การระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพส่วนบุคคลสำหรับอุปกรณ์สวมใส่โดยใช้ไอซีเข้ารหัส

นิพนธ์ สมหมาย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยบูรพา
สิงหาคม 2561

คณะกรรมการควบคุมวิทยานิพนธ์ และคณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาวิทยานิพนธ์ของ นิพนธ์ สมหมาย ฉบับนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า ของมหาวิทยาลัยบูรพาได้

คณะกรรมการควบคุมวิทยานิพนธ์

..... อาจารย์ที่ปรึกษาหลัก
(รองศาสตราจารย์ วิรุฬห์ ศรีบริรักษ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธาน
(รองศาสตราจารย์ ณัฐวุฒิ ขวัญแก้ว)

..... กรรมการ
(รองศาสตราจารย์ วิรุฬห์ ศรีบริรักษ์)

..... กรรมการ
(ดร. ภาณุวัฒน์ ด่านกลาง)

..... กรรมการ
(ดร. ทนงศักดิ์ เทพสนธิ)

คณะวิศวกรรมศาสตร์อนุมัติให้รับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า ของมหาวิทยาลัยบูรพา

..... คณบดีคณะวิศวกรรมศาสตร์
(ดร. อาณัติ ดีพัฒนา)
วันที่ ๙ เดือน สิงหาคม พ.ศ. 2561

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยการได้รับความกรุณาให้คำปรึกษาเสนอแนะแนวทางที่ถูกต้องและตรวจแก้ไขข้อบกพร่องต่าง ๆ อย่างดียิ่งจาก รองศาสตราจารย์ วิรุฬห์ ศรีบริรักษ์ อาจารย์ที่ปรึกษาหลักที่ให้คำแนะนำชี้แนะแนวทาง และดร.อภิรัฐ ลิ่มมณี ที่สนับสนุนช่วยเหลือ ประธานคณะกรรมการสอบวิทยานิพนธ์ คณะกรรมการสอบวิทยานิพนธ์ ที่ให้คำแนะนำ ผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณทุกท่านเป็นอย่างสูงไว้ ณ ที่นี้

วิทยานิพนธ์ฉบับนี้ได้รับทุนสนับสนุนการวิจัยจากงบประมาณเงินรายได้ (เงินอุดหนุนจากรัฐบาล) ประจำปีงบประมาณ พ.ศ. 2560 (ตามโครงการ Innovation Hubs เพื่อสร้างเศรษฐกิจฐานนวัตกรรมของประเทศตามนโยบายไทยแลนด์ 4.0) มหาวิทยาลัยบูรพา (การพัฒนา Smart Living สำหรับอุตสาหกรรมบริการสุขภาพอัจฉริยะ-Smart Living for Smart City)

ขอขอบพระคุณ บริษัท เบสแล็บ จำกัด (BAESLab Co., Ltd.) ที่ให้ความช่วยเหลือในการพัฒนาอุปกรณ์ไอโอทีส่วนบุคคลและการทำงานของระบบ

ขอขอบพระคุณผู้ทรงคุณวุฒิทุกท่านที่ได้กรุณาตรวจสอบความสมบูรณ์และให้คำแนะนำแก้ไขเครื่องมือในการวิจัย รวมทั้งผู้เชี่ยวชาญทุกท่าน

ท้ายที่สุดผู้วิจัยขอกราบขอบพระคุณ บิดา มารดา พี่ น้อง และเพื่อน ๆ ที่ได้ให้ความช่วยเหลือและกำลังใจ ตลอดจนผู้ที่เกี่ยวข้องทุกท่านที่มิได้กล่าวถึงในที่นี้

คุณค่าและประโยชน์ของวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบเป็นกตัญญูกตเวทิตาแด่บิดา มารดา ครู อาจารย์ และผู้มีพระคุณทุกท่าน ที่ได้อบรมสั่งสอนและให้กำลังใจแก่ผู้วิจัยเสมอมา

นิพนธ์ สมหมาย

56910413: สาขาวิชา: วิศวกรรมไฟฟ้า; วศ.ม. (วิศวกรรมไฟฟ้า)
คำสำคัญ: ความปลอดภัยในไอโอที/ กระบวนการระบุตัวตน/ การเข้ารหัสข้อมูล/ ไอซีเข้ารหัส

นิพนธ์ สมหมาย: การระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพส่วนบุคคลสำหรับอุปกรณ์สวมใส่โดยใช้ไอซีเข้ารหัส (AUTHENTICATION AND ENCRYPTION OF PERSONAL HEALTH INFORMATION FOR WEARABLE DEVICE USING CRYPTOGRAPHICAL INTEGRATED CIRCUIT) คณะกรรมการควบคุมวิทยานิพนธ์: วิรุฬห์ ศรีบริรักษ์, วศ.ม. 80 หน้า. ปี พ.ศ. 2561.

สืบเนื่องจากการเติบโตของการใช้งานอุปกรณ์ไอโอทีเป็นผลทำให้เกิดจำนวนของผู้ใช้ในงานด้านสุขภาพเพิ่มมากขึ้น อุปกรณ์สวมใส่ที่มีฟังก์ชันการทำงานได้แก่ การตรวจจับท่าทางของผู้ใช้งาน การตรวจจับจำนวนก้าเดิน การตรวจจับอัตราการเต้นของหัวใจ การตรวจจับระดับออกซิเจนในเลือดและการตรวจจับอุณหภูมิร่างกาย ซึ่งอุปกรณ์เหล่านี้ถูกนำมาใช้ในผู้คนที่หลากหลาย แน่นอนว่าอุปกรณ์ไอโอทีเหล่านี้ต้องส่งข้อมูลส่งต่อไปยังศูนย์กลางการเก็บข้อมูลเพื่อเก็บบันทึกข้อมูล ซึ่งช่องทางในการส่งข้อมูลระหว่างอุปกรณ์ไอโอทีไปยังศูนย์กลางการเก็บข้อมูลยังขาดความปลอดภัยในการส่งข้อมูลอยู่นั่น จึงเป็นความเสี่ยงที่อาจจะทำให้ผู้ไม่หวังดีแอบขโมยข้อมูลบางอย่างไปจากผู้ใช้งาน อันก่อให้เกิดความเสียหายต่อผู้ใช้งาน

ผู้ทำวิจัยจึงตระหนักถึงความสำคัญในเรื่องความปลอดภัยที่อยู่ในอุปกรณ์ไอโอทีส่วนบุคคล จึงนำเสนอการใช้ตัวไอซีเข้ารหัสซึ่งออกแบบมาให้รองรับอุปกรณ์สวมใส่ ให้สามารถรองรับกระบวนการระบุตัวตนและการเข้ารหัสแลกกุญแจรหัสลับข้อมูลระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับตัวรับข้อมูลเกตเวย์ และมีการเข้ารหัส AES ในการเข้ารหัส สุดท้ายแล้วมีการเพิ่มเทคนิคการเข้ารูปแบบ ก่อนที่จะทำการเข้ารหัสข้อมูล AES โดยจะใช้เทคนิค Huffman Encoding ซึ่งจะทำให้ระบบการส่งข้อมูลระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์มีความปลอดภัยมากขึ้น

จากการทดสอบกระบวนการระบุตัวตนและกระบวนการแลกรหัสลับ สามารถสรุปเวลาของกระบวนการทำงานได้ 1,416.482 มิลิวินาที ในส่วนของกระบวนการเข้ารหัสลับข้อมูลสามารถสรุปเวลาของกระบวนการได้ 2.0699 มิลิวินาที ซึ่งไม่กระทบต่อกระบวนการติดต่อสื่อสารของระบบ และสุดท้ายในของการเพิ่มความปลอดภัย เมื่อศัตรูใช้วิธีการ Brute force หารหัสลับ ศัตรูจะต้องใช้ทรัพยากรในการคำนวณถึง 1,252.87 เท่า ถ้าระบบใช้เทคนิค Huffman coding เมื่อเทียบกับการที่ระบบไม่ได้ใช้เทคนิค Huffman coding

56910413: MAJOR: ELECTRICAL ENGINEERING; M.Eng. (ELECTRICAL ENGINEERING)
KEYWORD: SECURITY OF IoT/ AUTHENTICATION/ ENCRYPTION/ CRYPTO ENGINE

NIPON SOMMAI: AUTHENTICATION AND ENCRYPTION OF PERSONAL HEALTH INFORMATION FOR WEARABLE DEVICE USING CRYPTOGRAPHICAL INTEGRATED CIRCUIT. ADVISORY COMMITTEE: WIROON SRIBORRIRUX, M.Eng. 80 P. 2018.

Due to the growing usage of IoT devices, the number of users in health care has increased. Wearable accessories include motion detection, step count detection, heart rate detection, oxygen saturation in blood and body temperature measurements. With many users, these devices have to forward recorded personal data to the data center via data channel, which could pose a threat regarding privacy invasion. Eavesdropper may steal user information, causing severe damage to users.

In this thesis, we are aware of the importance to significant security concerns of personal IoT devices, we therefore propose to include Cryptographical Integrated Circuit in the IoT wearable device for personal health. It uses authentication between devices and the gateway such that a common session key is derived for a particular device-gateway pair. The session key will later be used for encapsulating AES secret key for health data encryption. At the end, we also add the Huffman Coding process to improve the security of AES encrypted data.

Experimental results show that the process of authentication and encryption key agreement takes only 1,416.482 ms, whereas AES encryption takes only 2.0699 ms. These amounts of time do not have considerable effect on the communication process of the system. In addition, with Huffman Coding of health information, the enemy's brute force in search of AES key will consume 1,252.87 times more computational resource than the normal process without Huffman Coding.

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

สืบเนื่องจากการเติบโตของการใช้งานอุปกรณ์ไอโอที (IoT) เป็นผลทำให้เกิดจำนวนของผู้ใช้เพิ่มมากขึ้นอย่างมากมายด้วยเช่นกัน ไม่ว่าจะเป็นการใช้ในเมืองใหญ่ (Smart City) การใช้งานในบ้านที่อยู่อาศัย (Smart Living) และที่ใกล้ตัวเรามากที่สุด คือ การใช้งานด้านสุขภาพ (Smart Health care) ที่มีความจำเป็นอย่างมาก เพราะเป็นสิ่งที่เกี่ยวข้องกับเรื่องสุขภาพ อีกทั้งในยุคปัจจุบันมีแนวโน้มการดูแลสุขภาพมากขึ้น เทคโนโลยีไอโอทีและอุปกรณ์ไอโอทีส่วนบุคคล จึงเข้ามามีบทบาทมากขึ้น ตัวอย่างที่เห็นได้ชัดในปัจจุบัน ก็คือ ตัวอุปกรณ์สวมใส่ (Wearable devices) ที่มีขายอยู่ในท้องตลาด มีฟังก์ชันการทำงานที่มากมาย ได้แก่ การตรวจจับท่าทางของผู้ใช้งาน การตรวจจับจำนวนก้าวเดิน การตรวจจับเวลาในการทำกิจกรรมบางอย่างในชีวิตประจำวัน การตรวจจับอัตราการเต้นของหัวใจ การตรวจจับระดับออกซิเจนในเลือดและการตรวจจับอุณหภูมิร่างกาย ซึ่งอุปกรณ์เหล่านี้ถูกนำมาใช้ในผู้คนหลายระดับ ที่มีอายุแตกต่างกัน และรวมไปถึงผู้ใช้ที่แข็งแรงชอบออกกำลังกายเป็นประจำ ไปจนถึงผู้ป่วยที่แทบจะไม่มีแรงช่วยเหลือตัวเองได้ เหล่านี้มักจะมีอุปกรณ์ไอโอทีติดตัวแทบทั้งนั้น แน่นอนว่าอุปกรณ์ไอโอทีเหล่านี้นอกจากจะเก็บค่าต่าง ๆ ด้วยตัวเซนเซอร์ของมันเองแล้ว มันยังต้องส่งข้อมูลส่งต่อไปยังศูนย์กลางการเก็บข้อมูล เพื่อเป็นการเก็บบันทึกที่สามารถดูประวัติหรือการคำนวณอะไรบางอย่างที่มากกว่า หน่วยความจำหรือหน่วยประมวลผลของอุปกรณ์ไอโอทีจะทำไหวในขณะนั้น ซึ่งช่องทางในการส่งข้อมูลระหว่างอุปกรณ์ไอโอทีไปยังศูนย์กลางการเก็บข้อมูลยังขาดความปลอดภัยในการส่งข้อมูลอยู่นั่น จึงเป็นความเสี่ยงที่อาจจะทำให้ผู้ไม่หวังดีแอบขโมยข้อมูลบางอย่างไปจากผู้ใช้งาน อันก่อทำให้เกิดความเสียหายต่อผู้ใช้งานหรือถ้ามีจำนวนมาก ๆ ก็อาจจะส่งผลต่อระบบขนาดใหญ่ขององค์กรได้ โดยความปลอดภัยที่ยังขาดอยู่ในปัจจุบัน ได้แก่ กระบวนการระบุตัวตนเพื่อเป็นการการันตีตัวตนของอุปกรณ์ระหว่างตัวรับกับตัวส่งกันเอง และการเข้ารหัสข้อมูลความปลอดภัยระหว่างข้อมูลของอุปกรณ์ตัวรับกับตัวส่ง ซึ่งจะทำให้ผู้ใช้งานอุปกรณ์ไอโอทีมีความปลอดภัยด้านข้อมูลและมีความอุ่นใจ ในการใช้งานอุปกรณ์ไอโอทีส่วนบุคคลมากยิ่งขึ้น

ผู้ทำวิจัยจึงตระหนักถึงความสำคัญในเรื่องความปลอดภัยที่อยู่ในอุปกรณ์ไอโอทีส่วนบุคคล จึงนำเสนอตัวไอซีเข้ารหัส (Crypto engine) ซึ่งออกแบบมาให้รองรับอุปกรณ์สวมใส่

และอุปกรณ์ไอโอทีส่วนบุคคลให้สามารถทำกระบวนการระบุตัวตนและการเข้ารหัสแลกกุญแจรหัสลับข้อมูลระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับตัวรับข้อมูลเกตเวย์ (Gateway) โดยไอซีนี้จะใช้เทคนิค Elliptic Curve Cryptography (ECC) อยู่บนพื้นฐานฮาร์ดแวร์ โดยจะช่วยให้การคำนวณรวดเร็วมากขึ้นกว่าการใช้ซอฟแวร์ นอกจากนั้นหลังจากกระบวนการระบุตัวตน เพื่อการันตีว่าเป็นตัวจริงเสร็จสิ้นจะมีการเข้ารหัส Advance Encryption Standard (AES) แบบ ECB ขนาด 128 บิตในการเข้ารหัส โดยจะใช้กุญแจที่ได้จากกระบวนการเข้ารหัสแลกกุญแจรหัสลับข้อมูล มาใช้ในการเป็นกุญแจรหัสลับของ AES แต่กระนั้นการเข้าข้อมูลรหัสลับยังอาจจะไม่ปลอดภัยอันเนื่องมาจากการที่ข้อมูลของอุปกรณ์ไอโอทีมีการเปลี่ยนแปลงน้อยจึงอาจจะทำให้ให้ถูกเดารหัสลับได้ง่าย ตัวอย่างเช่น อ่านค่าการเต้นของหัวใจได้ค่าเดิม ๆ ซ้ำ ๆ ของผู้ใช้ ซึ่งทำให้ค่าเซนเซอร์ที่เข้ารหัสถูกดักขโมย จนสามารถเดากลับจนเจอกุญแจรหัสลับได้ จึงต้องเพิ่มเทคนิคการเข้ารูปแบบข้อมูล (Data coding) ก่อนที่จะทำการเข้ารหัสข้อมูล AES โดยจะใช้เทคนิค Huffman coding ซึ่งจะทำให้ข้อมูลที่ออกไปจากอุปกรณ์ไอโอทีส่วนบุคคลไม่ซ้ำกัน แม้ว่าข้อมูลนั้นจะมีค่าที่ซ้ำกันบ่อย ๆ จึงทำให้ยากต่อการเดาหากุญแจรหัสลับ ซึ่งจะทำให้ระบบการส่งข้อมูลระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์มีความปลอดภัยมากขึ้น เพื่อให้ผู้ใช้งานมั่นใจได้ว่าอุปกรณ์ไอโอทีส่วนบุคคลที่สวมใส่อยู่นั้นมีความปลอดภัยในการรักษาความลับข้อมูลของตนเอง

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการทำงานการระบุตัวตน (Authentication) และการเข้ารหัสลับ (Encryption) ข้อมูลสุขภาพโดยการใช้ไอซีเข้ารหัสระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์
2. เพื่อพัฒนากระบวนการสื่อสารเพื่อการระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพโดยใช้ไอซีเข้ารหัสระหว่างอุปกรณ์สวมใส่ส่วนบุคคลกับเกตเวย์
3. เพื่อวิเคราะห์ประสิทธิภาพของการทำงานกระบวนการเข้ารหัสข้อมูลโดยใช้ไอซีเข้ารหัสเข้ารหัสระหว่างอุปกรณ์สวมใส่ส่วนบุคคลกับเกตเวย์

ขอบเขตของการวิจัย

1. ศึกษากระบวนการระบุตัวตน (Authentication) โดยใช้ Elliptic Curve Digital Signature Algorithm (ECDSA) ระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์
2. ศึกษาการเข้ารหัสแลกกุญแจรหัสสลับข้อมูล (Encryption key agreement) โดยใช้ Elliptic Curve Diffie-Hellman Algorithm (ECDH) ระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์
3. ศึกษาการเข้ารหัสลับ AES ระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์

4. วิเคราะห์ประสิทธิภาพของการทำงานการระบุตัวตน (Authentication) ระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์

5. วิเคราะห์ความปลอดภัยของการทำงานการเข้ารหัสลับของข้อมูลระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์

6. วิเคราะห์ความปลอดภัยโดยรวมเมื่อมีการเพิ่มกระบวนความปลอดภัยเข้าไป

ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. ได้สร้างการการันตีของการระบุตัวตนระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์ได้

2. ได้สร้างการป้องกันการปลอมแปลงระหว่างอุปกรณ์ไอโอทีส่วนบุคคลที่จะเชื่อมต่อเข้าใช้งานระบบกับเกตเวย์

3. ได้สร้างความเป็นส่วนตัวให้กับผู้ใช้งาน เพราะข้อมูลที่ส่งออกไปจากอุปกรณ์ไอโอทีส่วนบุคคลเป็นความลับ

4. สร้างความมั่นใจในด้านความปลอดภัยของข้อมูลให้แก่ผู้ใช้งานอุปกรณ์ไอโอทีส่วนบุคคล

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

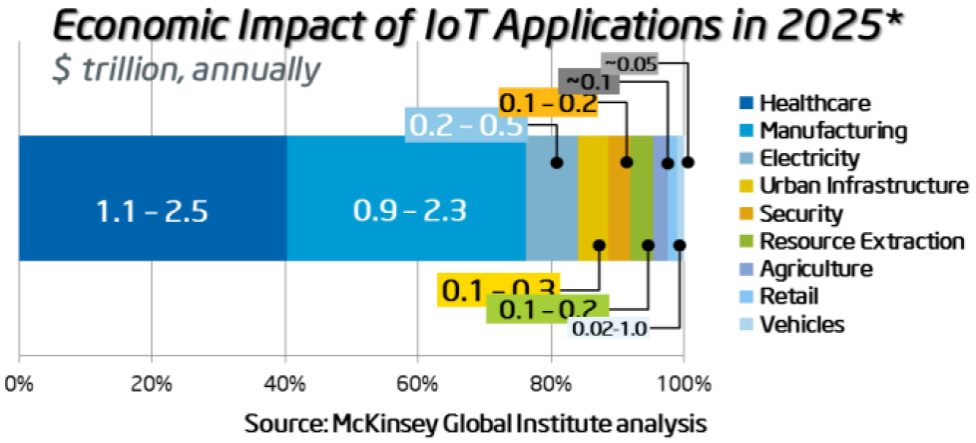
การระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพส่วนบุคคลในอุปกรณ์สวมใส่โดยใช้ไอซีเข้ารหัสในระบบไอโอที ผู้วิจัยได้ทำการศึกษา ค้นคว้า เอกสารและงานวิจัยที่เกี่ยวข้องต่าง ๆ สรุปสาระสำคัญดังนี้

1. แนวโน้มการขยายตัวของการใช้อุปกรณ์สวมใส่ไอโอที
2. องค์ประกอบของความปลอดภัยในอุปกรณ์สวมใส่ไอโอที
3. เทคโนโลยีการเข้ารหัส AES
4. เทคโนโลยีการเข้ารหัส ECC
5. เทคโนโลยีการระบุตัวตนด้วยกระบวนการ ECDSA
6. เทคโนโลยีการแลกเปลี่ยนกุญแจ ECDH
7. ใบรับรองอิเล็กทรอนิกส์ X.509
8. เทคโนโลยี Huffman coding
9. เทคโนโลยี Bluetooth low energy (BLE)

แนวโน้มการขยายตัวของการใช้อุปกรณ์สวมใส่ไอโอที

เทคโนโลยีอินเตอร์เน็ตในทุกสิ่ง Internet of Things (IoT) คือ การเชื่อมต่ออุปกรณ์ต่าง ๆ เข้ากับระบบอินเตอร์เน็ต ซึ่งทำให้ทุกสิ่งทุกอย่างสามารถเชื่อมต่อสื่อสารกันได้ เป็นประโยชน์ต่อมนุษย์ในการอ่านค่าข้อมูลของการทำงานและการสั่งงานควบคุมได้ง่ายขึ้น ทำให้คุณภาพของมนุษย์สะดวกสบายมากขึ้น ในงานวิจัยของ (Mirjana, Vladimir & Branko, 2015) ได้กล่าวคุณลักษณะของไอโอทีมีดังนี้ การเชื่อมต่อกับทุกสิ่ง การยืนยันตัวตนกับทุกสิ่ง และการปฏิสัมพันธ์กับทุกสิ่ง เฉกเช่น การทำงานของเซนเซอร์โหนด (Sensor node) ที่รวมกันหลาย ๆ ตัวจนกลายเป็นเครือข่ายเซนเซอร์ WSN (Wireless sensor network) ที่ต้องมีการทำงานที่แม่นยำและสามารถส่งข้อมูลมาแสดงยังหน้าเซนเซอร์เว็บ (Sensor web) ได้ ในการประยุกต์ใช้งานไอโอทีมีหลายด้านและหลายระดับ เช่น รอบตัวภายในบ้าน งานด้านการศึกษา งานด้านอุตสาหกรรม งานด้านการแพทย์ งานด้านการทหาร งานวิทยาศาสตร์ ฯลฯ โดยเฉพาะงานด้านสุขภาพ (Healthcare) ที่มีแนวโน้มของการขยายตัวมากขึ้น สถาบันระดับโลกชื่อ McKinsey Global Institute ได้ให้พยากรณ์การเศรษฐกิจของไอโอทีทางด้านสุขภาพว่าจะมีอัตราขยายตัวถึง 40% ในปี ค.ศ. 2025 คิดเป็นมูลค่าถึง 2.5

ล้านล้านเหรียญสหรัฐ นั่นหมายความว่า จะมีการใช้อุปกรณ์ไอโอทีด้านสุขภาพเพิ่มมากขึ้น ตัวอย่างการใช้งาน เช่น การใช้งานเพื่อทางการแพทย์ การใช้งานเพื่อดูแลผู้สูงอายุ การใช้งานเพื่อผู้ป่วยติดเตียง การใช้งานเพื่อดูแลสุขภาพ การใช้งานในด้านกีฬา ฯลฯ



ภาพที่ 2-1 การพยากรณ์การเติบโตทางเศรษฐกิจของไอโอทีในปี 2025

เมื่อกล่าวถึงอุปกรณ์สวมใส่ไอโอที (Wearable device IoT) โดยเฉพาะในงานด้านสุขภาพ มีการทำเป็นอุปกรณ์สวมใส่ให้กับผู้สวมใส่ ซึ่งมีความสามารถในการเก็บข้อมูลพื้นฐานที่เกี่ยวข้องกับร่างกายของผู้ใช้งานเป็นเวลา 24 × 7 หรือการทำงานตลอดเวลา อาทิเช่น อัตราการเต้นของหัวใจ อุณหภูมิของร่างกาย อัตราก้าวเดิน ลักษณะกิจวัตรประจำวัน ฯลฯ ข้อมูลเหล่านี้จะถูกส่งต่อไปยังเซิร์ฟเวอร์ เพื่อให้ส่งข้อมูลแสดงไปยังส่วนต่าง ๆ ได้แก่ หน้าเว็บ (Web application) แอพพลิเคชั่นบนโทรศัพท์ (Smartphone application) และข้อความ SMS เพื่อให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องได้รับทราบพารามิเตอร์ที่ผิดปกติของผู้ใช้งาน เพื่อเป็นการระวัง หรือช่วยเหลือเมื่อเกิดเหตุการณ์ที่มีผลต่อสุขภาพของผู้ใช้งาน หรือการดูประวัติสุขภาพเพื่อประเมินระดับสุขภาพของผู้ใช้งาน เนื่องจากการขยายตัวของจำนวนอุปกรณ์ที่มากขึ้นจึงได้มีการศึกษาและคาดการณ์การเติบโตของตลาดอุปกรณ์สวมใส่ไอโอที (Suranga Seneviratne, Yining Hu & Tham Nguyen, 2017) ในปี ค.ศ. 2016 มีการเพิ่มขึ้นของอุปกรณ์สวมใส่ไอโอที 44.4% เมื่อเทียบกับปี ค.ศ. 2015 ซึ่งในขณะนั้นจะมีอุปกรณ์ถึง 80 ล้านชิ้น และจะเพิ่มขึ้นอีกเป็น 200 ล้านชิ้นในปี ค.ศ. 2019 และมีมูลค่าของตลาด 57,635 ล้านเหรียญสหรัฐ นับเป็นเวลา 3 ปีตั้งแต่ปี ค.ศ. 2016 มีมูลค่าเพิ่มขึ้นเป็น 19,633 ล้านเหรียญสหรัฐ

องค์ประกอบของความปลอดภัยในอุปกรณ์สวมใส่ไอโอที

ความต้องการทางด้านความปลอดภัยของการสื่อสารไอโอที (IoT communication) มีด้วยกัน 3 ด้านดังนี้

1. การรักษาความลับ

การรักษาความลับ (Confidentiality) หมายถึง การอนุญาตให้ผู้ที่สามารถเข้าถึงข้อมูลได้เท่านั้นที่สามารถจะเข้าถึงข้อมูล เพราะถ้าข้อมูลถูกเปิดเผยอาจจะทำให้เจ้าของข้อมูลเกิดอันตรายหรือหน่วยงานที่เป็นเจ้าของข้อมูลเกิดความเสียหายได้ การรักษาความลับของการสื่อสารไอโอทีในอุปกรณ์สวมใส่ ก็ต้องป้องกันข้อมูลที่จะส่งจากสายรัดข้อมือไปยังเกตเวย์ผ่านอากาศให้เป็นความลับ เพราะข้อมูลบางอย่างสามารถก่อให้เกิดความเสียหายให้กับคนใช้ได้ ยกตัวอย่าง ปัญหาการรักษาความลับ เช่น ข้อมูลเซนเซอร์วัดความเร่งแกน xyz ที่สามารถวิเคราะห์กลับหาการกดตัวเลขตู้กดเงินได้ การตรวจจับพฤติกรรมอยู่นิ่งของเจ้าของบ้านจากข้อมูลสายรัดข้อมือ ทำให้โจรได้จังหวะเข้ามาขโมยของในขณะเจ้าของบ้านหลับ ดังนั้นจึงต้องมีกระบวนรักษาความลับด้วยการเข้ารหัสข้อมูลเพื่อเป็นการรักษาความลับ

2. ความน่าเชื่อถือของข้อมูล

ความน่าเชื่อถือของข้อมูล (Integrity) หมายถึง ความน่าเชื่อถือได้ของข้อมูล การป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงจากสภาพเดิม หรือการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเปลี่ยนแปลงข้อมูลได้ ยกตัวอย่างปัญหาความน่าเชื่อถือของการสื่อสารไอโอทีในอุปกรณ์สวมใส่ในกรณีที่อลิสต้องใช้อุปกรณ์ในการอ่านค่าบางอย่างที่เกี่ยวข้องกับสุขภาพ แต่ปรากฏว่ามีผู้ไม่หวังดีต้องการแกล้งอลิส โดยการไปดักขโมยข้อมูลนั้นกลางอากาศแล้วเปลี่ยนแปลงค่านั้นให้เกินจริงแล้วส่งไปยังเกตเวย์ เมื่อข้อมูลนั้นขึ้นจอแสดงผลของระบบก็อาจจะทำให้อลิสเกิดอาการตกใจได้ เพราะข้อมูลสุขภาพบางอย่างมีผลต่อสุขภาพจิตใจของผู้ใช้งาน ดังนั้นจึงต้องมีกระบวนการรักษาความน่าเชื่อถือของข้อมูลโดยระบบจะตรวจสอบจากค่าแฮชของข้อมูลว่าถูกต้องหรือไม่ก่อนนำข้อมูลไปแสดงผล เพื่อให้ผู้ใช้งานอลิสเกิดความมั่นใจได้ว่าข้อมูลนั้นคือข้อมูลของจริง

3. การพิสูจน์ตัวจริง

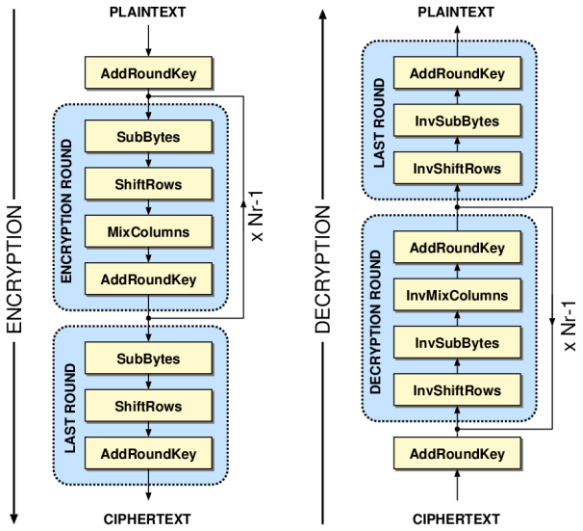
การพิสูจน์ตัวจริง (Authentication) หมายถึง การพิสูจน์ตัวจริงหรือระบุตัวตนว่าบุคคลที่ส่งข้อมูลมานั้น เป็นบุคคลผู้นั้นจริง ๆ ไม่ใช่ผู้อื่นที่ปลอมตัวมา ยกตัวอย่าง ปัญหาของการพิสูจน์ตัวจริงในอุปกรณ์สวมใส่ เช่น อุปกรณ์สวมใส่ของผู้สวมใส่ คือ อลิสมีคุณสมบัติในการกดแจ้งเตือนขอความช่วยเหลือ เมื่ออลิสกดขอความช่วยเหลือจะมีหน่วยฉุกเฉินเข้ามาช่วยเหลือทันที แต่ถ้ามีบ็อบปลอมตัวมาเป็นอลิส เมื่อบ็อบกดขอความช่วยเหลือ หน่วยฉุกเฉินก็จะเข้ามาเสียเที่ยวกลายเป็นว่าเสียเวลาและตัดโอกาสในการเข้าไปช่วยเหลือผู้อื่นที่ประสบเหตุจริง ดังนั้นจึงต้องมี

กระบวนการการพิสูจน์ตัวจริงของอลิสและบ็อบกับเกตเวย์ ก่อนการใช้งานเพื่อเป็นการการันตีว่าใครเป็นตัวจริง จากนั้นเกตเวย์จะรับข้อมูลจากตัวจริงเท่านั้น ทำให้มีความมั่นใจได้ว่าอุปกรณ์ที่จะส่งข้อมูลเข้ามาในระบบมีเป็นตัวจริง

เทคโนโลยีการเข้ารหัส AES

ในปี ค.ศ. 2001 Standards and Technology (NIST) เป็นหน่วยงานราชการภายใต้การดูแลของกระทรวงพาณิชย์ ประเทศสหรัฐอเมริกา ได้มีการพัฒนามาตรฐานการเข้ารหัส (สัญฉกร วุฒิสิทธิกุลกิจ, ธงชัย โรจน์กังสดาล, วรากร ศรีเชวงทรัพย์, นพดล พรมภักษรและสุวิทย์ นาคพีระยุทธ, 2556) ได้มีการพัฒนาการเข้ารหัสลับข้อมูลขึ้นมาใหม่ มีชื่อเรียกว่า Advance encryption standard (AES) เป็นกระบวนการเข้ารหัสแบบ Symmetric มีกระบวนการแบบอัลกอริทึมซึ่งทำการเข้ารหัสข้อมูลโดยใช้และขนาดของกุญแจซึ่งมีด้วยกัน 3 แบบ ได้แก่ 128 192 และ 256 บิต ซึ่งเรียกอัลกอริทึมเหล่านี้ว่า AES-128, AES-192 และ AES-256 มาตรฐานใหม่นี้มีขีดความสามารถในการป้องกันและให้ความปลอดภัยแก่ข้อมูลได้อย่างมีประสิทธิภาพ

การเข้ารหัสแบบ AES มีความคล้ายคลึงกับมาตรฐาน DES ซึ่งมีการแบ่งกระบวนการการทำงานออกเป็น 2 ด้าน คือ ด้านข้อมูลต้นฉบับที่เข้ารหัสลับ (Plaintext) และด้านกุญแจที่ใช้ในการเข้ารหัส (Key) ในขั้นตอนการเข้ารหัสจะทำทีละ 128 บิต หรือที่เรียกว่า 1 บล็อก (Block cipher) ซึ่งตามมาตรฐานของ AES-128 จะมีการวนเข้ารหัสทั้งหมด 10 รอบ AES-192 จะมีการวนเข้ารหัสทั้งหมด 12 รอบ และ AES-256 จะมีการวนเข้ารหัสทั้งหมด 14 รอบ

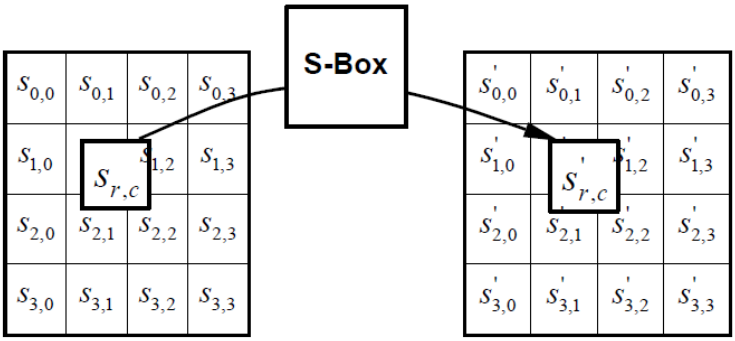


ภาพที่ 2-2 ขั้นตอนการเข้ารหัสและถอดรหัสด้วยอัลกอริทึม AES

อัลกอริทึม AES ดังภาพที่ 2-2 กำหนดไซเฟอร์ที่ใช้ในการเข้าและถอดรหัสลับ มีการทำงานเป็นรอบ ๆ โดยแต่ละรอบจะมีการแปลงข้อมูลระดับไบต์ทั้งหมด 4 ขั้นตอน ดังนี้

1. Sub bytes

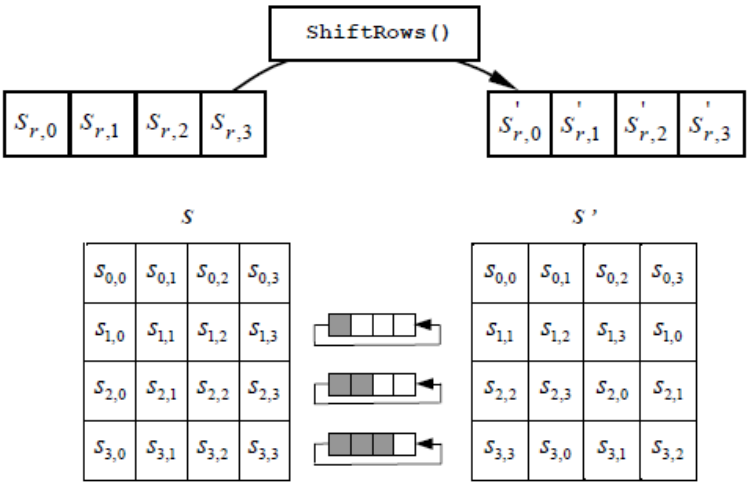
Sub bytes (จตุชัย แพงจันทร์, 2553) คือ ขั้นตอนแรกในแต่ละรอบของการเข้ารหัส คือ การทำซับไบต์ (Sub bytes) ซึ่งเป็นการแทนที่แต่ละไบต์ในสเตท ด้วยค่าใหม่ที่อ่านได้จากตาราง S-box (Substitution table) เนื่องจากขั้นตอนนี้เป็นการแทนค่าแบบหนึ่งต่อหนึ่งทำให้ขั้นตอนนี้เป็นฟังก์ชันแบบ Non-linear ทำให้ยากต่อการโจมตี โดยการเข้ารหัสแบบนี้จะควบคุมการแปลงค่าคุณสมบัติเฉพาะของการแปลงค่า S-box รวมทั้งข้อกำหนดของ S-box ดังภาพที่ 2-3



ภาพที่ 2-3 กระบวนการแทนที่ไบต์โดยใช้ตาราง

2. Shift rows

Shift rows (จตุชัย แพงจันทร์, 2553) คือ การแปลงค่าแบบเลื่อนตำแหน่งของไบต์ในแต่ละแถวของตารางสเตท ซึ่งจะเรียกว่า ShiftRows ซึ่งเป็นการเลื่อนตำแหน่งแบบวนกลับตามค่าออฟเซตที่กำหนด ในอัลกอริทึมนี้แถวแรกจะไม่ถูกเลื่อนตำแหน่งหรือคงไว้เหมือนเดิม แถวที่สองจะถูกเลื่อนตำแหน่งไปทางซ้ายหนึ่งตำแหน่ง เช่น ไบต์ที่ตำแหน่ง $s_{1,0}$ จะถูกเลื่อนไปแทนที่ตำแหน่งไบต์ $s_{1,3}$ และไบต์ในตำแหน่ง $s_{1,1}$ ก็จะถูกมาแทนที่ตำแหน่งของไบต์ $s_{1,0}$ ดังภาพที่ 2-4 ส่วนไบต์ที่ 2 และ 3 ก็จะเลื่อนตำแหน่งไปทางซ้ายเช่นกันแต่ตำแหน่งไปทางซ้ายเช่นกันแต่ตำแหน่งที่เลื่อนไปจะเป็น 2 และ 3 ตำแหน่งตามลำดับ ดังภาพที่ 2-4



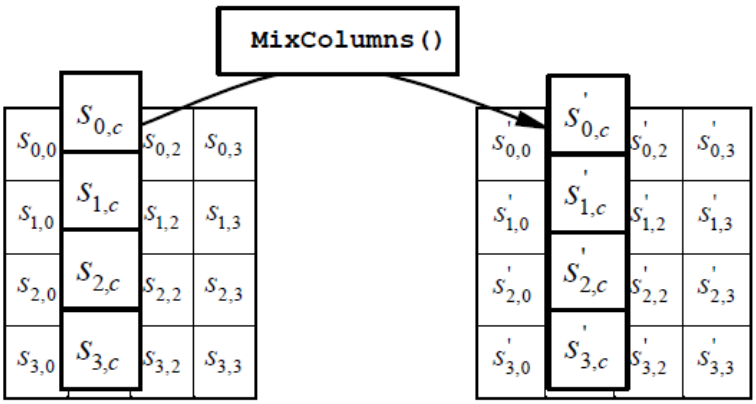
ภาพที่ 2-4 การเลื่อนไบต์ในแนวแถวของอาร์เลย์

3. Mix columns

Mix columns (จตุชัย แพงจันทร์, 2553) คือ ขั้นตอนการแปลงค่าในแต่ละคอลัมน์ในสเตทเทเบิลโดยใช้ฟังก์ชันทางคณิตศาสตร์ ซึ่งจะกระทำกับทั้งสี่ไบต์ในคอลัมน์เดียวกัน ฟังก์ชันที่ใช้ในการคำนวณเป็นสมการโพลิโนเมียลดังนี้

$$C(x) = a_0x^3 + a_1x^2 + a_2x + a_3 \quad (2\text{-}1)$$

โดยที่ $s'(x) = C(x) \otimes s(x)$ (2-2)



ภาพที่ 2-5 การผสมผสานข้อมูลภายในคอลัมน์แต่ละคอลัมน์ของอาร์เรย์สเตท

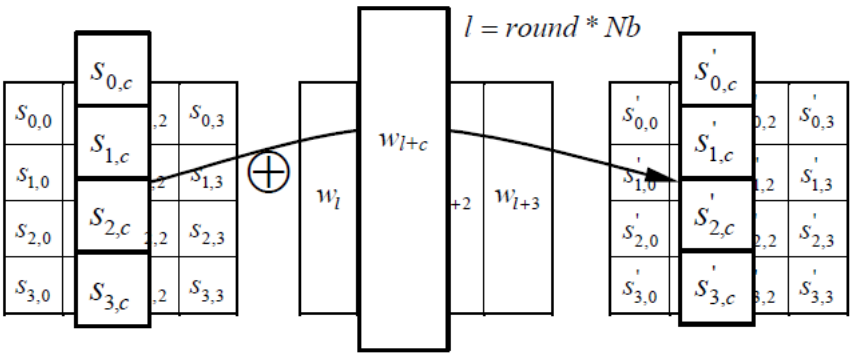
4. Add round key

Add round key (จตุชัย แพงจันทร์, 2553) คือ ขั้นตอนที่ใช้ซับคีย์กับข้อมูลในสเตทเทเบิล ในแต่ละรอบนั้นซับคีย์จะสร้างในขั้นตอน Key schedule โดยซับคีย์ที่ได้นั้นจะมีค่าเท่ากับสเตทเทเบิล ผลลัพธ์จะได้จากการทำ XOR ระหว่างค่าในสเตทเทเบิลกับค่าของซับคีย์ในตำแหน่งเดียวกัน

คีย์ของ AES อาจจะมีความยาว 128 192 หรือ 256 บิต ซึ่งคีย์นี้จะใช้เป็นค่าในการคำนวณหาซับคีย์ที่ใช้ในการเข้ารหัสข้อมูลในแต่ละรอบ ซึ่งเรียกว่า ราวด์คีย์ (Round key) คีย์นี้จะมีขนาดเท่ากับขนาดของบล็อกข้อมูลหรือสเตท เนื่องจากคีย์ที่ใช้ในแต่ละรอบนั้นมีค่าที่แตกต่างกับ ดังนั้น ต้องมีการหาคีย์ใหม่สำหรับใช้ในแต่ละรอบ

ในแต่ละราวด์คีย์จะประกอบไปด้วย $Nb\ word$ จาก Key Schedule โดยที่ $Nb\ word$ จะถูกเพิ่มเข้าไปในแต่ละคอลัมน์ของสเตทเทเบิลได้ดังนี้

$$[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c}] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] \oplus [W_{round*Nb+c}]\ for\ 0 \le c < Nb$$

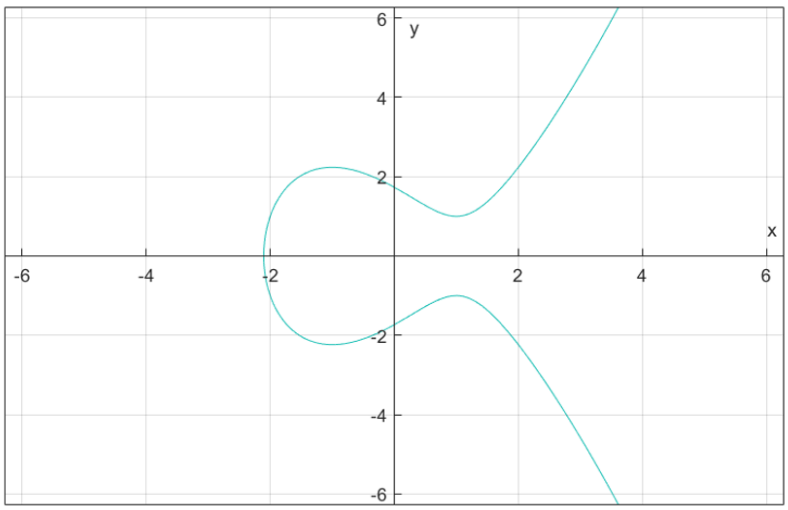


ภาพที่ 2-6 การบวกค่ากุญแจในแต่ละรอบกับอาเรย์สเตท

เทคโนโลยีการเข้ารหัส ECC

ในปี 1985 Neal Koblitz และ Victor S. Miller ได้เสนออัลกอริทึมแบบ Asymmetric มีชื่อเรียกว่า Elliptic curve cryptography (ECC) เป็นอัลกอริทึมนี้ได้พัฒนามาจากสมการของเส้นโค้งวงรีจากสมการ

$$y^2 = x^3 + ax + c \tag{2-3}$$



ภาพที่ 2-7 กราฟแสดงความสัมพันธ์ของสมการ Elliptic curve

ในบทความของ (ภูกิจ บุรีภักดี และปราโมทย์ กั่วเจริญ, 2555) ได้กล่าวไว้ว่า ECC มีข้อดีที่เหนือกว่า Rivest shamir adleman (RSA) คือ จะใช้ Key ที่สั้นกว่าแต่สามารถให้ความปลอดภัยเท่ากับ RSA ถ้าใช้ Key มีความยาวเท่ากัน ECC จะมีความปลอดภัยสูงกว่านั่นคือ หากต้องการโจมตีแบบ Brute-Force จะใช้เวลา มากกว่า RSA เนื่องจาก ECC ใช้ Key ที่มีขนาดเล็กกว่า RSA มาก และมีความสามารถในการคำนวณที่รวดเร็ว ใช้พลังงานต่ำ และใช้หน่วยความจำน้อย ดังนั้น ECC จึงเหมาะสำหรับการใช้งานในอุปกรณ์เคลื่อนที่ขนาดเล็ก

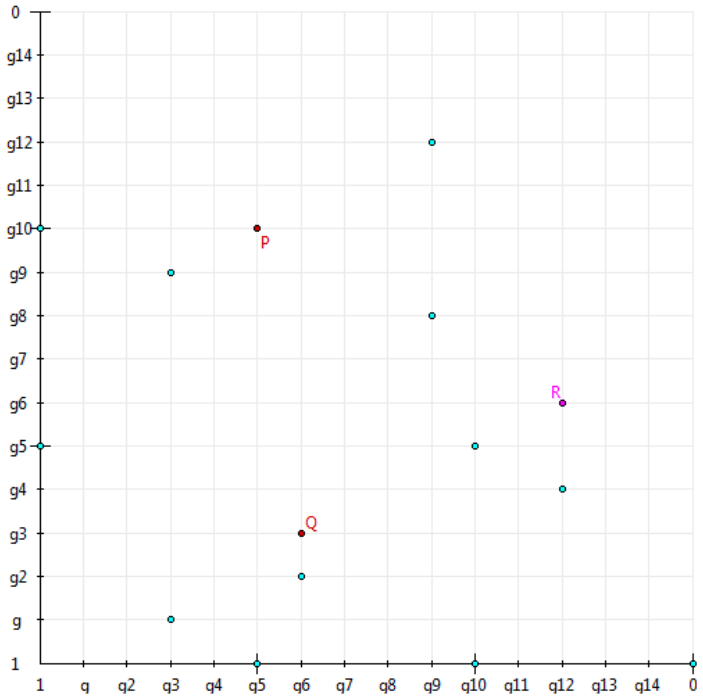
security level	RSA	ECC	
		$\mathbb{F}_p$	$\mathbb{F}_{2^m}$
	$\|n\|$ [bits]	$\|p\|$ [bits]	m [bits]
56	512	112	113
64	704	128	131
80	1024	160	163
96	1536	192	193
112	2048	224	233
128	3072	256	283
192	7680	384	409
256	15360	521	571

ภาพที่ 2-8 ขนาดของกุญแจรหัสลับกับความปลอดภัยระหว่าง RSA และ ECC

1. ลักษณะคุณสมบัติกราฟ Elliptic curve group

1.1 กราฟ Over GF(2^m) (Polynomials)

เป็นกราฟที่ได้จากสมการ $y^2 + xy = x^3 + ax + b$ โดยที่ $b \neq 0$ กำหนดให้ $P = (x_1, y_1)$, $Q = (x_2, y_2)$ คือ จุดบนกราฟของสมการ ดังภาพที่ 2-9



ภาพที่ 2-9 กราฟ Elliptic curve over GF(2^m)

จากภาพที่ 2-9 จะเห็นได้ว่า

P = (g5 | g10)

Q = (g6 | g3)

$R = P + Q$ = (g12 | g6)

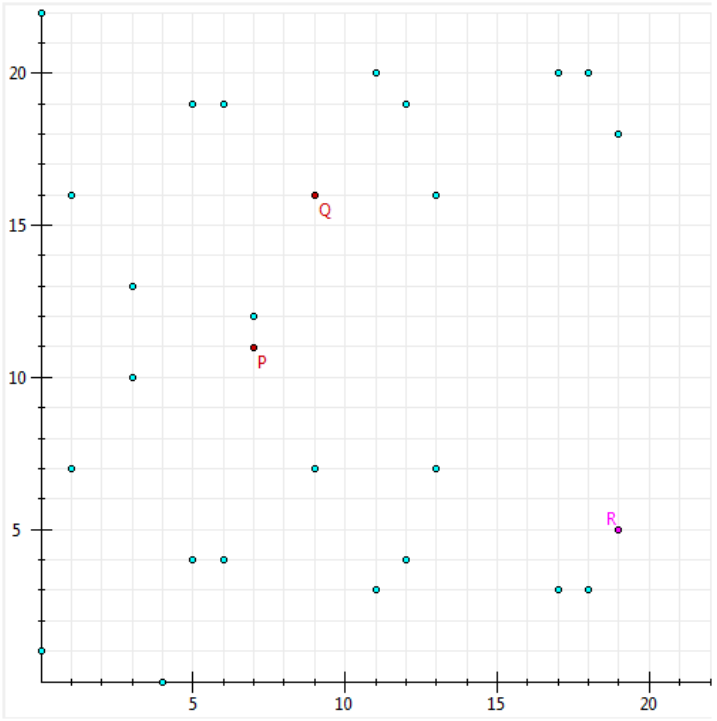
$y^2 + xy = x^3 + x^2 + 1$ (2-4)

$Polynom\ f = x^4 + x + 1; m = 4$

1.2 กราฟ Over GF(p) (Prime Number)

เป็นกราฟที่ได้จากสมการ $y^2\ mod\ p = (x^3 + x + 1) mod\ p$ (2-5)

โดยที่ $4a^2 + 27b^2 mod\ p \neq 0$ ดังภาพที่ 2-10



ภาพที่ 2-10 กราฟ Elliptic curve over GF(23)

จากภาพที่ 2-10 จะเห็นได้ว่า

P = (7 | 11)

Q = (9 | 16)

$R = P + Q$ = (19 | 5)

$$y^2 \ mod\ 23 = (x^3 + x + 1)\ mod\ 23$$

2. กฎการบวกระหว่างจุดบนกราฟ GF(p)

กำหนดให้ $P = (x_1, y_1)$ และ $Q = (x_2, y_2)$ คือ จุดบนกราฟของสมการ $P + Q = R = (x_3, y_3)$ โดยที่

$$x_3 = \lambda^2 - x_1 - x_2 , y_3 = \lambda (x_1 - x_3) - y_1 \quad (2\text{-}6)$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & if\ P \neq 0 \\ \frac{2x_1^2 + a}{2y_1} & if\ P = 0 \end{cases} \quad (2\text{-}7)$$

3. กฎการลบระหว่างจุดบนกราฟ GF(p)

กำหนดให้ $P = (x_1, y_1)$ และ $Q = (x_2, y_2)$ คือ จุดบนกราฟของสมการ $P + Q = P + (-Q)$ โดยที่

$$-Q = (x_2 , y_3\ mod\ p) \quad (2\text{-}8)$$

4. กฎการคูณค่าคงที่ กับจุดบนกราฟ GF(p)

กำหนดให้ $P = (x_1, y_1)$ และ $Q = (x_2, y_2)$ คือ จุดบนกราฟของสมการกราฟ $P = Q$ จะได้

$$P + P = 2P = R = (x_3, y_3) \quad (2\text{-}9)$$

เมื่อ k คือจำนวนเต็มบวกใด ๆ จะได้

$$Q = kP = \underbrace{P + P + \cdots + P}_{k} \quad (2\text{-}10)$$

เช่น ถ้า $k = 9$, $Q = kP = 9P = 2(2(2P)) + P$

5. การเข้ารหัสและถอดรหัส (ECC Encryption and Decryption)

5.1 การเข้ารหัส ผู้ส่ง คือ อลิสนำข้อความ P_m มาคำนวณหาข้อความที่เข้ารหัสลับ C_m แล้วส่งหาผู้รับ คือ บ็อบ ซึ่ง

$$C_m = \{kG, P_m + kP_B\} \quad (2\text{-}11)$$

โดยที่

G คือ จุดที่ได้จากการ Generate บน Elliptic Curve

k คือ ตัวเลขสุ่มจำนวนเต็มบวกที่เลือกโดย A

P_B คือ Public Key ของ B ซึ่ง $P_B = n_B \times G$

n_B คือ Private Key ของ B

5.2 การถอดรหัส ผู้รับ คือ บ็อบนำ Private key มาคูณค่าจุดแรก และนำผลลัพธ์ไปลบออกจากค่าจุดที่สอง ดังต่อไปนี้

$$P_m + kP_B - n_B(kG) = P_m + k(n_B)G - n_B(kG) = P_m \quad (2\text{-}12)$$

5.3 ตัวอย่างการเข้ารหัสและถอดรหัส GF(p)

$E_p(a,\ b) = E_{23}(1,1)$ จะได้ a = 1, b = 1, p = 23 เขียนเป็นสมการได้ดังนี้ $y^2\ mod\ 23 = (x^3 + x + 1)\ mod\ 23$ ซึ่งสามารถหาจุดบนกราฟ GF(23) ดังตารางที่ 2-1

ตารางที่ 2-1 จุด GF (23) บนกราฟทั้งหมด

จุด P	จุด Q	จุด R
(0,1)	(6,4)	(12, 19)
(0,22)	(6,19)	(13, 7)
(1,7)	(7,11)	(13, 16)
(1,16)	(7,12)	(17, 3)
(3,10)	(9,7)	(17, 20)
(3,13)	(9,16)	(18, 3)
(4,0)	(11,3)	(18, 20)
(5,4)	(11,20)	(19, 5)
(5,19)	(12,4)	(19, 18)

กำหนดให้ G = (1, 7)

P_m = (9,7) ซึ่งแทนด้วยอักษร “M”

อลิส:

Private Key $= n_A = 3$

Public Key $= n_A \times G = 3^*(1,7) = (18, 20)$

บ็อบ:

Private Key $= n_B = 5$

Public Key $= n_B \times G = 5^*(1,7) = (0, 1)$

เมื่ออลิสต้องการส่งข้อความให้บ็อบ

1. อลิสสุ่มตัวเลขได้ k = random = 9
2. คำนวณ $C_m = \{kG, P_m + kP_B\}$

$$C_m = \{9^*(1,7),\ (9,7) + 9^*(0,1)\}$$
$$= \{(9,16),\ (9,7) + (19,18)\}$$
$$= \{(9,16),\ (13,7)\}$$

อลิสส่ง $C_m = \{(9,16),\ (9,7) + (19,18)\}$

เมื่อบ็อบรับข้อความจากสมการ

$$P_m + kP_B - n_B(kG) = P_m + k(n_B)G - n_B(kG) = P_m$$
$$P_m = (13,7) - (9,16)$$
$$= (13,7) + (9,-18) \quad \text{(จากกฎการลบ)}$$
$$= (13,7) + (19,5) \quad : (5 = -18 \bmod 23)$$
$$= (9,7)$$

ดังนั้นบ็อบได้รับจุด (9,7) แทนด้วยอักษร “M”

เทคโนโลยีการระบุตัวตนด้วยกระบวนการ ECDSA

Elliptic curve digital signature algorithm (ECDSA) คือ กระบวนการระบุตัวตน (Authentication) โดยใช้อัลกอริทึม ECC กระบวนการระบุตัวตน ECDSA ถูกนำเสนอครั้งแรกเมื่อปี ค.ศ.1992 โดย Scott Vanstone ในการทำงานให้กับ NIST’s (National institute of standards and technology) เพื่อสร้างรูปแบบการตรวจสอบลายเซ็นดิจิทัล เหมือนการเทียบคู่ลายเซ็นที่เขียนด้วยมือว่าเหมือนกันหรือไม่ ลายเซ็นดิจิทัล (Digital signature) คือ ตัวเลขที่ขึ้นอยู่กับกุญแจรหัสลับที่รู้เฉพาะคนเซ็น (Signer) บนเนื้อหาที่ใช้ในการเซ็น โดยปกติแล้วลายเซ็น (Signature) จะถูกเข้าถึงได้โดยกุญแจรหัสลับส่วนตัวของคนเซ็น (Signer’s private key) ดังนั้นจึงไม่ใครสามารถที่จะปลอมลายเซ็นได้

1. การสร้างลายเซ็น (Signing)

เมื่ออลิสต้องการส่งลายเซ็นดิจิทัลไปให้บ็อบ ทั้งสองจะทำการเลือกชุดตัวเลข $\mathbb{F}_q$ บนเส้นโค้ง E แล้วกำหนดจุด G จำนวน n โดยอลิสกำหนดกุญแจรหัสลับไว้สำหรับเปรียบเทียบ คือ (d, Q) เมื่อ d คือ กุญแจรหัสลับส่วนตัว (Private key) ของอลิสและ Q คือ กุญแจสาธารณะ (Public key) ของอลิส จากนั้นอลิสทำการเซ็นข้อความ M โดยมีขั้นตอนดังนี้

1.1 เลือกจำนวนตัวเลขสุ่ม (Random number) k โดยที่ $k : 1 \leq k \leq n-1$

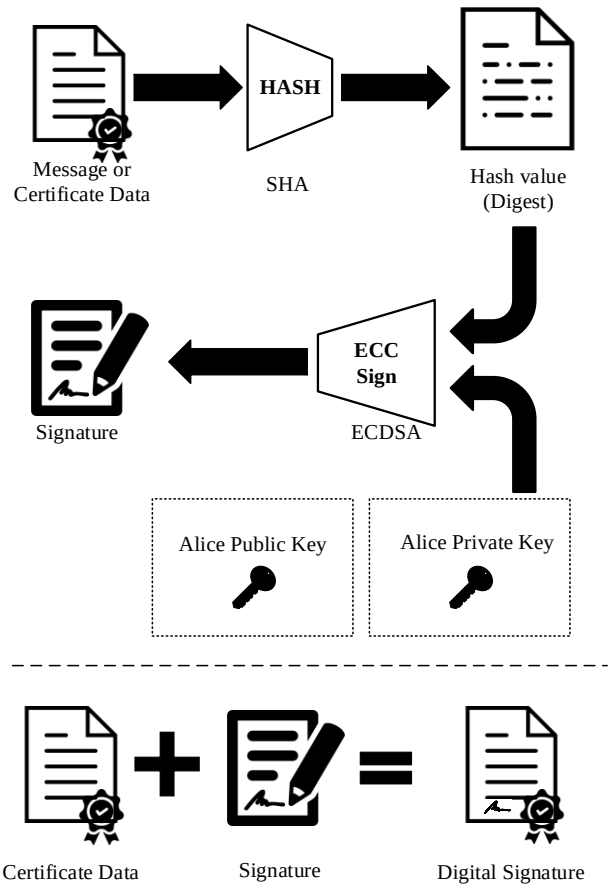
1.2 คำนวณ $kG = (x_1, y_1)$ และ $r = x_1 \bmod n$ ถ้า $r = 0$ ให้กลับไปทำข้อ 1.1 ใหม่

1.3 คำนวณ $k^{-1}\ mod\ n$

1.4 คำนวณจากค่าแฮช $e = SHA - 1(M)$

1.5 คำนวณ $s = k^{-1}\ (e + dr)\ mod\ n$ ถ้า $s = 0$ ให้กลับไปทำข้อ 1.1

1.6 อลิสได้ลายเซ็นดิจิทัล (Signature) สำหรับข้อความ M คือ (r, s)



ภาพที่ 2-11 ขั้นตอนการสร้างลายเซ็นดิจิทัล

2. การตรวจสอบลายเซ็น (Verification)

เมื่อบ็อบต้องการตรวจสอบลายเซ็นดิจิทัลของอลิส (r, s) บนข้อความ M บ็อบจะรับกุญแจสาธารณะ (Public key) ของอลิส โดยบ็อบจะมีขั้นตอนนการตรวจสอบลายเซ็นดิจิทัลของอลิสดังนี้

2.1 ตรวจสอบ r, s ที่เป็นจำนวนเต็มในช่วง $[1, n-1]$

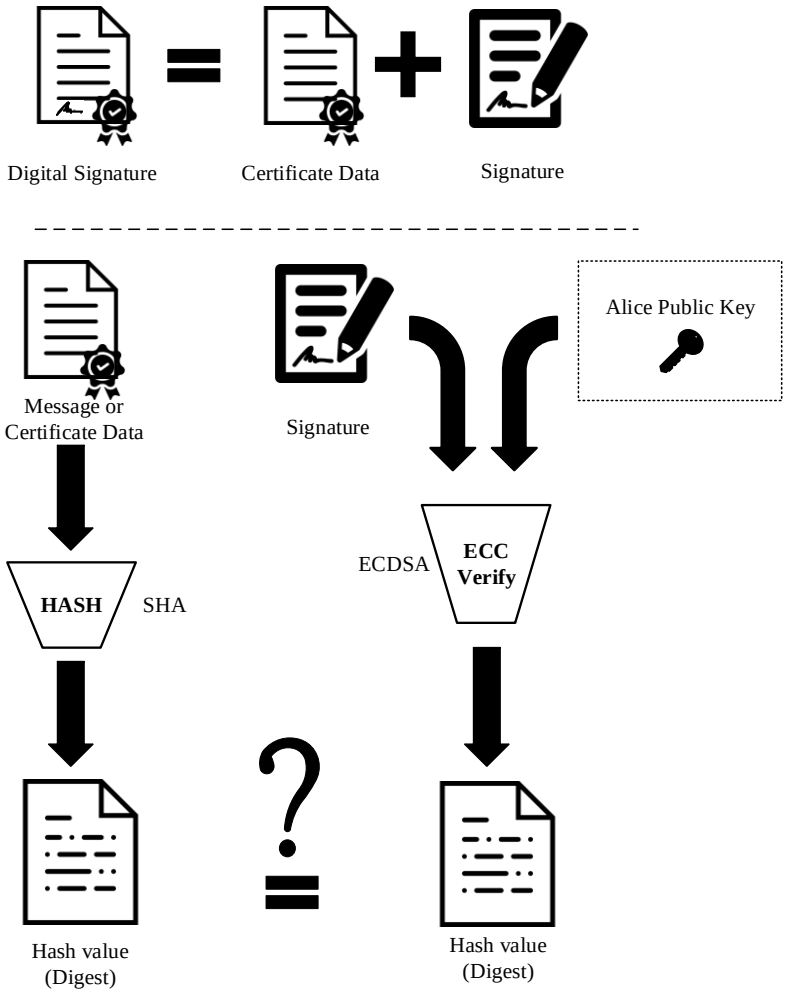
2.2 คำนวณจากค่าแฮช $e = SHA - 1(M)$

2.3 คำนวณ $w = s^{-1} mod\ n$

2.4 คำนวณ $u_1 = ew \ mod \ n$ และ $u_2 = rw \ mod \ n$

2.5 คำนวณ $X = u_1G + u_2Q$ ถ้า $X = 0$ ให้ปฏิเสธลายเซ็นดิจิทัลนั้น แต่ในกรณีอื่นให้คำนวณ $v = x_1 \ mod \ n$ เมื่อ $X = (x_1, y_1)$

2.6 ถ้าคำนวณ $v = r$ ถือว่าลายเซ็นดิจิทัลเป็นของจริง



ภาพที่ 2-12 ขั้นตอนการตรวจสอบลายเซ็นดิจิทัล

เทคโนโลยีการแลกเปลี่ยนกุญแจ ECDH

Elliptic-Curve Diffie-Hellman (ECDH) คือ อัลกอริทึมการตกลงกุญแจได้รับการพัฒนาขึ้นโดย Diffie และ Hellman ในปี ค.ศ. 1976 (สัญฉกร วุฒิสิทธิกุลกิจ และคณะ, 2556) ในบทความชื่อ “New directions in cryptography” อัลกอริทึมนี้มีวัตถุประสงค์เพื่อให้ผู้ใช้ 2 ราย สามารถแลกเปลี่ยนกุญแจลับระหว่างกันผ่านทางช่องสื่อสารที่ไม่ปลอดภัยได้โดยไม่ต้องมีข้อมูลลับใด ๆ มาก่อนเลย อัลกอริทึมมีการใช้งานพารามิเตอร์ในระบบจำนวน 2 ตัว ได้แก่ p และ g โดยค่าทั้งสองเป็นที่เปิดเผยต่อสาธารณะและผู้ใช้ทุกรายในระบบสามารถนำมาใช้งานได้ พารามิเตอร์ p เป็นจำนวนเฉพาะขนาดใหญ่ค่าหนึ่ง ส่วนพารามิเตอร์ g เป็นจำนวนเต็มที่มีค่าน้อยกว่า p และมีคุณสมบัติพิเศษคือสามารถให้กำเนิดตัวเลขทุกตัวตั้งแต่ 0 ถึง p -1 เมื่อนำไปคูณกับตัวเองซ้ำ ๆ ภายใต้มอดูโล (Modulo) p ดังนั้น จึงมักจะเรียกตัวเลขนี้ว่า ตัวกำเนิด (generator) และในทางคณิตศาสตร์จะกล่าวว่า g เป็นรากพริทีทิฟ (primitive root) ของ p

สมมติว่าบ็อบและอลิสจะทำการตกลงกุญแจลับระหว่างกันค่าหนึ่งโดยอาศัยวิธีการของ Diffie-Hellman ให้ดำเนินการดังนี้ ขั้นแรกให้อลิสสุ่มค่าตัวเลขจำนวนเต็ม a ขึ้นมาค่าหนึ่ง ซึ่งค่าดังกล่าวนี้อลิสจะเก็บไว้ส่วนตัวไม่เปิดเผย และบ็อบเองก็สุ่มตัวเลขจำนวนเต็ม b ขึ้นมาค่าหนึ่งด้วยเช่นกัน โดยเก็บไว้เป็นความลับส่วนตัวอลิสนำค่า a ไปผ่านการคำนวณกับพารามิเตอร์ของระบบคือ p และ g เพื่อให้ได้เป็นค่าที่จะนำไปเปิดเผยต่อสาธารณะโดยใช้สมการความสัมพันธ์ ดังนี้

$$A = g^a mod\ p \tag{2-13}$$

ในทำนองเดียวกันบ็อบก็คำนวณค่าที่ได้เปิดเผยต่อสาธารณะโดยการนำ b ไปคำนวณได้ดังนี้

$$B = g^b mod\ p \tag{2-14}$$

จากนั้นบ็อบและอลิสจะแลกเปลี่ยนตัวเลขที่ใช้คำนวณได้ระหว่างกัน ทางอลิสนำค่าที่ได้ไปคำนวณต่อดังนี้

$$K_{AB} = (B)^A mod\ p \tag{2-15}$$

และบ็อบจะนำค่าที่ได้รับไปคำนวณต่อดังนี้

$$K_{BA} = (A)^B mod\ p \tag{2-16}$$

เนื่องจากค่าทั้งสองคำนวณได้เป็นค่าเดียวกันกล่าวคือ

$$K = K_{AB} = (B)^A mod\ p = g^{AB}\ mod\ p = (A)^B mod\ p$$

ดังนั้นทั้งอลิสและบ็อบก็จะกำหนดให้ K เป็นกุญแจลับส่วนตัวกันได้

ตัวอย่างการใช้งานสมมติให้ $p = 3$ และ $g = 5$

จากฝั่งอลิสเลือกตัวเลข a = 1 : $A = g^a mod\ p$

$A = 5^1 mod\ 3 = 2$ และส่งค่า A = 2 ไปให้บ็อบ

จากฝั่งบ็อบเลือกตัวเลข b = 2: B = $g^b mod\ p$

B = $5^2 mod\ 3 = 1$ และส่งค่า B = 1 ไปให้อลิส

คำนวณหาค่า K_{AB} จาก: $K_{AB} = (B)^A mod\ p$

$K_{AB} = (1)^1 mod\ 3 = 1$

คำนวณหาค่า K_{BA} จาก: $K_{BA} = (A)^B mod\ p$

$K_{BA} = (2)^2 mod\ 3 = 1$

ดังนั้นจะเห็นได้ว่าค่า $K_{AB} = K_{BA}$ ซึ่งเป็นกุญแจลับที่สร้างขึ้นทั้งสองฝั่งนั่นเอง

ใบรับรองอิเล็กทรอนิกส์ X.509

(Wikipedia, 2018) ได้กล่าวไว้ว่า X.509 เป็นรูปแบบมาตรฐาน ITU-T สำหรับโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และโครงสร้างพื้นฐานการจัดการสิทธิ์ (PMI) ซึ่ง X.509 จะระบุหมวดหมู่ที่หลากหลายของรูปแบบมาตรฐานสำหรับใบรับรองกุญแจสาธารณะ รายการเพิกถอนใบรับรอง ใบรับรอง และขั้นตอนการตรวจสอบเส้นทางการรับรอง

X.509 ถูกออกมาใช้ในวันที่ 3 กรกฎาคม ค.ศ. 1988 และมีความเกี่ยวข้องกับมาตรฐาน X.500 ซึ่งก็ถือว่าเป็นระบบลำดับชั้นที่เข้มงวดของผู้มีอำนาจในการออกใบรับรอง Certificate authority (CA) ซึ่งทำหน้าที่ในการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งปัจจุบัน X.509 มีรุ่นล่าสุด คือ รุ่น 3 ซึ่งจะมีโครงสร้างของใบรับรองดิจิทัล X.509 v3 ดังนี้

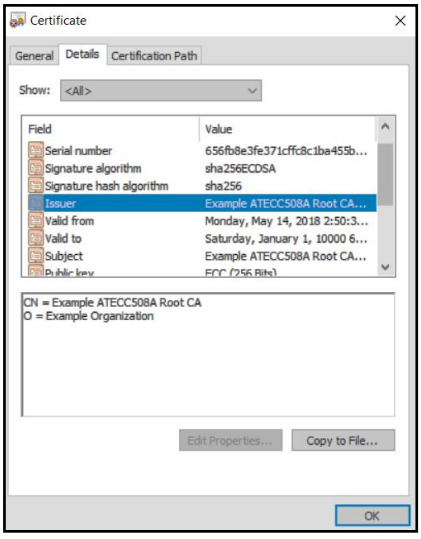
1. ใบรับรอง (Certificate)
   - 1.1 รุ่นของใบรับรอง (Version number)
   - 1.2 หมายเลขลำดับ (Serial number)
   - 1.3 อัลกอริทึมไอดี (Signature algorithm ID)
   - 1.4 ผู้ออกใบรับรอง (Issuer name)
   - 1.5 ความถูกต้อง (Validity period)
   - 1.6 หัวข้อ (Subject name)
   - 1.7 ข้อมูลกุญแจสาธารณะ (Subject public key info)
     - 1.7.1 อัลกอริทึมของกุญแจสาธารณะ (Public key algorithm)
     - 1.7.2 หัวข้อของกุญแจสาธารณะ (Subject public key)
   - 1.8 ตัวเอกลักษณ์ของผู้ออก (Issuer unique identifier)
   - 1.9 ตัวเอกลักษณ์ของหัวข้อ (Subject unique identifier)
   - 1.10 ส่วนขยายอื่น ๆ (Extensions)
2. อัลกอริทึมของลายเซ็นใบรับรอง (Certificate signature algorithm)

3. ลายเซ็นใบรับรอง (Certificate signature)

ในการใช้งานไอซี ATECC จะมีด้วยกัน 2 ประเภท ได้แก่ ใบรับรองอิเล็กทรอนิกส์ผู้ลงนาม (Signer certification) และใบรับรองอิเล็กทรอนิกส์อุปกรณ์ (Device certification) จะมีฟิลด์ต่าง ๆ ดังตารางที่ 2-2

ตารางที่ 2-2 ฟิลด์ของใบรับรองผู้อิเล็กทรอนิกส์ในไอซี ATECC

ฟิวด์	คำอธิบาย
Serial number	คำนวณจากหมายเลขซีเรียวของไอซี ATECC
Issue date	วันที่ออกใบรับรอง “YYMMDDHHMMSSZ”
Expire date	วันหมดอายุใบรับรอง “YYMMDDHHMMSSZ”
Signer ID	หมายเลขของผู้ลงนาม
Public key X	กุญแจสาธารณะ X (โดยปกติจะเป็น None)
Public key Y	กุญแจสาธารณะ Y (โดยปกติจะเป็น None)
Authority key identifier	ค่าแฮชที่ได้จาก SHA (04 + Issuer public key X&Y)
Subject key identifier	ค่าแฮชที่ได้จาก SHA (04 + Signer public key X&Y)
Signature R	ลายเซ็นของใบรับรอง R (โดยปกติจะเป็น None)
Signature S	ลายเซ็นของใบรับรอง R (โดยปกติจะเป็น None)



ภาพที่ 2-13 ใบรับรองผู้อิเล็กทรอนิกส์ในไอซี ATEC

เทคโนโลยี Huffman coding

จากบทความ (Wikipedia, 2018) ในปี ค.ศ. 1951 เดวิด ฮัฟแมน (David Huffman) และเพื่อนร่วมชั้นเรียนที่วิชาทฤษฎีข้อมูลที่ MIT โดยศาสตราจารย์โรเบิร์ต ฟาโน (Robert M. Fano) ให้นักเรียนในชั้นเลือกทำรายงานส่ง หรือสอบปลายภาค หัวข้อรายงาน คือ ให้หารหัสไบนารีที่มีประสิทธิภาพที่สุด ในขณะที่ฮัฟแมนเกือบจะล้มเลิกทำรายงานไปเตรียมตัวอ่านหนังสือสอบนั้น เขามีความคิดที่จะใช้แผนภูมิต้นไม้สองทางแบบเรียงความถี่ (Frequency-sorted binary tree) ขึ้นมาได้ และเขาก็ได้พิสูจน์ถึงประสิทธิภาพของรหัสที่เขาคิดขึ้นมา

Huffman code เป็นการเข้ารหัสแบบเอนโทรปี (Entropy) ใช้ในการบีบอัดข้อมูลให้มีขนาดเล็กลง โดยความยาวของบิตที่ใช้แทนข้อมูลซึ่งเป็นสัดส่วนที่แปรผกผันกับความถี่ของข้อมูล ถ้าความถี่ของข้อมูลน้อยจำนวนบิตที่ถูกบีบก็จะน้อยลง ทำให้ประหยัดเวลาในการส่ง ซึ่งจะไม่เหมือนการส่งด้วยรหัส ASCII หรือ Unicode ที่ต้องกำหนดจำนวนไบต์ที่ตายตัว โดยหลักการของ Huffman codes มีดังนี้

1. เริ่มจากสองตัวสุดท้ายของตัวอักษร A แทนด้วยสัญลักษณ์ γ และสัญลักษณ์ δ ถ้ารหัสอักษร (Code word) γ เท่ากับ [m]0 และรหัสอักษร δ เท่ากับ [m]1 เมื่อ [m] คือ ข้อความจาก 1'S และ 0'S

2. ทั้งสองสัญลักษณ์สามารถรวมกันเป็นสัญลักษณ์ตัวใหม่ คือ ψ โดยที่ตัวอักษร ψ เกิดจากค่าความน่าจะเป็นของ

$$P(\gamma) + P(\delta) \text{ ดังนั้น } \psi = P(\gamma) + P(\delta) \tag{2-17}$$

3. ทำซ้ำโดยการกำหนดรูปแบบบิตของ [m] ให้เป็นชุดของตัวอักษรใหม่

จากตัวอย่างของ (Chun-Jen, 2014) การหา Huffman code กำหนดให้

$$A = \{a_1, \dots, a_5\}, P(a_i) = \{0.2, 0.4, 0.2, 0.1, 0.1\}$$

Symbol	Step1	Step2	Step3	Step4	Codeword
a_2	0.4 →	0.4 →	0.4 →	0.6 0	1
a_1	0.2 →	0.2 →	0.4 0	0.4 1	01
a_3	0.2 →	0.2 0	0.2 1		000
a_4	0.1 0	0.2 1			0010
a_5	0.1 1				0011

ภาพที่ 2-14 ขบวนการ Huffman code

จากภาพที่ 2-14 สามารถหารหัสอักษร (Code word) ของ a_5 ได้ตามขั้นตอนดังนี้

ขั้นตอนที่ 1 ให้เรียงลำดับตัวอักษรแต่ละตัวจากมากสุดลงมาหาน้อย เมื่อต้องการหารหัสอักษร a_5 กำหนดให้ $P(\gamma) = P(a_5)$ พร้อมทั้งแทนรหัสอักษร a_5 ด้วย 1 และ $P(\delta) = P(a_4)$ พร้อมทั้งแทนรหัส a_4 อักษรด้วย 0

ขั้นตอนที่ 2 จาก $\psi = P(\gamma) + P(\delta) = P(a_5) + P(a_4) = 0.1 + 0.1 = 0.2$ จากนั้นให้เรียงค่าใหม่จากน้อยไปหามาเหมือนเดิมถ้าตัวเลขไม่มากกว่าด้านบนก็ไม่ต้องเปลี่ยนตำแหน่ง พร้อมทั้งแทนรหัสอักษร a_4 ด้วย 1 และแทนรหัสอักษรใน a_3 ด้วย 0

ขั้นตอนที่ 3 จาก $\psi = P(\gamma) + P(\delta) = P(a_5a_4) + P(a_3) = 0.2 + 0.2 = 0.4$ จากนั้นให้เรียงค่าใหม่จากน้อยไปหามาเหมือนเดิมภาพที่ 2-14 ค่า 0.4 มากกว่า 0.2 จึงถูกเลื่อนขึ้นไปแทนค่า 0.2 พร้อมทั้งแทนรหัสอักษร a_1 ด้วย 0 และแทนรหัสอักษรใน a_3 ด้วย 1

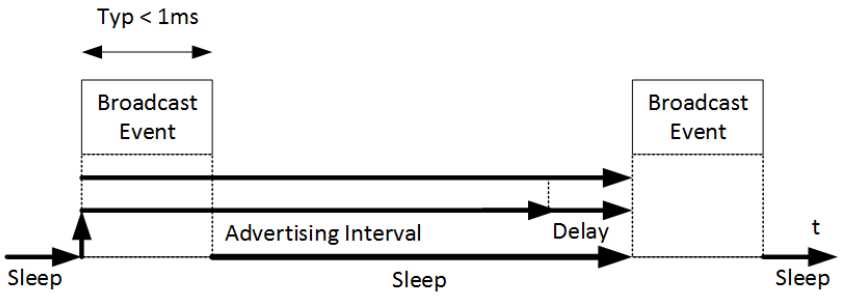
ขั้นตอนที่ 4 จาก $\psi = P(\gamma) + P(\delta) = P(a_5a_4a_3) + P(a_1) = 0.4 + 0.2 = 0.6$ จากนั้นให้เรียงค่าใหม่จากน้อยไปหามาเหมือนเดิมภาพที่ 2-14 ค่า 0.6 มากกว่า 0.4 จึงถูกเลื่อนขึ้นไปแทนค่า 0.4 พร้อมทั้งแทนรหัสอักษร a_2 ด้วย 0 และแทนรหัสอักษรใน a_1 ด้วย 0

ขั้นตอนที่ 5 จาก $\psi = P(\gamma) + P(\delta) = P(a_5a_4a_3a_1) + P(a_2) = 0.6 + 0.4 = 1$ เป็นอันสิ้นสุดรอบการวนซ้ำ เมื่อต้องการหารหัสอักษรของ a_5 จะต้องไล่กลับไปจาก (0.6), 0 ➔ (0.4), 0 ➔ (0.2), 1 ➔ (0.1), 1 = 0011 ดังนั้นรหัสอักษรของ $a_5 = 0011$

เทคโนโลยี Bluetooth low energy (BLE)

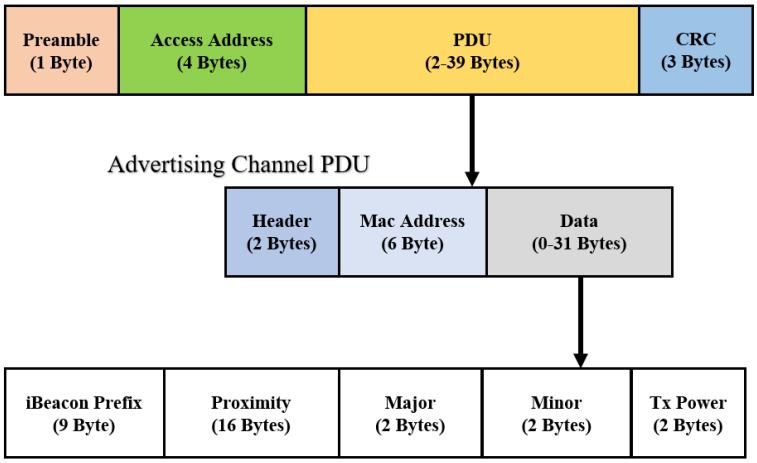
การเชื่อมต่อไร้สายผ่านบลูทูธ (Bluetooth) จะอยู่ในช่วงสัญญาณวิทยุความถี่สูง 2.4 GHz ในงานวิจัยนี้จะใช้ Bluetooth version 4.0 หรือที่นิยมเรียกกันว่า Bluetooth low energy (BLE) บนมาตรฐาน IEEE 802.15.1 โดยการเขียนโปรแกรมติดต่อสื่อสารกับอุปกรณ์ปล่อยสัญญาณ BLE จำเป็นจะต้องเข้าใจรูปแบบของการติดต่อสื่อสาร (Protocol) เพื่อใช้ในการส่งข้อมูล หรือรูปแบบการทำงานของการปล่อยสัญญาณ

จากที่กล่าวไปข้างต้นอุปกรณ์ปล่อยสัญญาณ BLE จะทำการปล่อยสัญญาณในลักษณะของการกระจาย (Broadcast) ข้อมูลออกไปภายในรัศมีทำการ 50-160 เมตร ซึ่งในที่นี่จะเรียกว่า Advertising interval หลังจากที่ปล่อยสัญญาณข้อมูลในช่วงระยะเวลาหนึ่งแล้ว จะทำการเข้าสู่โหมดประหยัดพลังงานหรือที่เรียกกันว่า Sleep mode จากนั้นอุปกรณ์จะทำการปิดตัวส่งสัญญาณและปิดส่วนประกอบต่าง ๆ ของบอร์ดเพื่อประหยัดพลังงาน เมื่อถึงช่วงเวลาที่กำหนด อุปกรณ์จะทำการตื่นขึ้นมาเพื่อปล่อยสัญญาณในรอบต่อไป ดังภาพที่ 2-15



ภาพที่ 2-15 การกระจาย (Broadcast) ข้อมูล

ในการปล่อยสัญญาณเพื่อส่งข้อมูลนั้น รูปแบบการส่งข้อมูลของ BLE จะมีขนาด 47 ไบต์ ตามรูปแบบการติดต่อสื่อสาร ดังภาพที่ 2-16



ภาพที่ 2-16 แพ็คเก็ตของข้อมูล BLE

ข้อมูลที่สามารถกำหนดหรือเปลี่ยนแปลงได้จะอยู่ในส่วนของ PDU ของรูปแบบการส่งข้อมูลแบบ BLE ซึ่ง PDU จะประกอบด้วย Header ขนาด 2 ไบต์ Mac address ขนาด 6 ไบต์ และ Data ขนาด 31 ไบต์ ส่วนที่จะอยู่ภายในการทดสอบนี้คือส่วนของข้อมูลที่มีขนาดทั้งหมด 31 ไบต์ โดยภายในข้อมูลของ Data จะถูกเรียกว่า Advertisement data จะแยกออกเป็นประเภทของข้อมูล ดังนี้

Advertisement Data Type		
AD Data Type	Data Type Value	Description
Flags	0x01	Device Discovery Capabilities
Service UUID	0x02 – 0x07	Device GATT Service
Local Name	0x08 – 0x09	Device Name
TX Power Level	0x0A	Device Output Power
Manufacture Specific Data	0xFF	User Defined

ภาพที่ 2-17 ส่วนประกอบของ Advertisement data type

ในส่วนของ Flags เป็นข้อมูล 3 ไบต์แรกที่ถูกกระจาย (Broadcast) สัญญาณข้อมูลออกไปเพื่อที่จะบอกถึงความสามารถของอุปกรณ์ ซึ่งเป็นไปตามภาพที่ 2-18

Advertisement Data Type, Flags			
Byte	Bit	Flag/Value	Description
0		0x02	Length of this data
1		0x01	GAP AD Type Flags
2	0	LE Limited Discoverable Mode	180s Advertising
	1	LE General Discoverable Mode	Indefinite Advertising Time
	2	BR/EDR Not Supported	
	3	Simultaneous LE and BR/EDR (Controller)	
	4	Simultaneous LE and BR/EDR (Host)	
	5-7		Reserved

ภาพที่ 2-18 ส่วนประกอบของ Flag ใน Advertisement data

ในส่วนของ Manufacturer specific data จะเป็นข้อมูลของผู้ผลิตที่ต้องการกำหนดให้ปล่อยกระจายสัญญาณข้อมูลใด ๆ ออกไปตามภาพที่ 2-19

Advertisement Data Type, Manufacturer Specific Data Format		
Byte	Value	Description
0	0x03 – 0x1F	Length of this data
1	0xFF	Manufacturer Specific Data Flag
2	0x0D	Company ID
3	0x00	(Example, 0x000D – Texas Instruments)
4 - 31	-	User defined Data (Optional)

ภาพที่ 2-19 ส่วนประกอบของ Manufacturer specific data

Raw Data:: 0x02 0x01 0x06 0x1A 0xFF 0x4C 0x00 0x02 0x15 0xB9 0x40 0x7F 0x30 0xF5 0xF8 0x46 0x6E 0xAF 0xF9 0x25 0x55 0x6B 0x57 0xFE 0x6D 0x00 0x49 0x00 0x0A 0xC5

ภาพที่ 2-20 ตัวอย่างการกำหนดแพ็คเก็ตของการกระจายข้อมูล Advertisement Data

จากภาพที่ 2-20 เมื่อนำมาถอดรูปแบบของข้อมูลจะแบ่งออกมาเป็นดังนี้

Flags: 0x02 ความยาวของข้อมูลขนาด 2 ไบต์

0x01 คือ GAP AD Type Flags

0x06 จากตารางของ Advertisement Data Type, Flags 0x06 จะแปลงเป็น bit ได้คือ 00000110 นั่นคือ LE/ General Discoverable Mode, BR/EDR Not Support

0x1A คือ ความยาวของข้อมูลขนาด 26 ไบต์

0xFF คือ Manufacturer-Specific data flag

0x4C และ 0x00 คือ Company identifier code (0x004C == Apple)

0x02 คือ Byte 0 of iBeacon advertisement indicator

0x15 คือ Byte 1 of iBeacon advertisement indicator

0x00 และ 0x49 คือ ข้อมูล Major

0x00 และ 0x0A คือ ข้อมูล Minor

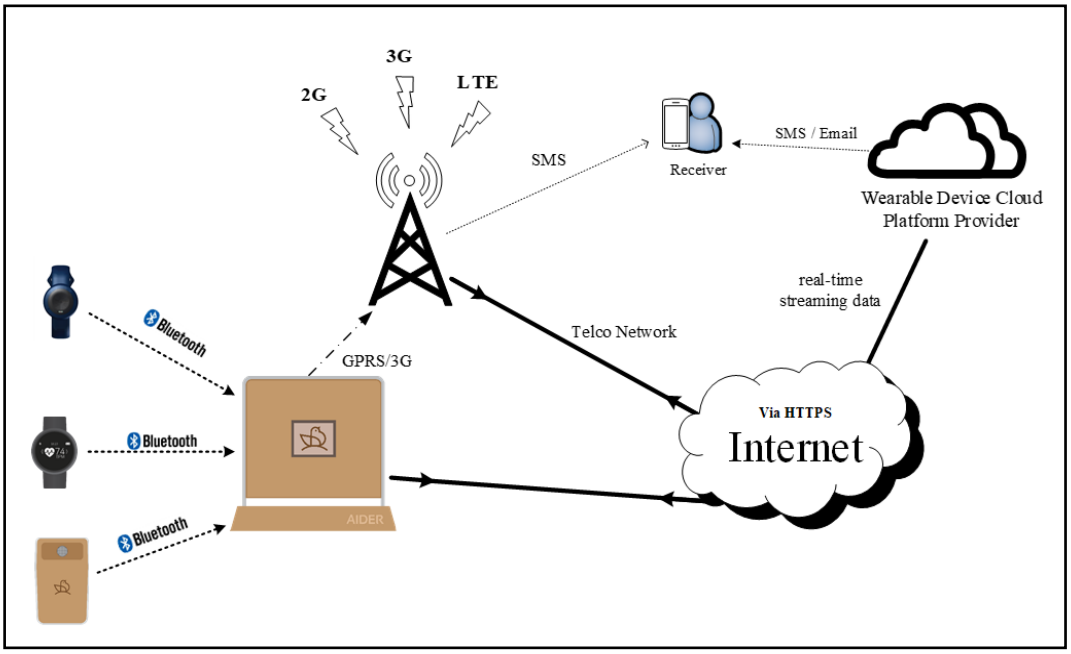
0xC5 คือ Complement of measured Tx power

บทที่ 3
ขั้นตอนและวิธีดำเนินการ

ระบบในงานวิจัยนี้ มีที่มาจากระบบที่ถูกพัฒนาขึ้นมาเพื่อเป็นระบบแจ้งเตือนความผิดปกติทางสุขภาพของผู้สูงอายุและความผิดปกติภายในบ้านของผู้พักอาศัยภายในบ้าน ซึ่งส่วนใหญ่เป็นผู้สูงอายุที่อยู่บ้านคนเดียวเมื่อลูกหลานออกไปทำงานนอกบ้านหรือเป็นผู้สูงอายุที่อยู่ในบ้านพักคนชราที่มีความหนาแน่นของผู้สูงอายุ จนทำให้เจ้าหน้าที่อาจดูแลไม่ทั่วถึง โดยผู้สูงอายุต้องสวมใส่อุปกรณ์ติดตามตัวในลักษณะใส่ข้อมือหรือห้อยคอตลอดเวลา เพื่อเป็นการเฝ้าระวังการกดขอความช่วยเหลือหรือการล้มแบบฉุกเฉินที่อุปกรณ์สามารถตรวจจับได้ตลอดเวลา เนื่องจากในวัยของผู้สูงอายุมีอัตราความเสี่ยงในการเกิดอุบัติเหตุภายในที่พักอาศัย ซึ่งถ้าเข้าไปช่วยเหลือไม่ทันท่วงทีเมื่อเกิดอุบัติเหตุ อาจจะทำให้เกิดการสูญเสียของชีวิตได้ ในส่วนของบริเวณของห้องต่าง ๆ โดยเฉพาะห้องน้ำจะมีอุปกรณ์ไว้กดหรือดึงขอความช่วยเหลือด้วย เนื่องจากบางครั้งผู้สูงอายุอาจจะลืมใส่อุปกรณ์ติดตามตัว จะได้สามารถกดหรือดึงขอความช่วยเหลือได้ นอกจากนี้ยังมีระบบเซนเซอร์ตรวจจับความผิดปกติของอุณหภูมิและแก๊สรั่ว ภายในบ้านของผู้อาศัยในกรณีที่เจ้าของบ้านอาจจะลืมปิด ระบบจะทำการแจ้งเจ้าของบ้านให้สามารถไปป้องกันไม่เหตุการเกิดความร้ายแรงขึ้นได้ ทำให้ผู้ที่อยู่อาศัยเกิดความอุ่นในใจในการพักอาศัยภายในบ้าน

ในงานวิจัยนี้จะหยิบยกประเด็นในเรื่องของความปลอดภัยของข้อมูลจากอุปกรณ์ที่ใช้กับผู้สูงอายุไปยังเกตเวย์ เพื่อสร้างความมั่นใจให้กับผู้ใช้งานในเรื่องความปลอดภัยของข้อมูล ซึ่งทำให้เกิดความเป็นส่วนตัวกับผู้ใช้งาน จากระบบแจ้งเตือนความผิดปกติทางสุขภาพของผู้สูงอายุที่เดิมนั้นไม่มีความปลอดภัยของข้อมูล งานวิจัยนี้จึงได้เพิ่มความปลอดภัยให้กับอุปกรณ์สวมใส่ โดยใช้ไอซีเข้ารหัส สร้างกระบวนการระบุตัวตนเพื่อเป็นการยืนยันผู้ใช้งานตัวจริง การแลกเปลี่ยนกุญแจรหัสลับโดยที่เกตเวย์ไม่จำเป็นต้องส่งข้อมูลไปให้อุปกรณ์สวมใส่ และเพิ่มการเข้ารหัสลับของข้อมูลอุปกรณ์สวมใส่ส่วนบุคคลไปยังเกตเวย์ เพื่อให้ผู้ใช้งานมีความเป็นส่วนตัวของข้อมูลมากขึ้น

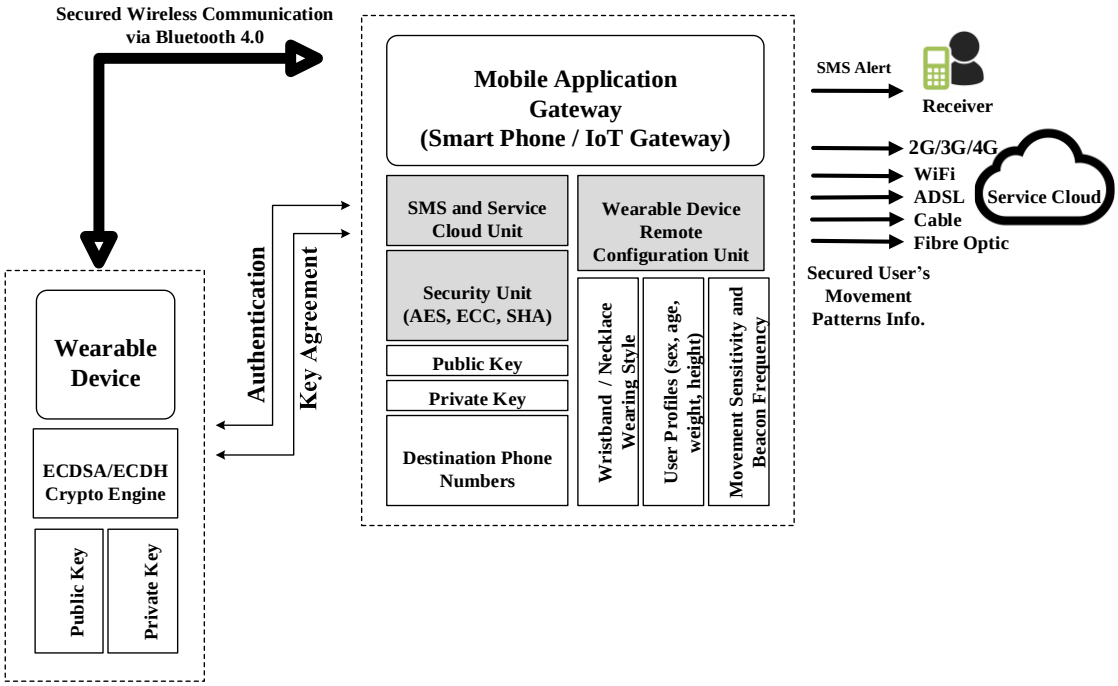
ภาพรวมของระบบ



ภาพที่ 3-1 ภาพรวมของระบบการดูแลสุขภาพอัจฉริยะ (Smart health care)

จากภาพที่ 3-1 คือ การทำงานของระบบการระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพส่วนบุคคลในอุปกรณ์สวมใส่โดยใช้ไอซีเข้ารหัสในระบบไอโอที จะประกอบไปด้วยส่วนของอุปกรณ์ไอโอทีที่รับข้อมูล Bluetooth low energy (BLE) ย่านความถี่วิทยุ 2.4 GHz มาที่เกตเวย์ และจากเกตเวย์จะส่งต่อข้อมูลไปยังวส์เซิร์ฟเวอร์ (Cloud server) เพื่อเก็บและจัดการข้อมูลที่จะส่งต่อไปยังส่วนของ SMS และหน้าจอเฝ้าระวัง

อุปกรณ์ไอโอทีส่วนบุคคลเป็นอุปกรณ์ที่คอยรับการแจ้งเตือนความผิดปกติทางสุขภาพของผู้สูงอายุและความผิดปกติภายในบ้านของผู้พักอาศัยภายในบ้านพัฒนาโดยบริษัทเบสแล็บ (BAESLab Co., Ltd.) ได้แก่ สายรัดข้อมือ Aider A1 และสายรัดข้อมือAider A2 จากภาพที่ 3-2 เป็นส่วนประกอบการทำงานของอุปกรณ์สวมใส่และเกตเวย์ โดยที่ฝั่งเกตเวย์มีการเตรียมการในส่วนที่สร้างความปลอดภัย (Security unit) ให้รองรับการทำงานของข้อมูลที่มาจากฝั่งอุปกรณ์สวมใส่ที่มีไอซีเข้ารหัส (Crypto engine) ฝั่งอยู่ในอุปกรณ์



ภาพที่ 3-2 ส่วนประกอบของการทำงานของอุปกรณ์สวมใส่กับเกตเวย์

การทำงานของสายรัดข้อมือ Aider A1 และ Aider A2 จะเป็นการตรวจรับการแจ้งเตือนการกดขอความช่วยเหลือและการตรวจจับการล้มของผู้ใช้ โดยการสวมใส่ไว้กับตัวตลอดเวลา นอกจากนั้นอุปกรณ์ยังสามารถจับเวลาของการประกอบกิจกรรม ได้แก่ การอยู่เฉย การเดิน และการวิ่ง รวมถึงการตรวจจับจำนวนก้าวเดินและจำนวนแคลลอรี่ที่ใช้ ส่วนในรุ่น Aider A2 จะมีฟังก์ชันการทำงานที่เพิ่มมากกว่า Aider A1 ได้แก่ การวัดอัตราการเต้นของหัวใจ การวัดระดับออกซิเจนในเลือด และการวัดอุณหภูมิ การทำงานของ Sensor hub จะใช้เป็นอุปกรณ์เซนเซอร์ที่วัดความผิดปกติในบ้านได้แก่ ค่าอุณหภูมิที่ผิดปกติและค่าแก๊สที่ผิดปกติอาจจะเกิดจากการรั่วไหล โดยอุปกรณ์เหล่านี้จะทำการอ่านข้อมูลตามเวลาที่กำหนดหรือในกรณีเกิดเหตุฉุกเฉินแล้วส่งออกผ่าน BLE ในลักษณะกระจายข้อมูล (Broadcast data) หรือบีคอน (Beacon) ไปยังอุปกรณ์เกตเวย์ โดยในส่วนนี้จะมีการเข้ารหัส AES เพื่อป้องกันการดักฟังของข้อมูล

อุปกรณ์เกตเวย์จะเป็นตัวรับข้อมูลต่าง ๆ จากอุปกรณ์ไอโอทีส่วนบุคคลมากจากการรับข้อมูล Beacon จากนั้นเกตเวย์จะทำการส่งข้อมูลต่อไปยังคาวส์เซิร์ฟเวอร์ผ่านการส่งข้อมูลแบบ MQTT เมื่อคาวส์เซิร์ฟเวอร์ได้รับข้อมูลจะเก็บข้อมูลลงฐานข้อมูล (Database) ต่อจากนั้นเซิร์ฟเวอร์จะทำการส่ง SMS ไปยังเบอร์ที่เคยลงทะเบียนไว้และแสดงข้อมูลที่หน้าจอเฝ้าระวังของหน่วยงาน เช่น ห้องเฝ้าระวังของเทศบาล ห้องฉุกเฉินของโรงพยาบาล ศูนย์รับเหตุฉุกเฉิน ฯลฯ

ตัวอย่างการทำงานของAider A1 เมื่อผู้สูงอายุสวมใส่อุปกรณ์แล้วเกิดการล้มขึ้น อุปกรณ์จะส่งข้อมูลที่เข้ารหัส AES ด้วย BLE ผ่านทางอากาศยังเกตเวย์ เกตเวย์จะทำการถอดรหัสข้อมูลแล้วทำการส่งข้อมูลขึ้นคาวส์เซิร์ฟเวอร์ด้วย MQTT จากนั้นข้อมูลจะถูกประมวลผลด้วยเซิร์ฟเวอร์แล้วส่งข้อความไปหาเบอร์ของลูกหลานที่ถูกลงทะเบียนไว้ ซึ่งในเวลาเดียวกันนั้นระบบก็จะแสดงข้อความฉุกเฉินของหน้าเว็ปเฝ้าระวังของศูนย์เฝ้าระวัง โดยเมื่อเจ้าหน้าที่รับเรื่องแล้วจะรีบดำเนินการเข้าไปให้การช่วยเหลือยังแผนที่ ที่ปรากฏอยู่ที่จอเฝ้าระวัง

ภาพที่ 3-3 หน้าจอเฝ้าระวังจากโครงการพัฒนา SMART LIVING สำหรับอุตสาหกรรมบริการสุขภาพอัจฉริยะ 2017

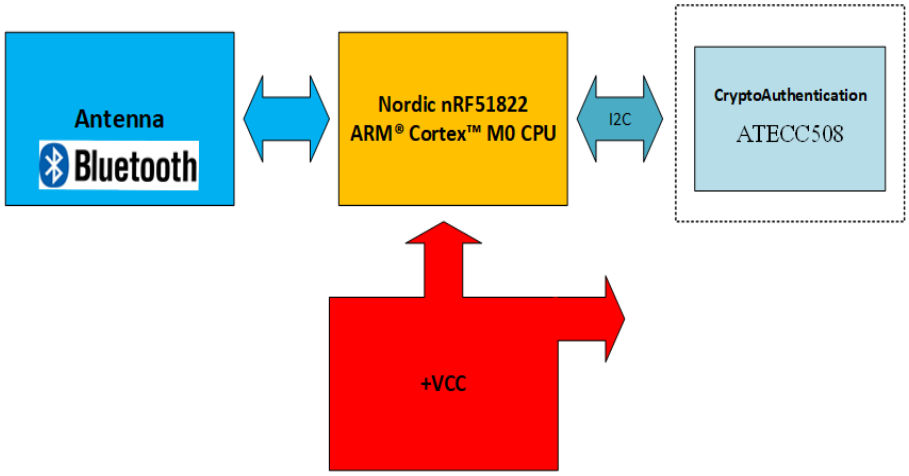
ในส่วนของการออกแบบกระบวนการดำเนินงานของระบบนั้นสามารถแบ่งออกได้เป็น 2 ส่วนหลักๆ ได้แก่ กระบวนการออกแบบอุปกรณ์ และกระบวนการทำงานของระบบ

กระบวนการออกแบบอุปกรณ์

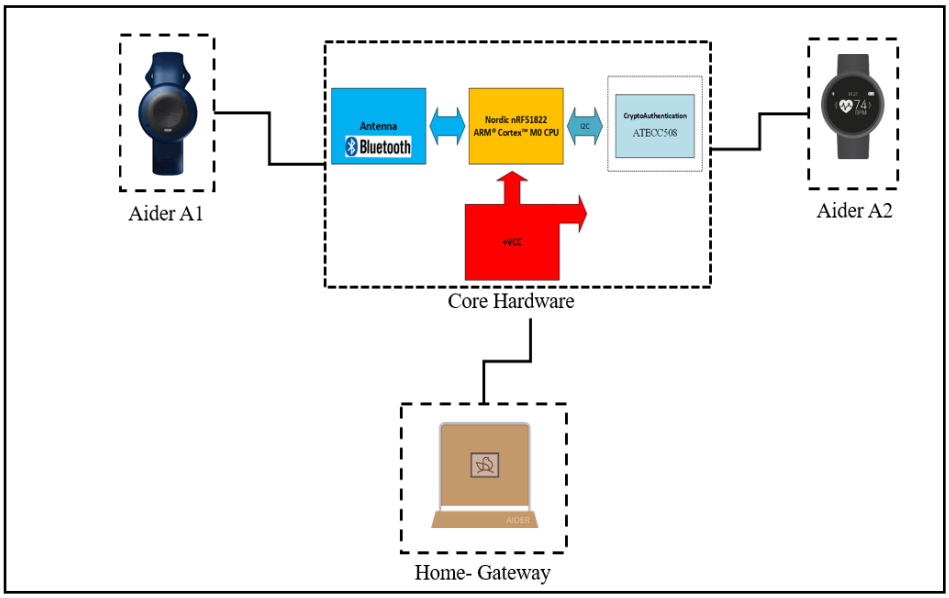
1. การออกแบบรูปแบบการทำงานวงจรของอุปกรณ์

การออกแบบการทำงานของวงจรอุปกรณ์ไอโอทีส่วนบุคคล ได้แก่ Aider A1, Aider A2 และ Home-Gateway จะใช้ไฟเลี้ยง +VCC ใช้ไมโครคอนโทรลเลอร์ควบคุมการทำงานจากบริษัท Nordic Semiconductor โดยใช้เบอร์ nRF51822 ซึ่งเป็นไมโครคอนโทรลเลอร์สถาปัตยกรรม ARM

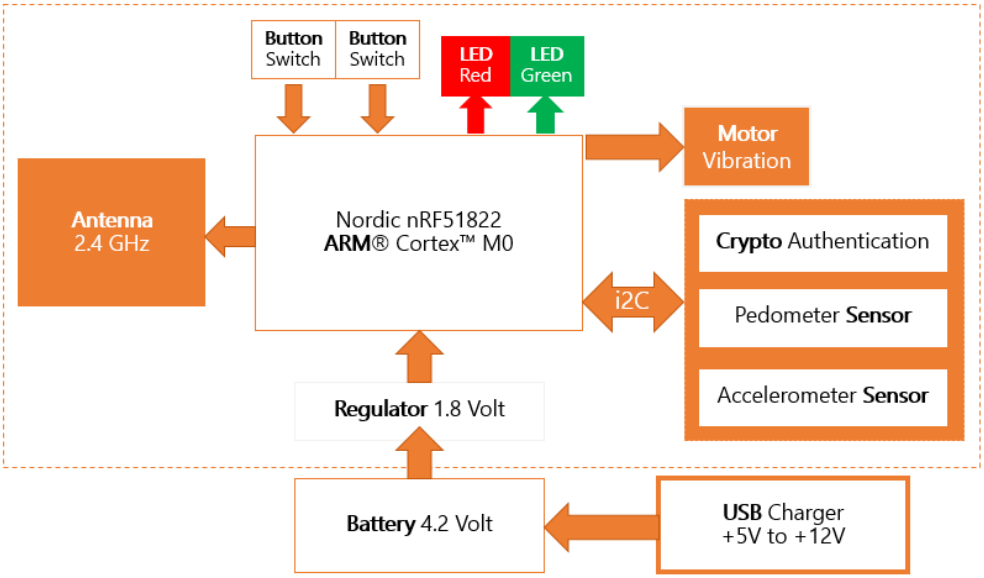
Cortex M0 และผนวกโมดูลบนไอซี (SOC: System on chip) ได้แก่ การทำงานของ Bluetooth low energy 4.0 (BLE4.0) และการเข้ารหัส AES แบบ ECB โดยไมโครคอนโทรลเลอร์จะเป็นตัวควบคุมการทำงานทั้งหมดของแอปพลิเคชัน และมีการสั่งงานไปยังไอซี ATECC508 ผ่านบัส I2C ตามภาพที่ 3-4 โดยหลักการทำงานของวงจรจะทำงานด้วยเทคโนโลยี ดังภาพที่ 3-5 และภาพที่ 3-6 แสดงบล็อกไดอะแกรมของวงจรอุปกรณ์สวมใส่ส่วนบุคคล



ภาพที่ 3-4 บล็อกไดอะแกรมของฮาร์ดแวร์แกนหลักของอุปกรณ์ไอโอทีส่วนบุคคล



ภาพที่ 3-5 ความสัมพันธ์ของวงจรฮาร์ดแวร์แกนหลักกับอุปกรณ์ไอโอทีส่วนบุคคล



ภาพที่ 3-6 บล็อกไดอะแกรมของวงจรอุปกรณ์สวมใส่ส่วนบุคคล

1.1 คุณสมบัติเบื้องต้นของไมโครคอนโทรลเลอร์ nRF51822 มีดังนี้

1.1.1 ใช้ส่งสัญญาณในย่านความถี่วิทยุ 2.4 GHz (BLE: Bluetooth low energy)

1.1.2 ปรับกำลังความแรงสัญญาณได้แต่ -20 dBm ถึง +4 dBm

1.1.3 สถาปัตยกรรม ARM Cortex M0

1.1.4 มีพื้นที่ในการเก็บโปรแกรม (Program memory) ขนาด 256 กิโลไบต์ (kB)

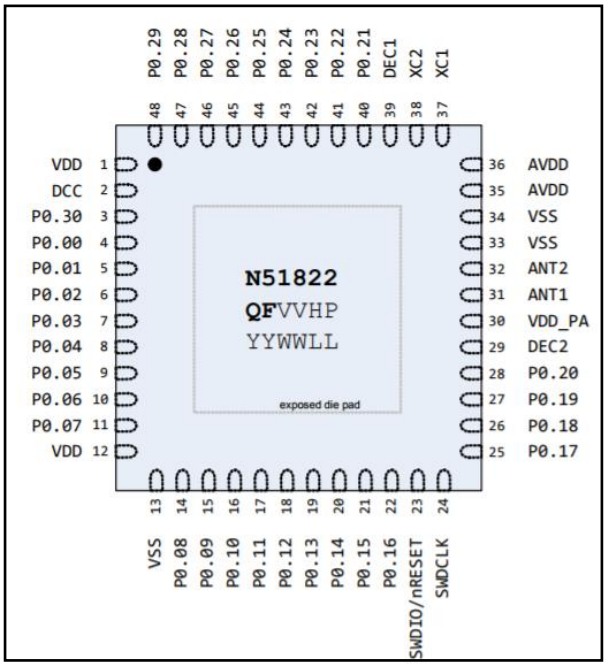
1.1.5 มีพื้นที่ความจำชั่วคราว (RAM) ขนาด 32 กิโลไบต์ (kB)

1.1.6 ไฟเลี้ยงตั้งแต่ +1.8 โวลต์ ถึง +3.6 โวลต์

1.1.7 สามารถสั่งงานขา I/O ได้ 31 ขา

1.1.8 มีบัส UART, SPI และ I2C

1.1.9 มีการเข้ารหัส AES Hardware encryption



ภาพที่ 3-7 ฟังก์ชันการใช้งานของขาไมโครคอนโทรลเลอร์ nRF51822

1.2 คุณสมบัติเบื้องต้นไอซี ATECC508 ของดังนี้

1.2.1 มีที่เก็บกุญแจรหัสลับ (Key storage) ในการเก็บกุญแจรหัสลับขนาด 32 ไบต์มีทั้งหมด 7 สล็อตตั้งแต่สล็อต 0 ถึง 7 และกุญแจรหัสลับขนาด 64 ไบต์มีทั้งหมด 7 สล็อต ตั้งแต่สล็อต 8 ถึง 15

1.2.2 ใช้กระบวนการ ECDSA: FIPS186-3 Elliptic curve digital signature algorithm ระหว่างฝั่งอุปกรณ์แม่ (Host device) และฝั่งอุปกรณ์ลูก (Client device)

1.2.3 ใช้กระบวนการ ECDH: FIPS SP800-56A Elliptic curve Diffie-Hellman algorithm ในการแลกกุญแจรหัสลับระหว่างฝั่งอุปกรณ์แม่และฝั่งอุปกรณ์ลูก

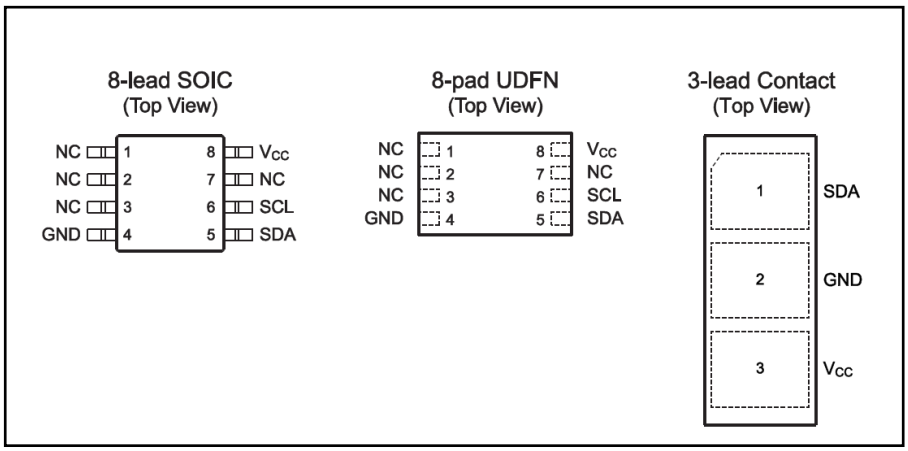
1.2.4 มี EEPROM สำหรับกุญแจรหัสลับ (Keys) และข้อมูล (Data) ขนาด 10 KB

1.2.5 ใช้บัส I2C ในการติดต่อกับโมดูลในการใช้งาน

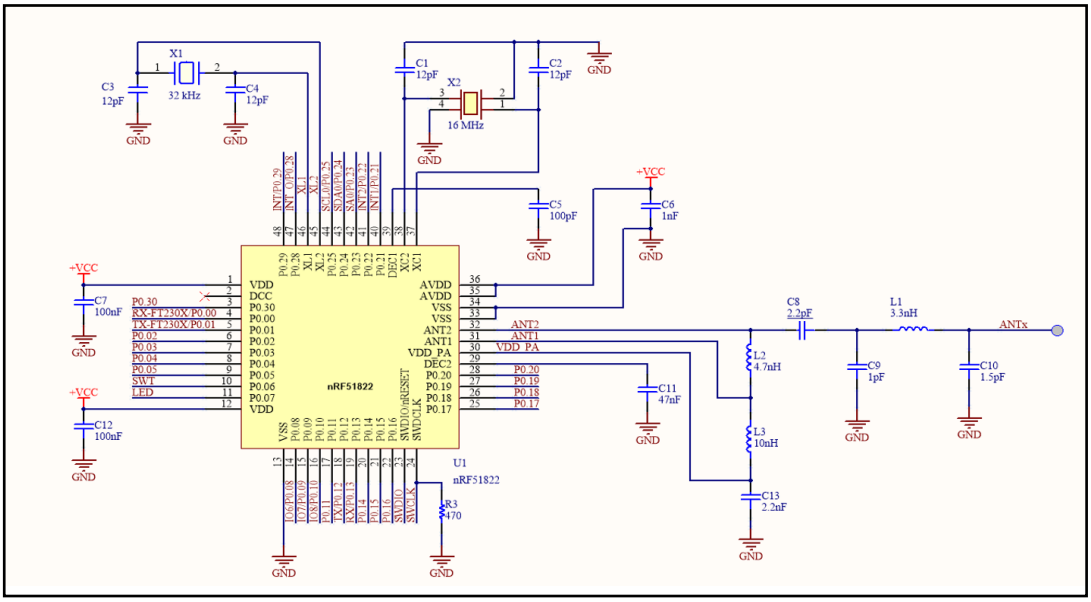
1.2.6 ไฟเลี้ยงตั้งแต่ +2.0 โวลต์ ถึง +5.5 โวลต์

1.2.7 การกินกระแสจะน้อยกว่า 150nA เมื่อ Sleep

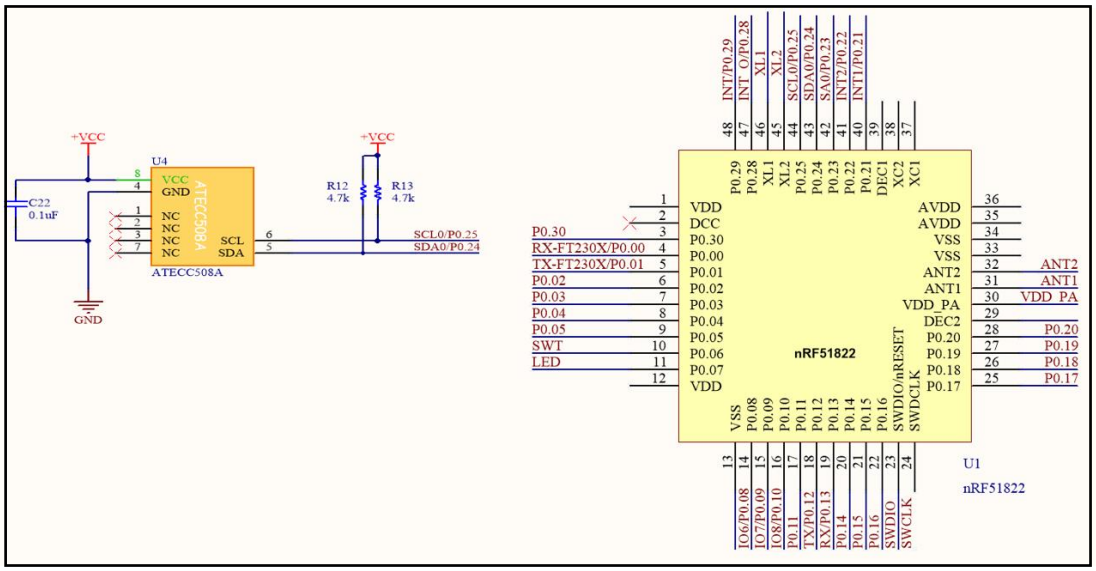
1.2.8 การประยุกต์ใช้งานได้แก่ ความปลอดภัยในการโหลดโปรแกรม (Secure download and Boot) การควบคุมระบบนิเวช (Ecosystem control) ป้องกันการโคลน (Anti-cloning) และความปลอดภัยการส่งข้อความ (Message security)



ภาพที่ 3-8 ขนาดและฟังก์ชันการใช้งานของขาไอซี ATECC508



ภาพที่ 3-9 แผนผังวงจร (Schematic circuit) ของวงจรส่วนของ Bluetooth low energy

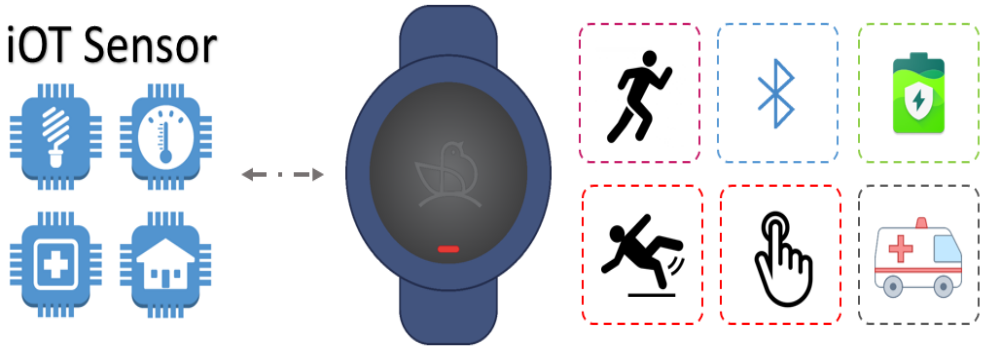


ภาพที่ 3-10 แผนผังวงจร (Schematic circuit) ของการเชื่อมต่อไอซี ATECC508A

2. การออกแบบฟังก์ชันการทำงานของอุปกรณ์

อุปกรณ์ไอโอทีส่วนบุคคลเป็นอุปกรณ์ที่พัฒนาโดยบริษัทเบสแล็บ (BAESLab Co., Ltd.) มีอุปกรณ์ดังนี้

2.1 สายรัดข้อมือ (Aider A1)



ภาพที่ 3-11 สายรัดข้อมือ Aider A1

คุณสมบัติของสายรัดข้อมือ Aider A1 ได้แก่

2.1.1 สามารถตรวจรับการแจ้งเตือนจากการกดขอความช่วยเหลือ

2.1.2 สามารถตรวจจับการล้ม

2.1.3 สามารถจับเวลาของการประกอบกิจกรรม การอยู่เฉย การเดิน และการวิ่ง

2.1.4 สามารถตรวจจับจำนวนก้าวเดิน

2.1.5 สามารถคำนวณจำนวนแคลลอรี่

2.1.6 สามารถปล่อยข้อมูลดิบของความเร่งแกน x, y และ z ได้

2.1.7 สามารถอ่านค่าแบตเตอรี่และแจ้งเตือนระดับแบตเตอรี่ได้

2.1.8 ส่งสัญญาณผ่าน BLE

2.2 สายรัดข้อมือ (Aider A2)

ภาพที่ 3-12 สายรัดข้อมือ Aider A2

คุณสมบัติของสายรัดข้อมือ Aider A2 ได้แก่

2.2.1 สามารถตรวจรับการแจ้งเตือนจากการกดขอความช่วยเหลือ

2.2.2 สามารถตรวจจับการล้ม

2.2.3 สามารถจับเวลาการประกอบกิจกรรม การอยู่เฉย การเดิน และการวิ่ง

2.2.4 สามารถตรวจจับจำนวนก้าวเดิน

2.2.5 สามารถคำนวณจำนวนแคลลอรี่

2.2.6 สามารถวัดอัตราการเต้นของหัวใจ

2.2.7 สามารถวัดปริมาณออกซิเจนในเลือดได้

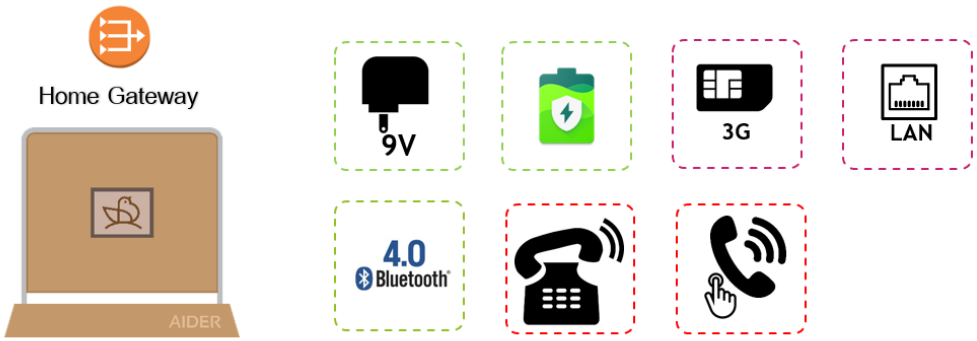
2.2.8 สามารถวัดอุณหภูมิร่างกายบริเวณที่สวมใส่ได้

2.2.9 มีจอแสดงผล

2.2.10 สามารถอ่านค่าแบตเตอรี่และแจ้งเตือนระดับแบตเตอรี่ได้

2.2.11 ส่งสัญญาณผ่าน BLE

2.4 เกตเวย์ (Home-Gateway)



ภาพที่ 3-13 เกตเวย์ Home-Gateway

คุณสมบัติของอุปกรณ์เกตเวย์

2.4.1 รับข้อมูลจากอุปกรณ์ไอโอทีส่วนบุคคลผ่านทาง BLE

2.4.2 สามารถส่งข้อมูลขึ้นคาวส์เซิร์ฟเวอร์ผ่าน MQTT

2.4.3 สามารถติดต่อสื่อสารผ่านออกอินเตอร์เน็ตผ่านสายอินเตอร์เน็ต (LAN) ได้

2.4.4 สามารถติดต่อสื่อสารผ่านออกอินเตอร์เน็ตผ่านเครือข่ายสามจี (3G) ได้

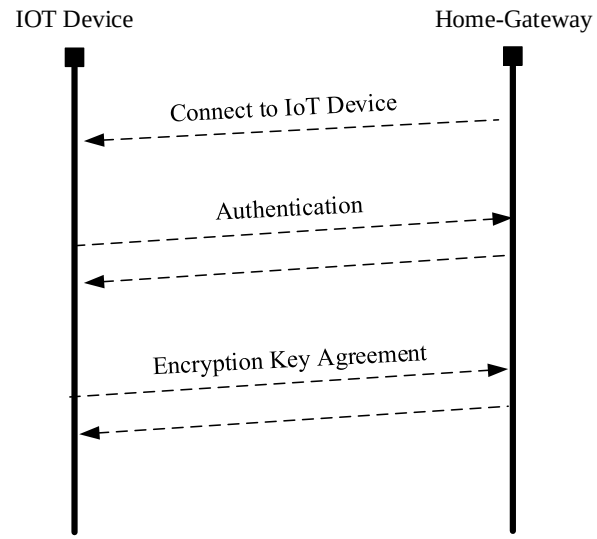
กระบวนการทำงานของระบบ

การออกแบบกระบวนการของระบบการทำงานอุปกรณ์ไอโอทีส่วนบุคคล สามารถแบ่งเป็นกระบวนการได้ 3 ส่วนหลัก ๆ ได้แก่ การออกแบบการติดต่อสื่อสารระหว่างอุปกรณ์ การออกแบบกระบวนการความปลอดภัยของอุปกรณ์ไอโอทีส่วนบุคคล และการออกแบบกระบวนการทำงานของโปรแกรม

1. การออกแบบการติดต่อสื่อสารระหว่างอุปกรณ์ไอโอที

การติดต่อสื่อสารระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์มีส่วนของการสื่อสารอยู่ด้วยกัน 2 ส่วน ได้แก่ การเชื่อมต่อ BLE และการปล่อยบีคอน (Beacon)

1.1 การเชื่อมต่อ BLE



ภาพที่ 3-14 ลักษณะการเชื่อมต่อ BLE

การเชื่อมต่อ BLE เป็นขั้นตอนครั้งแรก ก่อนที่อุปกรณ์ไอโอทีส่วนบุคคลจะสามารถส่งข้อมูลด้วยการบีคอนเพื่อส่งข้อมูลให้เกตเวย์ได้ เกตเวย์จะทำการตรวจสอบว่าอุปกรณ์ที่มาใหม่นั้นเป็นอุปกรณ์ในเครือข่ายหรือไม่ โดยเกตเวย์จะทำการเชื่อมต่อ BLE ไปหาอุปกรณ์ จากนั้นเมื่อเชื่อมต่อกันสำเร็จจะเริ่มทำกระบวนการระบุตัวตน (Authentication) ว่าเป็นตัวจริงหรือไม่ ถ้าเป็นตัวจริงก็จะทำกระบวนการแลกเปลี่ยนกุญแจรหัสลับกัน สุดท้ายแล้วเมื่อเสร็จกระบวนการเกตเวย์จะทำการตัดการเชื่อมต่อกับอุปกรณ์ ในการเชื่อมต่อ BLE มีการกำหนดโครงสร้างของข้อมูลใช้ในการสื่อสารระหว่างเกตเวย์และอุปกรณ์ ให้มีข้อมูลขนาด 71 ไบต์ ดังภาพที่ 3-15 มีการกำหนดส่วนของโครงสร้างเป็น 5 ส่วน ดังนี้

1.1.1 หัวของแพ็คเก็ต (Header) ขนาด 1 ไบต์

1.1.2 ความยาวของแพ็คเก็ต (Length) ขนาด 1 ไบต์

1.1.3 ข้อมูลของแพ็คเก็ต (Data) ขนาด 1 ไบต์ถึง 65 ไบต์

1.1.4 ส่วนตรวจสอบความถูกต้องของแพ็คเก็ต (CRC)

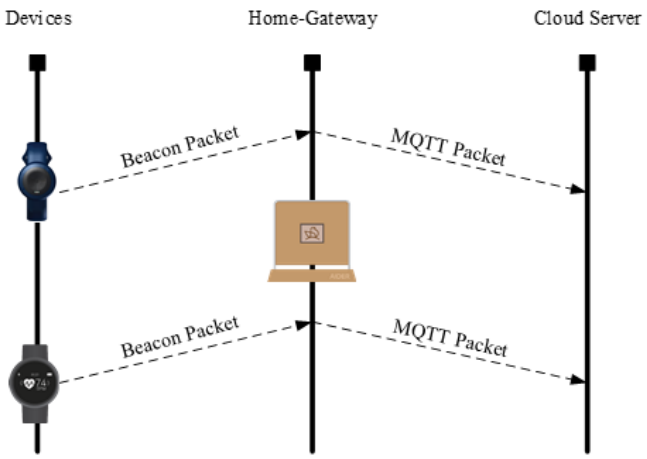
1.1.5 ส่วนปิดท้ายของแพ็คเก็ต (Footer)

Header	Length	Data	CRC	Footer
1 Byte	1 Byte	1 Byte – 65 Bytes	2 Bytes	2 Bytes

Header	Length	Data	CRC	Footer
':'	0x41	$D_1, D_2, D_2 \ldots, D_n$	0x1122	0x0D0A

ภาพที่ 3-15 โครงสร้างข้อมูลของการสื่อสารระหว่างเกตเวย์และอุปกรณ์ไอโอทีส่วนบุคคล

1.2 การปล่อยบีคอน (Beacon) การปล่อยบีคอนระหว่างอุปกรณ์ไอโอทีส่วนบุคคลไปยังเกตเวย์ ดังภาพที่ 3-16 เป็นการกำหนดให้อุปกรณ์ไอโอที ได้แก่ สายรัดข้อมือ Aider A1 สายรัดข้อมือ Aider A2 และอุปกรณ์วัดค่าเซนเซอร์ภายในบ้าน (Sensor hub) ให้ส่งข้อมูลผ่าน BLE ในลักษณะกระจายข้อมูล (Broadcast data) หรือบีคอน (Beacon) ผ่านทางอากาศ จากนั้นเกตเวย์จะแสกน เพื่อรับข้อมูลและคัดกรองข้อมูล แล้วจึงส่งต่อข้อมูลไปยังคาวส์เซิร์ฟเวอร์ต่อไป



ภาพที่ 3-16 ลักษณะการปล่อยข้อมูลบีคอนระหว่างอุปกรณ์ไอโอทีกับเกตเวย์

ในการกระจายข้อมูล (Broadcast data) ข้อมูลแต่ละครั้งผ่านทาง BLE ของอุปกรณ์ไอโอทีจะมีข้อมูลอยู่ 2 ส่วน ได้แก่ Advertise data และ Service data โดยส่วนที่จะห่อหุ้มข้อมูลไป คือ ส่วนของ Service data ที่มีขนาด 31 ไบต์ ข้อมูลของไบต์แรกเริ่มที่ไบต์ที่ 7 แล้วไปจบที่ไบต์ที่ 22 รวมข้อมูลทั้งหมดขนาด 16 ไบต์ ซึ่งข้างในข้อมูลถูกออกแบบให้สามารถส่งแยกตามชนิดข้อมูลของแต่อุปกรณ์ไอโอที ได้แก่ สายรัดข้อมือ Aider A1 และสายรัดข้อมือ Aider A2 โดยอุปกรณ์

แต่ละชนิดจะมีข้อมูลที่ถูกบรรจุที่แตกต่างกันไป โดยการจำแนกข้อมูลของ อุปกรณ์แต่ละตัวเป็นดังนี้

1.1 ข้อมูลของสายรัดข้อมือ Aider A1 มีข้อมูลดังนี้

1.1.1 ระดับการใช้แบตเตอรี่

1.1.2 สถานะของการตรวจจับการกดขอความช่วยเหลือ

1.1.3 สถานะของการตรวจจับการล้ม

1.1.4 เวลาการประกอบกิจกรรม การอยู่เฉย การเดิน และการวิ่ง

1.1.5 จำนวนก้าวเดิน

1.1.6 จำนวนแคลลอรี่

1.1.7 ความเร่งแกน x, y และ z

1.2 ข้อมูลของสายรัดข้อมือ Aider A2 มีข้อมูลดังนี้

1.2.1 ระดับการใช้แบตเตอรี่

1.2.2 สถานะของการตรวจจับการกดขอความช่วยเหลือ

1.2.3 สถานะของการตรวจจับการล้ม

1.2.4 เวลาการประกอบกิจกรรม การอยู่เฉย การเดิน และการวิ่ง

1.2.5 จำนวนก้าวเดิน

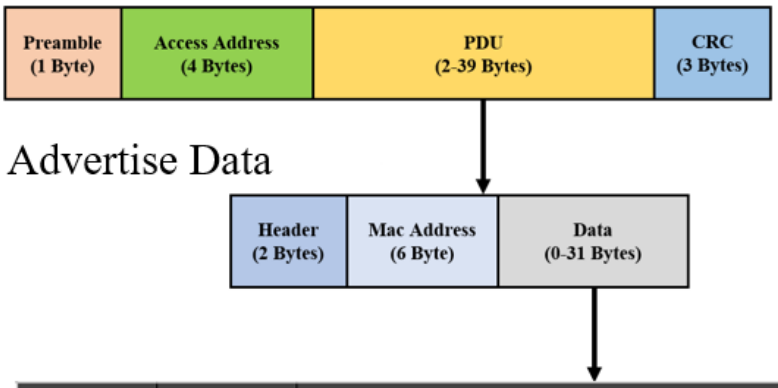
1.2.6 จำนวนแคลลอรี่

1.2.7 ความเร่งแกน x, y และ z

1.2.8 อัตราการเต้นของหัว

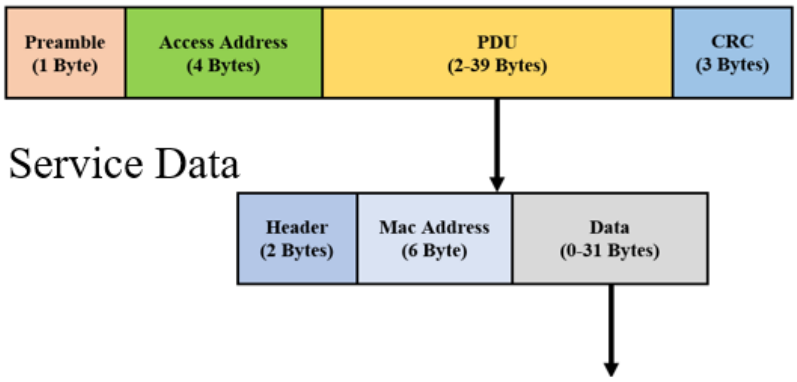
1.2.9 ปริมาณออกซิเจนในเลือด

1.2.10 อุณหภูมิของร่างกาย



Byte No.	Data Type	Define
0	Length	0x02
1	GAP Type	GAP_ADTYPE_FLAGS (0x01)
2	Data	0x06
3	Length of Data	0x1A(26)
4	GAP Type	0xFFGAP_ADTYPE_MANUFACTURER_SPECIFIC (0xFF)
5	Data	0x4C
6	Data	0x00
7	Data	0x02
8	Data	0x15
9	service UUIDs	0x4A
10	service UUIDs	0x03
11	service UUIDs	0x03
12	service UUIDs	0x99
13	service UUIDs	0x00
14	service UUIDs	0x00
15	service UUIDs	0x11
16	service UUIDs	0xA0
17	service UUIDs	0x01
18	service UUIDs	0x06
19	service UUIDs	0x00
20	service UUIDs	0x01
21	service UUIDs	0x02
22	service UUIDs	0x03
23	service UUIDs	0x04
24	service UUIDs	0x05
25	Data	Major Value[0]
26	Data	Major Value[1]
27	Data	Minor Value[0]
28	Data	Minor Value[1]
29	Data	0xC6

ภาพที่ 3-17 โครงสร้างข้อมูล Advertise data ของ BLE



Byte No.	Data Type	Define
0	Length of name	0x03
1	GAP Type	GAP_ADTYPE_LOCAL_NAME_COMPLETE (0x09)
2	Name	'A'
3	Name	1'
4	Length of Data	0x1A(26)
5	GAP Type	GAP_ADTYPE_SERVICE_DATA (0x16)
6	Data	0x00
7	Data	Data Value[0]
8	Data	Data Value[1]
9	Data	Data Value[2]
10	Data	Data Value[3]
11	Data	Data Value[4]
12	Data	Data Value[5]
13	Data	Data Value[6]
14	Data	Data Value[7]
15	Data	Data Value[8]
16	Data	Data Value[9]
17	Data	Data Value[10]
18	Data	Data Value[11]
19	Data	Data Value[12]
20	Data	Data Value[13]
21	Data	Random[0]
22	Data	Random[1]
23	Data	Empty (0x00)
24	Data	Empty (0x00)
25	Data	Empty (0x00)
26	Data	Empty (0x00)
27	Data	Empty (0x00)
28	Data	Empty (0x00)
29	Data	Empty (0x00)
30	Data	Empty (0x00)

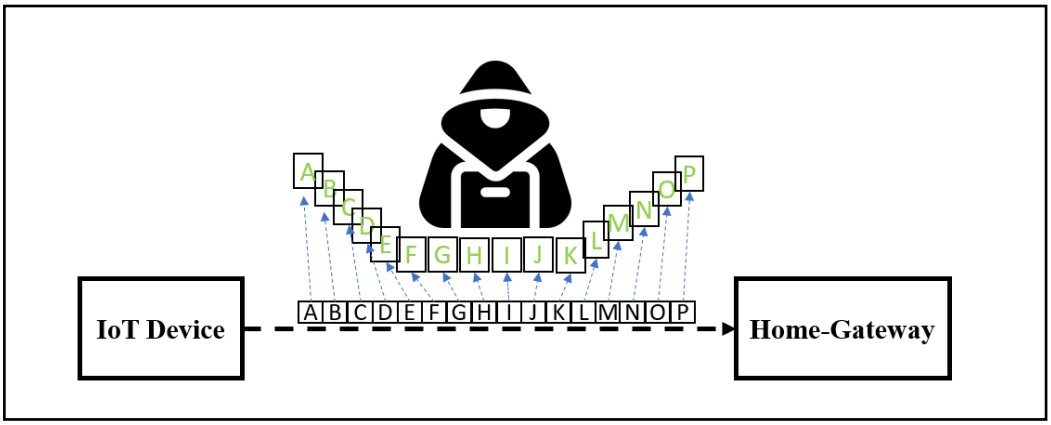
ภาพที่ 3-18 โครงสร้างแบบข้อมูล Service data ของ BLE

จากภาพที่ 3-17 และภาพที่ 3-18 เป็นส่วนหนึ่งของรูปแบบข้อมูล BLE ที่ปล่อยออกมา ได้แก่ ส่วนของ Advertise data และส่วนของ Service data โดยส่วนที่จะถูกพัฒนาให้มีความปลอดภัยของข้อมูล คือ ส่วนของ Service data ซึ่งในงานวิจัยจะทำการส่งข้อมูลและเข้ารหัส AES แบบ Electronic codebook (ECB) ขนาด 16 ไบต์ จากภาพที่ 3-18 จะเห็นได้จากไบต์ที่ 7 ถึง

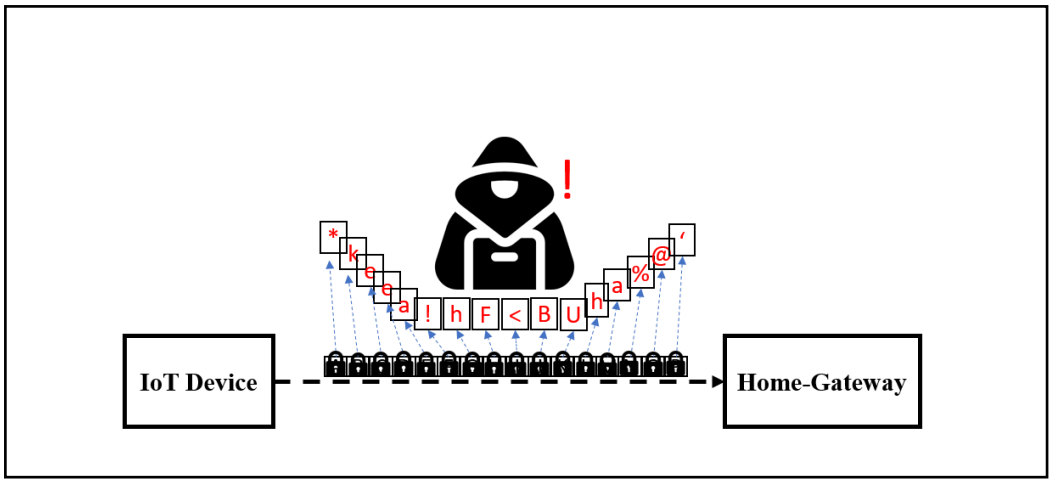
ไบต์ที่ 22 ขนาด 16 ไบต์จะใช้ในการใส่ข้อมูลที่จะส่งจากอุปกรณ์ไอโอทีส่วนบุคคลไปยังเกตเวย์ ซึ่งส่วนนี้จะถูกเข้ารหัสลับ

2. การออกแบบกระบวนสร้างการความปลอดภัยของอุปกรณ์ไอโอทีส่วนบุคคล

จากเดิมที่การส่งข้อมูลจากอุปกรณ์ไอโอทีส่วนบุคคลไปยังเกตเวย์ผ่านทาง BLE จะทำการกระจายส่งข้อมูลไปทางอากาศ เมื่อไม่มีการเข้ารหัสลับ แน่นอนว่าผู้ไม่หวังดีจากภาพที่ 3-19 สามารถที่จะล่วงรู้ข้อมูลของผู้ใช้งานได้ ซึ่งทำให้ผู้ใช้อุปกรณ์ไอโอทีส่วนบุคคลถูกล่วงละเมิดทางข้อมูล อาจจะทำให้เกิดผลเสียตามมาอีกมากมายในอนาคตได้ ดังนั้นระบบการใช้งานและการเชื่อมต่อข้อมูลระหว่างอุปกรณ์ไอโอทีไปยังเกตเวย์ จึงต้องมีมาตรฐานทางความปลอดภัย โดยการเข้ารหัสลับกับข้อมูลที่จะส่งไปจากอุปกรณ์ไอโอทีส่วนบุคคลไปยังเกตเวย์ ทำให้ผู้หวังดีไม่สามารถร่วงรู้ข้อมูลได้ ดังภาพที่ 3-20

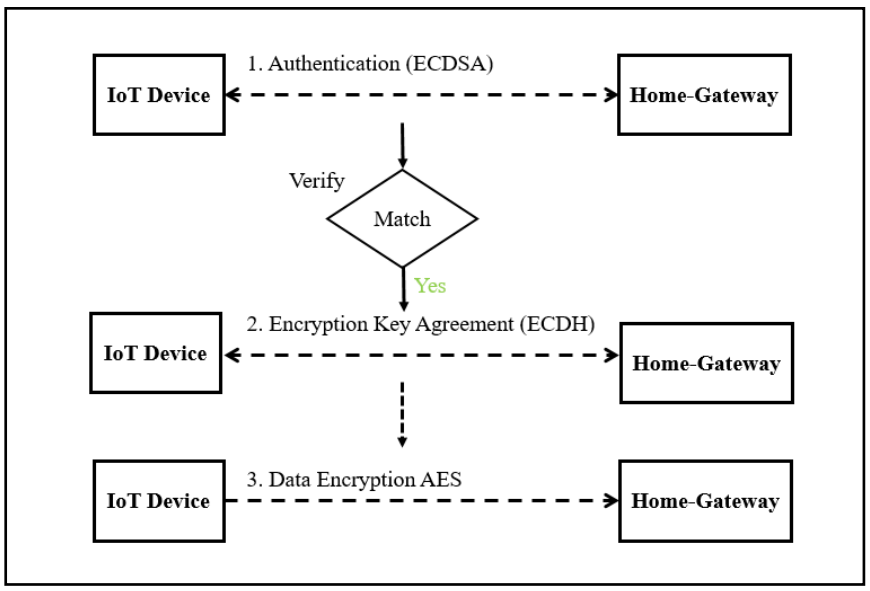


ภาพที่ 3-19 การส่งข้อมูลจากอุปกรณ์ไอโอทีส่วนบุคคลไปยังเกตเวย์โดยไม่ได้เข้ารหัสลับ



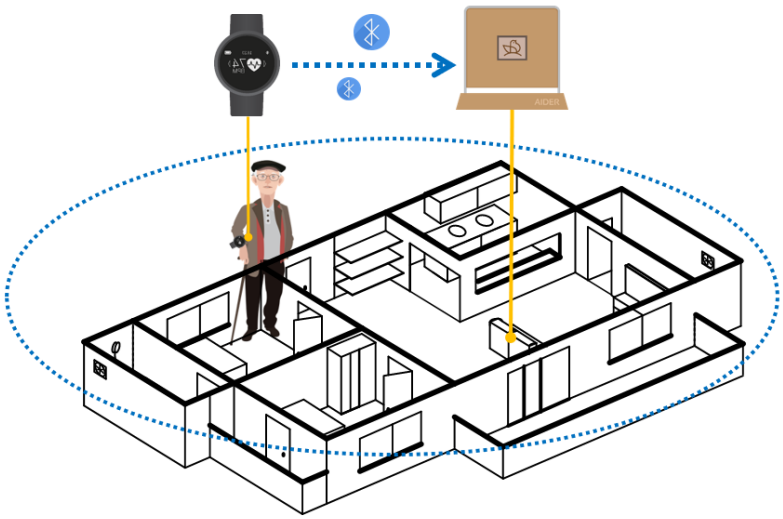
ภาพที่ 3-20 การส่งข้อมูลจากอุปกรณ์ไอโอทีส่วนบุคคลไปยังเกตเวย์โดยเข้ารหัสลับ

จากปัญหาของความไม่ปลอดภัยของของระบบและอุปกรณ์ไอโอที ในงานวิจัยจึงเพิ่มความปลอดภัยให้กับอุปกรณ์ไอโอทีส่วนบุคคลได้ 4 ส่วนหลัก ๆ ได้แก่ การออกแบบกระบวนการระบุตัวตน (Authentication) การออกแบบกระบวนการแลกรหัสลับ (Encryption key agreement) การออกแบบกระบวนการเข้ารหัสข้อมูลแบบ AES และการเพิ่มความปลอดภัยการเข้ารหัสข้อมูล ตามภาพที่ 3-21



ภาพที่ 3-21 การออกแบบกระบวนการสร้างความปลอดภัยของอุปกรณ์ไอโอทีส่วนบุคคล

จากภาพที่ 3-21 คือ กระบวนการสร้างความปลอดภัยของอุปกรณ์ไอโอทีส่วนบุคคล เพื่อให้เห็นตัวอย่างการใช้งาน จากภาพที่ 3-22 คือ ตัวอย่างการติดตั้งใช้งานจริง เมื่อเปิดระบบขึ้นมากครั้งแรก เกตเวย์จะทำการเชื่อมต่อกับอุปกรณ์ Aider A2 ด้วยการเชื่อมต่อแบบการจับคู่ (Paring) เมื่อจับคู่สำเร็จก็จะทำกระบวนการระบุตัวตน (Authentication) เพื่อเป็นตรวจสอบว่าอุปกรณ์เป็นตัวจริงไม่ใช่ตัวปลอม เมื่อตรวจสอบว่าเป็นตัวจริงแล้วก็จะทำกระบวนการแลกกุญแจรหัสลับซึ่งทั้งเกตเวย์และอุปกรณ์จะได้กุญแจรหัสลับชั่วคราวจากกระบวนการนี้ และต่อจากนั้นเกตเวย์ก็จะใช้กุญแจรหัสลับชั่วคราวที่ได้มาเข้ารหัส AES ของข้อมูลที่จะส่งไปให้กับอุปกรณ์ โดยข้อมูลในครั้งแรกที่เข้ารหัส AES จะใช้เป็นกุญแจรหัสลับของระบบ จากนั้นก็ส่งกลับไปให้อุปกรณ์ เมื่อสิ้นสุดขั้นตอนเกตเวย์จะตัดการเชื่อมต่อกับอุปกรณ์ ต่อจากนั้นทุกครั้งที่อุปกรณ์จะส่งข้อมูลบีคอนมาให้เกตเวย์ อุปกรณ์จะต้องเข้ารหัสลับด้วยกุญแจรหัสลับมาให้กับเกตเวย์เสมอ



ภาพที่ 3-22 การใช้งานอุปกรณ์ไอโอทีส่วนบุคคลภายในบ้าน

ดังนั้นการทำงานของระบบกระบวนการสร้างความปลอดภัยของอุปกรณ์ไอโอทีส่วนบุคคล สามารถสรุปเป็นขั้นตอนดังนี้

ขั้นตอนที่ 1 ในขั้นตอนการผลิต อุปกรณ์ไอโอทีส่วนบุคคลทุกรูปแบบจะต้องถูกเขียนใบรับรอง (Write certificates) ของเจ้าของผลิตภัณฑ์อุปกรณ์ (Signer) และอุปกรณ์ (Device) ลงบนไอซี ATECC508 ซึ่งระบบสามารถสร้างกุญแจส่วนตัว (Private Key_{ECC}) ให้กับไอซี หรือให้ไอซีสร้างเองก็ได้ ซึ่งจะอยู่ในกระบวนสร้างใบรับรองก่อนเขียนลงไปในไอซี จากนั้นก็จะทำ

การล็อกข้อมูลใบรับรองในสล็อตข้อมูลขนาด 64 ไบต์

ขั้นตอนที่ 2 อุปกรณ์ที่ใช้จะต้องถูกลงทะเบียนเข้าสู่ระบบผ่านทางหน้าเว็ป ซึ่งระบบจะมีใบรับรอง (Certificates) ของไอซี ATECC508 ผูกกับหมายเลขของอุปกรณ์ รวมถึงการกำหนดกุญแจกลาง ($Key_{AES\ Share}$) ของการเข้ารหัส AES ที่จะใช้กับเกตเวย์และอุปกรณ์ไอโอทีส่วนบุคคลของบ้านแต่หลัง

ขั้นตอนที่ 3 เมื่อติดตั้งเกตเวย์เสร็จเรียบร้อยแล้ว ผู้ใช้นำอุปกรณ์เข้ามาใกล้บริเวณเกตเวย์เพื่อให้เกตเวย์ตรวจสอบว่ามีอุปกรณ์นี้มีการลงทะเบียนนี้หรือไม่ ถ้ายังไม่มีเกตเวย์จะทำการเข้าสู่กระบวนการให้ระบุตัวตน (Authentication) ระหว่างอุปกรณ์กับเกตเวย์ด้วยกระบวนการ ECDSA โดยที่เกตเวย์จะทำการเชื่อมต่อเข้าไปยังอุปกรณ์ผ่าน BLE Connect เพื่อทำการเชื่อมต่อแบบจับคู่ (Bluetooth pairing)

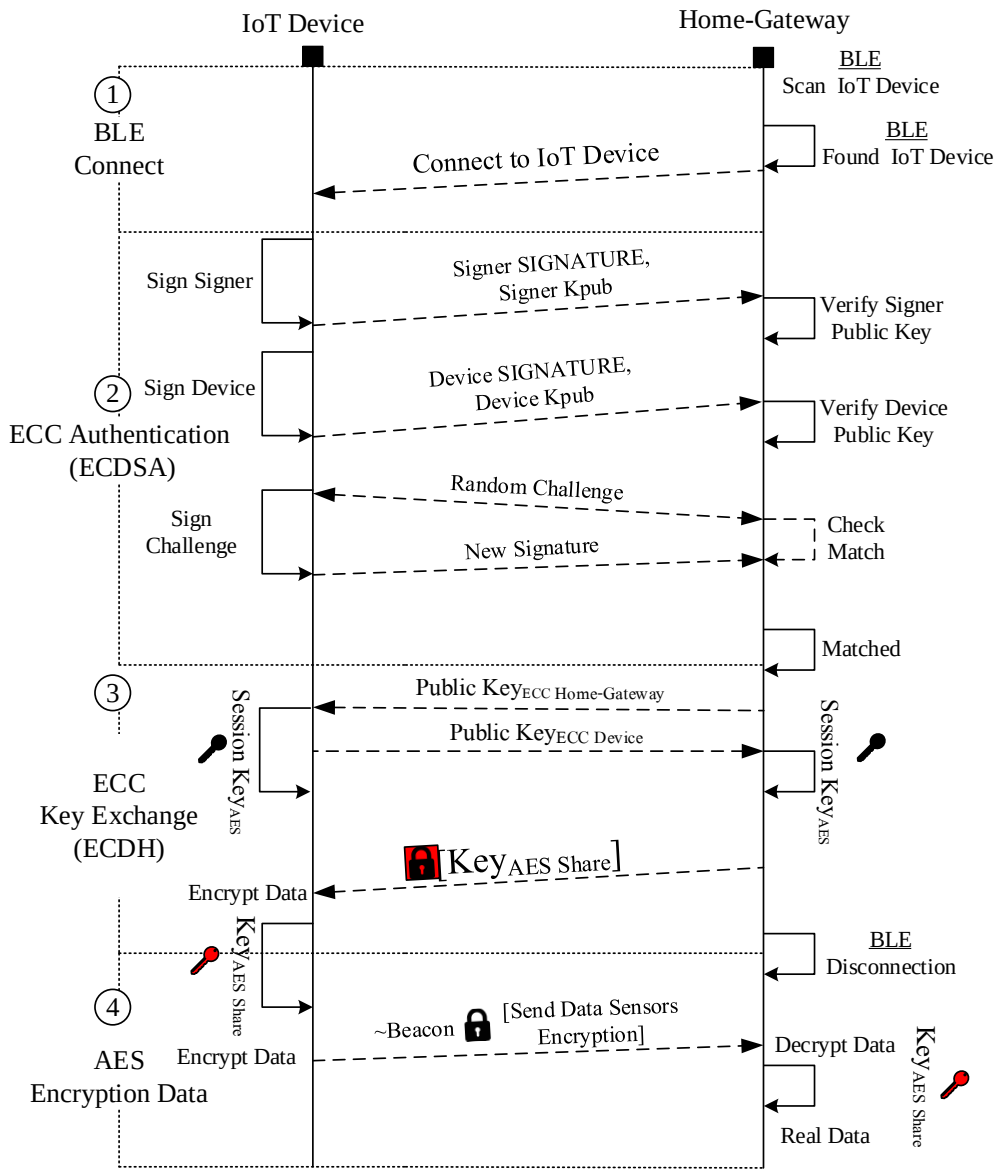
ขั้นตอนที่ 4 เมื่อเกตเวย์ตรวจสอบแล้วว่าอุปกรณ์มีตัวตนถูกต้อง เกตเวย์จะยอมรับการรับข้อมูลจากอุปกรณ์

ขั้นตอนที่ 5 เกตเวย์จะทำกระบวนการแลกเปลี่ยนกุญแจกลาง ($Session\ Key_{AES}$) ของการเข้ารหัส AES กับอุปกรณ์ โดยการแลกเปลี่ยนกุญแจสาธารณะ ($Public\ Key_{ECC}$) ซึ่งกันและกัน จากนั้นทั้งเกตเวย์และอุปกรณ์จะทำการนำกุญแจสาธารณะที่ได้มาเข้ากระบวนการเข้ารหัสแลกกุญแจรหัสลับข้อมูล (Encryption key agreement) ของตัวเอง จะได้กุญแจ ($Session\ Key_{AES}$) ของ AES ออกมา

ขั้นตอนที่ 6 เมื่อทั้งเกตเวย์และอุปกรณ์ได้กุญแจ ($Session\ Key_{AES}$) ของ AES มาจากนั้นเกตเวย์จะเข้ารหัสกุญแจของระบบ ($Key_{AES\ Share}$) ด้วยกุญแจ ($Session\ Key_{AES}$) ของ AES มายังอุปกรณ์ ซึ่งอุปกรณ์เมื่อถอดรหัสแล้วจะได้กุญแจของระบบ อุปกรณ์จะยึดถือกุญแจระบบ ($Key_{AES\ Share}$) เป็นกุญแจรหัสลับกลางในการส่งข้อมูลเข้ารหัส AES มายังเกตเวย์

ขั้นตอนที่ 7 เมื่ออุปกรณ์ไอโอทีส่วนบุคคลได้อ่านข้อมูลหรือได้รับข้อมูลฉุกเฉินก็เข้ารหัสข้อมูลแบบ AES ด้วยกุญแจระบบ ($Key_{AES\ Share}$) มายังเกตเวย์

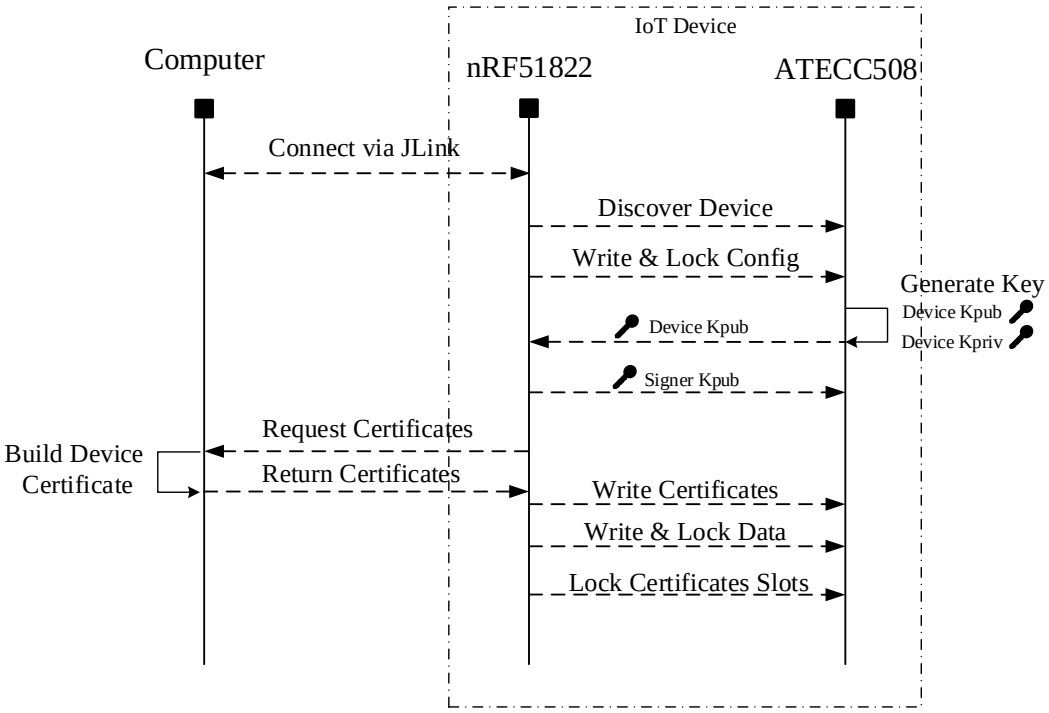
กระบวนการระบุตัวตน (Authentication) ตั้งแต่ขั้นตอนที่ 3 ถึงขั้นตอนที่ 7 สามารถสรุปได้จากภาพที่ 3-23 ดังนี้



ภาพที่ 3-23 แผนภาพการออกแบบการติดต่อสื่อสารระหว่างอุปกรณ์กับเกตเวย์

2.1 การออกแบบกระบวนการระบุตัวตน (Authentication)

2.1.1 การจัดเตรียม (Provisioning) ไอซี ATECC508



ภาพที่ 3-24 แผนภาพขั้นตอนการออกแบบการจัดเตรียม (Provisioning) ไอซี ATECC508

จากภาพที่ 3-24 แสดงขั้นตอนการจัดเตรียมให้ไอซี ATECC508 ในอุปกรณ์ไอโอทีส่วนบุคคล เพื่อเตรียมพร้อมต่อการใช้งาน ซึ่งเป็นการตั้งค่าเริ่มต้นการใช้งานและการเก็บข้อมูลที่สำคัญลงไปยังไอซี ATECC508 จะประกอบไปด้วยขั้นตอนดังนี้

ขั้นตอนที่ 1 ฝั่งคอมพิวเตอร์ (Computer) เชื่อมต่อเข้ามายังอุปกรณ์ไอโอทีส่วนบุคคลผ่านทางดีบัคเกอร์ JLink เพื่อติดต่อสื่อสารกับชิป nRF51822 ซึ่งเป็นไมโครคอนโทรเลอร์หลักในการทำงาน จากนั้นไมโครคอนโทรเลอร์จะทำการค้นหาไอซี ATECC508 ที่อยู่ในบอร์ดวงจร เมื่อพบแล้ว อุปกรณ์จะสั่งงานไปยังไอซี ATECC508 เพื่อทำการตั้งค่าในส่วนของ Configure data และทำการล๊อคโซน (Lock zone) ได้แก่ ตั้งค่า Configure zone ตั้งค่า Data zone และตั้งค่า OTP Zone

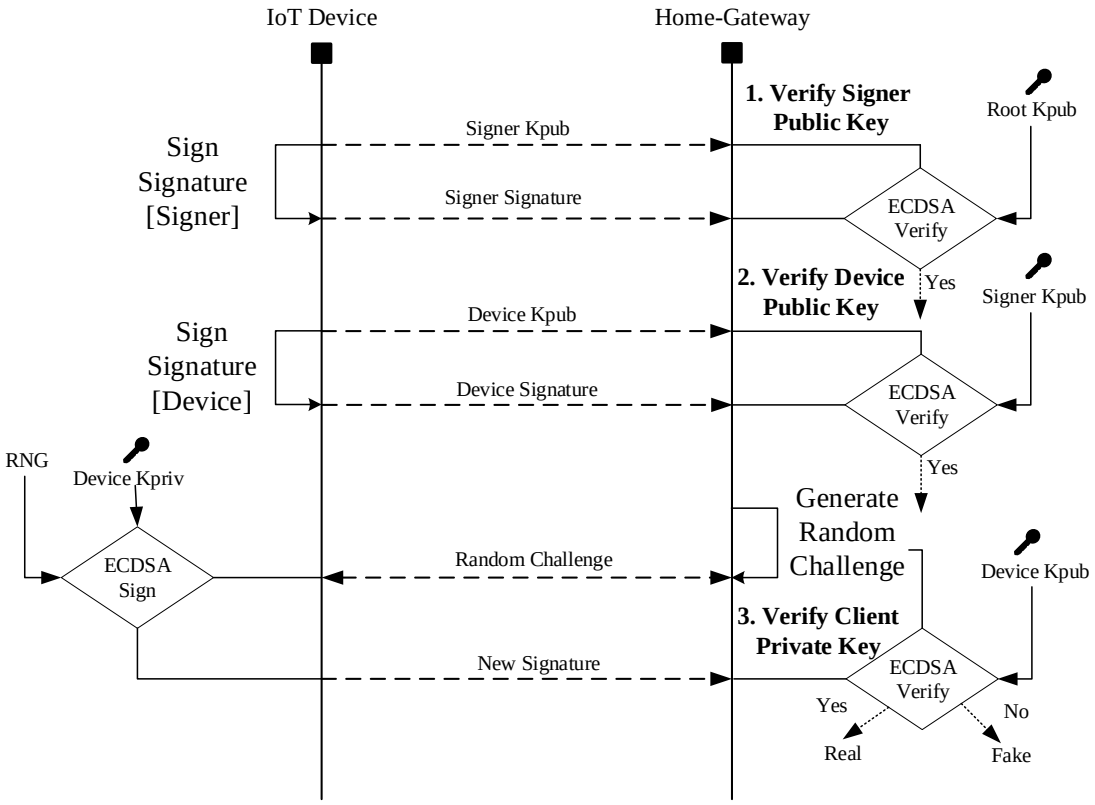
ขั้นตอนที่ 2 ฝั่งอุปกรณ์และฝั่งคอมพิวเตอร์ทำการแลกเปลี่ยนกุญแจสาธารณะ (Public Key_{ECC}) ซึ่งกันและกัน

ขั้นตอนที่ 3 อุปกรณ์ทำการขอใบรับรอง (Request certificates) จากฝั่งของคอมพิวเตอร์ ฝั่งคอมพิวเตอร์จะทำตัวเป็นคนออกใบรับรอง CA (Certification authority) ที่ทำหน้าที่ออกใบ

รับรองจากนั้นฝั่งคอมพิวเตอร์จะส่งมาให้กับอุปกรณ์

ขั้นตอนที่ 4 อุปกรณ์สั่งงานไปยังไอซี ATECC508 ให้เขียนข้อมูลใบรับรอง (Certificates) ที่ได้มาขนาด 72 ไบต์ลงไปในฐานเก็บข้อมูลของไอซี (Data storage) เพื่อให้ในขั้นตอนการระบุตัวตน (Authentication) ต่อไป แล้วจากนั้นให้ทำการล็อคสล๊อต (Lock certificate slots)

2.1.2 การออกแบบการทำงานของการระบุตัวตน (Authentication)



ภาพที่ 3-25 แผนภาพขั้นตอนการทำงานของ ECC Authentication

จากภาพที่ 3-25 เมื่ออุปกรณ์ไอโอทีส่วนบุคล เข้าสู่กระบวนการระบุตัวตน (Authentication) กับเกตเวย์จะประกอบด้วย 3 ขั้นตอนดังนี้

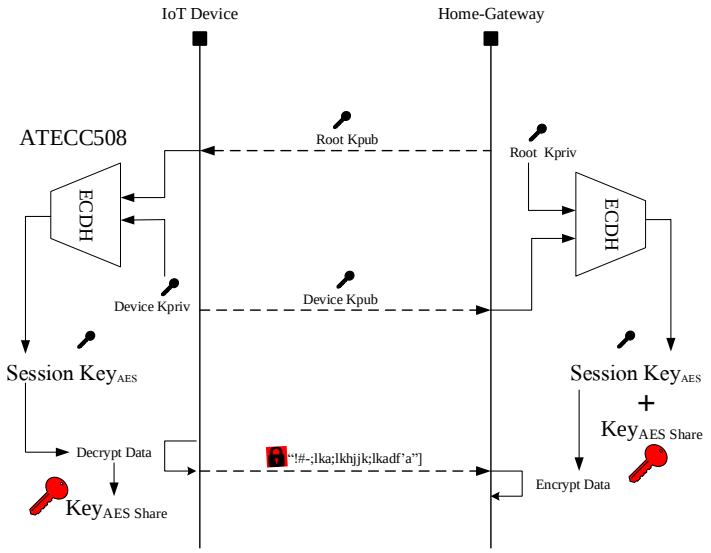
ขั้นตอนที่ 1 การตรวจสอบเจ้าของผลิตภัณฑ์อุปกรณ์ (Verify signer) อุปกรณ์จะทำการรับรอง (Sign) ใบรับรอง Signer certificates ที่ถูกเก็บไว้ในฐานเก็บข้อมูลของไอซี ATECC508 จากนั้นจะส่ง Signer signature ขนาด 64 ไบต์ และกุญแจสาธารณะ Signer Kpub ไปยังเกตเวย์

จากนั้นเกตเวย์จะทำการตรวจสอบด้วยกระบวนการ ECDSA ว่าถูกต้องหรือไม่ ถ้าถูกต้องให้ไปต่อได้ในขั้นตอนที่ 2

ขั้นตอนที่ 2 การตรวจสอบอุปกรณ์ (Verify device) อุปกรณ์จะทำการรับรอง (Sign) ใบรับรอง Device certificates ที่ถูกเก็บไว้ในฐานเก็บข้อมูลของไอซี ATECC508 จากนั้นจะส่ง Device signature ขนาด 64 ไบต์ และกุญแจสาธารณะ Device Kpub ไปยังเกตเวย์ จากนั้นเกตเวย์จะทำการตรวจสอบด้วยกระบวนการ ECDSA ว่าถูกต้องหรือไม่ ถ้าถูกต้องให้ไปต่อได้ในขั้นตอนที่ 3

ขั้นตอนที่ 3 การตรวจสอบ Random challenge หรือข้อความลับที่กำหนดขึ้น (Challenge message) ในกรณีนี้สามารถตั้งใหม่ได้ในโปรแกรมไม่ต้องบันทึกไว้ในหน่วยความจำเหมือน Signer signature และ Device signature แม้ว่าจะมาจากการผลิตล็อตเดียวกัน แต่เมื่อต้องการใช้งานในโครงการที่ไม่เหมือนกันสามารถกำหนด Random challenge ใหม่ได้ โดยจะทำการกำหนดจากฝั่งเกตเวย์แล้วส่งมายังฝั่งอุปกรณ์ เมื่อฝั่งอุปกรณ์ได้รับข้อความลับ อุปกรณ์จะทำการรับรอง (Sign) ด้วยกุญแจส่วนตัวของตัวเอง (Private key) นั่นคือ Device Kpriv และค่า Random number generator (RNG) จนได้ข้อมูล New signature ออกมา จากนั้นอุปกรณ์จะส่งข้อมูลไปให้เกตเวย์ เกตเวย์จะใช้ Challenge message, Device Kpub และ New signature มาเข้ากระบวนการ ECDSA ว่าถูกต้องหรือไม่ ถ้าถูกต้องแสดงว่าอุปกรณ์ไอโอทีส่วนบุคคลนี้เป็นตัวจริง

2.2 การออกแบบกระบวนการแลกรหัสลับ (Encryption key agreement)

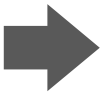


ภาพที่ 3-26 แผนภาพขั้นตอนการทำงานของ ECC Encryption key agreement

จากภาพที่ 3-26 เมื่ออุปกรณ์ไอโอทีส่วนบุคคลต้องการกุญแจ ($Key_{AES\ share}$) ของการเข้ารหัส AES จากเกตเวย์ อุปกรณ์จะทำการส่งกุญแจสาธารณะ Device Kpub ไปยังเกตเวย์ และในเวลาเดียวกันเกตเวย์ก็จะให้กุญแจสาธารณะ Root Kpub มายังอุปกรณ์ จากนั้นทั้งเกตเวย์และอุปกรณ์จะต่างคนต่างเข้ากระบวนการแลกกุญแจรหัสลับข้อมูล (Encryption key agreement) ด้วยกุญแจส่วนตัว (Private Key_{ECC}) ของตัวเอง Root Kpriv และ Device Kpriv หลังจากนั้นเกตเวย์และอุปกรณ์จะได้กุญแจ (Session Key_{AES}) หรือกุญแจ AES ชั่วคราวมา ต่อจากนั้นเกตเวย์จะใช้กุญแจ (Session Key_{AES}) มาเข้ารหัส AES กับข้อมูลที่เป็นกุญแจ ($Key_{AES\ share}$) เพื่อส่งมาให้กับอุปกรณ์ สุดท้ายเมื่ออุปกรณ์ถอดรหัสจากกุญแจ (Session Key_{AES}) จะได้ข้อมูลที่เป็นกุญแจ ($Key_{AES\ share}$) โดยอุปกรณ์จะกำหนดให้ตัวเองใช้กุญแจรหัสลับอันใหม่นี้เป็นกุญแจ AES อันใหม่ เพื่อใช้ในการส่งข้อมูลเข้ารหัส AES ในครั้งต่อไป

2.3 การออกแบบกระบวนการเข้ารหัสข้อมูลแบบ AES หลังจากกระบวนการแลกกุญแจรหัสลับสำเร็จ อุปกรณ์ไอโอทีส่วนบุคคลจะได้รับกุญแจ ($Key_{AES\ share}$) เพื่อไว้ใช้ในการเข้ารหัส AES เมื่ออุปกรณ์ได้ต้องการจะส่งข้อมูลไปยังเกตเวย์ อุปกรณ์จะทำการเข้ารหัส เมื่อเข้ารหัสสำเร็จก็ได้ข้อมูลที่เข้ารหัสขนาด 16 ไบต์ ก็จะถูกนำไปใส่ในตำแหน่งเดิมของข้อมูล BLE ดังภาพที่ 3-27 จากนั้นก็อัพเดทข้อมูลเพื่อให้ส่งสัญญาณกระจายข้อมูลผ่านอากาศไปยังเกตเวย์ต่อไป เมื่อเกตเวย์ได้รับข้อมูลที่เข้ารหัส มันก็จะทำการถอดรหัสด้วย ($Key_{AES\ share}$) เมื่อถอดรหัสสำเร็จเกตเวย์ก็จะส่งข้อมูลต่อไปยังเซิร์ฟเวอร์ต่อไป

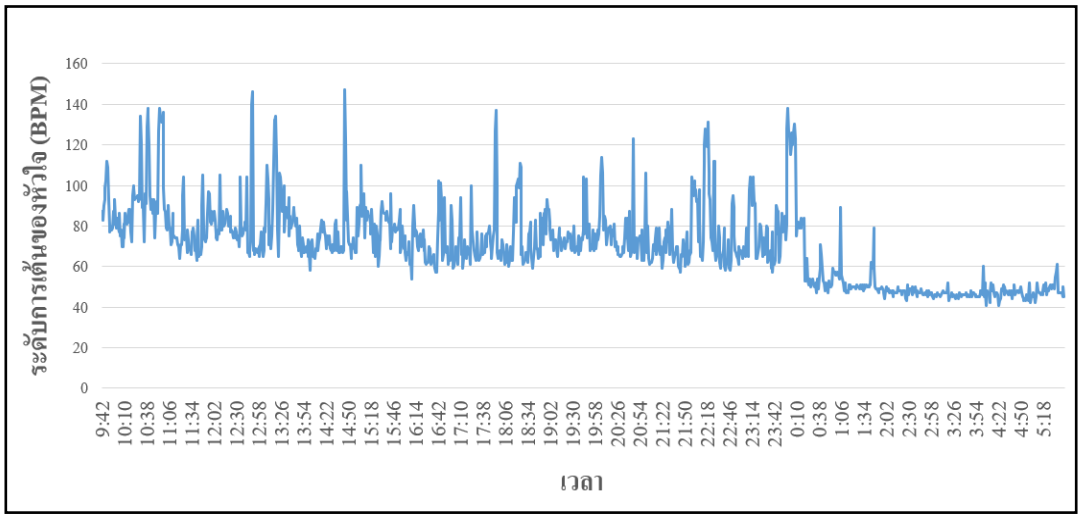
Byte No.	Data Type	Define
0	Length of name	0x03
1	GAP Type	GAP_ADTYPE_LOCAL_NAME_COMPLETE (0x09)
2	Name	'A'
3	Name	'1'
4	Length of Data	0x1A(26)
5	GAP Type	GAP_ADTYPE_SERVICE_DATA (0x16)
6	Data	0x00
7	Data	Data Value[0]
8	Data	Data Value[1]
9	Data	Data Value[2]
10	Data	Data Value[3]
11	Data	Data Value[4]
12	Data	Data Value[5]
13	Data	Data Value[6]
14	Data	Data Value[7]
15	Data	Data Value[8]
16	Data	Data Value[9]
17	Data	Data Value[10]
18	Data	Data Value[11]
19	Data	Data Value[12]
20	Data	Data Value[13]
21	Data	Random[0]
22	Data	Random[1]
23	Data	Empty (0x00)
24	Data	Empty (0x00)
25	Data	Empty (0x00)
26	Data	Empty (0x00)
27	Data	Empty (0x00)
28	Data	Empty (0x00)
29	Data	Empty (0x00)
30	Data	Empty (0x00)



Byte No.	Data Type	Define
0	Length of name	0x03
1	GAP Type	GAP_ADTYPE_LOCAL_NAME_COMPLETE (0x09)
2	Name	'A'
3	Name	'1'
4	Length of Data	0x1A(26)
5	GAP Type	GAP_ADTYPE_SERVICE_DATA (0x16)
6	Data	0x00
7	Data	Encrypt Data
8	Data	
9	Data	
10	Data	
11	Data	
12	Data	
13	Data	
14	Data	
15	Data	
16	Data	
17	Data	
18	Data	
19	Data	
20	Data	
21	Data	
22	Data	
23	Data	Empty (0x00)
24	Data	Empty (0x00)
25	Data	Empty (0x00)
26	Data	Empty (0x00)
27	Data	Empty (0x00)
28	Data	Empty (0x00)
29	Data	Empty (0x00)
30	Data	Empty (0x00)

ภาพที่ 3-27 ตำแหน่งของข้อมูลที่ถูกเข้ารหัส

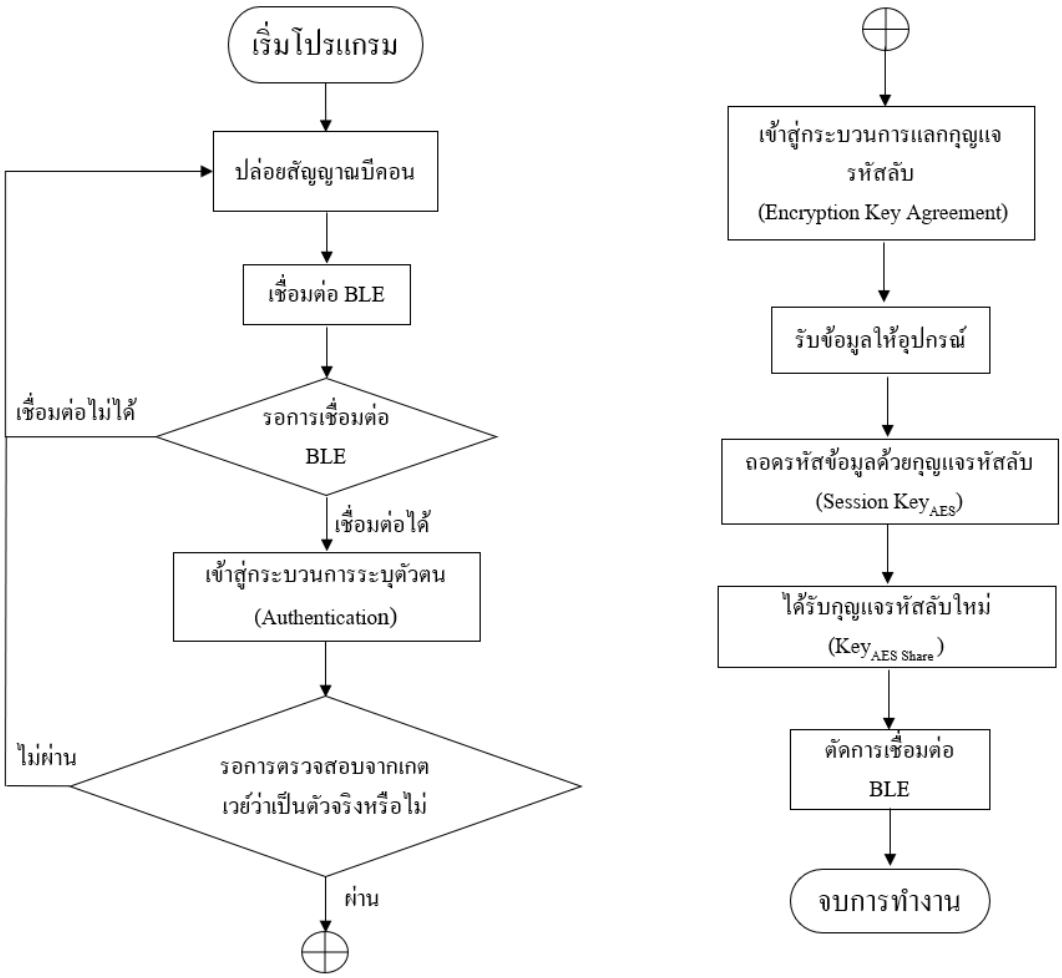
2.4 การเพิ่มความปลอดภัยของการเข้ารหัสข้อมูล จากปัญหาข้อมูลของอุปกรณ์ไอโอทีมีการเปลี่ยนแปลงน้อยหรือผู้ดักขโมยข้อมูล สามารถรู้ข้อมูลได้ อาจจะรู้จากการอ่านค่าที่หน้าจอของอุปกรณ์สวมใส่นั้น จึงอาจจะทำให้ถูกเดารหัสลับได้ง่าย ตัวอย่างเช่น อ่านค่าการเต้นของหัวใจได้ค่าเดิม ๆ ซ้ำ ๆ ของผู้ใช้ ซึ่งทำให้ค่าเซนเซอร์ที่เข้ารหัสถูกดักขโมย จนสามารถเดากลับจนเจอกุญแจรหัสลับได้ เพราะผู้ดักขโมยสามารถจับรูปแบบของข้อมูลได้ จึงต้องมีการเพิ่มเทคนิคการเข้ารูปแบบข้อมูล (Data encoding) ก่อนที่จะทำการเข้ารหัสข้อมูล AES โดยจะใช้เทคนิค Huffman coding เพื่อหา Codding ใหม่ออกมาขนาด 2 ไบต์ ในงานวิจัยนี้จะหยิบยกตัวอย่างข้อมูลของอัตราการเต้นของหัวใจในเวลา 1 วัน ดังภาพที่ 3-28 เพื่อนำมาเป็นสถิติในการหาและสร้างตารางให้ได้ Huffman code ตามวิธีการหา Huffman coding เมื่อได้ Huffman code มาแล้ว ให้กำหนดลงในโปรแกรมทั้งสองฝั่งระหว่างอุปกรณ์สวมใส่กับเกตเวย์ เมื่ออุปกรณ์อ่านค่าเซนเซอร์ได้ให้ทำการเข้ารหัส (Encode) ด้วย Huffman code ตามจำนวนไบต์ของแพ็คเก็ต (Packet) จากนั้นให้ส่งไปให้เกตเวย์ เมื่อเกตเวย์ได้รับข้อมูล มันจะทำการถอดรหัส (Decode) ด้วย Huffman code เพื่อให้ได้ข้อมูลที่ถูกต้องออกมา



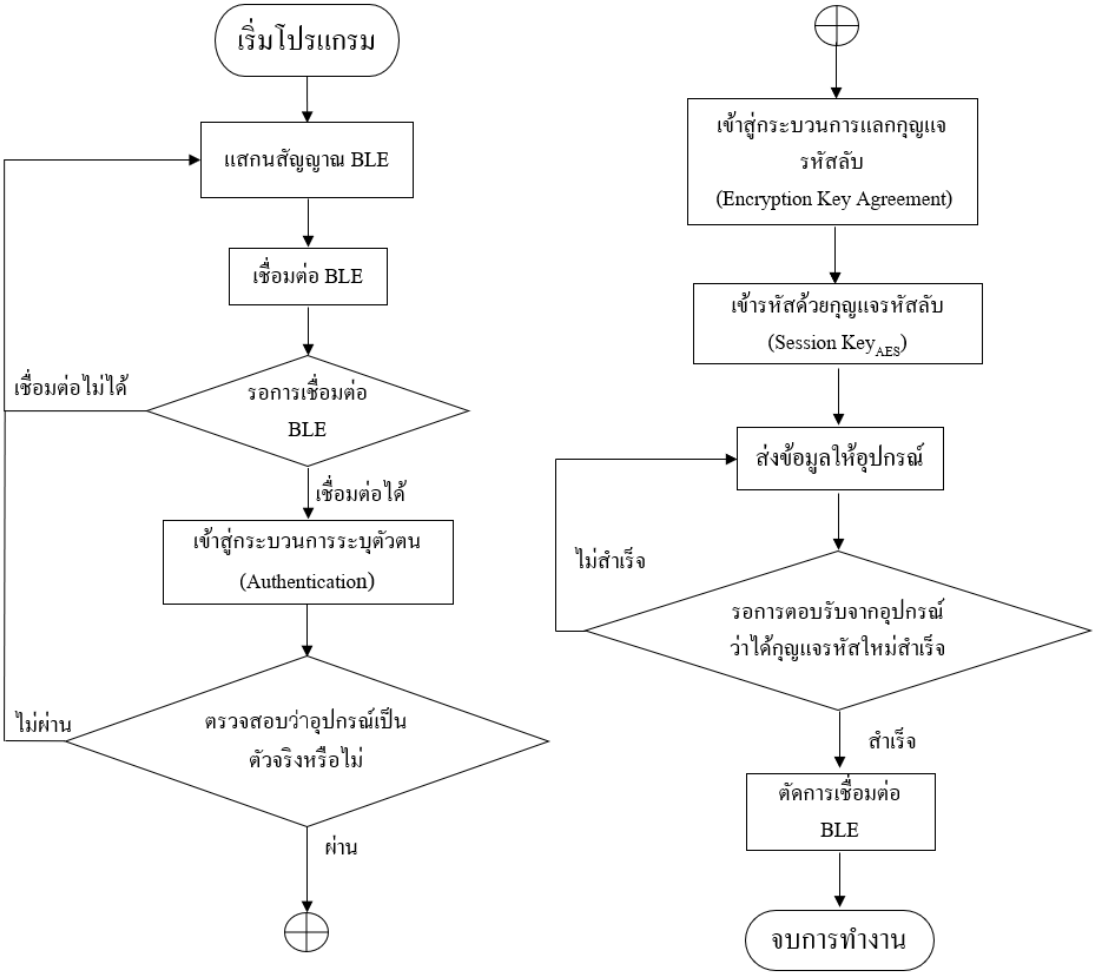
ภาพที่ 3-28 กราฟแสดงอัตราการเต้นใน 1 วัน

3. การออกแบบกระบวนการทำงานของโปรแกรม

ในงานวิจัยนี้ใช้งานไอซีเข้ารหัสของบริษัท Atmel ในที่นี้จะไอซี ATECC508 โดยจะเป็นการระบุตัวตน (Authentication) ด้วยกระบวนการ Elliptic curve digital signature algorithm (ECDSA) ซึ่งกระบวนการนี้จะมีลักษณะการทำงานเหมือนการตรวจสอบตัวตนจากอีกฝั่งมายังอีกฝั่ง มีลักษณะคล้ายการตรวจสอบลายเซ็นต์ ซึ่งโปรแกรมการทำงานจะอยู่บนชิป nRF51822 ซึ่งเป็นไมโครคอนโทรเลอร์หลักในการทำงาน โดยจะมีกระบวนการโปรแกรมในหัวข้อที่ 2.1.2 ของกระบวนการระบุตัวตนในฝั่งอุปกรณ์สวมใส่ส่วนบุคคล ดังภาพที่ 3-29 และโปรแกรมของกระบวนการระบุตัวตนในฝั่งเกตเวย์ ดังภาพที่ 3-30

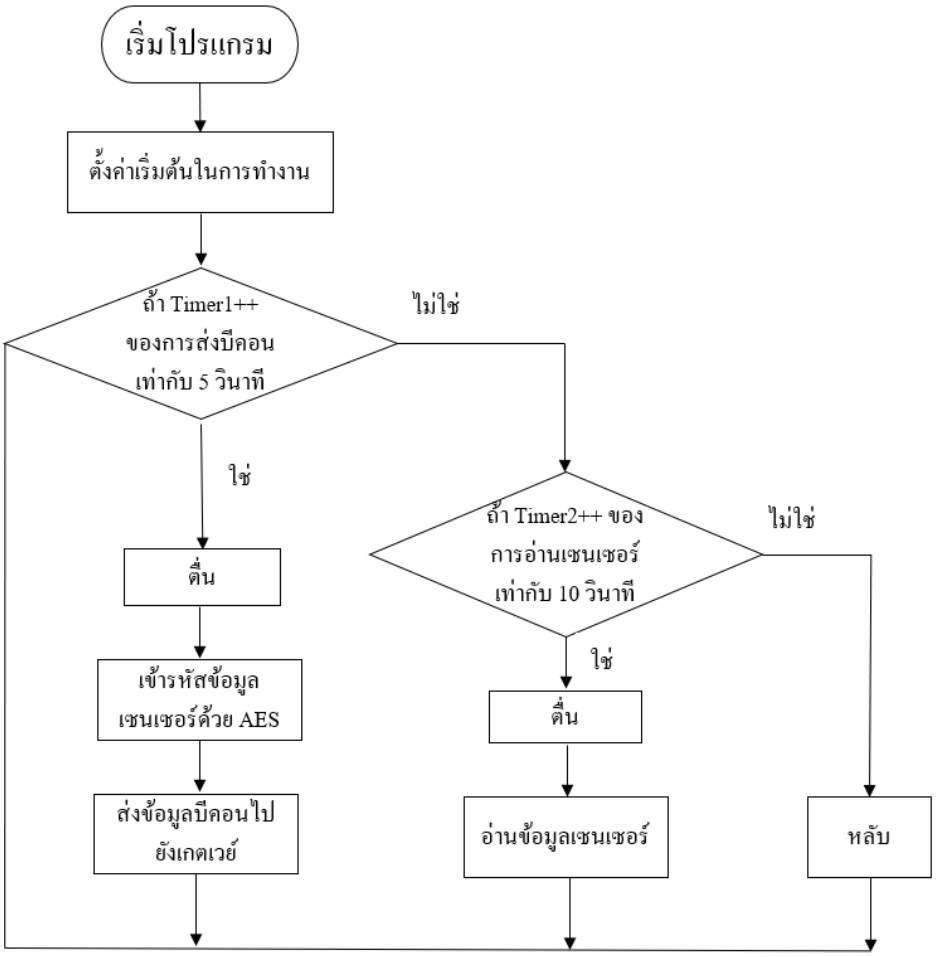


ภาพที่ 3-29 บล็อกไดอะแกรมของกระบวนการระบุตัวตนฝั่งอุปกรณ์สวมใส่ส่วนบุคคล

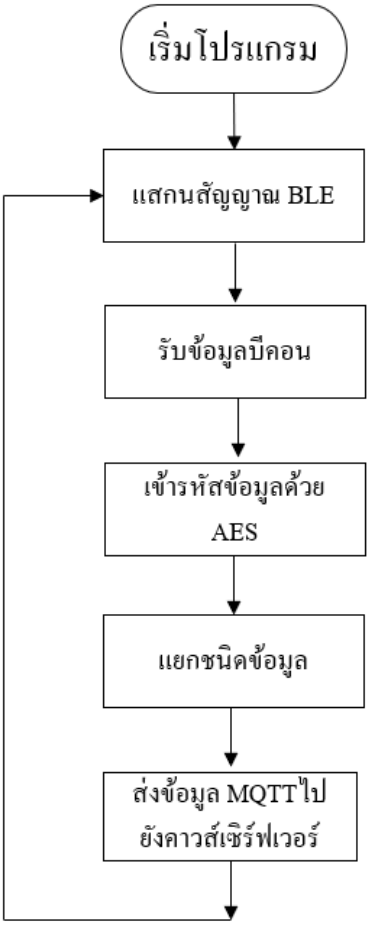


ภาพที่ 3-30 บล็อกไดอะแกรมของกระบวนการระบุตัวตนฝั่งเกตเวย์

กระบวนการโปรแกรมในหัวข้อที่ 2.3 ของการออกแบบกระบวนการเข้ารหัสข้อมูลแบบ AES ของอุปกรณ์ส่งไปให้เกตเวย์สามารถแสดงในภาพที่ 3-31 และโปรแกรมของกระบวนการเกตเวย์ในการรับและถอดข้อมูลการเข้ารหัส AES จากอุปกรณ์ ดังภาพที่ 3-32



ภาพที่ 3-31 บล็อกไดอะแกรมของกระบวนการส่งข้อมูลเข้ารหัส AES ของอุปกรณ์ส่งไปให้เกตเวย์



ภาพที่ 3-32 บล็อกไดอะแกรมของเกตเวย์ในการรับและถอดข้อมูลการเข้ารหัส AES จากอุปกรณ์

บทที่ 4
การทดสอบและวิเคราะห์ประสิทธิภาพ

ในบทความนี้จะกล่าวถึงวิธีการทดสอบและวิเคราะห์ประสิทธิภาพในการทำงานของระบบการระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพส่วนบุคคลสำหรับอุปกรณ์สวมใส่โดยใช้ไอซีเข้ารหัส โดยมีรายละเอียดดังนี้

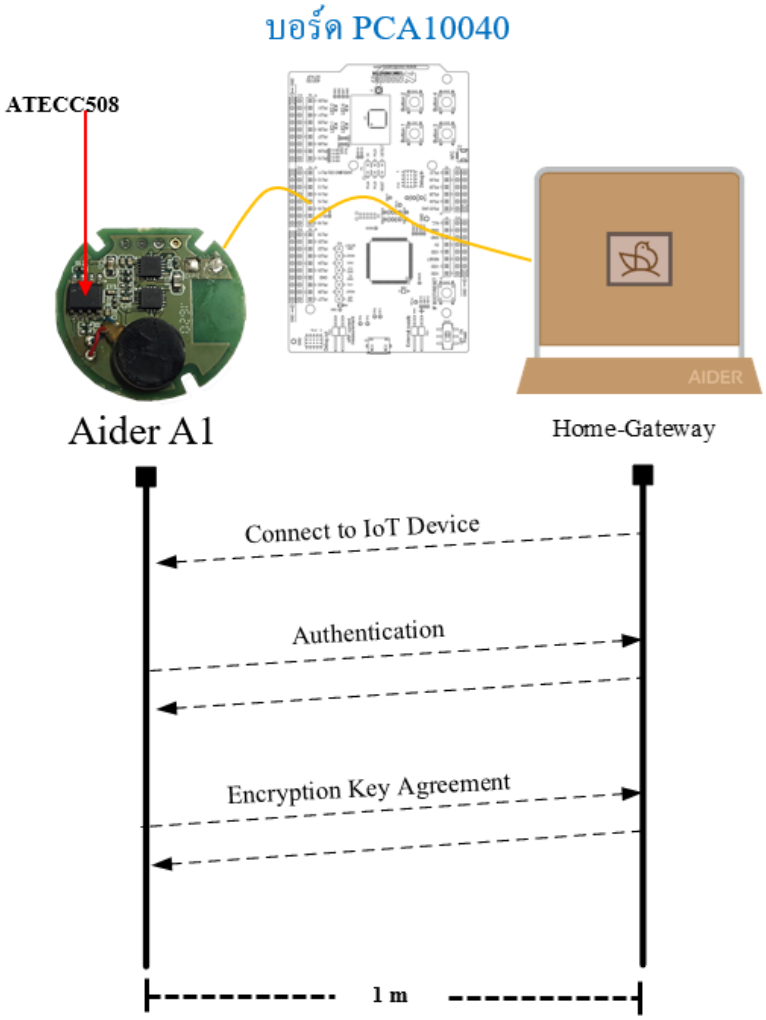
1. วิธีการทดสอบ
2. ผลการทดสอบ
3. การวิเคราะห์การเพิ่มความปลอดภัย

วิธีการทดสอบ

การทดสอบการทำงานประกอบไปด้วยการทดสอบในเรื่องของเวลาและเรื่องการใช้กระแสในการทำงานของขั้นตอนที่ต้องทำการเชื่อมต่อ BLE ระหว่างอุปกรณ์สวมใส่ส่วนบุคคลกับเกตเวย์ ได้แก่ การระบุตัวตน (Authentication) กับการแลกรหัสลับ (Encryption key agreement) และขั้นตอนการปล่อยบีคอน ที่อุปกรณ์สวมใส่ส่วนบุคคลต้องปล่อยบีคอนข้อมูลไปยังเกตเวย์ โดยในการทดสอบจะใช้อุปกรณ์สวมใส่ส่วนบุคคล Aider A1 ซึ่งมีส่วนการทำงานที่เหมือนกันกับอุปกรณ์สวมใส่ส่วนบุคคล Aider A2 ถูกกำหนดให้มีฟังก์ชันการทำงาน ได้แก่ การอ่านค่าเซนเซอร์วัดความเร่ง (Accelerometer) การเชื่อมต่อ BLE และการปล่อยบีคอน โดยวิธีการทดสอบจะถูกกำหนดได้ดังนี้

1. วิธีการทดสอบการทำงานของขั้นตอนการระบุตัวตนและการแลกรหัสลับ

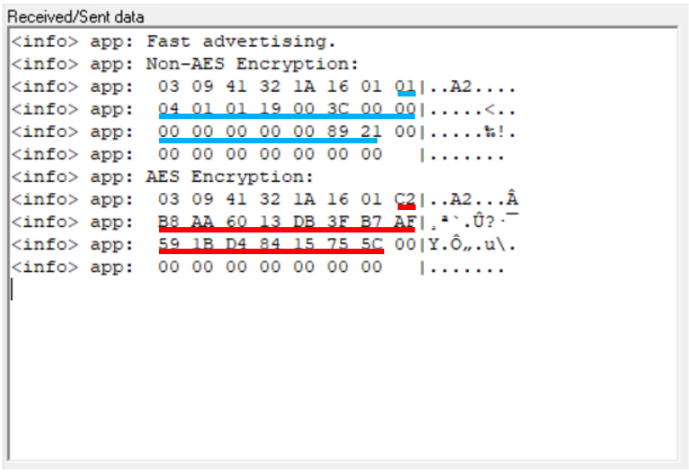
การทดสอบขั้นตอนการระบุตัวตนเป็นขั้นตอนของการระบุตัวตนและการแลกรหัสลับที่ต้องทำการเชื่อมต่อ BLE วิธีการทดสอบจะกำหนดให้เกตเวย์กับอุปกรณ์ Aider A1 ให้วางห่างกัน 1 เมตร และจากนั้นให้ทำการเชื่อมต่อ BLE แล้วทำตามขั้นตอนของการระบุตัวตนกับการแลกรหัสลับเป็นจำนวน 1,000 ครั้ง โดยเมื่อเสร็จกระบวนการแต่ละครั้งจะทำการตัดการเชื่อมต่อ BLE แล้วเริ่มทำการเชื่อมต่อ BLE ใหม่ทุกครั้งเมื่อเริ่มทำงานในครั้งต่อไป ซึ่งจะมีบอร์ด PCA10040 เป็นบอร์ดที่ใช้ในการจับเวลาของกระบวนการทำงาน ดังภาพที่ 4-1



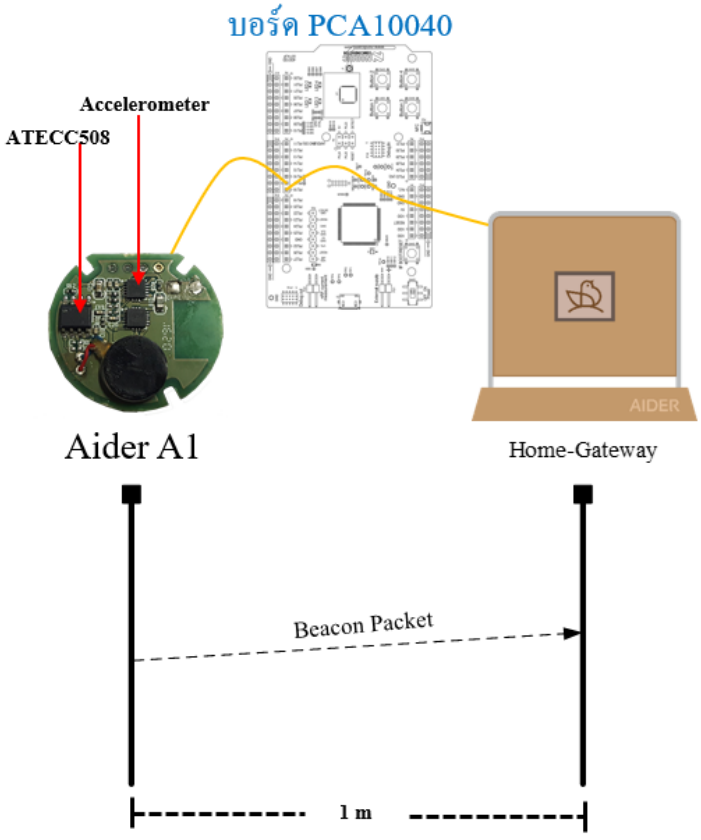
ภาพที่ 4-1 ไดอะแกรมของการทดสอบเวลาของการระบุตัวตนและการแลกรหัสลับ

2. วิธีการทดสอบทำการงานของการปล่อยบีคอน

การทดสอบการทำงานการปล่อยบีคอนของอุปกรณ์สวมใส่ส่วนบุคคล มีวิธีการทดสอบที่กำหนดให้เกตเวย์กับอุปกรณ์ Aider A1 ให้วางห่างกัน 1 เมตร แล้วให้อุปกรณ์ปล่อยบีคอนของข้อมูลการอ่านเซนเซอร์วัดความเร่ง (Accelerometer) เป็นจำนวน 10,000 แพ็คเก็ต ให้กับเกตเวย์ โดยในการทดสอบนี้จะทำการเทียบเวลาในการทำงานของข้อมูลบีคอนที่ไม่ได้เข้ารหัสกับข้อมูลที่เข้ารหัส ดังภาพที่ 4-2 ว่ามีการใช้เวลาในการทำงานต่างกันมากแค่ไหน โดยในการทดสอบจะใช้บอร์ด PCA10040 เป็นบอร์ดในการจับเวลาที่ใช้ในกระบวนการทำงาน ดังภาพที่ 4-3



ภาพที่ 4-2 ข้อมูลจริงของสายรัดข้อมือ Aider ที่ไม่ได้เข้ารหัส AES และเข้ารหัส AES

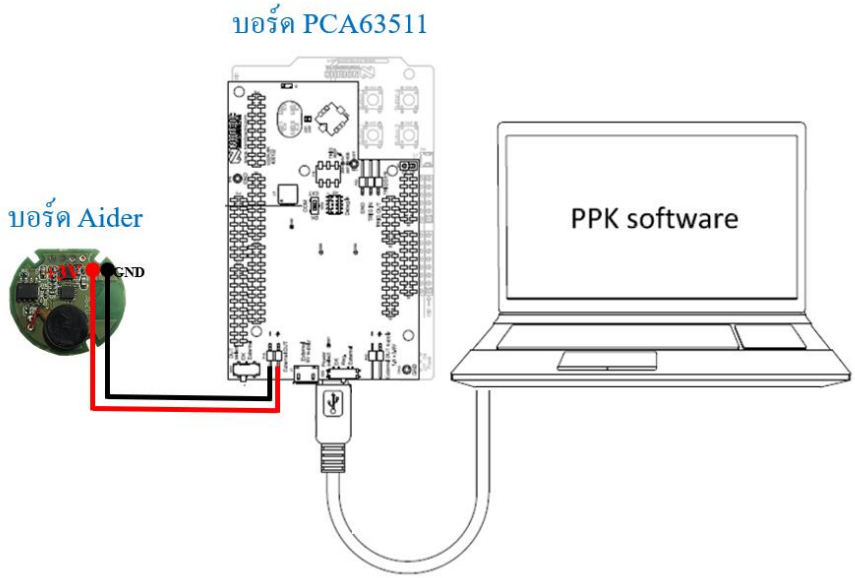


ภาพที่ 4-3 ไดอะแกรมของการทดสอบเวลาของการปล่อยบีคอนของข้อมูล

3. วิธีการทดสอบหากระแสของการทำงาน

การทดสอบหากระแสการทำงานของขั้นตอนการระบุตัวตนกับการแลกรหัสลับและขั้นตอนการปล่อยบีคอน มีวิธีการทดสอบที่กำหนดให้อุปกรณ์ต่อกับบอร์ด PCA63511 ซึ่งเป็นบอร์ดที่ใช้ในการตรวจสอบการใช้กระแสเมื่อมีการทำงาน ในที่นี้อุปกรณ์จะใช้แหล่งจ่ายไฟเลี้ยงจากบอร์ด PCA63511 เป็นแหล่งพลัง ซึ่งจะทำให้บอร์ด PCA63511 สามารถวัดกระแสของการทำงานได้ ดังภาพที่ 4-4 ในการวัดกระแสจะวัดเฉพาะฝั่งของอุปกรณ์ Aider A1 เพราะเป็นส่วนที่ใช้แบตเตอรี่ในการทำงาน และกระแสที่ได้จะนำมาคำนวณเพื่อให้ได้ค่าประมาณของกระแสเฉลี่ยดังสมการ

$$I_{avg} = \frac{\sum(\Delta I * \Delta t)}{\Delta t} \quad (4\text{-}1)$$



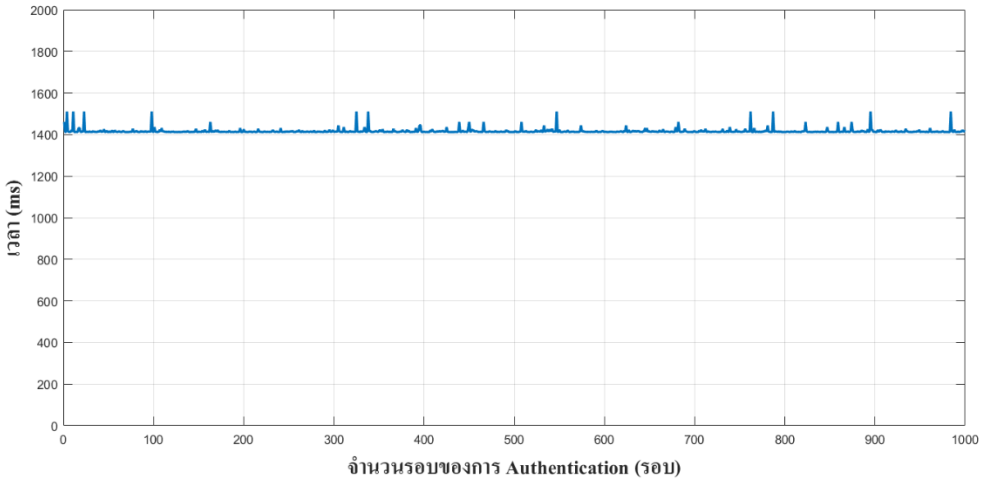
ภาพที่ 4-4 วิธีการทดสอบหากระแสของการทำงานในอุปกรณ์สวมใส่ Aider A1

ผลการทดสอบ

ผลการทดสอบการทำงานของระบบการระบุตัวตนและการเข้ารหัสข้อมูลสุขภาพส่วนบุคคลสำหรับอุปกรณ์สวมใส่โดยใช้ไอซีเข้ารหัส มีดังนี้

1. ผลการทำงานขั้นตอนการระบุตัวตนและการแลกรหัสลับ

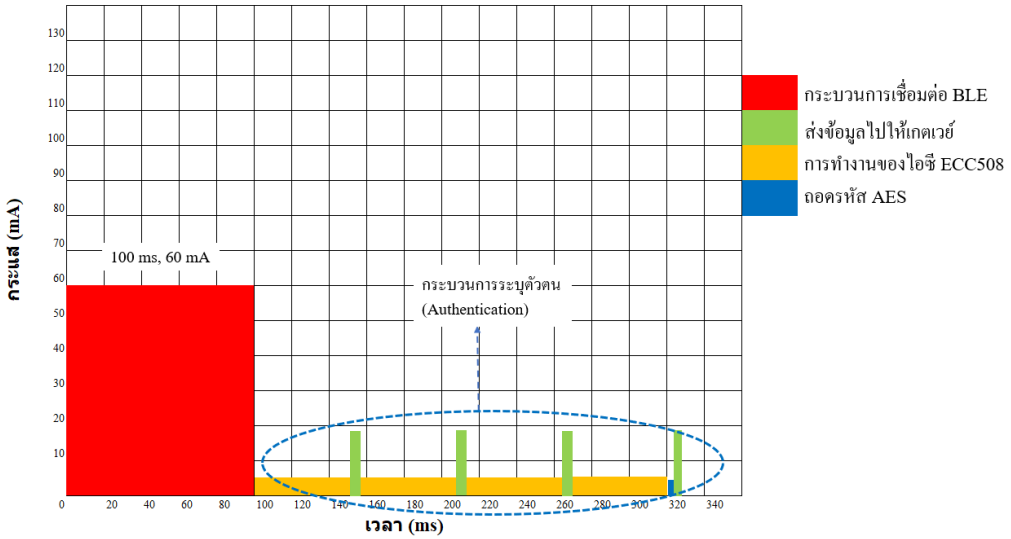
1.1 ผลการทดสอบเวลาของขั้นตอนการระบุตัวตนและการแลกรหัสลับ ผลการทดสอบเวลาของขั้นตอนการระบุตัวตนและการแลกรหัสลับที่ต้องทำการเชื่อมต่อ BLE ระหว่างเกตเวย์กับอุปกรณ์ Aider A1 เป็นจำนวน 1,000 ครั้ง สามารถแสดงกราฟการใช้เวลาดังภาพที่ 4-5



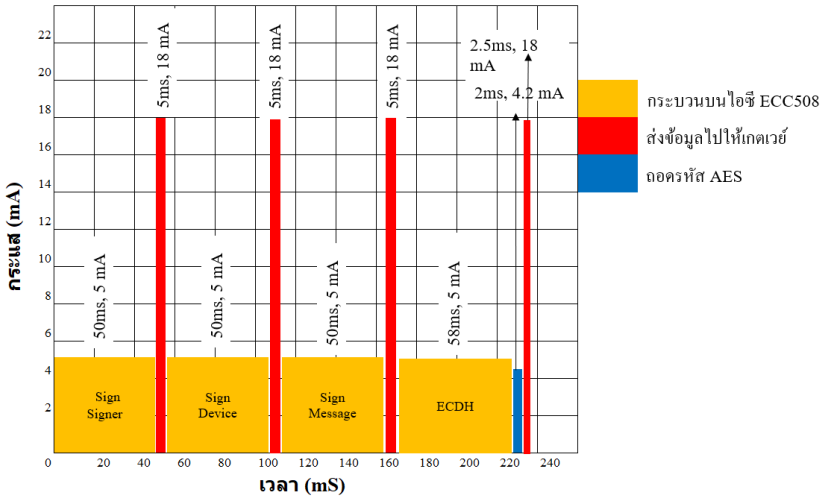
ภาพที่ 4-5 กราฟกระบวนการระบุตัวตนและการแลกรหัสลับ

จากการทดสอบขั้นตอนของการระบุตัวตนและการแลกรหัสลับ ใช้เวลาเฉลี่ยในการเชื่อมต่อ 1 ครั้งเท่ากับ 1,416.48 มิลิวินาที

1.2 ผลการทดสอบการใช้กระแสของขั้นตอนการระบุตัวตนและการแลกรหัสลับ ผลการทดสอบการใช้กระแสของขั้นตอนการระบุตัวตนและการแลกรหัสลับที่ต้องทำการเชื่อมต่อ BLE ระหว่างเกตเวย์กับอุปกรณ์ Aider A1 แต่จะทำการวัดการใช้กระแสเฉพาะฝั่งอุปกรณ์ Aider A1 สามารถแสดงกราฟการใช้กระแสได้ ดังภาพที่ 4-6



ภาพที่ 4-6 กราฟการใช้กระแสของกระบวนการระบุตัวตนและการแลกรหัสลับ



ภาพที่ 4-7 กราฟขยายส่วนการใช้กระแสของกระบวนการระบุตัวตนและการแลกรหัสลับ

หากระแสเฉลี่ยได้จากสมการที่ (4-1)

โดยที่ $\sum(\Delta I * \Delta t) = (100*60) + (50*5) + (5*18) + (50*5) + (5*18) + (50*5) + (5*18)$

$+ (5*18) + (2*4.2) + (2.5*1.8)$

$= 7{,}122.9$

และ $\Delta t = 100 + 50 + 5 + 50 + 5 + 50 + 5 + 5 + 2 + 2.5$

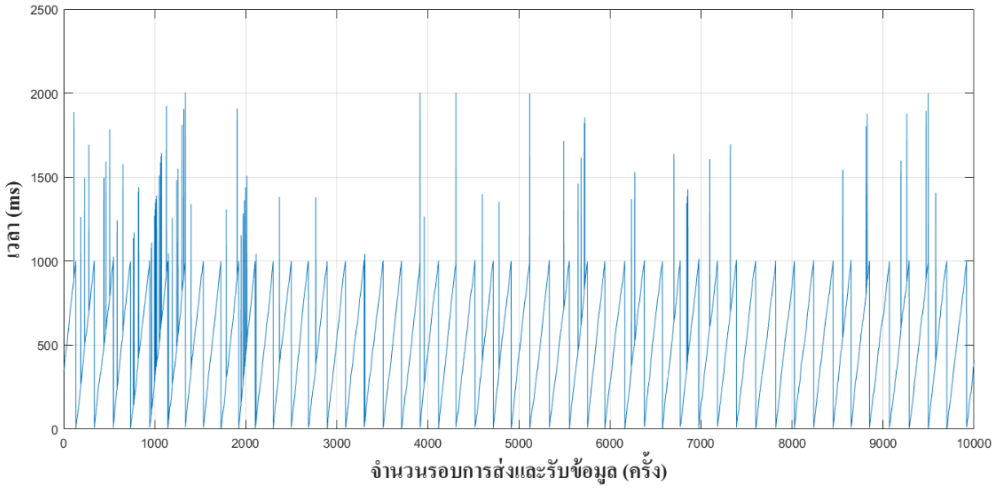
$$= 247.5$$

ดังนั้น $I_{avg} = \frac{7,122.9}{247.5} \approx 28.77$ mA

จากการทดสอบการใช้กระแสของขั้นตอนการระบุตัวตนและการแลกรหัสลับใช้กระแสเฉลี่ยในการเชื่อมต่อ 1 ครั้งประมาณ 28.77 มิลิแอมป์

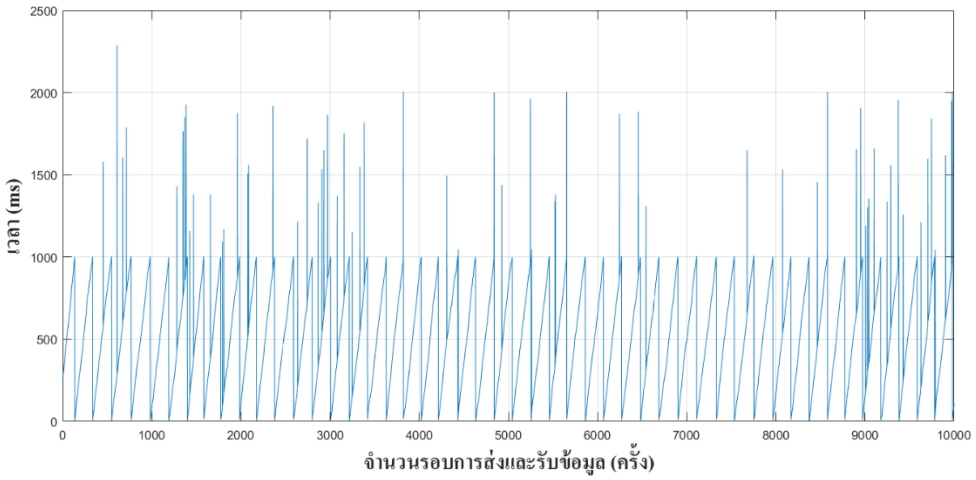
2. การทดสอบเวลาของการปล่อยบีคอนของข้อมูล

2.1 ผลการทดสอบปล่อยบีคอนของข้อมูลที่ยังไม่ได้เข้ารหัส AES การทดสอบปล่อยบีคอนของข้อมูลที่ยังไม่ได้เข้ารหัส AES ในการอ่านเซนเซอร์เป็นจำนวน 10,000 แพ็คเก็ตให้กับเกตเวย์ ในการวัดเวลาจะเริ่มจับเวลาเมื่อฝั่ง Aider A1 ตั้งแต่การอ่านเซนเซอร์และไปหยุดเวลาเมื่อฝั่งเกตเวย์ได้รับข้อมูลเรียบร้อย โดยในการทดสอบครั้งนี้ใช้เวลาเฉลี่ยในการส่งข้อมูลต่อ 1 แพ็คเก็ตเท่ากับ 512.713 มิลิวินาที สามารถแสดงกราฟการใช้เวลาได้ ดังภาพที่ 4-8



ภาพที่ 4-8 กราฟการปล่อยบีคอนข้อมูลที่ยังไม่ได้เข้ารหัส AES

2.2 ผลการทดสอบปล่อยบีคอนของข้อมูลที่เข้าและถอดรหัส AES การทดสอบปล่อยบีคอนของข้อมูลที่ได้เข้ารหัส AES ในการอ่านเซนเซอร์เป็นจำนวน 10,000 แพ็คเก็ตให้กับเกตเวย์ ในการวัดเวลาจะเริ่มจับเวลาตั้งแต่การอ่านเซนเซอร์แล้วเข้ารหัส AES จากฝั่ง Aider A1 และไปหยุดเวลาเมื่อฝั่งเกตเวย์ถอดรหัสเรียบร้อย โดยในการทดสอบครั้ง นี้ใช้เวลาเฉลี่ยในการส่งข้อมูล 1 แพ็คเก็ตเท่ากับ 514.8009 มิลิวินาที สามารถแสดงกราฟการใช้เวลาได้ดังภาพที่ 4-9

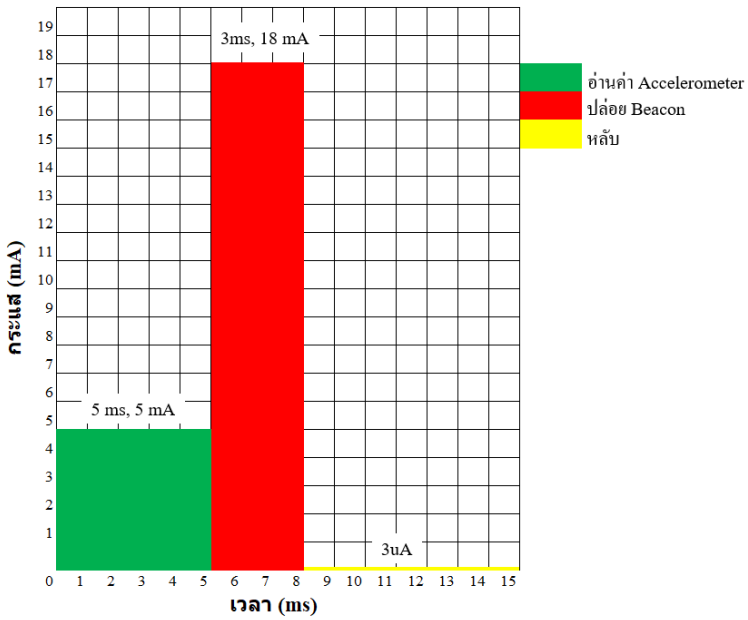


ภาพที่ 4-9 กราฟการปล่อยบีคอนของข้อมูลเข้าและถอดรหัส AES

จากการทดสอบพบว่าการส่งข้อมูลที่ยังไม่ได้เข้ารหัส AES ใช้เวลาเฉลี่ยในการส่งข้อมูล 1 แพ็คเก็ตเท่ากับ 512.713 มิลิวินาที และการส่งข้อมูลเข้ารหัส AES ใช้เวลาเฉลี่ยในการส่งข้อมูล 1 แพ็คเก็ตเท่ากับ 514.8009 มิลิวินาทีซึ่งมีค่าความต่างกันเพียง 2.0699 มิลิวินาที ดังนั้นเวลาที่สูญเสียไปกับการเข้ารหัส AES และส่งข้อมูลเท่ากับ 2.0699 มิลิวินาที

2.3 ผลการทดสอบการใช้กระแสของขั้นตอนการปล่อยบีคอน

2.3.1 ข้อมูลที่ไม่ได้เข้ารหัส AES ผลการทดสอบการใช้กระแสของขั้นตอนการปล่อยบีคอนจากอุปกรณ์ Aider A1 ไปหาเกตเวย์ โดยข้อมูลที่ส่งไปนั้นเป็นข้อมูลที่ไม่ได้เข้ารหัส AES แต่จะทำการวัดการใช้กระแสเฉพาะฝั่งอุปกรณ์ Aider A1 สามารถแสดงกราฟการใช้กระแสได้ดังภาพที่ 4-10



ภาพที่ 4-10 กราฟการใช้กระแสของการปล่อยบีคอนข้อมูลที่ยังไม่ได้เข้ารหัส AES

หากระแสเฉลี่ยได้จากสมการที่ 4-1

โดยที่ $\sum(\Delta I * \Delta t) = (5*5) + (3*18)$

$= 79$

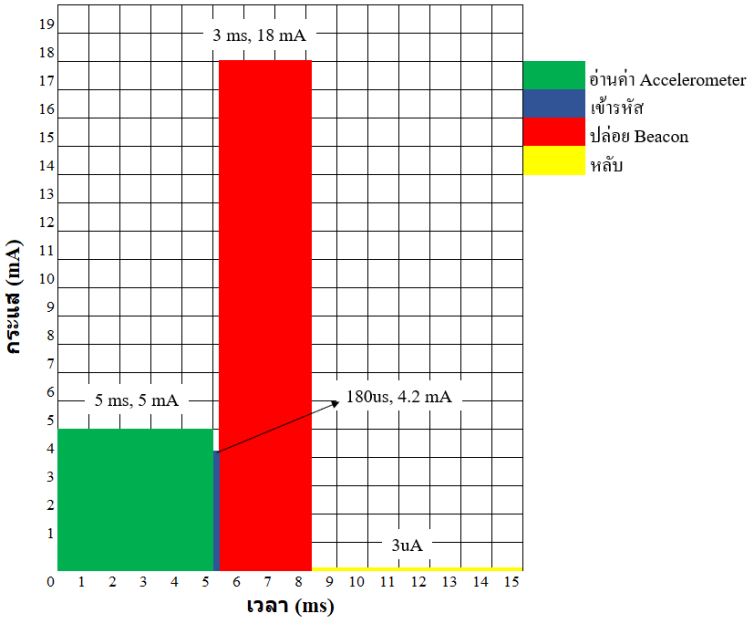
และ $\Delta t = 5 + 3$

$= 8$

ดังนั้น $I_{avg} = \frac{79}{8} \approx 10$ mA

จากการทดสอบการใช้กระแสของขั้นตอนการปล่อยบีคอนของข้อมูลที่ไม่ได้เข้ารหัส AES ใช้กระแสเฉลี่ยในการเชื่อมต่อ 1 ครั้งประมาณ 10 มิลิแอมป์

2.3.2 ข้อมูลที่ได้ทำการเข้ารหัส AES ผลการทดสอบการใช้กระแสของขั้นตอนการปล่อยบีคอนจากอุปกรณ์ Aider A1 ไปหาเกตเวย์ โดยข้อมูลที่ส่งไปนั้นเป็นข้อมูลที่เข้ารหัส AES แต่จะทำการวัดการใช้กระแสเฉพาะฝั่งอุปกรณ์ Aider A1 สามารถแสดงกราฟการใช้กระแสได้ดังภาพที่ 4-11



ภาพที่ 4-11 กราฟการใช้กระแสของการปล่อยบีคอนข้อมูลที่เข้ารหัส AES

หากระแสเฉลี่ยได้จากสมการที่ 4-1

โดยที่ $\sum(\Delta I * \Delta t) = (5*5) + (3*18) + (0.18*4.2)$

$= 79.756$

และ $\Delta t = 5 + 3 + 0.18$

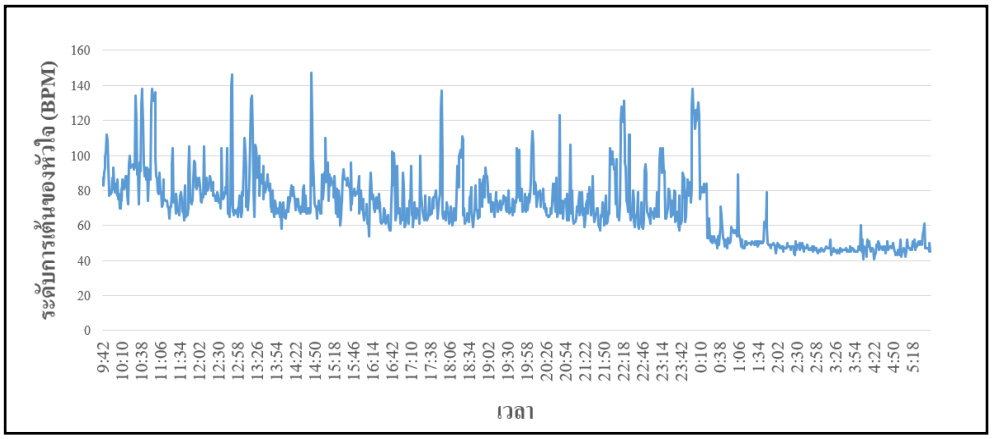
$= 8.18$

ดังนั้น $I_{avg} = \frac{79.756}{8.18} \approx 10$ mA

จากการทดสอบการใช้กระแสของขั้นตอนการปล่อยบีคอนของข้อมูลที่เข้ารหัส AES ใช้กระแสเฉลี่ยในการเชื่อมต่อ 1 ครั้งประมาณ 10 มิลิแอมป์

การวิเคราะห์การเพิ่มความปลอดภัย

ในการเพิ่มความปลอดภัยของการเข้ารหัส AES จะต้องมีการใช้ Huffman coding มาเข้ารหัสข้อมูลก่อนการเข้ารหัส AES เพื่อให้การเดากุญแจของ AES ยากขึ้น โดยการหา Huffman coding จะต้องใช้สถิติช่วงหนึ่ง ในงานวิจัยนี้จะหยิบยกตัวอย่างข้อมูลของอัตราการเต้นของหัวใจตามภาพที่ 4-12 ในเวลาประมาณ 1 วันเพื่อนำมาเป็นสถิติในการหาและสร้างตารางของ Huffman code



ภาพที่ 4-12 กราฟแสดงอัตราการเต้นใน 1 วัน

จากข้อมูลดังกล่าว ต้องนำข้อมูลมาสรุปหาจำนวนของอัตราการเต้นของหัวใจในแต่ละค่าว่ามีจำนวนเท่าไหร่และทำการเรียงลำดับจากมากลงไปหาน้อย และจากนั้นจึงคำนวณหาค่าความน่าจะเป็นจากจำนวนทั้งหมด เพื่อนำไปใช้ในกระบวนการหา Huffman coding ต่อไป ซึ่งในงานวิจัยนี้จะใช้ฟังก์ชันในโปรแกรมแมทแลบ (Matlab) ในการหา Huffman code ออกมากตามตารางที่ 4-1 โดยใช้ฟังก์ชัน ดังนี้ dict = huffmandict (symbols, prob)

โดยที่

ตัวแปร dict คือ ตารางอาเรย์ของค่า Huffman code ออกมาในรูปเลขแบบฐานสอง

ฟังก์ชัน huffmandict คือ ฟังก์ชันในการหาตารางอาเรย์ของ Huffman code

พารามิเตอร์ Symbols คือ ชนิดของอัตราการเต้นของหัวใจเช่น หัวใจเต้น 47 ครั้งต่อนาที หัวใจเต้น 68 ครั้งต่อนาที เป็นต้น

พารามิเตอร์ prob คือ ความน่าจะเป็นของจำนวนอัตราการเต้นของหัวในแต่ละช่วงข้อมูล

ตารางที่ 4-1 จำนวนของอัตราการเต้นของหัวใจค่าความน่าจะเป็นและ Huffman coding

ลำดับ	อัตราการเต้นของหัวใจ	จำนวน	ความน่าจะเป็น	Huffman code
1	47	61	0.050748752	[1,0,1,1]
2	68	46	0.038269551	[0,0,1,0,1]
3	67	45	0.037437604	[0,1,0,0,1]
4	48	45	0.037437604	[0,1,0,0,0]

ตารางที่ 4-1 (ต่อ)

ลำดับ	อัตราการเต้นของหัวใจ	จำนวน	ความน่าจะเป็น	Huffman code
5	46	42	0.034941764	[0,1,0,1,0]
6	74	37	0.03078203	[0,1,1,0,1]
7	70	36	0.029950083	[0,1,1,1,1]
8	65	35	0.029118136	[1,0,0,0,0]
9	75	33	0.027454243	[1,0,0,0,1]
10	66	32	0.026622296	[1,0,0,1,1]
11	45	31	0.025790349	[1,1,0,0,0]
12	79	29	0.024126456	[1,1,1,0,0]
13	72	29	0.024126456	[1,1,0,1,1]
14	50	29	0.024126456	[1,1,0,1,0]
15	77	27	0.022462562	[0,0,0,0,0,1]
16	78	27	0.022462562	[0,0,0,0,0,0]
17	73	27	0.022462562	[1,1,1,1,1]
18	71	26	0.021630616	[0,0,0,0,1,1]
19	69	26	0.021630616	[0,0,0,0,1,0]
20	81	25	0.020798669	[0,0,0,1,1,0]
21	64	24	0.019966722	[0,0,1,0,0,1]
22	63	24	0.019966722	[0,0,1,0,0,0]
23	80	23	0.019134775	[0,0,1,1,1,0]
24	51	23	0.019134775	[0,0,1,1,0,1]
25	49	23	0.019134775	[0,0,1,1,0,0]
26	76	20	0.016638935	[0,1,1,0,0,0]
27	83	19	0.015806988	[0,1,1,0,0,1]
28	62	18	0.014975042	[0,1,1,1,0,0]
29	87	16	0.013311148	[1,0,1,0,1,0]
30	84	15	0.012479201	[1,1,0,0,1,0]
31	86	14	0.011647255	[1,1,1,0,1,1]

ตารางที่ 4-1 (ต่อ)

ลำดับ	อัตราการเต้นของหัวใจ	จำนวน	ความน่าจะเป็น	Huffman code
32	88	14	0.011647255	[1,1,1,0,1,0]
33	61	14	0.011647255	[1,1,1,1,0,1]
34	59	14	0.011647255	[1,1,1,1,0,0]
35	85	13	0.010815308	[0,0,0,1,0,0,1]
36	82	13	0.010815308	[0,0,0,1,0,0,0]
37	93	12	0.009983361	[0,0,0,1,1,1,1]
38	90	11	0.009151414	[0,1,0,1,1,0,0]
39	52	11	0.009151414	[0,0,1,1,1,1,1]
40	44	10	0.008319468	[0,1,0,1,1,1,0]
41	89	9	0.007487521	[0,1,1,1,0,1,1]
42	57	9	0.007487521	[0,1,1,1,0,1,0]
43	95	8	0.006655574	[1,0,1,0,0,0,0]
44	104	8	0.006655574	[1,0,1,0,0,1,1]
45	60	8	0.006655574	[1,0,1,0,0,1,0]
46	43	7	0.005823627	[1,1,0,0,1,1,1]
47	94	6	0.004991681	[0,0,0,1,0,1,1,1]
48	96	6	0.004991681	[0,0,0,1,0,1,1,0]
49	91	6	0.004991681	[0,0,0,1,1,1,0,1]
50	54	6	0.004991681	[0,0,0,1,1,1,0,0]
51	53	6	0.004991681	[0,0,0,1,0,1,0,1]
52	99	5	0.004159734	[0,1,0,1,1,1,1,1]
53	100	5	0.004159734	[0,1,0,1,1,1,1,0]
54	92	5	0.004159734	[0,1,0,1,1,0,1,1]
55	102	4	0.003327787	[0,0,0,1,0,1,0,0,0]
56	112	4	0.003327787	[1,0,1,0,0,0,1,1]
57	134	4	0.003327787	[1,0,1,0,0,0,1,0]
58	120	4	0.003327787	[1,0,1,0,1,1,0,1]

ตารางที่ 4-1 (ต่อ)

ลำดับ	อัตราการเต้นของหัวใจ	จำนวน	ความน่าจะเป็น	Huffman code
59	105	4	0.003327787	[1,0,1,0,1,1,0,0]
60	106	4	0.003327787	[1,0,1,0,1,1,1,1]
61	98	4	0.003327787	[1,0,1,0,1,1,1,0]
62	58	4	0.003327787	[1,1,0,0,1,1,0,1]
63	56	4	0.003327787	[1,1,0,0,1,1,0,0]
64	138	3	0.00249584	[0,0,1,1,1,1,0,0,1]
65	131	3	0.00249584	[0,0,1,1,1,1,0,0,0]
66	97	3	0.00249584	[0,0,1,1,1,1,0,1,1]
67	103	3	0.00249584	[0,0,1,1,1,1,0,1,0]
68	123	3	0.00249584	[0,1,0,1,1,0,1,0,1]
69	126	3	0.00249584	[0,1,0,1,1,0,1,0,0]
70	42	3	0.00249584	[0,0,0,1,0,1,0,0,1]
71	109	2	0.001663894	[1,0,0,1,0,0,0,1,1]
72	127	2	0.001663894	[1,0,0,1,0,0,0,1,0]
73	132	2	0.001663894	[1,0,0,1,0,1,1,0,1]
74	110	2	0.001663894	[1,0,0,1,0,1,1,0,0]
75	111	2	0.001663894	[1,0,0,1,0,1,1,1,1]
76	114	2	0.001663894	[1,0,0,1,0,1,1,1,0]
77	101	2	0.001663894	[1,0,0,1,0,1,0,0,1]
78	128	2	0.001663894	[1,0,0,1,0,1,0,0,0]
79	55	2	0.001663894	[1,0,0,1,0,1,0,1,1]
80	41	2	0.001663894	[1,0,0,1,0,1,0,1,0]
81	121	1	0.000831947	[1,0,0,1,0,0,0,0,0,1]
82	129	1	0.000831947	[1,0,0,1,0,0,0,0,0,0]
83	136	1	0.000831947	[1,0,0,1,0,0,0,0,1,1]
84	140	1	0.000831947	[1,0,0,1,0,0,0,0,1,0]
85	146	1	0.000831947	[1,0,0,1,0,0,1,1,0,1]

ตารางที่ 4-1 (ต่อ)

ลำดับ	อัตราการเต้นของหัวใจ	จำนวน	ความน่าจะเป็น	Huffman code
86	147	1	0.000831947	[1,0,0,1,0,0,1,1,0,0]
87	122	1	0.000831947	[1,0,0,1,0,0,1,1,1,1]
88	137	1	0.000831947	[1,0,0,1,0,0,1,1,1,0]
89	119	1	0.000831947	[1,0,0,1,0,0,1,0,0,1]
90	124	1	0.000831947	[1,0,0,1,0,0,1,0,0,0]
91	115	1	0.000831947	[1,0,0,1,0,0,1,0,1,1]
92	130	1	0.000831947	[1,0,0,1,0,0,1,0,1,0]

การวิเคราะห์หาความปลอดภัย จะสมมติโอกาสของการเดารหัสลับจากผู้ที่ต้องการขโมยข้อมูลโดยการ Brute force เป็น 2 กรณี ได้แก่ กรณีที่มีค่าเลขสุ่ม (Random) กับข้อมูลปกติในแพ็คเก็ต (Packet) และกรณีที่มีค่าเลขสุ่มกับข้อมูลที่เข้ารหัส Huffman code จากภาพที่ 4-13 เป็นแพ็คเก็ตใช้ในการส่งข้อมูลจากอุปกรณ์ Aider A1 ไปยังเกตเวย์ ซึ่งข้อมูลในไบต์ที่ 7 ถึงไบต์ที่ 18 คือ ข้อมูลที่กำหนดให้ซ้ำกันเสมอ ส่วนข้อมูลในไบต์ที่ 19 กับ 20 คือ ข้อมูลการเต้นของหัวใจ และข้อมูลในไบต์ที่ 21 กับ 22 เป็นข้อมูลค่าเลขสุ่ม

ลักษณะรูปแบบการ Brute force โดยใช้ตาราง จะสมมติให้ผู้ดักฟังใช้วิธี Brute force หากุญแจลับ โดยสร้างตารางรอไว้ n ตาราง เมื่อ n เท่ากับจำนวนกุญแจที่เป็นไปได้ทั้งหมดในแต่ละตารางที่ *i* จะแสดงแพ็คเก็ตที่เข้ารหัสโดยกุญแจ *i* จากข้อมูลดิบที่เป็นอัตราการเต้นของหัวใจ และข้อมูลสุ่มดังภาพที่ 4-14 เมื่อผู้ดักฟังสร้างตารางครบทุก n ตารางที่เป็นไปได้แล้ว จะนำแพ็คเก็ตที่ดักฟังได้มาตรวจสอบกับแพ็คเก็ตที่บันทึกในตารางใด ๆ ถือว่ามีความเป็นไปได้ที่กุญแจที่ใช้เข้ารหัสจะเป็นตัวเดียวกันกับในตารางนั้น

Byte No.	Data Type	Define
0	Length of name	0x03
1	GAP Type	GAP_ADTYPE_LOCAL_NAME_COMPLETE (0x09)
2	Name	'A'
3	Name	'1'
4	Length of Data	0x1A(26)
5	GAP Type	GAP_ADTYPE_SERVICE_DATA (0x16)
6	Data	0x00
7	Data	Data Value[0]
8	Data	Data Value[1]
9	Data	Data Value[2]
10	Data	Data Value[3]
11	Data	Data Value[4]
12	Data	Data Value[5]
13	Data	Data Value[6]
14	Data	Data Value[7]
15	Data	Data Value[8]
16	Data	Data Value[9]
17	Data	Data Value[10]
18	Data	Data Value[11]
19	Data	Data Value[12]
20	Data	Data Value[13]
21	Data	Random[0]
22	Data	Random[1]
23	Data	Empty (0x00)
24	Data	Empty (0x00)
25	Data	Empty (0x00)
26	Data	Empty (0x00)
27	Data	Empty (0x00)
28	Data	Empty (0x00)
29	Data	Empty (0x00)
30	Data	Empty (0x00)

ภาพที่ 4-13 แพ็คเก็ตข้อมูลที่ส่งบีคอนจากอุปกรณ์ Aider A1 ไปยังเกตเวย์

กุญแจรหัสลับ	อัตราการเต้นของหัวใจ	ข้อมูลสุ่ม	แพ็คเก็ตที่สร้างขึ้น
i	h_1	1 2 . . . . m	P_{11} P_{12} . . . . P_{1m}
	h_2	1 2 . . . . m	P_{21} P_{22} . . . . P_{2m}
	. . .	. . .	. . .
	h_q	1 2 . . . . m	P_{q1} P_{q2} . . . . P_{qm}

ภาพที่ 4-14 ข้อมูลสุ่มของรูปแบบ Brute force โดยใช้ตาราง

จะเห็นได้ว่าความยาวของการ Brute force นี้จะต้องมีการสร้างตารางหลายตารางซึ่งจะต้องใช้หน่วยความจำสูง หรือถ้าสร้างแบบ Real-time ก็ต้องใช้ความเร็วซีพียู (CPU) สูงเช่นกัน ตลอดจนการค้นหาแพ็คเก็ตในตารางที่ตรงกับที่ดักฟังมา ก็ต้องใช้ทรัพยากรของคอมพิวเตอร์มากอีกด้วยดังนั้น ในงานวิจัยนี้จะวิเคราะห์ความยากที่ผู้ดักฟังจะสามารถหากุญแจรหัสลับได้จากขนาดของตารางรวมทั้งหมด

ในการวิเคราะห์หาความปลอดภัยจะใช้ข้อมูลในไบต์ที่ 19 ถึงไบต์ที่ 22 ที่มีการเปลี่ยนแปลงของข้อมูลขนาด 4 ไบต์ในการหากุญแจรหัสลับจากการถูก Brute force โดยใช้การเข้ารหัส AES ในอุปกรณ์จะใช้กุญแจรหัสลับขนาด 128 ไบต์ ดังนั้นสามารถแยกการวิเคราะห์การเดากุญแจรหัสลับเป็น 2 กรณี ดังนี้

1. กรณีที่มีค่าเลขสุ่มกับข้อมูลปกติในแพ็คเก็ต

ในกรณีที่มีค่าเลขสุ่มกับข้อมูลปกติในแพ็คเก็ตจะประกอบไปด้วยข้อมูลขนาด 4 ไบต์ ได้แก่ ค่าเลขสุ่มขนาด 2 ไบต์และข้อมูลการเต้นของหัวใจขนาด 2 ไบต์ โดยจากการเก็บสถิติการเต้นของหัวใจใน 1 วัน มีชนิดของอัตราการเต้นของหัวใจทั้งหมด 92 รูปแบบ ดังนั้นจำนวนแถวในตารางทั้งหมดจะมีค่าเท่ากับ

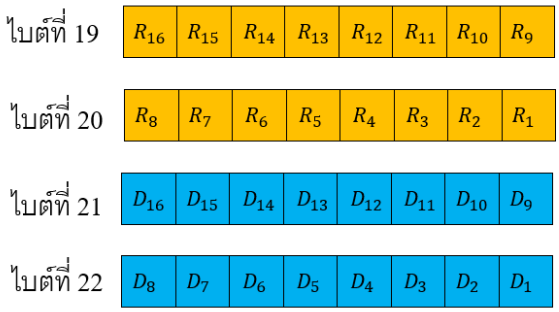
$$n(K_a) = 2^{128}(92 \times 2^{16})$$

โดยที่ n เป็นจำนวนตาราง เนื่องจากใช้ AES 128 บิต จึงมี 2^{128} ตาราง

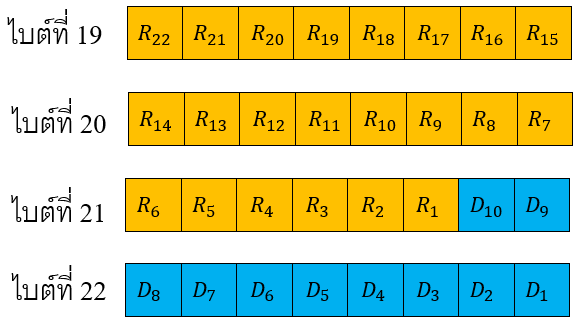
และ K_a เป็นจำนวนแถวในแต่ละตาราง คำนวณจากรูปแบบการเต้นของหัวใจที่เป็นได้ 92 รูปแบบ และเลขสุ่มขนาด 2 ไบต์ที่เป็นได้ 2^{16} รูปแบบ

2. กรณีที่มีค่าเลขสุ่มกับข้อมูลที่เข้ารหัส Huffman code

ในกรณีที่มีค่าเลขสุ่มกับข้อมูลปกติในแพ็คเก็ตจะประกอบไปด้วยข้อมูลขนาด 4 ไบต์ ได้แก่ ค่าเลขสุ่มขนาด 2 ไบต์และข้อมูลการเต้นของหัวใจขนาด 2 ไบต์ที่ถูกแทนที่ด้วย Huffman code จากตารางที่ 4-1 แสดงให้เห็นว่าขนาดความยาวของ Huffman code ที่ได้มีจำนวนไม่เท่ากันจึงทำให้สามารถเพิ่มตำแหน่งของค่าเลขสุ่มเข้าไปเพิ่มในบิตที่ไม่ได้ใช้งานได้ เมื่อเทียบกับภาพที่ 4-14 คือ ตำแหน่งบิตของข้อมูลปกติที่มีค่าเลขสุ่ม 2^{16} ตลอด แต่ในภาพที่ 4-15 คือ ตำแหน่งบิตของข้อมูลที่เปลี่ยนไปเนื่องจากค่า Huffman code ที่เปลี่ยนไปตามตาราง ทำให้ตำแหน่งของค่าเลขสุ่มมากขึ้น



ภาพที่ 4-15 ตำแหน่งของบิตข้อมูลในแต่ละไบต์ของข้อมูลปกติ



ภาพที่ 4-16 ตำแหน่งของบิตข้อมูลในแต่ละไบต์ของข้อมูลที่เข้า Huffman code

จากตารางที่ 4-1 สามารถแยกจำนวนแถวของแต่ละตารางของ Huffman code ได้ดังนี้

2.1 จำนวน Huffman code ที่มีความยาวเป็น 4 มี 1 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป 2^{22} แถว

2.2 จำนวน Huffman code ที่มีความยาวเป็น 7 มี 14 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป $14x2^{23}$ แถว

2.3 จำนวน Huffman code ที่มีความยาวเป็น 8 มี 19 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป $19x2^{24}$ แถว

2.4 จำนวน Huffman code ที่มีความยาวเป็น 9 มี 12 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป $12x2^{25}$ แถว

2.5 จำนวน Huffman code ที่มีความยาวเป็น 10 มี 16 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป $16x2^{26}$ แถว

2.6 จำนวน Huffman code ที่มีความยาวเป็น 11 มี 18 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป $18x2^{27}$ แถว

2.7 จำนวน Huffman code ที่มีความยาวเป็น 12 มี 12 จำนวนดังนั้นเมื่อสร้างตารางจากผู้ดักฟัง กลุ่มนี้จะกินจำนวนแถวไป $12x2^{28}$ แถว

ดังนั้นจำนวนแถวในทุกตารางจะรวมเป็น $n(K_b) = 2^{128}(2^{22} + 14x2^{23} + 19x2^{24} + 12x2^{25} + 16x2^{26} + 18x2^{27} + 12x2^{28})$ โดยที่ K_b เป็นจำนวนแถวรวมในแต่ละตาราง

ดังนั้นความปลอดภัยของการเข้ารหัสที่เพิ่มขึ้น $= \frac{n(K_b)}{n(K_a)} = 1,252.87$ เท่า

บทที่ 5
สรุปผล อภิปรายผล และข้อเสนอแนะ

สรุปผลการศึกษา

จากการศึกษากระบวนการระบุตัวตน (Authentication) โดยใช้กระบวนการ Elliptic curve digital signature algorithm (ECDH) และการศึกษากระบวนการแลกกุญแจรหัสลับของข้อมูลที่ใช้กระบวนการ Elliptic curve diffie-hellman algorithm (ECDH) โดยกระบวนการเหล่านี้อยู่บนไอซีเข้ารหัส จึงนำมาใช้เพื่อเป็นส่วนหนึ่งในกระบวนการสร้างความปลอดภัยให้กับข้อมูลของอุปกรณ์ที่เกี่ยวกับด้านข้อมูลสุขภาพส่วนบุคคล ในงานวิจัยได้ประยุกต์ใช้กับอุปกรณ์ไอโอทีที่ใช้ในโครงการการพัฒนา Smart living สำหรับอุตสาหกรรมบริการสุขภาพอัจฉริยะ-Smart living for smart city ปี 2017 เพื่อเป็นระบบแจ้งเตือนความผิดปกติทางสุขภาพของผู้สูงอายุและความผิดปกติภายในบ้านของผู้พักอาศัยภายในบ้านมีอุปกรณ์ไอโอทีที่ใช้ ได้แก่ สายรัดข้อมือ (Wristband) รุ่น Aider A1 และสายรัดข้อมือ Aider A2 โดยมีกระบวนการสร้างความปลอดภัยทางข้อมูลทางสุขภาพส่วนบุคคลที่ประกอบด้วยไปด้วยกระบวนการระบุตัวตน กระบวนการแลกรหัสลับและกระบวนการเข้ารหัสลับข้อมูล

จากการทดสอบกระบวนการระบุตัวตนกับกระบวนการแลกรหัสลับ สามารถสรุปเวลาของกระบวนการทำงานได้ 1,416.482 มิลิวินาที ในส่วนของกระบวนการเข้ารหัสลับข้อมูลสามารถสรุปเวลาของกระบวนการได้ 2.0699 วินาที และการเพิ่มกระบวนการ Huffman coding สามารถเพิ่มความปลอดภัยของการเข้ารหัสข้อมูลได้ถึง 1,252.87 เท่า

ข้อเสนอแนะแนวทางในอนาคต

จากการใช้งานระบบและการทดสอบประสิทธิภาพ พบว่าการใช้งานกระบวนการทางความปลอดภัยของอุปกรณ์ไอโอทีได้แก่ กระบวนการระบุตัวตนผ่านกระบวนการ ECDSA การแลกกุญแจรหัสลับผ่านกระบวนการ ECDH ระหว่างอุปกรณ์ไอโอทีส่วนบุคคลกับเกตเวย์ มีประสิทธิภาพในการทำงาน สามารถระบุอุปกรณ์ที่เป็นตัวจริงได้ กระบวนการเข้ารหัสผ่าน AES สามารถเข้ารหัสข้อมูลไม่ให้ถูกขโมยได้ และการเพิ่มกระบวนการ Huffman coding ในข้อมูลให้มีความปลอดภัยมากยิ่งขึ้น สามารถสร้างความปลอดภัยให้กับอุปกรณ์ไอโอทีที่ส่งข้อมูลให้กับระบบได้ การจะเพิ่มความปลอดภัยในระบบให้เพิ่มมากขึ้นจะต้องมีการอัพเดทกุญแจรหัสลับให้กับอุปกรณ์ของระบบตามเวลาที่ถูกกำหนดไว้ ทั้งนี้แล้วประสิทธิภาพของการทำงานอุปกรณ์ไอโอที

ในแง่เรื่องพลังงาน ในอนาคตจะต้องมีการศึกษาและพัฒนาในเรื่องของการกำหนดระยะเวลาในการอัพเดทกุญแจรหัสลับเพื่อไม่ให้กระทบกับการใช้พลังงานของอุปกรณ์ และการพัฒนากระบวนการ Huffman coding ให้สามารถปรับได้ทั้งฝั่งอุปกรณ์และฝั่งเกตเวย์ โดยไม่ต้องกำหนดในโปรแกรมไว้ก่อน ซึ่งมันจะกลายเป็น Adaptive huffman coding ที่สามารถสร้าง Huffman code ที่เหมือนกันทั้งสองฝั่งเพื่อใช้ในการถอดและเข้ารหัสได้ ซึ่งมันจะช่วยเสริมความปลอดภัยมากขึ้น

บรรณานุกรม

จตุชัย แพงจันทร์. (2553*). Master in Security 2nd Edition* (หน้า 8-143). นนทบุรี: ไอดีซี ฯ.

ภูกิจ บุรีภักดี และปราโมทย์ กั่วเจริญ. (2555). การเพิ่มความปลอดภัยและประสิทธิภาพในการรับส่งข้อความ SMS.

สัญฉกร วุฒิสิทธิกุลกิจ, ธงชัย โรจน์กังสดาล, วรากร ศรีเชวงทรัพย์, นพดล พรมภักษรและสุวิทย์ นาคพีระยุทธ. (2556). วิทยาการรหัสลับเบื้องต้น (หน้า 56-95). โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

อภิรัฐ ลิ่มมณี, วิรุฬห์ ศรีบริรักษ์, และนิพนธ์ สมหมาย. (2561). ความปลอดภัยของไอโอทีบลูทูธสำหรับระบบตรวจวัดตัวบ่งชี้สุขภาพโดยใช้ไอซีเข้ารหัส: การออกแบบและการใช้งานจริง.

Apirath, L., Sorakrai, K., Wiroon, S,. & Nipon, S. (2016). Adaptive hybrid encryption and secret mixing in resource-and-bandwidth-constrained systems.

Arnaud Tisserand. (2016). Introduction to Elliptic Curve Cryptography (ECC) Hardware Implementation. 1-41.

Atmel Corporation. (2015). ATECC508A Crypto Element witch ECDH key Agreement. 33-59.

Atmel Corporation. (2015). Compressed Certification Definition ATECC CryptoAuthentication Device Family. 4-14.

Atmel Corporation. (2014). *Security at our Core*. 3-31.

Christopher G. (2011). Atmel White Paper: Using a Cryptographic IC for Key Management and Logistical Support.

Chun-Jen, T. (2014), Huffman Coding. 2-19.

Danial, B. (2015, March 19). Wireless Solution – Enabling IoT ATMEL | SMARTConnect (pp. 1-62).

Ding, D., Mauro, C., & Agusti, S. (2016). A Smart Health Application and its Related Privacy Issues.

Effy, R, N., Dr. Hemraj, S., & Mukesh, S. (2017). A Recent Review on Lightweight Cryptography in IoT.

Elisabeth, O. (2002). Introduction to Elliptic Curve Cryptography. 15-16.

Mirjana, M., Vladimir, V., & Branko P. (2015). A Custom Internet of Things Healthcare System.

NIST. (2001). Announcing the ADVANCED ENCRYPTION STANDDARD (AES).

Shengling, W., Rongfang B., Feng, Z., Nan, Z. Xiuzhen C., & Hyeong-Ah, C. (2016). Security in Wearable Communications.

Suranga, S., Yining H., Than, N., Guohao, L., Sara, K., Kanchana, T., Mahbub H., & Aruna S. (2017). A Survey of Wearable Devices and Challenges. 2573-2574.

Talwana, J, C. Huang, J, H. (2016). Smart World of Internet of Things (IoT) and It's Security concerns. 241-243.

Thomas M. Cover, Joy A. (2006). HUFFMAN CODES. Elements of information theory Second Edition (pp.118-125). Printed in the United States of America: A Wiley-Interscience publication.

Wikipedia. (2018). Block cipher mode of operation. Retrieved from https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_Codeboo_(ECB)

Wikipedia. (2018). Elliptic Curve Digital Signature. Retrieved from https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Wikipedia. (2018). Huffman coding. Retrieved from https://en.wikipedia.org/wiki/Huffman_coding