Securing Integrated CGM and Insulin Pump Systems with Machine Learning

Taruni Sankabathula*, Dr. Lavanya Mandava

Computer Science & Information Systems, Bradley University

Introduction

- **Diabetes Management with iCGM Systems:** Integrated Continuous Glucose Monitoring (iCGM) systems and insulin pumps automate insulin delivery, greatly improving diabetes care. These systems allow real-time blood glucose monitoring and communication with external devices like smartphones for better patient control and convenience.
- **Challenges:** With increased interconnectivity, these systems are susceptible to cyberattacks such as data breaches, unauthorized access, and potential malicious control.

Objectives

- Review the architecture and vulnerabilities of iCGM systems.
- Explore how machine learning (ML) can be leveraged to strengthen security and mitigate risks in these interconnected devices.

Architecture

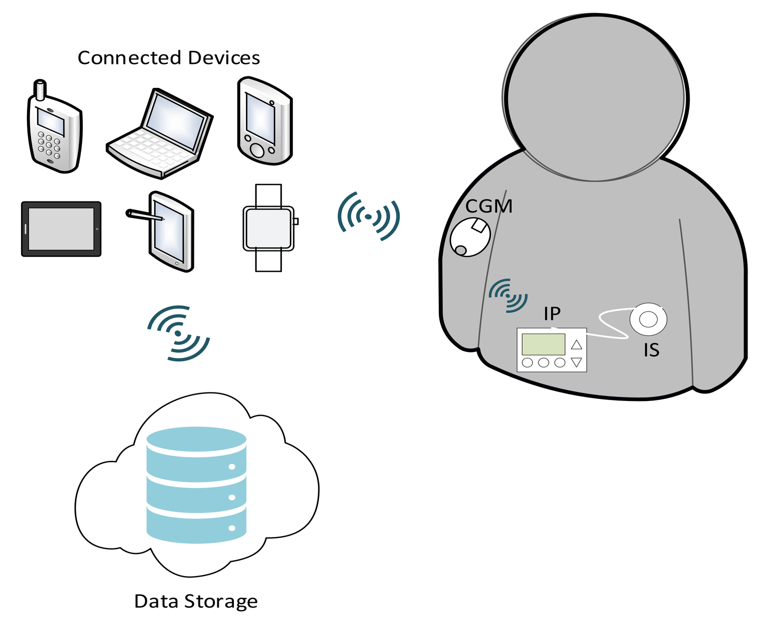

Fig. 1: General Architecture of Insulin Pump with iCGM System

- Continuous Glucose Monitor (CGM): Measures blood glucose levels.
- Insulin Pump (IP): Administers insulin doses based on CGM data through Infusion Set (IS).
- Smart Device Interface: Smartphone or external device to monitor and control the system remotely.
- Closed-loop System: Enables the IP to respond directly to CGM readings without human intervention.
- Communication Pathways: These devices communicate wirelessly via Bluetooth or other wireless protocols, creating opportunities for security breaches if not properly secured.
- Database: Serves to compile and organize the collected readings for analysis and reference.

iCGM Bluetooth Security Specifications & Key Vulnerabilities

Table 1: Bluetooth BR/EDR Specifications

Characteristic	Version 4.0 & earlier	Versions 4.1, 4.2
Piconet slaves active	7	7
Piconet slaves total	255	255
Pairing algorithms	P-192 Elliptic Curve, HMAC-SHA-256	P-256 Elliptic Curve, HMAC-SHA-256
Encryption algorithms	E0/SAFER+	AES-CCM
Authentication algorithms	E1/SAFER	HMAC-SHA-256

Table 2: Bluetooth LE Specifications

Characteristic	Version 4.1 & earlier	Version 4.2
Piconet slaves active	Unlimited	Unlimited
Piconet slaves total	Unlimited	Unlimited
Pairing algorithms	AES-128	P-256 Elliptic Curve, AES-CMAC
Encryption algorithms	AES-CCM	AES-CCM
Authentication algorithms	AES-CCM	AES-CCM

- **Role of Bluetooth in iCGM Systems:** iCGM systems use Bluetooth 4.0 and later versions for connectivity, ensuring compatibility with a wide range of devices. Bluetooth technology allows the transmission of glucose readings from transmitters to users' devices, as well as managing tasks like connection establishment and error handling.
- **Dual-Mode Operation:** iCGM systems support dual-mode Bluetooth:
  - Basic Rate/Enhanced Data Rate (BR/EDR): Handles bond management and other core functions.
  - Bluetooth Low Energy (LE): Used for continuous monitoring, as it consumes less power.

- **MITM Attacks & Weak Authentication:** Devices using Bluetooth 4.0-4.2 are vulnerable to Man-in-the-Middle (MITM) attacks, especially when multiple devices share piconets without robust authentication.
- **Weak Encryption:** Bluetooth 4.0 uses the weak E0 cipher, making data susceptible to decryption. Backward compatibility with older devices further weakens security.
- **Device, Not User, Authentication:** Bluetooth authenticates devices but not users, increasing the risk of unauthorized access.
- **Privacy & Tracking:** Bluetooth LE offers device address privacy, but BR/EDR lacks this, exposing devices to tracking threats.
- **Data Transmission Risks:** Transmission of glucose and insulin data to remote servers risks breaches, which could affect future treatments.
- **Consequences:** Exploiting these vulnerabilities could lead to incorrect insulin dosages, posing severe health risks.

Machine Learning-Based Security Solutions

- **Dataset Utilization:** We utilized an open-source dataset containing records from various age groups, including both diabetic and non-diabetic individuals. The data includes blood glucose levels and external body parameters such as body temperature, heart rate, and blood pressure.
- **Data Preprocessing:** We performed data cleaning and transformation to prepare the raw data for machine learning models, ensuring it was in a suitable format for analysis.
- **Exploratory Data Analysis (EDA):** Through EDA, we visualized and summarized the data to identify patterns and relationships, helping guide further analysis and model development.

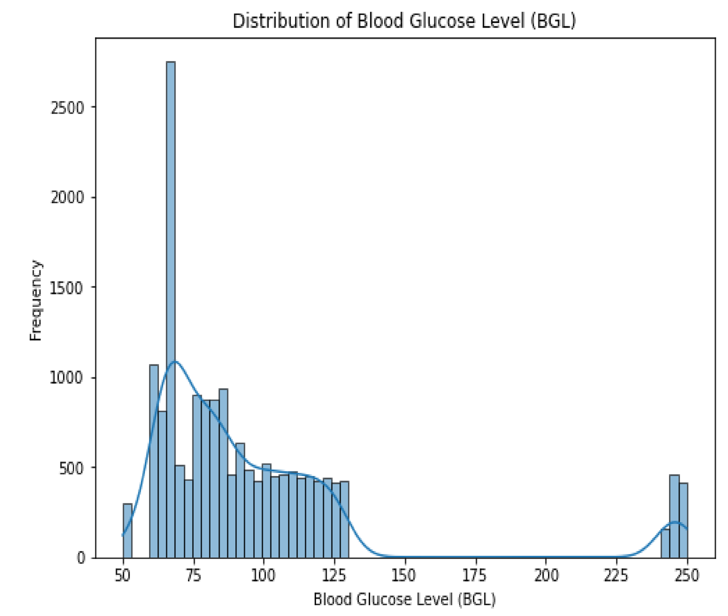

Fig. 2: Histogram Interpretation of BGL vs Frequency

Fig. 3: Line Plot of BGL vs Age

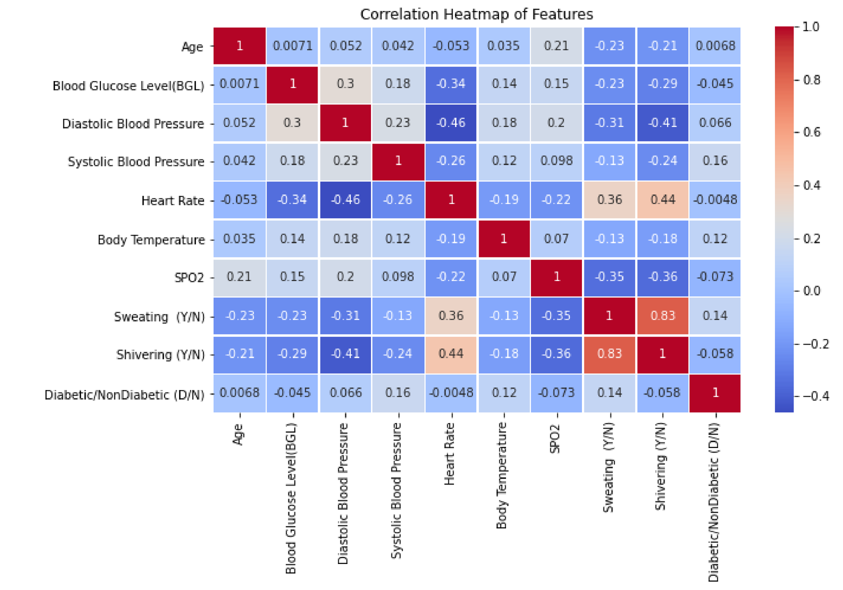

Fig. 4: Correlation Heatmap of Features

- **Anomaly Detection:** Machine learning models demonstrate high accuracy in detecting unauthorized access attempts and abnormal device behavior.
- **Reduction in False Positives:** ML-based systems can reduce false alarms compared to rule-based systems, offering more precise threat detection.

Table 3: Model Performance Summary

Model	Accuracy
Logistic Regression	0.98
Random Forest	0.99
Support Vector Machine	0.98
K-Nearest Neighbors	0.93

Risk Mitigation and Countermeasures

- **User Training & Awareness:** Provide security training for iCGM users and medical personnel. Educate on vulnerabilities and best practices to foster security awareness. Tailor training to various ages, backgrounds, and tech literacy levels.
- **Securing Bluetooth Connections:** Address Bluetooth vulnerabilities like unlimited authentication requests. Implement increasing wait times for repeated authentication attempts. Upgrade to stronger encryption (Bluetooth 4.1+). Ensure user authentication and end-to-end encryption to prevent unauthorized access.
- **Preventing MITM Attacks:** Use MITM protection mechanisms and refuse unauthenticated link keys. Incorporate unique, changing key pairs and random passkeys during device pairing.
- **Minimizing Adversary Exposure:** Pair devices in secure environments. Limit discoverable/connectable mode duration to reduce exposure to attacks.
- **Audit & Non-repudiation Services:** Implement audit and non-repudiation services as overlay mechanisms to enhance accountability and forensic capabilities.

Conclusion

- **Impact on Patient Safety:** The integration of machine learning into iCGM systems enhances security and reduces the risk of malicious attacks, thus ensuring that patients can safely rely on these devices for diabetes management.
- **Importance of ML in Future iCGM Systems:** Machine learning should be a key component of future CGM and insulin pump designs to proactively defend against emerging security threats. This approach can improve both data privacy and overall patient safety.
- **Balancing Security and Usability:** While enhancing security, it is also crucial to maintain the ease of use and low latency in device operations, particularly for real-time critical functions like insulin delivery.
- **Conclusion:** A multi-layered approach is essential - education, technological upgrades, and strict protocols ensure the security and privacy of iCGM systems.

References

- L. Mandava, H. Ghazaleh, and G. Zhao, "Securing modern insulin pumps with iCGM system: protecting patients from cyber threats in diabetes management," in *Cybersecurity in Emerging Healthcare Systems*, Chapter 14, pp. 427-444, Editors: A. L. Imoize, C. Meshram, J. B. Awotunde, Y. Farhaoui, and D. Do, The Institution of Engineering and Technology, 2024

Real Time Communications Conference and Expo at Illinois Tech

IEEE International Conference

IEEE RTC 2024 - October 8-10, 2024 - IIT, Chicago, IL, USA