfaction
Confidence of usefulness
Reliability
Battery Life
Must last a full working day
Authentication Server
Must be accessible 24/7
Must be scaled to handle high usage
Third-Party Database
Must be accessible 24/7
Must house data in encrypted form
Compatibility
Web browsers
Must be usable by common web browsers
Security
TLS Implementation
Important
Device to authentication server
Device to third-party database
Authentication server to third-party database
Device/user authentication
Private key passphrase
Device Safekeeping
Minimal local storage
GPS equipped
No PII present
Portability
Regional Considerations
Standard residential/commercial main voltages
Data transmission rates and limitations
Local Considerations
Operates near foreign, benign devices
Effective despite atmospheric challenges
After-market Transfer
Can be reset, accommodating new owners
Compliance
Regulatory
Abides relevant regulations regarding data handling
Abides relevant regulation regarding electronic privacy
3rd Parties
Must comply with third-party terms & conditions
Usability
Documentation
Must be documented to satisfy user needs
Physical design
Must be easily usable even with disability
Must be sufficiently small for transportation and handheld use
Ease of access
Must be Intuitive
Must conform with common UI design

Diagram 3: Non-functional Requirements

Team Strategy and Execution

Collectively, the team worked on project management, budgeting, and designing at the onset and then took a divide-and-conquer approach to work on both parts simultaneously during the implementation phase. Agile SCRUM methodology was utilized.

One team member focused on the IoT hardware device, integrating the detection sensors on Raspberry Pi boards [5], including sonic and infrared sensors for motion detection, GPS sensors, micro-SD cards, power adapters, and servo motors to support the requirement for monitoring without human interaction in omnidirectional sweeps [13]. The device also had onboard wireless capabilities that the team member configures to communicate with the cloud application.

Another team member worked on the cloud infrastructure, setting up identity and access management, configuring a NoSQL database to store the incoming sensor telemetry data, and subscribing to a cloud vendor software-as-a-service to connect IoT devices remotely. Another requirement by the client stated the team must follow best practices in cloud security [4] to ensure that any potentially sensitive data collected by the devices is protected securely from adversaries. From a legal perspective, the team learned why applying these protections is called due diligence, especially in the event of a data breach when law enforcement initiates a criminal investigation. All team members were assigned role-based access privileges on a need-to-have basis, along with strict password rules and multifactor authentication. The cloud vendor added security by encrypting the data at rest and in motion.

The other two team members worked on coding the cloud application, which included the following features:

- Creating the necessary APIs to communicate with the SIHDD

- Parsing and synchronizing the incoming telemetry data and building the workflows to populate the database and other storage
- Generating prediction models based on data collected from several popular spy cameras donated by the client

Eating One's Own Dog Food

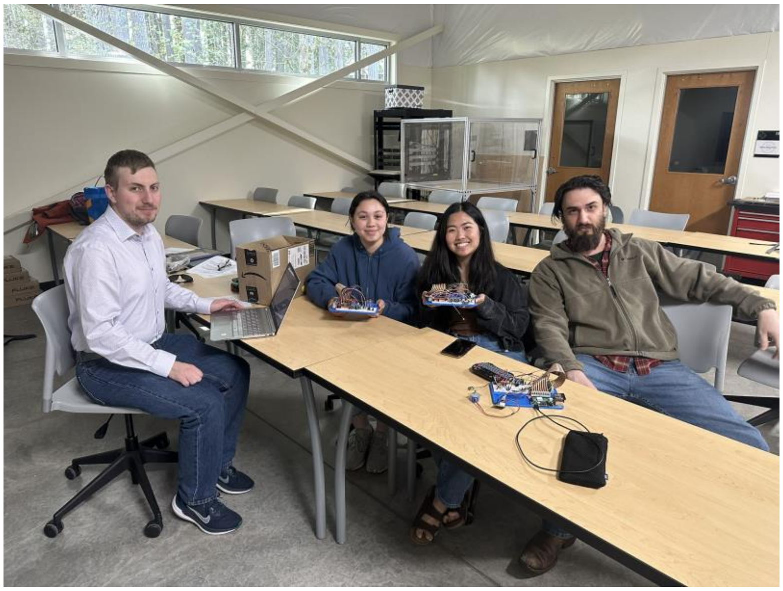
Every team member took ownership of a device to test and use, following an old engineering practice more affectionally known as "eating one's own dog food [8]." The team learned the IoT device's limitations and strengths, gaining confidence in its effectiveness as it matured. By possessing the device, each team member had to consider if the IoT device had a reasonable chance in the marketplace.

Intellectual Property Rights and Patents

Questions about intellectual property rights became a discussion point amongst the university, client, and students. The client asked the team to meet with a patent expert at the university to learn more about the submission process, its associated costs, and if the project is patentable. Even if students decide not to file a patent, institutions with a capstone program should have this discussion with all stakeholders at the very beginning of the project to avoid any potential misunderstandings later. At the time of the writing, the students are filing a provisional patent application for their technical work.

Conclusion

The project was delivered on time in April 2024 and the students won the computer science capstone project of the year competition and were honored at the annual Saint Martin's Scholar's Day event. They architected a solution that helps protect people's privacy and is capable of cryptographically packaging the data as forensic evidence that law enforcement can use to catch criminals. The senior project’s wide range of experiences cultivated new, marketable job skills, including IoT hardware, cloud technologies, cryptography, planning, budgeting, intellectual property rights, and networking. However, more importantly, the students delivered a product with their newfound skills to help protect people's privacy.



Team SIHDD (from left to right): Garrett Orwig, Nadaa Elbarbary, Krizia Ragotero, Hayden Jones

References

[1] S. Sami, B. Sun, S. Tan, and J. Han, "LAPD: Hidden Spy Camera Detection using Smartphone Time-of-Flight Sensors," *in SenSys '21, Coimbra, Portugal. November 15-17, 2021*. Available: https://dl.acm.org/doi/pdf/10.1145/3485730.3485941

[2] Z. Yu, Z. Li, Y. Chang, S. Fong, J. Liu, and N. Zhang, "HeatDeCam: Detecting Hidden Spy Cameras via Thermal Emissions," *in CCS, Los Angeles. CA. November 7-11, 2022*. Available: https://mosis.eecs.utk.edu/publications/yu2022heatdecam.pdf

[3] L. Chappell, *Wireshark 101: Essential Skills for Network Analysis*. La Vergne, TN: Lightning Source Inc., 2013

[4] M. Chapple, and D. Seidl, *(ISC)2 CCSP Certified Cloud Security Professional Official Study Guide, 3rd Edition*. Alameda, CA: Sybex, 2022

[5] K. Karvinen, T. Karvinen, *Getting Started with Sensors: Measure the World with Electronics, Arduino, and Raspberry Pi*. Sebastopol, CA: Maker Media Inc., 2014

[6] A. Bhattacharya, “Amazon is still selling the clothes hook spy cameras it’s being sued over,” *Quartz,* Dec. 12, 2023. https://qz.com/amazon-is-still-selling-the-clothes-hook-spy-cameras-it-1851091831.

[7] M. Murney, “Son of Buc-ee’s co-founder arrested for hiding cameras in home bathrooms,” *Chron*, Oct. 05, 2023. Accessed: Feb. 08, 2024. [Online]. Available:

https://www.chron.com/news/houston-texas/article/bucees-son-arrested-cameras-18408739.php

[8] “What Is ‘Dogfooding’? (Published 2022),” *The New York Times*, 2024. Accessed: Feb. 08, 2024. [Online]. Available: https://www.nytimes.com/2022/11/14/business/dogfooding.html

[9] R. Edwards, “Security Camera Laws, Rights, and Rules,” *SafeWise*, Oct. 13, 2023. https://www.safewise.com/security-camera-laws/

[10] G. Harris and M. C. Richardson, “PCAP Capture File Format,” *Ietf.org*, Dec. 21, 2020. https://www.ietf.org/archive/id/draft-gharris-opsawg-pcap-01.html

[11] “South Korea: number of spycam crimes 2022 | Statista,” *Statista*, 2022. https://www.statista.com/statistics/1133121/south-korea-number-of-spycam-crimes/

[12] C. Steele, “Does Your Airbnb Have Hidden Cameras? Here’s How to Check,” *PCMAG*, Dec. 23, 2023. https://www.pcmag.com/how-to/how-to-check-for-hidden-cameras-airbnb-vacation-rental

[13] Maker. io Staff, “How to Control Servo Motors with a Raspberry Pi,” *DigiKey*, Feb. 10, 2021. https://www.digikey.com/en/maker/tutorials/2021/how-to-control-servo-motors-with-a-raspberry-pi

[14] “Global Hidden Camera Spy Camera Market – Industry Reports,” *Precisionreports.co*, 2022. https://www.precisionreports.co/global-hidden-camera-spy-camera-market-21808975.

[15] S. Herodotou, F. Hao, "Spying on the Spy: Security Analysis of Hidden Cameras," *Warwick University, Coventry, United Kingdom. June 1 2023.* Available: https://arxiv.org/pdf/2306.00610.pdf