กลไกการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตสำหรับการประยุกต์ใช้งานในการเฝ้าระวังผู้ป่วย

Internet of Things Logging Mechanism for Patient Monitoring Applications

ปิยวัฒน์ มณีนวล

Piyawat Maneenual

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญา
วิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
มหาวิทยาลัยสงขลานครินทร์

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Management of Information Technology
Prince of Songkla University
2562

ชื่อวิทยานิพนธ์ กลไกการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต สำหรับการประยุกต์ใช้งานในการเฝ้าระวังผู้ป่วย

ผู้เขียน นายปิยวัฒน์ มณีนวล

สาขาวิชา การจัดการเทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

.....

(ผู้ช่วยศาสตราจารย์ ดร.แสงสุรีย์ วสุพงศ์อัยยะ)

คณะกรรมการสอบ

.....ประธานกรรมการ

(ดร.สมชัย หลิมศิโรรัตน์)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ปัญญยศ ไชยกาฬ)

.....กรรมการ

(รองศาสตราจารย์ ดร.อนันต์ ผลเพิ่ม)

บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ

.....

(ศาสตราจารย์ ดร.ดำรงศักดิ์ ฟ้ารุ่งสาง)

คณบดีบัณฑิตวิทยาลัย

ขอรับรองว่า ผลงานวิจัยนี้มาจากการศึกษาวิจัยของนักศึกษาเอง และได้แสดงความขอบคุณบุคคลที่มีส่วนช่วยเหลือแล้ว

ลงชื่อ .....
(ผู้ช่วยศาสตราจารย์ ดร.แสงสุรีย์ วสุพงศ์อัยยะ)
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

ลงชื่อ .....
(นายปิยวัฒน์ มณีนวล)
นักศึกษา

ข้าพเจ้าขอรับรองว่า ผลงานวิจัยนี้ไม่เคยเป็นส่วนหนึ่งในการอนุมัติปริญญาในระดับใดมาก่อน และไม่ได้ถูกใช้ในการยื่นขออนุมัติปริญญาในขณะนี้

ลงชื่อ .....

(นายปิยวัฒน์ มณีนวล)

นักศึกษา

ชื่อวิทยานิพนธ์ กลไกการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต สำหรับการประยุกต์ใช้งานในการเฝ้าระวังผู้ป่วย
ผู้เขียน นายปิยวัฒน์ มณีนวล
สาขาวิชา การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา 2561

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบและทดลองรูปแบบการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตด้านการแพทย์ด้วยเน็ตพายซึ่งพัฒนาโดย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) เพื่อใช้ลดข้อจำกัดด้านระยะทางในการติดตามการรักษาผู้ป่วยอย่างต่อเนื่องและการเก็บข้อมูลสุขภาพในแต่ละช่วงเวลาอย่างละเอียด โดยระบบบันทึกธุรกรรมใช้ข้อมูลพื้นฐานของการสื่อสารและไม่ล่วงล้ำความเป็นส่วนตัวของเจ้าของข้อมูล มีการทดสอบรูปแบบการบันทึกธุรการสามแบบ ได้แก่ บันทึกธุรกรรมเฉพาะแต่ละสรรพสิ่ง บันทึกธุรกรรมเฉพาะเน็ตพาย และบันทึกธุรกรรมทุกส่วน เพื่อเน้นการตรวจสอบความผิดปกติทั้งสิ้น 4 แบบ ได้แก่ อุปกรณ์ใหม่ที่เชื่อมต่อเข้ามาครั้งแรก ข้อมูลธุรกรรมการรับส่งข้อมูลอย่างปกติสมบูรณ์ ข้อมูลธุรกรรมการรับส่งข้อมูลอย่างปกติสมบูรณ์แต่ล่าช้า ข้อมูลธุรกรรมการสื่อสารสูญหายระหว่างสรรพสิ่งและเน็ตพาย

ผลการทดลองการทดสอบบันทึกธุรกรรมจากเซ็นเซอร์วัดค่าร่างกาย 4 ชิ้นต่อผู้ป่วย 1 คน ของผู้ป่วยจำนวน 30 คนด้วยการส่งข้อมูลทุก 250 มิลลิวินาที ส่งข้อมูลไปยังคอมพิวเตอร์แพทย์ที่โรงพยาบาลด้วยเน็ตพายด้วยกระบวนการบันทึกธุรกรรมทั้งสามแบบพบว่า การบันทึกธุรกรรมสามารถตรวจสอบพบการเชื่อมต่อใหม่และความล่าช้าในการสื่อสารของสรรพสิ่งได้ทั้งหมด แต่รูปแบบการตรวจสอบหาการสูญหายของข้อมูลมีความละเอียดในการตรวจพบแตกต่างไป หากบันทึกธุรกรรมที่สรรพสิ่งเท่านั้น จะไม่สามารถระบุรูปแบบการสูญหายได้ หากมีการบันทึกธุรกรรมที่เน็ตพายเพียงจุดเดียวจะไม่สามารถระบุรูปแบบการสูญหายก่อนถึงเน็ตพายได้ ดังนั้น การบันทึกธุรกรรมทุกส่วนจะสามารถตรวจสอบความผิดปกติได้ทั้ง 4 แบบ โดยขนาดพื้นที่ในการจัดเก็บข้อมูลธุรกรรมของการบันทึกธุรกรรมที่สรรพสิ่งคิดเป็นร้อยละ 0.4 ที่เน็ตพายคิดเป็นร้อยละ 0.2 และการบันทึกทุกส่วนคิดเป็นร้อยละ 0.61 ของปริมาณข้อมูลในการสื่อสาร ดังนั้น พื้นที่สำหรับเก็บข้อมูลในการบันทึกธุรกรรมมีขนาดเล็กกว่าร้อยละ 1 ของข้อมูลทั้งหมดในการสื่อสาร อย่างไรก็ตาม การบันทึกธุรกรรมทุกส่วนจะส่งผลให้การสื่อสารเกิดความล่าช้า โดยมีปริมาณข้อมูลร้อยละ 0.091 ใช้เวลาเดินทางในระบบเฉลี่ยเกิน 1 วินาทีเล็กน้อย

Thesis Title Internet of Things Logging Mechanism for Patient Monitoring Applications
Author Mister Piyawat Maneenual
Major Program Management of Information Technology
Academic Year 2018

ABSTRACT

This research aims to design and evaluate the logging pattern suitable for Internet of things usage in medical fields with NETPIE, developed by National Electronics and Computer Technology Center (NECTEC), which reduces the distance issue in the patient monitoring applications and stores the health information of each period in details. The proposed logging mechanism uses the basic communication information without violating the data owner. There are three logging types including logging at things, logging at NETPIE and logging both. There are four issues to be checked by the system including new device, complete communication, complete communication with delay, and data lost.

The evaluation result from 4 sensors on each patient; there are 30 patients; the data is sent every 250ms to the doctor computer at the hospital via NETPIE using each logging type. The results show that the logging mechanism can detect all new connections and delays. However, the lost and delay can be detected differently for each logging type. For logging at things only, the lost cannot be detected. For logging at NETPIE only, the lost-before-NETPIE cannot be detected. For logging at both, all issues can be detected. The storage for the logging data for logging at things is 0.4%, 0.2% for the logging at NETPIE and 0.61% for logging at both. Thus, the storage for the logging data is less than 1% of all communication data. However, the logging at both can affect the delay. There are 0.91% of data take the average travel time slightly larger than 1 second.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยการให้ความช่วยเหลือแนะนำจาก ผู้ช่วยศาสตราจารย์ ดร.แสงสุรีย์ วสุพงศ์อัยยะ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาให้คำแนะนำ ข้อคิดเห็น แนวทางการวิจัย รวมถึงการตรวจสอบ และแก้ไขวิทยานิพนธ์มาโดยตลอด ผู้เขียนจึงขอกราบขอบพระคุณไว้ ณ โอกาสนี้

ผู้เขียนขอกราบขอบพระคุณ ดร.สมชัย หลิมศิโรรัตน์ ที่กรุณาให้เกียรติเป็นประธานกรรมการสอบ ดร.ปัญญยศ ไชยกาศ และรองศาสตราจารย์ ดร.อนันต์ ผลเพิ่ม กรรมการในการสอบวิทยานิพนธ์ ซึ่งได้กรุณาให้คำแนะนำและตรวจแก้ไขวิทยานิพนธ์ฉบับนี้ให้ถูกต้องสมบูรณ์ยิ่งขึ้น ซึ่งทุกท่านเป็นผู้เชี่ยวชาญที่ให้คำชี้แนะแนวทางด้านเทคนิคให้งานสามารถสำเร็จลุล่วง

ขอขอบคุณ โรงพยาบาลราษฎร์ยินดี ที่ให้เครื่องมืออุปกรณ์ระหว่างการทดลองตลอดงานวิจัย ตลอดจนให้ใช้อุปกรณ์แม่ข่าย และให้คำปรึกษาด้านข้อมูลทางการแพทย์ที่เป็นประโยชน์ในการจัดทำวิทยานิพนธ์ให้ผู้เขียนตลอดมา ทำให้การค้นคว้าหาข้อมูลในการจัดทำวิทยานิพนธ์ของผู้เขียนครั้งนี้สำเร็จลุล่วงไปด้วยดี

ท้ายนี้ผู้เขียนขอขอบคุณผู้ที่เกี่ยวข้องอื่น ๆ ที่มีส่วนช่วยเหลืออำนวยความสะดวกตลอดมาในการจัดทำวิทยานิพนธ์ให้สำเร็จลุล่วงไปด้วยดี อีกทั้งบิดา มารดา ครอบครัวของผู้เขียน และผู้สนับสนุนทุกท่านที่คอยให้กำลังใจช่วยเหลือตลอดมา ตลอดจนผู้เขียนหนังสือ และบทความที่เกี่ยวข้องต่าง ๆ ที่ให้ความรู้แก่ผู้เขียนจนสามารถจัดทำวิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี

ปิยวัฒน์ มณีนวล

สารบัญ

รายการภาพประกอบ .....(11)

รายการตาราง .....(13)

บทที่ 1 บทนำ 1

1.1 ที่มาและความสำคัญ..... 1

1.2 วัตถุประสงค์..... 2

1.3 ขอบเขตของการวิจัย..... 2

1.4 ประโยชน์ที่คาดว่าจะได้รับ..... 3

1.5 ขั้นตอนและวิธีการดำเนินการวิจัย 3

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 4

2.1 ทฤษฎีและหลักการ..... 4

2.1.1 อินเตอร์เน็ตออฟทิง (Internet of Things)..... 4

2.1.2 การสื่อสารระหว่างสรรพสิ่งด้านการแพทย์ผ่านอินเตอร์เน็ต..... 7

2.1.3 เน็ตพาย..... 8

2.1.4 การบันทึกธุรกรรม..... 10

2.1.5 เครื่องมืออุปกรณ์ทางการแพทย์และการให้บริการสุขภาพ..... 11

2.2 งานวิจัยที่เกี่ยวข้อง 14

บทที่ 3 ระเบียบวิธีวิจัย 19

3.1 ผลการรวบรวมข้อมูลเกี่ยวกับอุปกรณ์ทางการแพทย์สำหรับผู้ป่วย 19

3.2 รูปแบบธุรกรรมที่จัดการโดยระบบบันทึกธุรกรรม..... 20

3.2.1 อุปกรณ์ใหม่ที่เชื่อมต่อเข้ามาครั้งแรก..... 20

สารบัญ (ต่อ)

บทที่ 3 ระเบียบวิธีวิจัย (ต่อ)

3.2.2 ข้อมูลธุรกรรมการรับส่งข้อมูลอย่างปกติสมบูรณ์ 22

3.2.3 ข้อมูลธุรกรรมการรับส่งข้อมูลที่สมบูรณ์แต่ล่าช้า 24

3.2.4 ข้อมูลธุรกรรมการรับส่งข้อมูลที่ไม่สมบูรณ์ 24

3.2.5 การวิเคราะห์ความผิดปกติ 26

3.3 การจัดเก็บข้อมูลธุรกรรม 27

3.3.1 ระบบฐานข้อมูล 28

3.3.2 กระบวนการเข้ารหัสข้อมูล 31

3.4 กระบวนการจัดเก็บข้อมูลธุรกรรม 32

3.5 การทดสอบระบบ 35

3.6 การวิเคราะห์ข้อมูล 43

3.6.1 การวิเคราะห์อัตรารับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม 43

3.6.2 การวิเคราะห์ขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย 44

3.6.3 การวิเคราะห์ผลการบันทึกธุรกรรมทางการแพทย์ผ่านเน็ตพาย 44

บทที่ 4 ผลการทดลองและวิเคราะห์ผล 46

4.1 การทดสอบเพื่อหาอัตราการรับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม 46

4.2 การทดสอบเพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย 50

4.3 การทดสอบบันทึกธุรกรรมทางการแพทย์ในสภาพแวดล้อมของเน็ตพาย 52

4.4 แนวทางการประยุกต์ใช้ระบบบันทึกธุรกรรมที่นำเสนอ 63

บทที่ 5 บทสรุปและข้อเสนอแนะ 65

5.1 สรุปผลการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งแบบต่าง ๆ 67

สารบัญ (ต่อ)

บทที่ 5 บทสรุปและข้อเสนอแนะ (ต่อ)

5.1.1 สรุปผลการแบบไม่บันทึกธุรกรรม 67

5.1.2 สรุปผลการแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น 67

5.1.3 สรุปผลการแบบบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น 67

5.1.4 สรุปผลการแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด 68

5.2 ข้อเสนอแนะ 69

บรรณานุกรม 70

ภาคผนวก ก 73

ภาคผนวก ข 75

ภาคผนวก ค 79

ประวัติผู้เขียน 87

รายการภาพประกอบ

รูปที่ 1 แผนภาพการรับส่งข้อมูลในรูปแบบโพรโทคอลเอ็มคิวทีที 5
รูปที่ 2 แผนผังความสัมพันธ์ด้านความปลอดภัยของแต่ละโหนด 15
รูปที่ 3 แนวคิดการรับส่งข้อมูลอย่างปลอดภัยของวาโทรและคณะ 16
รูปที่ 4 แนวคิดการรับส่งข้อมูลอย่างปลอดภัยของโวรูกันติและคณะ 16
รูปที่ 5 แนวคิดการรับส่งข้อมูลอย่างปลอดภัยของภูมิภัทร สุขภิมนตรี และศุภกร กังพิสดาร..... 18
รูปที่ 6 เหตุการณ์การรับข้อมูลจากอุปกรณ์ใหม่ไปยังสรรพสิ่งปลายทาง..... 21
รูปที่ 7 การรับส่งข้อมูลระหว่างอุปกรณ์อย่างสมบูรณ์..... 23
รูปที่ 8 การวิเคราะห์ธุรกรรมการรับส่งข้อมูลระหว่างอุปกรณ์อย่างสมบูรณ์ 23
รูปที่ 9 การส่งข้อมูลสูญหายระหว่างส่งจากสรรพสิ่งต้นทางไปยังเน็ตพาย 24
รูปที่ 10 การส่งข้อมูลสูญหายระหว่างส่งจากเน็ตพายไปยังสรรพสิ่งปลายทาง..... 25
รูปที่ 11 ภาพรวมระบบวิเคราะห์ธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต 26
รูปที่ 12 ส่วนประกอบระบบบันทึกธุรกรรม..... 29
รูปที่ 13 ตัวอย่างหน้ารายงานแสดงข้อมูลธุรกรรมความผิดปกติที่พบ..... 31
รูปที่ 14 แนวคิดการเข้ารหัสข้อมูลเพื่อส่งข้อมูลจาก Publisher ไปยัง Broker 33
รูปที่ 15 โครงสร้างแนวคิดการยืนยันตัวตนสำหรับการบันทึกธุรกรรม..... 34
รูปที่ 16 แนวคิดการยืนยันตัวตนจากข้อมูลที่เข้ารหัสในฐานข้อมูล AuthDB 34
รูปที่ 17 แนวคิดการเข้ารหัสข้อมูลเพื่อส่งข้อมูลจาก Broker ไปยัง Subscriber 34
รูปที่ 18 ออกแบบการจำลองเหตุการณ์สื่อสารข้อมูลสุขภาพระหว่างผู้ป่วยกับโรงพยาบาล..... 36
รูปที่ 19 ตัวอย่างข้อมูลธุรกรรมของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตทั้งหมด 38
รูปที่ 20 รูปแบบภาพรวมการทดลองบันทึกธุรกรรมทางการแพทย์ในสภาพแวดล้อมของเน็ตพาย .. 40
รูปที่ 21 รูปแบบการวัดค่าผู้ป่วยโดยไม่บันทึกธุรกรรม..... 40
รูปที่ 22 รูปแบบการผู้ป่วยโดยบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น 40
รูปที่ 23 รูปแบบการวัดค่าผู้ป่วยโดยบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น..... 41
รูปที่ 24 รูปแบบการวัดค่าผู้ป่วยโดยบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด 41
รูปที่ 25 รูปแบบการบันทึกธุรกรรมในระหว่างการสื่อสารของสรรพสิ่ง..... 41
รูปที่ 26 รูปแบบการบันทึกธุรกรรมในระหว่างการสื่อสารของสรรพสิ่ง..... 42
รูปที่ 27 โครงสร้างเครือข่ายของแต่ละสรรพสิ่งที่เชื่อมต่อเน็ตพาย 66

รายการภาพประกอบ (ต่อ)

รูปที่ 28 ตัวอย่างข้อมูลทางการแพทย์ที่ส่งออกจากสรรพสิ่งของผู้ป่วย 74
รูปที่ 29 ตัวอย่างข้อมูลธุรกรรมในฐานข้อมูล RowLog 76
รูปที่ 30 ตัวอย่างข้อมูลธุรกรรมในฐานข้อมูล NetpieLog 77
รูปที่ 31 ตัวอย่างข้อมูลธุรกรรมในฐานข้อมูล ConnectDB 78

รายการตาราง

ตารางที่ 1 ตัวอย่างฐานข้อมูลการเชื่อมต่อระหว่างอุปกรณ์กับอุปกรณ์ ConnectDB 21
ตารางที่ 2 ข้อมูลการบันทึกธุรกรรมทั้งหมด 27
ตารางที่ 3 ข้อมูลการบันทึกธุรกรรมที่ผิดปกติ 28
ตาราง 4 ตารางเวลาการเริ่มส่งข้อมูลของสรรพสิ่งทั้ง 30 อุปกรณ์เป็นเวลาอุปกรณ์ละ 24 ชั่วโมง ... 43
ตาราง 5 ตารางแผนการเริ่มส่งข้อมูลของสรรพสิ่งทั้ง 30 อุปกรณ์เป็นเวลาอุปกรณ์ละ 24 ชั่วโมง ... 45
ตาราง 6 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 1 วินาที 47
ตาราง 7 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 500 มิลลิวินาที 47
ตาราง 8 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 250 มิลลิวินาที 48
ตาราง 9 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 125 มิลลิวินาที 48
ตาราง 10 ตารางผลการทดลองจำนวนอุปกรณ์การส่งข้อมูลทุก ๆ 250 มิลลิวินาที 49
ตาราง 11 ตารางแสดงผลภาพรวมของสรรพสิ่งที่ 16 ชิ้น ในการส่งข้อมูลในแต่ละชั่วโมง 50
ตาราง 12 ตารางผลการเปรียบเทียบเวลากับขนาดข้อมูล 51
ตาราง 13 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบไม่บันทึกธุรกรรม 53
ตาราง 14 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่ง ... 54
ตาราง 15 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบบันทึกธุรกรรมเฉพาะเน็ตพาย 55
ตาราง 16 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบบันทึกธุรกรรมทุกส่วน 56
ตาราง 17 ตารางสรุประยะเวลาการสื่อสารของการทดลองแต่ละแบบ 57
ตาราง 18 ตารางจำนวนข้อมูลธุรกรรมที่พบการสูญหายของข้อมูลการสื่อสารในแต่ละชั่วโมง
และแต่ละสรรพสิ่งใน 24 ชั่วโมง 59
ตาราง 19 ตารางแสดงการตรวจพบกรณีความผิดปกติในการสื่อสารจากการทดลองด้วยธุรกรรม ... 60
ตาราง 20 ผลการทดลองการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่ง
ผ่านอินเตอร์เน็ตทั้ง 4 แบบ 62

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

อินเตอร์เน็ตออฟทิง (Internet of Things) หรือ ไอโอที (IoT) [1] คือ แนวคิดอันประกอบไปด้วยสรรพสิ่ง (Things) ที่สามารถสื่อสารและเชื่อมต่อกันได้ผ่านอินเตอร์เน็ตซึ่งเป็นโพรโทคอลที่นิยมใช้ในการสื่อสารกันทั่วโลกทั้งแบบใช้สายและไร้สาย เพื่อให้สามารถลดข้อจำกัดด้านระยะทางการสื่อสารและรูปแบบระบบปฏิบัติการ จึงทำให้ทุกสรรพสิ่งมีปฏิสัมพันธ์และทำงานร่วมกันได้ ตัวอย่างเช่น การควบคุมเครื่องใช้ไฟฟ้าผ่านโทรศัพท์มือถือ หรือการควบคุมเครื่องใช้ไฟฟ้าจากการอ่านค่าสภาพแวดล้อมต่าง ๆ เป็นต้น ทำให้การสื่อสารระหว่างอุปกรณ์ทำงานร่วมกันได้อย่างดียิ่งขึ้น แต่อย่างไรก็ตาม โพรโทคอลที่ใช้ในการสื่อสารเป็นช่องทางสาธารณะ จึงเป็นช่องทางให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบได้ ดังนั้นโพรโทคอลสำหรับการเชื่อมต่อทุกสรรพสิ่งจะต้องมีการควบคุมด้านความปลอดภัยเพื่อป้องกันการกระทำใด ๆ จากผู้ไม่หวังดีในการโจรกรรมข้อมูลจากสรรพสิ่ง รวมถึงควบคุมสรรพสิ่งให้ทำงานอย่างถูกต้องตามวัตถุประสงค์ของผู้ใช้ [2] ซึ่งปัจจุบันการสื่อสารของสรรพสิ่งหนึ่งไปยังอีกสรรพสิ่งนั้นจะเชื่อมต่อจากกุญแจสาธารณะของระบบที่ทำหน้าที่เป็นตัวกลางการเชื่อมต่อ เมื่อสรรพสิ่งสามารถเชื่อมต่อสำเร็จ จะได้รับกุญแจส่วนตัวสำหรับสรรพสิ่งนั้นในการเข้าระบบในครั้งต่อไป [3] ทำให้สามารถยืนยันตัวตนในการสื่อสารได้

การบันทึกธุรกรรมของกิจกรรมต่าง ๆ ที่เกิดขึ้นในระบบอย่างเหมาะสม จึงมีความสำคัญในการสื่อสารของทุกสรรพสิ่ง เพื่อให้สามารถตรวจสอบความมั่นคงปลอดภัยของระบบภายหลังผ่านการติดตามสิ่งผิดปกติที่เกิดขึ้นในการสื่อสาร หากในกระบวนการสื่อสารของสรรพสิ่งไม่มีการบันทึกข้อมูลธุรกรรม อาจเป็นช่องทางให้ผู้ไม่หวังดีสามารถกระทำการใด ๆ ในระบบโดยไม่สามารถตรวจสอบได้ ทำให้การควบคุมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตไม่ปลอดภัยและไม่น่าเชื่อถือ แต่เนื่องจากการสื่อสารของทุกสรรพสิ่งมีรูปแบบการรับส่งข้อมูลตลอดเวลา ทำให้รูปแบบข้อมูลธุรกรรมของเหตุการณ์ที่เกิดขึ้นมีปริมาณมาก อีกทั้งสรรพสิ่งปัจจุบันรวมถึงเซ็นเซอร์หลายชนิดซึ่งไม่มีส่วนสำหรับการจัดเก็บข้อมูล จึงทำให้ไม่สามารถบันทึกข้อมูลธุรกรรมการสื่อสารระหว่างสรรพสิ่งได้อย่างสมบูรณ์และเหมาะสม ดังนั้นจึงต้องมีกระบวนการจัดการรูปแบบการบันทึกธุรกรรมที่เกิดขึ้นระหว่างการสื่อสารของสรรพสิ่ง เพื่อตรวจสอบสิ่งผิดปกติที่เกิดขึ้นและป้องกันผู้ไม่หวังดีในการก่อกวนการควบคุมสรรพสิ่งผ่านอินเตอร์เน็ต

แนวทางการจัดการส่วนของการบันทึกข้อมูลธุรกรรมสำหรับแนวคิดการเชื่อมต่อทุกสรรพสิ่งผ่านอินเตอร์เน็ตนั้น ต้องประกอบไปด้วยการจัดเก็บข้อมูลธุรกรรมการสื่อสารของทุกสรรพสิ่ง โดยมีกระบวนการบันทึกข้อมูลธุรกรรมที่เหมาะสมกับรูปแบบของการบันทึกกิจกรรมการสื่อสารที่เกิดขึ้นตลอดเวลา [4][5] อีกทั้ง ข้อมูลที่มีปริมาณมากจึงต้องมีกระบวนการคัดแยกข้อมูลในปริมาณที่เหมาะสมตามความจำเป็น โดยมีการจัดเก็บเฉพาะส่วนที่ผ่านการวิเคราะห์สรุปข้อมูลกิจกรรมต่าง ๆ ซึ่งประกอบไปด้วย ข้อมูลการยืนยันตัวตนของสรรพสิ่ง ข้อมูลการปฏิสัมพันธ์ตอบโต้ระหว่างสรรพสิ่ง ข้อมูลสถานะปัจจุบันของสรรพสิ่ง และข้อมูลควบคุมการสั่งการสรรพสิ่งให้ดำเนินการ เป็นต้น ทั้งนี้รูปแบบข้อมูลที่ตรวจสอบคือข้อมูลกิจกรรมที่เกิดขึ้นเป็นหลัก ไม่สนใจข้อมูลภายในการสื่อสาร เพื่อให้สามารถวิเคราะห์สิ่งที่เกิดขึ้นในระบบได้อย่างมีประสิทธิภาพและไม่ละเมิดความเป็นส่วนตัวของการสื่อสารระหว่างสรรพสิ่งของผู้ใช้ เพื่อให้การสั่งการควบคุมสรรพสิ่งต่าง ๆ ในทุกการดำเนินการรวมถึงข้อมูลจากการสื่อสารระหว่างสรรพสิ่งในระบบมีความน่าเชื่อถือ และปลอดภัยสำหรับการนำไปใช้งานมากยิ่งขึ้น [6] ทั้งนี้ผู้พัฒนาได้เลือกเน็ตพาย (NETPIE) เป็นต้นแบบผู้ให้บริการในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตในการพัฒนาแนวคิดการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งเนื่องจากผู้ให้บริการดังกล่าวพัฒนาในประเทศไทย ทำให้ประสิทธิภาพในการพัฒนาเป็นไปได้ดี และสามารถติดต่อประสานงานกับผู้พัฒนาได้ อีกทั้งเป็นการช่วยส่งเสริมการพัฒนานวัตกรรมภายในประเทศให้มีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์

1.2.1 ออกแบบโพรโทคอลบันทึกธุรกรรมของสรรพสิ่งผ่านอินเตอร์เน็ตสำหรับเน็ตพาย

1.2.2 พัฒนาต้นแบบโพรโทคอลบันทึกธุรกรรมสรรพสิ่งบนอินเตอร์เน็ตสำหรับเน็ตพาย

1.2.3 ทดสอบโพรโทคอลต้นแบบที่ได้พัฒนาขึ้นภายใต้บริบททางการแพทย์

1.3 ขอบเขตของการวิจัย

งานวิจัยชิ้นนี้มีเป้าหมายการออกแบบและพัฒนาต้นแบบการบันทึกธุรกรรมของโพรโตคอลการสื่อสารระหว่างสรรพสิ่งด้านการแพทย์ผ่านเน็ตพายโดยมีข้อจำกัด ดังนี้

1.3.1 ผู้ใช้และสรรพสิ่งต้องได้รับการลงทะเบียนสำหรับกระบวนการยืนยันตัวตนในการสื่อสารสำหรับการบันทึกธุรกรรม

1.3.2 โพรโทคอลการสื่อสารระหว่างสรรพสิ่งดำเนินการผ่านเน็ตพาย

1.3.3 ข้อมูลในการสื่อสารเป็นการส่งข้อมูลตามลำดับเวลาการส่งข้อมูลโดยไม่ขึ้นกับระดับความสำคัญของข้อมูลที่ใช้ในการสื่อสาร

1.3.4 ออกแบบต้นแบบการบันทึกธุรกรรมข้อมูลสุขภาพส่วนบุคคลด้วยการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตเท่านั้น

1.3.5 การวัดประสิทธิภาพดำเนินการผ่านการจำลองข้อมูลและทดสอบบนต้นแบบสรรพสิ่งด้านการแพทย์สำหรับผู้ป่วย 30 อุปกรณ์ที่มหาวิทยาลัยสงขลานครินทร์ส่งข้อมูลไปยังสรรพสิ่งสำหรับให้แพทย์อ่านผลที่โรงพยาบาลราษฎร์ยินดี 1 อุปกรณ์ ซึ่งมีระยะห่าง 3 กิโลเมตรในอำเภอหาดใหญ่ จังหวัดสงขลา

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 แนวคิดการบันทึกธุรกรรมที่เหมาะสมกับการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตที่เหมาะสมสำหรับข้อมูลทางการแพทย์

1.4.2 ระบบต้นแบบในการบันทึกธุรกรรมสำหรับการสื่อสารที่มีข้อมูลจำนวนมากในรูปแบบที่เหมาะสมและมีความน่าเชื่อถือ

1.5 ขั้นตอนและวิธีการดำเนินการวิจัย

1.5.1 รวบรวมความต้องการรูปแบบข้อมูลของโปรแกรมหรือระบบในสิ่งแวดล้อมที่มีการใช้งานโพรโทคอลการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตด้านการแพทย์

1.5.2 ออกแบบและพัฒนาระบบต้นแบบการบันทึกธุรกรรมในรูปแบบที่เหมาะสมกับโพรโทคอลการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตด้านการแพทย์

1.5.3 ทดสอบระบบต้นแบบการบันทึกธุรกรรมโดยการจำลองข้อมูลจากสิ่งแวดล้อมที่ได้รวบรวมมา ภายใต้บริบททางการแพทย์

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีและหลักการ

การบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตนั้น ต้องอาศัยโพรโทคอลพื้นฐานสำหรับการสื่อสารในแนวคิดที่เรียกว่าอินเตอร์เน็ตออฟทิง (Internet of Things) เพื่อให้การบันทึกธุรกรรมเป็นไปในทิศทางเดียวกับสิ่งที่เกิดขึ้นในการสื่อสารที่ตรงกับความเป็นจริง โดยใช้หลักการต่อไปนี้

2.1.1 อินเตอร์เน็ตออฟทิง (Internet of Things)

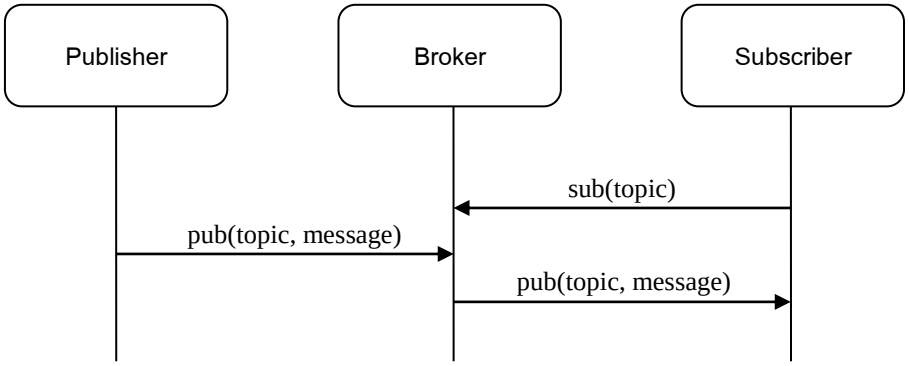
อินเตอร์เน็ตออฟทิง (Internet of Things) หรือ ไอโอที (IoT) คือ แนวคิดอันประกอบไปด้วยสรรพสิ่งที่สามารถสื่อสารและเชื่อมต่อกันได้ผ่านอินเตอร์เน็ตซึ่งเป็นโพรโทคอลที่นิยมใช้ในการสื่อสารกันทั่วโลกทั้งแบบใช้สายและไร้สายผ่านโพรโทคอลเอ็มคิวทีที (MQTT หรือ Message Queue Telemetry Transport) [7] ซึ่งเป็นช่องทางการสื่อสารในรูปแบบรับส่งข้อมูลแบบกลุ่มเมฆโดยไม่จำกัดรูปแบบของระบบปฏิบัติการ ผ่านตัวกลางในการจัดการการสื่อสาร ระหว่างสรรพสิ่ง (MQTT Broker) เพื่อทำหน้าที่ในการแปลงรูปแบบข้อมูลในการรับส่งไปยังสรรพสิ่งปลายทางที่ต้องการภายใต้หัวข้อ (Topic) ที่สรรพสิ่งสนใจ ทั้งนี้สรรพสิ่งปลายทางจะต้องมีส่วนของการรับข้อมูลการสื่อสารแบบเอ็มคิวทีทีเช่นกัน

รูปแบบการสื่อสารผ่านโพรโทคอลเอ็มคิวทีทีประกอบไปด้วย 3 ส่วนดังต่อไปนี้ [8]

- ผู้เผยแพร่ข้อมูล (Publisher) คือส่วนในการทำหน้าที่ส่งข้อมูลไปยังตัวกลางการสื่อสารในหัวข้อ (Topic) ที่กำหนด
- ตัวกลางการสื่อสาร (Broker) คือส่วนที่จะทำหน้าที่เป็นตัวกลางคอยจัดการรับส่งข้อมูล (Message) โดยอ้างอิงจากหัวข้อที่สรรพสิ่งกำหนด
- ผู้ติดตามข้อมูล (Subscriber) คือส่วนที่ทำหน้าที่รับข้อมูลจากตัวกลางการสื่อสารในหัวข้อที่ติดตามไว้ ซึ่งจะประมวลผลเมื่อข้อมูลเกิดการเปลี่ยนแปลง

ทั้งนี้การรับส่งข้อมูลในโพรโทคอลเอ็มคิวทีทีมีความสัมพันธ์โดยเริ่มจากผู้ติดตามข้อมูลเป็นผู้ระบุหัวข้อที่สนใจไปยังตัวกลางการสื่อสารเพื่อรอรับข้อมูล จากนั้นเมื่อผู้เผยแพร่ข้อมูลเริ่มส่งข้อมูลที่กำหนดหัวข้อไปยังตัวกลางการสื่อสารสำเร็จ ตัวกลางการสื่อสารจะทำหน้าที่เป็นตัวกลาง

คอยจัดการส่งข้อมูลที่กำหนดหัวข้อจากผู้เผยแพร่ข้อมูลไปยังผู้ติดตามข้อมูลที่กำลังรอรับข้อมูลในหัวข้อที่ผู้ติดตามข้อมูลสนใจตรงกับหัวข้อที่ผู้เผยแพร่ข้อมูลส่งข้อมูลมา ดังแสดงในรูปที่ 1



รูปที่ 1 แผนภาพการรับส่งข้อมูลในรูปแบบโพรโทคอลเอ็มคิวทีที [8]

ดังนั้นการรับส่งข้อมูลผ่านโพรโทคอลเอ็มคิวทีทีสามารถสนับสนุนการสื่อสารระหว่างสรรพสิ่งเฉพาะข้อมูลที่ต้องการโดยไม่มีข้อจำกัดของระบบปฏิบัติการ เพราะการจัดการข้อมูลการสื่อสารจะดำเนินการที่ตัวกลางการสื่อสารทั้งหมด โดยผู้เผยแพร่ข้อมูลทำหน้าที่ส่งข้อมูลและหัวข้อไปให้ตัวกลางการสื่อสารเท่านั้น ในขณะเดียวกันผู้ติดตามข้อมูลมีหน้าในการส่งหัวข้อที่สนใจไปให้ตัวกลางการสื่อสารและรอรับข้อมูลจากหัวข้อที่สนใจจากตัวกลางการสื่อสาร ซึ่งจะคัดแยกมาให้

อย่างไรก็ตามรูปแบบการรับส่งข้อมูลของสรรพสิ่งจำเป็นต้องมีการสื่อสารที่สอดคล้องกับเวลาจริง (Real Time) จึงต้องคำนึงถึงความเร็วในการสื่อสารรวมถึงคุณภาพของการรับส่งข้อมูล ทำให้ต้องมีการจัดการคุณภาพของการให้บริการ (Quality of Service หรือ QoS) [9] ซึ่งเป็นส่วนในการกำหนดรูปแบบการสื่อสารข้อมูล

รูปแบบของการรับรองคุณภาพการสื่อสารในการให้บริการของโพรโทคอลเอ็มคิวทีทีของการสื่อสารด้วยสรรพสิ่งมี 3 รูปแบบ ดังต่อไปนี้

- คิวโอเอส 0 คือ รูปแบบการส่งข้อมูลเพียงครั้งเดียว โดยไม่รอรับการตอบกลับจากปลายทาง การสื่อสารรูปแบบนี้มีความรวดเร็ว แต่ไม่รับรองโอกาสความสำเร็จในการสื่อสาร
- คิวโอเอส 1 คือ รูปแบบการส่งข้อมูลเพียงครั้งเดียว โดยไม่รอรับการตอบกลับจากปลายทาง แต่จะเก็บข้อมูลล่าสุดไว้เสมอ เมื่อมีสรรพสิ่งปลายทางเชื่อมต่อเข้ามา จะได้รับข้อมูลล่าสุด
- คิวโอเอส 2 คือ รูปแบบการส่งข้อมูลจนกว่าปลายทางจะได้รับข้อมูล ซึ่งจะมีการตรวจสอบสถานะการสื่อสารตลอดเวลา ทำให้มีความแม่นยำในการสื่อสารสูงสุด แต่ความรวดเร็วในการสื่อสารจะน้อยกว่าคิวโอเอส 0 และคิวโอเอส 1

ปัจจุบันได้มีผู้ให้บริการสำหรับเป็นตัวกลางในการสื่อสารระหว่างสรรพสิ่งที่หลากหลาย ซึ่งมีรูปแบบการอำนวยความสะดวกในการสื่อสารที่แตกต่างกันทั้งในด้านช่องทางการสื่อสารและความปลอดภัยในการรับส่งข้อมูล ตัวอย่างผู้ให้บริการดังนี้

เน็ตพาย (NETPIE) [10] คือ แพรตฟอร์มแบบกลุ่มเมฆที่ให้บริการในรูปแบบการให้บริการแพลตฟอร์ม (Platform-as-a-Service) เพื่ออำนวยความสะดวกให้กับนักพัฒนาสามารถพัฒนาให้อุปกรณ์ของตัวเองเชื่อมต่อและแลกเปลี่ยนข้อมูลกันได้ในแบบ การสื่อสารระหว่างสรรพสิ่ง (Internet of Things) ผลิตในประเทศไทย พัฒนาโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) มีการจัดการด้านความปลอดภัย โดยนำโอออท (OAuth) เข้ามาจัดการสำหรับการยืนยันตัวโดยใช้โทเคน (Token) รวมถึงการเข้ารหัสข้อมูลการยืนยันตัวตนในการสื่อสารโดยการใช้ข้อมูล APPID, APPKEY และ APPSECRET ในระบบที่จะสร้างขึ้นสำหรับการเชื่อมต่อเฉพาะให้กับอุปกรณ์นั้น ๆ โดยสามารถกำหนดสิทธิ์การใช้งานได้อีกด้วย

Cloudmqtt [11] เป็นผู้ให้บริการที่เปิดช่องทางการสื่อสารที่หลากหลาย ได้แก่ MQTT broker, SSL, ACL และ Websocket Monitor มีการเข้ารหัสข้อมูลการส่งข้อมูล แต่ถ้าใช้ในประเทศไทยแม่ข่ายอยู่ต่างประเทศทำให้การสื่อสารเกิดความล่าช้ากว่าระยะเวลาที่ MQTT กำหนดขั้นต่ำไว้

Xively [12] เป็นในรูปแบบการให้บริการแพลตฟอร์ม (Platform-as-a-Service) สำหรับการสื่อสารระหว่างสรรพสิ่ง (Internet of Things) โดยสามารถเขียน/อ่านข้อมูลที่ได้จากเซ็นเซอร์ไปเก็บไว้ที่แม่ข่าย และข้อมูลสามารถเก็บได้หลายแบบไม่ว่าจะเป็นค่าตัวเลข พิกัด และสามารถทำทริกเกอร์ (Triggers) ผ่านพอร์ตเฮชทีทีพี (Http Post) ได้ หากค่าที่อ่านได้จากเซ็นเซอร์ตรงกับเงื่อนไขที่ตั้งไว้ เช่น หากมีแสงแดดอุณหภูมิมากกว่า 35 องศาเซลเซียสให้เปิดเครื่องรดน้ำต้นไม้ หรือถ้าอุณหภูมิลดลงเหลือ 30 ให้ปิดเครื่องรดน้ำ เป็นต้น

IBM Bluemix [13] มีการจัดการความมั่นคงปลอดภัยต่าง ๆ ประกอบด้วยการเปิดปิดการใช้งานเอพีไอคีย์ (API Key) เป็นช่วงเวลา สื่อสารผ่านในรูปแบบเอสเอสแอล (SSL) ทั้งหมด อีกทั้งมีส่วนในการจัดการสรรพสิ่งที่กำลังสื่อสาร

อย่างไรก็ตาม จากตัวอย่างผู้ให้บริการที่ยกตัวอย่าง ผู้ให้บริการเน็ตพายมีความเหมาะสมที่จะนำมาพัฒนาแนวคิดการจัดเก็บธุรกรรมสำหรับการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต เนื่องจากเป็นแพรตฟอร์มฟรี และมีการยืนยันตัวตนพื้นฐานที่สะดวกต่อการใช้งานในสรรพสิ่งต่าง ๆ อีกทั้งเป็นแพรตฟอร์มที่พัฒนาในประเทศไทย ทำให้การทดลองในการสื่อสารมีประสิทธิภาพและสามารถติดต่อสอบถามกับผู้พัฒนาแพรตฟอร์มได้

2.1.2 การสื่อสารระหว่างสรรพสิ่งด้านการแพทย์ผ่านอินเตอร์เน็ต (Healthcare Internet of Things: HIoT) [14]

การสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตถูกนำมาใช้ในงานด้านต่าง ๆ เพื่อช่วยลดข้อจำกัดการสื่อสารระหว่างอุปกรณ์ ก่อให้เกิดการนำสภาพแวดล้อมสู่ระบบดิจิตอล ทำให้อุปกรณ์ต่าง ๆ สามารถเชื่อมต่อสื่อสารกันได้ในรูปแบบอุปกรณ์อัจฉริยะที่ทำงานร่วมกัน ทั้งนี้หัวข้อเรื่องสุขภาพและสาธารณสุขเป็นประเด็นที่น่าสนใจสำหรับแนวคิดการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต เพื่อเพิ่มประสิทธิภาพการรักษาแบบทันทีโดยแพทย์และผู้เกี่ยวข้องกับการรักษาสามารถติดตามผลสุขภาพและการรักษาต่าง ๆ ได้ตลอดเวลา ส่งเสริมให้การรักษามีความปลอดภัยและเกิดความแม่นยำยิ่งขึ้น อย่างไรก็ตาม เนื่องจากข้อมูลในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตเป็นโพรโตคอลสาธารณะ อาจเกิดความเสี่ยงต่อสิทธิ์ความเป็นส่วนตัวของผู้ป่วย จึงควรมีการจัดการสิทธิ์และมาตรฐานความปลอดภัยที่ดี ได้แก่ ความปลอดภัยระดับเซ็นเซอร์อุปกรณ์ทางการแพทย์ อุปกรณ์ทางการสื่อสาร การเข้ารหัสข้อมูล และการอนุญาตให้เข้าถึงข้อมูลต่าง ๆ รวมถึงบุคลากรทางการแพทย์ตามความต้องการของผู้ป่วยซึ่งเป็นเจ้าของข้อมูล

ทั้งนี้อุปกรณ์ทางการแพทย์ได้รับการกำหนดบทบาทไว้เพื่ออ่านค่าข้อมูลหรือสั่งการรูปแบบใด ๆ ตัวอย่างติดตั้งสรรพสิ่งด้านสุขภาพในบ้านผู้สูงอายุ อาจประกอบด้วยเซ็นเซอร์ติดตั้งภายนอกเพื่อตรวจสอบและวัดค่าสภาพแวดล้อมในบ้านผู้สูงอายุ เช่น เซ็นเซอร์วัดอุณหภูมิ กล้องอินฟราเรด เซ็นเซอร์อาเอฟไอดี (RFID) เพื่อตรวจสอบการเคลื่อนไหวของผู้สูงอายุ เป็นต้น และการติดตั้งเซ็นเซอร์บนร่างกายผู้สูงอายุ เช่น นาฬิกาวัดข้อมูลสุขภาพ อุปกรณ์วัดค่าติดตามร่างกาย แว่นตา หรืออุปกรณ์สวมใส่วัดค่าต่าง ๆ เป็นต้น โดยทุกสรรพสิ่งสามารถสื่อสารกันได้อย่างอัจฉริยะและมีความเชื่อมโยงกัน มีการแจ้งเตือนเมื่อเกิดความเสี่ยงต่อสุขภาพและความปลอดภัย ได้แก่ กรณีพบการเคลื่อนที่เร็วผิดปกติในแนวดิ่งจากเซ็นเซอร์ต่าง ๆ อาจเป็นกรณีที่ผู้สูงอายุเกิดการหกล้มหรือประสบอุบัติเหตุ รวมถึงกรณีค่าข้อมูลสุขภาพมีความผิดปกติจากการตรวจพบในเซ็นเซอร์ต่าง ๆ เช่น อัตราการเต้นของหัวใจ ระดับน้ำตาลในเลือด และความดันที่เกินค่ามาตรฐานเพื่อการช่วยเหลือในการเข้ารักษาทันท่วงที

รูปแบบดังกล่าวสามารถใช้ประโยชน์จากคุณสมบัติของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตเข้ามาเสริมรูปแบบการรักษาทางการแพทย์ โดยเฉพาะในกรณีที่ต้องการติดตามข้อมูลสุขภาพและความปลอดภัยของผู้ป่วยแบบทันทีตลอดเวลา ซึ่งทำให้ข้อมูลสุขภาพที่ใช้ในการสื่อสารระหว่างสรรพสิ่งเป็นรูปแบบข้อมูลขนาดใหญ่ (Big Data) จึงต้องมีวิธีในการบริหารจัดการอย่างมีประสิทธิภาพเพื่อให้ข้อมูลขนาดใหญ่นี้นำมาใช้เกิดประโยชน์มากที่สุด โดยทั้งนี้รูปแบบการสื่อสารระหว่างสรรพสิ่งทางการแพทย์ผ่านอินเตอร์เน็ตซึ่งประกอบไปด้วยข้อมูลสุขภาพขนาดใหญ่สามารถแบ่งย่อยและนำข้อมูลเท่าที่จำเป็นมาใช้ได้ เนื่องจากข้อมูลสุขภาพมีการเปลี่ยนแปลงแบบค่อยเป็น

ค่อยไป จึงไม่จำเป็นต้องนำข้อมูลทั้งหมดมาเก็บไว้ โดยข้อมูลถูกอาจเปลี่ยนแปลงเป็นรูปแบบข้อมูลเฉลี่ยหรือข้อมูลที่สำคัญในช่วงเวลาที่สนใจ เพื่อเป็นรูปแบบในการบริหารจัดการฐานข้อมูลขนาดใหญ่สำหรับข้อมูลสุขภาพส่วนบุคคล

2.1.3 เน็ตพาย

เน็ตพาย (NETPIE) คือ ผู้ให้บริการในรูปแบบการให้บริการแพลตฟอร์ม (Platform-as-a-Service) เพื่ออำนวยความสะดวกให้กับนักพัฒนาในการพัฒนาการเชื่อมต่อและแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ได้ในแบบการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตที่พัฒนาโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ผลิตในประเทศไทยเพื่อเป็นแพลตฟอร์มกลางในการสื่อสารภายใต้แนวคิดของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตซึ่งพัฒนาโดยคนไทย มีคุณลักษณะแนวคิดเพื่อในการจัดการการสื่อสารระหว่างอุปกรณ์ทุกชนิดที่สามารถเชื่อมต่ออินเตอร์เน็ตได้ และสามารถรับส่งข้อมูลไปยังตัวกลางซึ่งเป็นโพรโทคอลพื้นฐานโดยไม่จำเป็นต้องรู้ที่ตั้งของสรรพสิ่ง รวมถึงรูปแบบสรรพสิ่งปลายทางที่สื่อสาร เพื่อลดกระบวนการที่ซับซ้อนในการพัฒนาการใช้งานการควบคุมสื่อสารสรรพสิ่งผ่านอินเตอร์เน็ตให้ง่ายขึ้น เนื่องจากผู้พัฒนาไม่ต้องพัฒนาส่วนของการสื่อสารในอุปกรณ์ที่แตกต่างกัน ซึ่งมีขั้นตอนที่ยุ่งยากและต้นทุนสูง โดยรูปแบบการทำงานของเน็ตพายประกอบด้วยส่วนการจัดการการสื่อสารระหว่างสรรพสิ่งที่มีความปลอดภัยผ่านการยืนยันตัวตนและจัดการสิทธิ์การรับส่งข้อมูลซึ่งเป็นตัวกลางที่สรรพสิ่งจะใช้เป็นทางผ่านในการสื่อสาร โดยตัวกลางนี้ทำหน้าที่ค้นหาและจับคู่สรรพสิ่งที่สนใจในหัวข้อเดียวกันเพื่อให้สามารถรับส่งข้อมูลกันได้

ทั้งนี้สรรพสิ่งต้องสามารถเชื่อมต่อกับตัวกลางผ่านกุญแจสาธารณะในการสื่อสารด้วยการเข้ารหัสข้อมูลผ่านช่องทางการสื่อสารอย่างปลอดภัยเสมอ ได้แก่ ทีแอลเอส (TLS หรือ Transport Layer Security) ซึ่งเป็นโพรโทคอลเข้ารหัสข้อมูลด้วยกุญแจของผู้รับเพื่อยืนยันความถูกต้องของข้อมูล และยืนยันตัวตนของผู้สนทนาในระดับชั้นการสื่อสาร โดยส่งเสริมให้ข้อมูลมีความน่าเชื่อถือในด้านความเป็นส่วนตัวของการสื่อสาร การยืนยันตัวตนของคู่สนทนา และป้องกันการโจรกรรมข้อมูลจากผู้ไม่หวังดีในกรณีการเข้าถึงหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ข้อมูลที่สำคัญในการสื่อสารของเน็ตพายประกอบด้วย 3 ส่วน ได้แก่

- APPID คือ ชื่อของแอพพลิเคชั่นที่ใช้ในการสื่อสาร
- APPKEY คือ กุญแจสาธารณะที่ใช้ในการสื่อสาร
- APPSECRET คือ รหัสผ่านในการยืนยันสิทธิ์การเข้าถึงการสื่อสาร

สรรพสิ่งใช้ข้อมูลทั้ง 3 ส่วนนี้ในการเชื่อมต่อไปยังตัวกลาง ตัวกลางจะลงทะเบียนข้อมูลของสรรพสิ่งไว้ในระบบและสร้างโทเคน (Token) เพื่อใช้ในการยืนยันตัวตนในการสื่อสารของสรรพสิ่งนั้นภายในแอพพลิเคชั่นที่กำหนด ปัจจุบันเน็ตพายได้มีการพัฒนาการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตหลาย ๆ ส่วน ได้แก่ การควบคุมและติดตามการทำงานของบ้านอัจฉริยะในการเปิดปิดอุปกรณ์เครื่องใช้ไฟฟ้า รวมถึงการติดตามสภาพแวดล้อมต่าง ๆ ภายในบ้านผ่านโทรศัพท์มือถือหรือทางเว็บไซต์ เป็นต้น

เน็ตพายมีความยืดหยุ่นในการกำหนดสิทธิ์การเข้าถึงและการยืนยันตัวตนของแอพพลิเคชั่นและอุปกรณ์ โดยผู้ใช้เน็ตพายสามารถเลือกพัฒนารูปแบบระบบได้ 3 รูปแบบดังนี้

- ระบบที่ไว้วางใจ (Trusted System) วิธีนี้เหมาะสำหรับระบบที่พัฒนาขึ้นเพื่อการทดสอบ หรือระบบที่อุปกรณ์ทุกตัวอยู่ภายใต้การดูแลของเจ้าของระบบเดียวกัน อุปกรณ์ทุกตัวในระบบจะถูกติดตั้ง APPKEY และ APPSECRET ชุดเดียวกัน และมีสิทธิการเข้าถึงทุกอย่างเหมือนกันหมด ทำให้มีความสะดวกคล่องตัวในการจัดการตัวตนและการใช้งาน ตัวอย่างระบบที่เหมาะกับการใช้งานรูปแบบนี้ ได้แก่ ระบบเซ็นเซอร์สภาพแวดล้อมที่พัฒนาขึ้นเพื่อการใช้งานเฉพาะที่
- ระบบบุคคลที่สาม (Third-party System) วิธีนี้เหมาะสำหรับระบบที่ให้บริการต่อบุคคลอื่น และเมื่ออุปกรณ์อยู่ในสภาพแวดล้อมที่นอกเหนือจากการควบคุมของเจ้าของระบบ อุปกรณ์ทุกตัวจะใช้หมายเลขกุญแจของสรรพสิ่ง (Device Key) และ รหัสสำหรับการยืนยันตัวตนของสรรพสิ่ง (Device Secret) โดยใช้เป็นรูปแบบข้อมูลที่แตกต่างกัน และมีสิทธิการเข้าถึงแตกต่างกันไป เนื่องจากอุปกรณ์แต่ละตัวมีการระบุตัวตนที่แตกต่างกัน วิธีการนี้มีความปลอดภัยสูง แต่ก็ทำให้การบริหารจัดการสิทธิและตัวตนยากขึ้นกว่ารูปแบบแรก ตัวอย่างระบบที่เหมาะสมกับการใช้งานรูปแบบนี้ ได้แก่ ระบบอุปกรณ์อำนวยความสะดวกในบ้าน เช่น การควบคุมหลอดไฟผ่านแอพพลิเคชั่น เนื่องจากผู้พัฒนาไม่ได้พัฒนาหลอดไฟเพื่อใช้เองแต่เพื่อการค้าเมื่อผู้ใช้ซื้อหลอดไฟไปติดตั้งที่บ้านควรมีสิทธิ์ในการควบคุมเฉพาะหลอดไฟในบ้านของตนเท่านั้น ดังนั้นคีย์ (Key) ในหลอดไฟแต่ละหลอดต้องมีความแตกต่างกัน
- ระบบลูกผสม (Hybrid System) วิธีนี้เหมาะสำหรับระบบที่ประกอบด้วยอุปกรณ์ของเจ้าของระบบเองซึ่งติดตั้งด้วย APPKEY และ APPSECRET อุปกรณ์ที่ใช้งานโดยบุคคลอื่นติดตั้งด้วยคีย์ของสรรพสิ่ง (Device Key) และรหัสการยืนยันตัวตนของสรรพสิ่ง (Device Secret) เป็นการใช้งานที่ผสมผสานรูปแบบระบบที่ไว้วางใจ (Trusted System) และรูปแบบบุคคลที่สาม (Third-party System)

ทั้งนี้รูปแบบการสื่อสารระหว่างสรรพสิ่งด้านการแพทย์ผ่านเน็ตพายในการทดลองนี้จะใช้รูปแบบการจัดการสิทธิ์สรรพสิ่งแบบระบบบุคคลที่สาม (Third-party System) เนื่องจากรูปแบบการใช้งานการสื่อสารสรรพสิ่งด้านการแพทย์ ต้องสามารถใช้งานกับอุปกรณ์ทางการแพทย์ได้หลากหลายทั้งการใช้งานในโรงพยาบาลและการใช้งานโดยผู้ป่วยสามารถใช้งานจากอุปกรณ์ส่วนบุคคลในกรณีอยู่นอกโรงพยาบาล เช่น เซ็นเซอร์วัดค่าสุขภาพพื้นฐานต่าง ๆ ในรูปแบบอุปกรณ์สวมใส่ เป็นต้น

เนื่องจากการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตซึ่งเป็นโพรโทคอลสาธารณะนั้นมีความเสี่ยงจากการบุกรุกของผู้ไม่หวังดีเพื่อกระทำการใด ๆ ที่อาจส่งผลเสียต่อการควบคุมสรรพสิ่ง ดังนั้นกระบวนการบันทึกธุรกรรมในการสื่อสารระหว่างสรรพสิ่งมีความจำเป็น โดยสิ่งสำคัญในการวิเคราะห์ความเสี่ยงจากการบุกรุกของผู้ไม่หวังดี ซึ่งหลักการในการจัดเก็บข้อมูลธุรกรรมของกิจกรรมในระบบต่าง ๆ แสดงไว้ในหัวข้อต่อไปนี้

2.1.4 การบันทึกธุรกรรม

การบันทึกธุรกรรม (Logging) เป็นกระบวนการตรวจสอบความปลอดภัยของระบบโดยการบันทึกกิจกรรมการใช้งานที่เกิดขึ้น โดยจัดเก็บตามช่วงเวลาและผู้ใช้งาน เพื่อให้สามารถวิเคราะห์การกระทำการใด ๆ ที่อาจทำให้เกิดความผิดพลาดของระบบ รวมถึงความมั่นคงในการเข้าถึงข้อมูล ข้อมูลธุรกรรมที่จัดเก็บประกอบด้วยข้อมูลดังนี้ [15]

- การสร้าง การอ่าน การปรับปรุงหรือลบข้อมูล
- การเริ่มต้นการเชื่อมต่อเครือข่าย
- การตรวจสอบผู้ใช้และการอนุญาตผู้ใช้ให้สามารถเข้าสู่ส่วนต่าง ๆ ของระบบ
- บันทึกปรับเปลี่ยนหรือเพิกถอนสิทธิการเข้าถึง รวมถึงการเพิ่มผู้ใช้ใหม่หรือกลุ่มการเปลี่ยนแปลงระดับสิทธิ์ของผู้ใช้ เปลี่ยนสิทธิ์ของแฟ้ม เปลี่ยนสิทธิ์การเข้าถึงฐานข้อมูล การเปลี่ยนแปลงกฎของผู้ใช้งาน และเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งาน
- การเปลี่ยนแปลงการกำหนดค่าของระบบ หรือการกระทำการที่ส่งผลจากตัวระบบเอง
- ส่วนของระบบที่ประมวลผลผิดพลาด หรือผิดปรกติ
- ส่วนของกิจกรรมที่เป็นอันตราย และอาจสร้างผลกระทบต่อระบบหรือผู้ใช้งานอื่น ๆ

ทั้งนี้ กระบวนการบันทึกข้อมูลกิจกรรมในระบบควรบันทึกทุกกิจกรรมที่เกิดขึ้นเพื่อวิเคราะห์ข้อมูลสิ่งผิดปกติที่เกิดขึ้นในระบบ ทั้งนี้ควรได้รับการตรวจสอบความปลอดภัยในขั้นตอนแรกก่อนดำเนินการกับข้อมูล

ดังนั้นกระบวนการที่สำคัญในการควบคุมความปลอดภัยในการบันทึกธุรกรรมของการสื่อสารคือการยืนยันตัวตน เพื่อเป็นการยืนยันการสื่อสารมาจากบุคคลที่มีสิทธิ์ดำเนินการ และให้สามารถบันทึกข้อมูลธุรกรรมที่เกิดขึ้นได้อย่างถูกต้องและน่าเชื่อถือ ซึ่งในปัจจุบันมีโพรโทคอลมาตรฐานในการยืนยันตัวตนเพื่อความน่าเชื่อถือของข้อมูลธุรกรรมการสื่อสารที่ใช้สำหรับการตรวจสอบความผิดปกติด้วยโพรโทคอลมาตรฐาน เช่น โอออท (OAuth) [16]

การบันทึกธุรกรรมในระบบทั่วไปมีรูปแบบในการบันทึกข้อมูลกิจกรรมต่าง ๆ ที่เกิดขึ้นทั้งหมดในสภาพแวดล้อมของระบบเดียวกัน ทำให้รูปแบบการบันทึกธุรกรรมและนาฬิกาของระบบเป็นไปในทิศทางเดียวกัน แต่การสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต มีรูปแบบการสื่อสารระหว่างสรรพสิ่งที่อยู่ในที่ต่าง ๆ ซึ่งไม่ได้อยู่ในสภาพแวดล้อมเดียวกัน โดยแต่ละสรรพสิ่งจะสื่อสารกันผ่านอินเตอร์เน็ตเท่านั้น ส่งผลให้รูปแบบการบันทึกธุรกรรมพื้นฐานต้องมีการจัดเก็บข้อมูลธุรกรรมของแต่ละสรรพสิ่งไว้ที่ตนเอง โดยการบันทึกธุรกรรมของแต่ละสรรพสิ่งจะเป็นการบันทึกในมุมมองกิจกรรมของสรรพสิ่งนั้น ๆ ด้วยซิสล็อคเอ็นจี (syslog-ng) [17] ซึ่งเป็นรูปแบบการบันทึกธุรกรรมที่ได้รับความนิยมและสามารถใช้งานได้กับระบบปฏิบัติการต่าง ๆ โดยออกแบบมาเฉพาะอย่างยิ่งสำหรับเซ็นเซอร์และอุปกรณ์ฝังตัวขนาดเล็กต่าง ๆ โดยรูปแบบพื้นฐานในการบันทึกข้อมูลธุรกรรมของแต่ละสรรพสิ่งซิสล็อคเอ็นจี จะเป็นรูปแบบกิจกรรม ทั้งด้านระบบปฏิบัติการ กิจกรรมที่เกิดขึ้นและข้อผิดพลาดระหว่างการสื่อสาร แต่ในการบันทึกธุรกรรมรูปแบบนี้จะสามารถตรวจสอบและวิเคราะห์ปัญหาได้เพียงแต่ละสรรพสิ่งเท่านั้น ซึ่งยังไม่มีรูปแบบการบันทึกธุรกรรมในภาพรวมของทุกสรรพสิ่งที่สื่อสารกัน ทำให้ไม่สามารถวิเคราะห์ปัญหาที่เกิดขึ้นในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตทั้งหมด

ดังนั้นจึงควรเก็บบันทึกธุรกรรมของแต่ละสรรพสิ่งไว้ที่เดียวกันโดยใช้รูปแบบและเวลาในการบันทึกข้อมูลธุรกรรมไปในทิศทางเดียวกัน เพื่อให้การพิจารณาธุรกรรมมีความน่าเชื่อถือ โดยการบันทึกธุรกรรมของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตในงานวิจัยชิ้นนี้มุ่งเน้นไปที่การเกิดความผิดพลาดในการสื่อสารระหว่างสรรพสิ่ง เพื่อเคราะห์หาภัยคุกคามในการสื่อสารจากผู้ไม่หวังดีที่อาจเกิดขึ้นในเบื้องต้น เพื่อเป็นการเสริมความปลอดภัยในระหว่างการสื่อสารแบบเชิงรับ

2.1.5 เครื่องมืออุปกรณ์ทางการแพทย์และการให้บริการสุขภาพ

อุปกรณ์ทางการแพทย์เป็นสิ่งสำคัญในการดำเนินการและให้บริการทางการแพทย์เพื่อลดระยะเวลาการรักษา ลดข้อผิดพลาดด้านการรักษา และเพิ่มความแม่นยำในการวินิจฉัย โดยรูปแบบเครื่องมือทางการแพทย์มีรูปแบบเฉพาะกับกลุ่มโรคและข้อมูลที่ต้องการวัดค่า ซึ่งการใช้งานอุปกรณ์ประกอบด้วย เครื่องมือการวัดค่าสุขภาพสำหรับการวินิจฉัย ได้แก่ เครื่องวัดอัตราการหายใจ เครื่องวัดการเต้นของหัวใจ เครื่องวัดความดัน เป็นต้น และเครื่องมือสำหรับเพื่อการรักษา

ได้แก่ เครื่องฉีดยาอัตโนมัติ เครื่องให้น้ำเกลือและสารอาหาร เป็นต้น ซึ่งรูปแบบการใช้เครื่องมือทางการแพทย์ขึ้นอยู่กับดุลพินิจของแพทย์ผู้รักษาเพื่อให้อุปกรณ์ช่วยในการรักษาและติดตามอาการทดแทนแพทย์ต้องเฝ้าติดตามด้วยตนเองตลอดเวลา

ลักษณะตัวอย่างอุปกรณ์วัดค่าร่างกายทางการแพทย์ส่วนใหญ่มีรูปแบบการใช้งานสำหรับให้แพทย์สามารถนำไปวินิจฉัยต่อไป จึงมีผลลัพธ์ในการวัดค่าและแสดงผลในรูปแบบการสรุปข้อมูลและมีการเปลี่ยนแปลงข้อมูลภายใน 1 วินาที แต่ในความเป็นจริงของข้อมูลสุขภาพอาจจะมีรูปแบบความถี่ในการวัดค่าสุขภาพผู้ป่วยที่แตกต่างกันตามการตอบสนองของร่างกายผู้ป่วยและสิ่งที่ต้องการติดตามความเปลี่ยนแปลง โดยทั่วไปข้อมูลสุขภาพพื้นฐานที่ต้องติดตามตลอดเวลาคือข้อมูลสัญญาณชีพ (Vital signs) [18] ได้แก่ ค่าความดันโลหิต (Blood pressure) อุณหภูมิ (Temperature) ชีพจร (Pulse) และการหายใจ (Respiration) ซึ่งเป็นข้อมูลบ่งชี้การทำงานของร่างกายที่มีเปลี่ยนแปลง โดยแต่ละข้อมูลจะมีค่ากำหนดช่วงปกติ (Normal range) และรูปแบบข้อมูลที่แตกต่างกันไปดังนี้

- ความดันโลหิต (Blood pressure) คือ แรงดันของเลือดที่ส่งออกจากหัวใจห้องล่างซ้ายเข้าสู่ระบบหลอดเลือดแดงในร่างกาย ซึ่งมีลักษณะข้อมูลตัวเลขสองค่าในลักษณะเศษส่วน คือ ความดันของเลือดสูงสุดขณะหัวใจห้องล่างบีบตัว (Systolic blood pressure หรือ SBP) เป็นเลขส่วนบน ช่วงค่าปกติอยู่ที่ 90 – 119 มม.ปรอท และความดันเลือดที่ต่ำสุดขณะหัวใจห้องล่างคลายตัว (Diastolic blood pressure หรือ DBP) เป็นเลขส่วนล่าง ช่วงปกติของที่ 60 – 79 มม.ปรอท ทั้งนี้ข้อมูลช่วงปกติของแต่ละช่วงอายุอาจมีความแตกต่างกันขึ้นอู่กับการวินิจฉัยของแพทย์
- ชีพจร (Pulse) คือแรงสะเทือนของกระแสเลือด ซึ่งเกิดจากการบีบตัวของหัวใจห้องล่างด้านซ้าย ทำให้ผนังของหลอดเลือดแดงขยายออกเป็นจังหวะ เป็นผลให้สามารถจับชีพจรได้ สำหรับผู้ใหญ่และผู้สูงอายุอัตราการเต้นของชีพจร 60 - 100 (เฉลี่ย 80 ครั้ง/นาที)
- การหายใจ (Respiration) เป็นการแสดงการสูดออกซิเจนเข้าสู่ร่างกายโดยผ่านจมูก หลอดลม และปอด ที่เรียกว่า การหายใจเข้า และเป็นการแสดงการปล่อยคาร์บอนไดออกไซด์ออกจากร่างกายผ่านปอด หลอดลม และจมูก ที่เรียกว่า การหายใจออก สามารถตรวจนับการหายใจเป็นการสังเกตว่ามีการหายใจที่ผิดปกติจากจังหวะและจำนวนครั้งต่อนาที

ทั้งนี้ในการวัดค่าสุขภาพต่าง ๆ ด้วยเครื่องมือและการเปลี่ยนแปลงของข้อมูลที่แตกต่างกันตามการตอบสนองของร่างกาย โดยการติดตามข้อมูลสัญญาณชีพ (Vital signs) เป็นข้อมูลพื้นฐานของร่างกายในการตรวจวินิจฉัย แต่หากต้องการติดตามข้อมูลเฉพาะกลุ่มโรค เช่น โรคเบาหวาน โรคไต หรือโรคหัวใจ จะต้องใช้เครื่องมือตรวจวัดพิเศษสำหรับการรักษาโดยมีรูปแบบการเปลี่ยนแปลงที่น้อยข้อมูลสัญญาณชีพ

โดยเครื่องมือวัดค่าสัญญาณชีพของผู้ป่วยแต่ละเตียงจะประกอบไปด้วยเครื่องมือวัดค่าและเครื่องมือทางการแพทย์ดังนี้

- อัตราการเต้นของหัวใจ (Heart Rate) มีข้อมูลเปลี่ยนแปลงทุก 273 มิลลิวินาที (อัตราการเต้นของหัวใจมนุษย์สูงสุด 220 ครั้ง/นาที)
- เครื่องวัดคลื่นหัวใจ EKG มีข้อมูลเปลี่ยนแปลงทุก 40 มิลลิวินาที
- เครื่องวัดการหายใจมีข้อมูลเปลี่ยนแปลงทุก 2 วินาที (30 ครั้ง/นาที)

การนำกระบวนการบันทึกธุรกรรมทางการแพทย์จะติดตามรูปแบบเฉพาะการวัดค่าสุขภาพจากผู้ป่วยมายังแพทย์เท่านั้น เพราะเนื่องจากการติดตามบันทึกธุรกรรมของอุปกรณ์การรักษาโดยสั่งงานจากแพทย์ เช่น เครื่องฉีดยา (Syringe pump) เครื่องให้น้ำเกลือ (Infusion pump) รวมถึงเครื่องให้สารอินซูลิน (Insulin pump) มีจำนวนการส่งข้อมูลที่ไม่คงที่ โดยขึ้นอยู่กับการสั่งงานของแพทย์หรือพยาบาลที่เกี่ยวข้องตามสิทธิ์การอนุญาต โดยต้องใช้กระบวนการความมั่นคงปลอดภัยรูปแบบอื่น ในการสร้างความน่าเชื่อถือในเครื่องมือทางการแพทย์ดังกล่าว ทั้งนี้รูปแบบการใช้เครื่องมือทางการแพทย์สำหรับวัดค่าสุขภาพติดตามผู้ป่วยส่วนใหญ่จะใช้ในผู้ป่วยวิกฤติ หรือผู้ป่วยที่ต้องติดตามอาการอยู่ในโรงพยาบาล

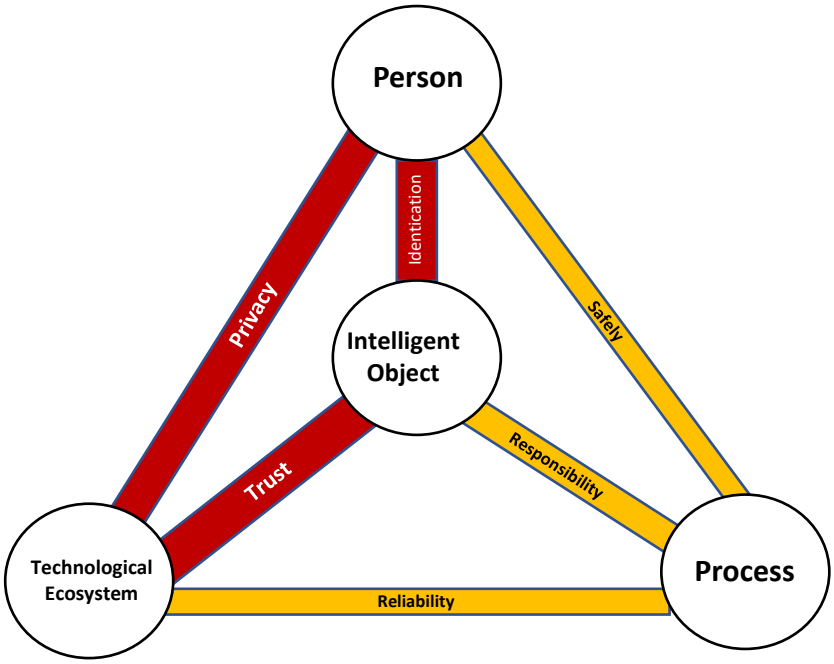
โรงพยาบาลในประเทศไทยมีรูปแบบการให้บริการตามปริมาณจำนวนเตียงและบุคลากรผู้ให้บริการสาธารณสุข 7 ประเภท [19] โดยมีรูปแบบที่แตกต่างกันดังนี้

- โรงพยาบาลที่มีขีดความสามารถรองรับผู้ป่วยที่ต้องการการรักษาที่ยุ่งยากซับซ้อนระดับเชี่ยวชาญและเทคโนโลยีขั้นสูงและมีราคาแพง (A: Advance-level Hospital)
- โรงพยาบาลที่มีขีดความสามารถรองรับผู้ป่วยที่ต้องการการรักษาที่ยุ่งยากซับซ้อนระดับเชี่ยวชาญเฉพาะ (S: Standard-level Hospital)
- โรงพยาบาลที่มีขีดความสามารถรองรับผู้ป่วยที่ต้องการการรักษาที่ยุ่งยากซับซ้อนระดับเชี่ยวชาญ (M1: Middle-level Hospital)
- โรงพยาบาลชุมชนขนาด 120 เตียงขึ้นไป ที่มีแพทย์เวชปฏิบัติ หรือแพทย์เวชศาสตร์ครอบครัว 3-5 คน และแพทย์เฉพาะทางครบทั้ง 6 สาขาหลัก สาขาละอย่างน้อย 2 คน (M2: Middle-level Hospital)
- โรงพยาบาลชุมชนขนาดเตียง 60-120 เตียง (F1: First-level Hospital)
- โรงพยาบาลชุมชนขนาดเตียง 30-90 เตียง (F2: First-level Hospital)
- โรงพยาบาลชุมชนขนาดไม่เกินเตียง 30 เตียง ที่มีแพทย์เวชปฏิบัติทั่วไปหรือแพทย์เวชศาสตร์ครอบครัว รวม 1-2 คน (F3: First-level Hospital)

จากรูปแบบโรงพยาบาลในประเทศไทยที่ให้บริการสำหรับผู้ป่วยตามประเภทต่าง ๆ โดยในการทดลองแนวคิดการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งด้านการแพทย์ในตัวอย่างโรงพยาบาลชุมชนขนาดเล็กสุด (F3) โดยรองรับผู้ป่วยขนาด 30 เตียง และมีแพทย์ดูแล 1 คน ทั้งนี้ผู้ป่วยอาจอยู่ในโรงพยาบาลหรือเป็นผู้ป่วยติดเตียงในบริเวณใกล้เคียง

2.2 งานวิจัยที่เกี่ยวข้อง

ปัจจุบันผู้ให้บริการสำหรับการสื่อสารระหว่างสรรพสิ่งแต่ละผู้ให้บริการได้ให้ความสำคัญด้านความปลอดภัย เพื่อสร้างความน่าเชื่อถือกับการนำระบบไปใช้งาน ทั้งนี้อีกหนึ่งกระบวนการที่สำคัญด้านความปลอดภัยของการป้องกันผู้ไม่หวังดี คือการติดตามกิจกรรมการสื่อสารต่าง ๆ ที่เกิดขึ้น ภายในระบบเพื่อการบันทึกธุรกรรมเหตุการณ์การสื่อสารระหว่างสรรพสิ่ง เนื่องจากการสื่อสารระหว่างสรรพสิ่งเป็นการสื่อสารตลอดเวลา จึงมีข้อมูลการสื่อสารที่มีปริมาณมาก จึงควรมีกระบวนการบันทึกข้อมูลธุรกรรมในการสื่อสารระหว่างสรรพสิ่งในรูปแบบที่เหมาะสม เพื่อป้องกันการใช้พื้นที่เก็บข้อมูลที่เกินความจำเป็นโดยจะต้องประกอบไปด้วยคุณสมบัติต่าง ๆ เท่าที่จำเป็นในการบันทึกข้อมูลเพื่อการวิเคราะห์ภายหลัง ทั้งนี้ข้อมูลธุรกรรมที่บันทึกจะต้องสามารถยืนยันตัวตนของผู้ใช้งานได้ว่าเป็นใคร สั่งงานมาจากอุปกรณ์อะไร เพื่อให้การติดตามพฤติกรรมของการสื่อสารมีความน่าเชื่อถือในการใช้งาน ซึ่งมีแนวคิดพื้นฐานในการยืนยันตัวตนและป้องกันการโจรกรรมข้อมูลในการสื่อสารในแบบต่าง ๆ งานวิจัยที่เกี่ยวข้องมีดังนี้ ริอฮิและคณะ [21] นำเสนอแนวคิดกระบวนการส่งเสริมปัจจัยด้านความปลอดภัยของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต ซึ่งประกอบไปด้วยโหนดต่าง ๆ ที่เป็นตัวแทนของสรรพสิ่งที่เกี่ยวข้องในการสื่อสาร ได้แก่ บุคคล ระบบนิเวศทางเทคโนโลยี กระบวนการ และระบบอัจฉริยะ ทั้งนี้แต่ละโหนดจะมีความสัมพันธ์ในบริบทที่แตกต่างกันในด้านความปลอดภัยที่ประกอบไปด้วยการยืนยันตัวตน ความเป็นส่วนตัว ความเชื่อมั่น ความปลอดภัย ความรับผิดชอบ และการป้องกันดังแสดงในรูปที่ 2



รูปที่ 2 แผนผังความสัมพันธ์ด้านความปลอดภัยของแต่ละโหนด [21]

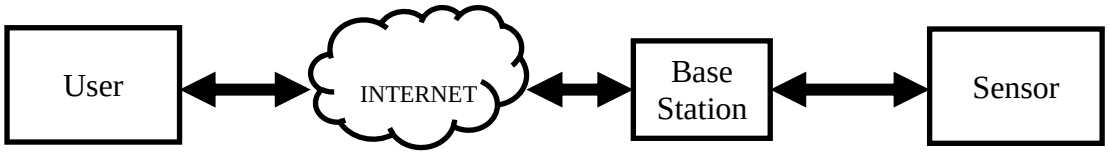
จากตัวอย่างในด้านระบบการดูแลสุขภาพควรมีการยืนยันตัวตนของบุคลากรทางการแพทย์ รวมถึงเครื่องมือทางการแพทย์ต่าง ๆ ซึ่งต้องมีการเก็บรักษาข้อมูลทางการแพทย์และการรักษาไว้เป็นความลับเช่นกัน ในขณะเดียวกันผู้ป่วยควรมีความไว้วางใจทางการแพทย์ทั้งในแง่ความเชื่อส่วนบุคคลต่าง ๆ ซึ่งจะต้องสร้างความสัมพันธ์ในรูปแบบที่ก่อให้เกิดความปลอดภัยในการสื่อสารในสรรพสิ่งที่สมเหตุสมผลยิ่งขึ้น โดยสามารถนำมาพัฒนาแนวคิดการสร้างความน่าเชื่อถือสำหรับพัฒนาการออกแบบธุรกรรมการสื่อสารระหว่างสรรพสิ่งโดยสร้างการเชื่อมโยงระหว่างผู้ใช้กับสรรพสิ่งที่ใช้งานให้เกิดความน่าเชื่อถือและมีความเป็นส่วนตัวด้วยกระบวนการยืนยันตัวตน

วาโทรและคณะ[22] ได้นำเสนอกระบวนการส่งข้อมูลระหว่างอุปกรณ์เซ็นเซอร์ไร้สายไปกับผู้ติดต่อจากภายนอกโดยกระบวนการเข้ารหัสจากผู้ติดต่อภายนอกโดยใช้กุญแจสาธารณะของเซ็นเซอร์ (Public Key: Sensor) เพื่อส่งไปหาเซ็นเซอร์ซึ่งภายในได้แนบกุญแจสาธารณะของผู้ติดต่อภายนอก (Public Key: User) ไปด้วย เมื่อเซ็นเซอร์ได้รับข้อมูลจะทำการถอดรหัสและตรวจสอบคำขอจากผู้ติดต่อภายนอก และส่งคีย์เซสชั่น (Session Key) ในการเชื่อมต่อกลับไปเพื่อส่งข้อมูลระหว่างกัน ดังแสดงในรูปที่ 3 การยืนยันตัวตนระหว่างสรรพสิ่งสำหรับการส่งข้อมูลจากเซ็นเซอร์มายังผู้ใช้งานที่มีสิทธิ์โดยตรงนั้น กระบวนการนี้อาจไม่เหมาะสมกับการเข้ารหัสหรือถอดรหัสสรรพสิ่งที่เป็นอุปกรณ์ประมวลผลขนาดเล็ก เพราะรูปแบบการใช้พลังงานและหน่วยประมวลผลไม่เหมาะสมกับการคำนวณที่ซับซ้อน อาจส่งผลให้ประสิทธิภาพในการวัดค่าต่างๆ เกิดความล่าช้ากว่า

ปกติ จึงควรมีหน่วยประมวลผลสำหรับการเข้ารหัสและถอดรหัสแยกออกจากเซ็นเซอร์ เพื่อช่วยจัดการประเด็นความปลอดภัยในส่วนนี้ให้กับอุปกรณ์เซ็นเซอร์ต่าง ๆ

รูปที่ 3 แนวคิดการรับส่งข้อมูลอย่างปลอดภัยของวาโทรและคณะ

โวรูกันติและคณะ [23] ได้นำเสนอกระบวนการการพัฒนาแนวคิดจากแนวคิดของวาโทรและคณะ จากเดิมพบว่าการสื่อสารระหว่างผู้ติดต่อภายนอกกับเซ็นเซอร์มีความปลอดภัยจากการแลกเปลี่ยนข้อมูลก่อนทำการส่งข้อมูล (Hand Shake) ซึ่งกระบวนการในการเข้าและถอดรหัสโดยเซ็นเซอร์เป็นกระบวนการที่ซับซ้อนสำหรับเซ็นเซอร์มีผลต่อการประมวลผลข้อมูล รวมทั้งปริมาณการใช้พลังงานที่มากขึ้น โวรูกันติและคณะจึงพัฒนามาตรฐานความปลอดภัยในการแลกเปลี่ยนข้อมูลระหว่างผู้ติดต่อภายนอกกับเซ็นเซอร์ โดยให้มีสถานีฐาน (Base Station) เป็นตัวกลางในการแลกเปลี่ยนข้อมูล โดยเริ่มต้นจากผู้ติดต่อภายนอกใช้กุญแจสาธารณะของสถานีฐาน (Public Key: Base Station) ในการเข้ารหัสข้อมูลการร้องขอไปยังสถานีฐาน เมื่อสถานีฐานได้รับข้อมูลจะทำการถอดรหัสคำร้องขอ และทำการเข้ารหัสใหม่ด้วยกุญแจที่ใช้ร่วมกันระหว่างสถานีฐานกับเซ็นเซอร์ (Key: Base Station & Sensor) เท่านั้น โดยแนบกุญแจสาธารณะของผู้ติดต่อภายนอกไปด้วย เมื่อส่งข้อมูลไปถึงเซ็นเซอร์ เซ็นเซอร์จะทำการถอดรหัสได้ทันทีจากกุญแจที่ใช้ร่วมกับสถานีฐานจากนั้นเซ็นเซอร์จะสร้างคีย์เซสชัน (Session Key) โดยเข้ารหัสกับกุญแจสาธารณะของผู้ติดต่อภายนอก และส่งกลับไปยังผู้ติดต่อภายนอกโดยตรง เพื่อสร้างการเชื่อมต่อดังแสดงในรูปที่ 4



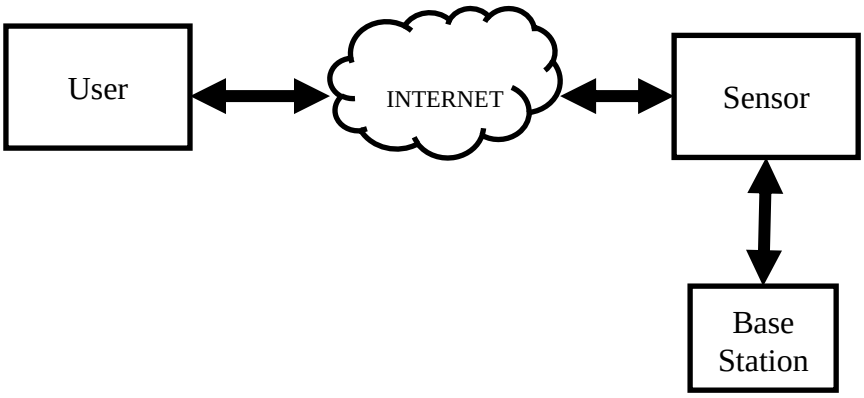
รูปที่ 4 แนวคิดการรับส่งข้อมูลอย่างปลอดภัยของโวรูกันติและคณะ

แนวคิดนี้ใช้สำหรับการยืนยันตัวของผู้ใช้เพื่อการเชื่อมต่อใหม่กับสถานีฐานเพื่อสามารถรับส่งข้อมูลกับเซ็นเซอร์ แต่ไม่ได้ตรวจสิทธิ์กำหนดการสื่อสารระหว่างผู้ใช้กับสรรพสิ่ง ซึ่งยังคงไม่เพียงพอต่อการยืนยันตัวตนสำหรับข้อมูลธุรกรรมทางการแพทย์เพราะข้อมูลการสื่อสารทาง

การแพทย์ให้ความสำคัญกับข้อมูลความเป็นส่วนตัว ดังนั้นจึงต้องยืนยันตัวตนการจับคู่การสื่อสารทั้งผู้ใช้งานและอุปกรณ์เซ็นเซอร์ในทุกครั้ง

ภูมิภัทร สุขภิมนตรี และศุภกร กังพิสดาร [24] ได้นำเสนอแนวคิดกระบวนการยืนยันตัวจริงในอุปกรณ์เซ็นเซอร์ เพื่อพัฒนาจากกระบวนการดังกล่าวทำให้มีประสิทธิภาพในการประมวลผลและความมั่งคงในการส่งข้อมูลผู้ติดต่อภายนอกไปยังเซ็นเซอร์ แต่อย่างไรก็ตามกระบวนการดังกล่าวยังไม่สามารถยืนยันการส่งข้อมูลได้ว่ามาจากผู้ร้องขอจริง โดยกระบวนการเริ่มต้นจากผู้ติดต่อภายนอกเข้ารหัสคำร้องขอด้วยกุญแจสาธารณะของสถานีฐาน (Public Key: Base Station) และเข้ารหัสข้อมูลอีกครั้งด้วยกุญแจส่วนตัวของผู้ติดต่อภายนอกเอง (Private Key: User) โดยแนบรหัสประจำตัวของผู้ติดต่อภายนอก (User ID) ไปด้วย เพื่อส่งข้อมูลไปให้กับเซ็นเซอร์ เมื่อเซ็นเซอร์ได้รับข้อมูลแล้ว เซ็นเซอร์จะไม่ถอดรหัส แต่จะทำการเข้ารหัสข้อมูลทั้งหมดเพิ่มด้วยกุญแจที่ใช้ร่วมกันระหว่างเซ็นเซอร์และสถานีฐานเท่านั้น (Key: Base Station & Sensor) และแนบหมายเลขประจำตัวเซ็นเซอร์ไปด้วย (Sensor ID) จากนั้นจึงส่งข้อมูลต่อไปยังสถานีฐาน เมื่อสถานีฐานได้รับข้อมูลทั้งหมด สถานีฐานจะทำการค้นหากุญแจถอดรหัสจากหมายเลขประจำตัวของเซ็นเซอร์ที่เคยลงทะเบียนไว้แล้ว เพื่อหากุญแจสำหรับถอดรหัสข้อมูลครั้งแรกด้วย เมื่อถอดรหัสข้อมูลครั้งแรกจะพบข้อมูลสองส่วนคือ ข้อมูลที่เข้ารหัสด้วยผู้ติดต่อภายนอกและหมายเลขประจำตัวผู้ติดต่อภายนอก สถานีฐานจะค้นหาหมายเลขกุญแจสาธารณะในฐานข้อมูลของตัวเองจากหมายเลขประจำตัวของผู้ติดต่อภายนอกเพื่อถอดรหัส เมื่อถอดรหัสสำเร็จได้คำร้องขอ สถานีฐานก็จะสร้างคีย์เซสชัน (Session Key) และเข้ารหัสโดยกุญแจสาธารณะของผู้ติดต่อภายนอกและเซ็นเซอร์ และส่งข้อมูลการเชื่อมต่อกลับไปตามเส้นทางเดิมเพื่อให้ผู้ติดต่อภายนอกได้รับคีย์เซสชัน (Session Key) ในการเชื่อมต่อกับเซ็นเซอร์ตามที่ร้องขอจากรูปที่ 5

กระบวนการนี้สามารถพัฒนาการยืนยันตัวตนระหว่างผู้ใช้และสรรพสิ่งในการเชื่อมต่อกันภายในครั้งเดียวสำหรับอุปกรณ์หน่วยประมวลผลขนาดเล็กชนิดเซ็นเซอร์ที่ใช้พลังงานต่ำ ซึ่งอุปกรณ์ทางการแพทย์บางชนิด เช่น เครื่องตรวจบันทึกคลื่นไฟฟ้าแบบติดตัวสำหรับผู้ป่วยโรคหัวใจ (Holter Monitoring) อาจต้องติดตั้งกับตัวผู้ป่วยตลอดเวลา 24 - 48 ชั่วโมง ขณะที่ผู้ป่วยสามารถออกไปใช้ชีวิตประจำวันได้ เพื่อให้แพทย์สามารถติดตามข้อมูลการเต้นของหัวใจได้ตลอดเวลา ดังนั้นการยืนยันตัวตนระหว่างผู้ใช้และสรรพสิ่ง ช่วยให้การบันทึกธุรกรรมการสื่อสารผ่านอินเตอร์เน็ตสร้างความน่าเชื่อถือและความเป็นส่วนตัวกับเจ้าของข้อมูลมากยิ่งขึ้น



รูปที่ 5 แนวคิดการรับส่งข้อมูลอย่างปลอดภัยของภูมิภัทร สุขภิมนตรี และศุภกร กังพิสดาร

รัวลากิสและคณะ [25] ได้แนะนำแนวคิดกระบวนการประยุกต์การบันทึกธุรกรรมของกิจกรรมในระบบ ให้สามารถรองรับเทคโนโลยีการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตภายใต้ความปลอดภัยและความเป็นส่วนตัวของข้อมูลที่สื่อสารในรูปแบบภัยคุมคามต่าง ๆ ที่อาจเกิดขึ้นกับการโจรกรรมข้อมูลธุรกรรมเพื่อเข้าสู่ระบบต่าง ๆ โดยการบันทึกธุรกรรมในรูปแบบการสื่อสารระหว่างสรรพสิ่งต้องคำนึงถึงความเป็นส่วนตัวของข้อมูลที่สื่อสาร จึงต้องบันทึกข้อมูลในปริมาณที่เหมาะสม ซึ่งหากข้อมูลธุรกรรมมีมากเกินไป ในกรณีที่ข้อมูลธุรกรรมสามารถเข้าถึงจากผู้ไม่มีสิทธิ์เข้าถึง อาจส่งผลให้เกิดการละเมิดความเป็นส่วนตัวของผู้ใช้ได้ ในกรณีบันทึกข้อมูลน้อยเกินไป อาจทำให้การตรวจสอบความผิดปกติที่เกิดขึ้นไม่เพียงพอ ทำให้ไม่เกิดประโยชน์ในการบันทึกกิจกรรมในระบบ ทั้งนี้การรับส่งข้อมูลธุรกรรมควรมีการเข้ารหัสในรูปแบบต่าง ๆ ได้แก่ กุญแจแบบอสมมาตร หรือกุญแจสมมาตร ตามรูปแบบความสามารถและข้อจำกัดของอุปกรณ์

บทที่ 3
ระเบียบวิธีวิจัย

งานวิจัยชิ้นนี้มีเป้าหมายการออกแบบและพัฒนาต้นแบบการบันทึกธุรกรรมของโพรโตคอลการสื่อสารระหว่างสรรพสิ่งด้านการแพทย์ผ่านเน็ตพายโดยมีข้อจำกัด ดังนี้

- ผู้ใช้และสรรพสิ่งต้องได้รับการลงทะเบียนสำหรับกระบวนการยืนยันตัวตนในการสื่อสารสำหรับการบันทึกธุรกรรม
- โพรโทคอลการสื่อสารระหว่างสรรพสิ่งดำเนินการผ่านเน็ตพาย
- ข้อมูลในการสื่อสารเป็นการส่งข้อมูลตามลำดับเวลาการส่งข้อมูลโดยไม่ขึ้นกับระดับความสำคัญของข้อมูลที่ใช้ในการสื่อสาร
- ออกแบบต้นแบบการบันทึกธุรกรรมข้อมูลสุขภาพส่วนบุคคลด้วยการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตเท่านั้น
- การวัดประสิทธิภาพดำเนินการผ่านการจำลองข้อมูลและทดสอบบนต้นแบบสรรพสิ่งด้านการแพทย์สำหรับผู้ป่วย 30 คน แต่ละคนจะมีอุปกรณ์ทางการแพทย์ติดอยู่ไม่เกิน 4 ชิ้น และมีสรรพสิ่งสำหรับให้แพทย์อ่านผลที่โรงพยาบาล 1 คน
- การจำลองสถานการณ์ใช้ระบบเครือข่ายอินเทอร์เน็ตจริงโดยมีสรรพสิ่งที่มหาวิทยาลัยสงขลานครินทร์เป็นต้นทาง สรรพสิ่งที่โรงพยายามราษฎร์ยินดีเพื่อเป็นปลายทาง ระบบเครือข่ายผู้ใช้บริการ และบริการของเน็ตพาย

3.1 ผลการรวบรวมข้อมูลเกี่ยวกับอุปกรณ์ทางการแพทย์สำหรับผู้ป่วย

จากการสำรวจและหาข้อมูลรูปแบบข้อมูลทางการแพทย์ที่จะนำมาใช้สำหรับการสื่อสารระหว่างสรรพสิ่ง (นำเสนอในหัวข้อ 2.1.5) จะเป็นข้อมูลที่มาจากเครื่องตรวจวัดค่าสุขภาพร่างกายสำหรับการรักษาและติดตามข้อมูลสุขภาพทั่วไป ซึ่งมีรูปแบบข้อมูลที่มีการเปลี่ยนแปลงอย่างน้อยทุก 1 วินาที โดยอุปกรณ์วัดค่าสุขภาพผู้ป่วยมีจำนวนสูงสุดไม่เกิน 16 ชนิดต่อคน ข้อมูลทั้งสองส่วนนี้จะถูกใช้เป็นกรอบในการจำลองการออกแบบระบบ และการทดสอบระบบ

รูปแบบเครื่องมือทางการแพทย์ที่ใช้ในห้องฉุกเฉินหรือเซ็นเซอร์วัดค่าสุขภาพผ่านอุปกรณ์ส่วนบุคคล เช่น เซ็นเซอร์วัดอัตราการเต้นของหัวใจ เครื่องวัดความดัน เครื่องวัดการหายใจ เครื่องวัดอุณหภูมิ เครื่องวัดระดับน้ำตาลในเลือด เป็นต้น โดยมีจำนวนสูงสุดที่ 16 ชนิดต่อคน ส่วนรูปแบบอุปกรณ์การวัดค่าอาจเชื่อมต่อกับอุปกรณ์สื่อสาร หรือติดตั้งสำหรับผู้ป่วยติดเตียง โดยมีแพทย์หรือพยาบาลผู้มีสิทธิ์ในการรักษาสามารถติดตามดูข้อมูลได้ตลอดเวลา

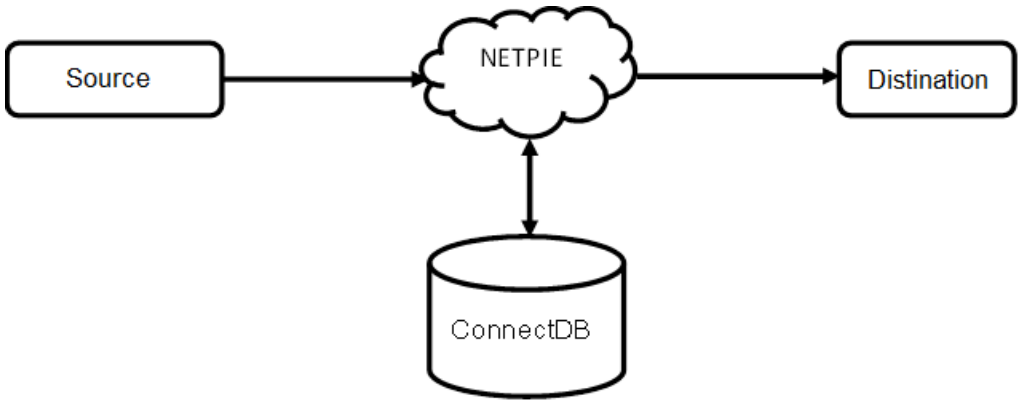
หากส่งข้อมูลสุขภาพผ่านอินเตอร์เน็ตซึ่งเป็นโพรโทคอลสาธารณะ ข้อมูลจำเป็นต้องผ่านกระบวนการเข้ารหัส การยืนยันตัวตนของอุปกรณ์ต้นทาง และการบันทึกธุรกรรมการสื่อสารข้อมูล ทั้งนี้ การดำเนินการต่างๆ จำเป็นต้องคำนึงถึงความเป็นส่วนตัวของเจ้าของข้อมูล ดังนั้นกระบวนการต่างๆ ต้องไม่ล่วงล้ำสิทธิ์ความเป็นส่วนตัวของข้อมูลในการสื่อสารที่ใช้ในการตรวจสอบด้วยเช่นกัน

3.2 รูปแบบธุรกรรมที่จัดการโดยระบบบันทึกธุรกรรม

ข้อมูลธุรกรรมเป็นข้อมูลที่ใช้สำหรับการติดตามตรวจสอบสถานะของระบบ ซึ่งสามารถตรวจสอบความมั่นคงปลอดภัยที่เกิดขึ้นระหว่างการติดต่อสื่อสารของอุปกรณ์ในระบบ โดยลักษณะของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตจะมีการจัดเก็บข้อมูลธุรกรรมที่แบ่งส่วนกัน ซึ่งถูกจัดเก็บในแต่ละอุปกรณ์ที่เชื่อมต่อเข้ามา ทำให้การวิเคราะห์ข้อมูลได้เฉพาะมุมมองของแต่ละอุปกรณ์เท่านั้น ดังนั้นการวิเคราะห์ธุรกรรมสำหรับการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตควรต้องวิเคราะห์จากทุกมุมมองของอุปกรณ์ที่เชื่อมต่อ เพื่อพิจารณาความมั่นคงปลอดภัยที่เกิดขึ้นในระบบได้ในภาพรวมทั้งหมดทุกกิจกรรม โดยระบบธุรกรรมสำหรับการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต ในงานวิจัยนี้มีการวิเคราะห์สิ่งที่เกิดขึ้นในระบบทั้งหมด 4 รูปแบบ ได้แก่ อุปกรณ์ใหม่ที่เชื่อมต่อเข้ามาครั้งแรก ข้อมูลธุรกรรมการรับส่งข้อมูลอย่างปกติสมบูรณ์ ข้อมูลธุรกรรมการรับส่งข้อมูลอย่างปกติสมบูรณ์แต่ล่าช้า ข้อมูลธุรกรรมการสื่อสารสูญหายระหว่างสรรพสิ่งและเน็ตพาย

3.2.1 อุปกรณ์ใหม่ที่เชื่อมต่อเข้ามาครั้งแรก

เหตุการณ์แรกของระบบ เป็นรูปแบบการแจ้งเตือนเมื่อมีอุปกรณ์ใหม่ที่ไม่เคยมีการเชื่อมต่อสื่อสารมายังสรรพสิ่งปลายทาง เพื่อตรวจสอบอุปกรณ์ใหม่ที่เข้ามานอกเหนือจากอุปกรณ์เดิมที่มีการติดต่อสื่อสารเป็นประจำ เพื่อสร้างความมั่นใจให้กับผู้ใช้เกี่ยวกับอุปกรณ์ที่เข้ามาร่วมสื่อสารกับสรรพสิ่งปลายทางเป็นไปตามที่ต้องการ และอยู่ในขอบเขตที่ผู้ดูแลอนุญาต ดังนั้นจึงควรมีฐานข้อมูลสำหรับการเก็บข้อมูลเกี่ยวกับประวัติการเชื่อมต่อแต่ละอุปกรณ์ ซึ่งจะเก็บข้อมูลของการส่งข้อมูลจากอุปกรณ์หนึ่งไปยังอีกอุปกรณ์หนึ่งในเวลาล่าสุด เมื่อต้องการตรวจสอบว่าอุปกรณ์ที่ส่งข้อมูลเข้ามาในอุปกรณ์ดังกล่าวเคยติดต่อสื่อสารกันหรือไม่ จะสามารถตรวจสอบจากฐานข้อมูลการเชื่อมต่อระหว่างอุปกรณ์ล่าสุดได้ ซึ่งหากไม่พบในฐานข้อมูลสามารถสรุปได้ว่าเป็นอุปกรณ์ใหม่ดังแสดงในรูปที่ 6



รูปที่ 6 เหตุการณ์การรับข้อมูลจากอุปกรณ์ใหม่ไปยังสรรพสิ่งปลายทาง

ฐานข้อมูลสำหรับเก็บข้อมูลการสื่อสารกันระหว่างอุปกรณ์ ประกอบด้วยชื่ออุปกรณ์ที่ส่งข้อมูล และชื่ออุปกรณ์ที่รับข้อมูล โดยมีเวลาการเชื่อมต่อล่าสุดของการรับส่งข้อมูลระหว่างสรรพสิ่งต้นทางและสรรพสิ่งปลายทาง โดยไม่พิจารณาหัวข้อการสื่อสารระหว่างทั้งสองสรรพสิ่ง แต่จะอ้างอิงการสื่อสารจากข้อมูลที่ได้รับการยืนยันตัวตนดังตารางที่ 1

ตารางที่ 1 ตัวอย่างฐานข้อมูลการเชื่อมต่อระหว่างอุปกรณ์กับอุปกรณ์ ConnectDB

Source	Destination	Timestamp	Timezone
DeviceA	DeviceB	09/04/2560 01:36:02	+00:00:03.024
DeviceC	DeviceB	02/04/2560 01:20:34	+00:00:00.486
DeviceB	DeviceD	03/04/2560 04:48:11	-00:00:01.017

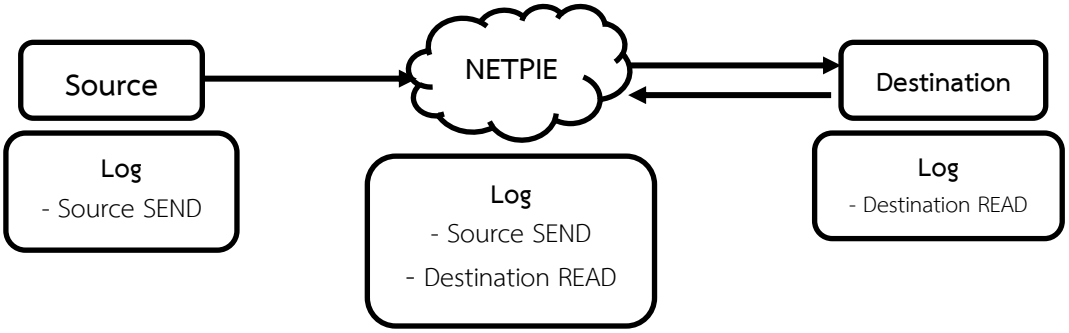
ฐานข้อมูล ConnectDB เป็นฐานข้อมูลที่จัดเก็บข้อมูลการจับคู่การเชื่อมต่อของแต่ละสรรพสิ่งที่เคยเกิดขึ้น เพื่อใช้ในการพิจารณาความน่าเชื่อถือของการเชื่อมต่อของสรรพสิ่ง ซึ่งหากเป็นการเชื่อมต่อจากสรรพสิ่งต้นทางไปยังสรรพสิ่งปลายทางที่ยังไม่เคยเกิดขึ้น ระบบจะทำการบันทึกธุรกรรมใน NetpieLog ว่าเกิดการเชื่อมต่อของสรรพสิ่งคู่ใหม่ และบันทึกข้อมูลคู่ของสรรพสิ่งที่สื่อสารใหม่ใน ConnectDB โดยทั้งนี้จะจัดเก็บข้อมูลส่วนต่างของเวลาสรรพสิ่งทั้งคู่โดยคำนวณจากความแตกต่างของข้อมูลการบันทึกเวลาในการเชื่อมต่อสรรพสิ่งซึ่งเกิดขึ้นในเวลาเดียวกัน เนื่องจากในความเป็นจริงแต่ละสรรพสิ่งจะมีนาฬิกาสำหรับประมวลผลไม่เท่ากันทุกประการ ซึ่งส่งผลให้การตรวจสอบความผิดปกติของการสื่อสาร ทั้งนี้สรรพสิ่งที่สื่อสารกันจำเป็นต้องใช้นาฬิกาการประมวลผลที่ใช้เวลาเท่ากันเพื่อความแม่นยำในการเทียบเวลาการสื่อสาร ดังนั้นในการบันทึกส่วนต่างของเวลาจากนาฬิกาของสรรพสิ่งคู่ใหม่ที่มีการจับคู่กันโดยใช้เวลาของสรรพสิ่งต้นทางเป็นเวลาอ้างอิงในคู่การ

สื่อสารเสมอ เพื่อให้สามารถเทียบเวลาได้อย่างถูกต้องเมื่อใช้ในการพิจารณาธุรกรรมในกรณีที่เวลาของสรรพสิ่งต้นทางและสรรพสิ่งปลายทางไม่ตรงตามเวลาโลกทั้งสองอุปกรณ์ เมื่อได้เวลาที่เทียบตรงกันแล้ว จะสามารถนำส่วนต่างของเวลามาปรับฐานของเวลาให้เสมือนใช้เวลาจากนาฬิกาประมวลผลเดียวกัน ทำให้การวิเคราะห์และพิจารณาความผิดปกติของธุรกรรมที่สรรพสิ่งใช้นาฬิกาประมวลผลต่างกันสามารถประมวลผลได้อย่างถูกต้องเสมือนหลักการเขตเวลาโลก (Timezone) [26] ซึ่งแต่ละประเทศจะใช้ฐานเวลาจากนาฬิกาไม่เท่ากันตามช่วงเวลาที่พระอาทิตย์ขึ้นและพระอาทิตย์ตกไม่พร้อมกัน ดังนั้นจึงใช้มาตรฐานเวลา UTC ในการตั้งฐานเวลาของแต่ละประเทศให้สามารถเปรียบเทียบนับฐานเวลาเดียวกันได้ โดยจะเทียบส่วนต่างของเวลาของทั้งสองสรรพสิ่งที่จับคู่กันทุกครั้ง เพื่อป้องกันความเหลื่อมล้ำของเวลาที่อาจเปลี่ยนแปลงหากแต่ละสรรพสิ่งมีการทำงานเป็นเวลานานโดยไม่ได้ปรับนาฬิกาให้ตรงอยู่เสมอ

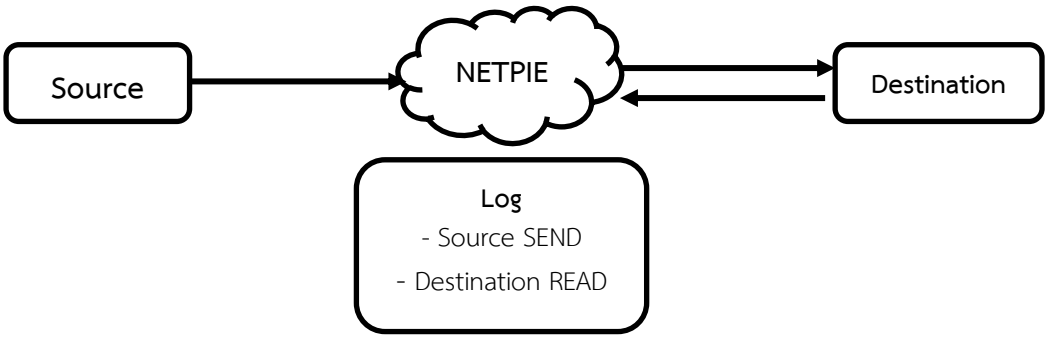
เมื่อระบบได้ตรวจพบการเชื่อมต่อเข้ามาของอุปกรณ์ใหม่มายังอุปกรณ์ในระบบ ซึ่งควรเป็นกระบวนการแรกในการตรวจสอบการสื่อสารระหว่างสรรพสิ่ง เพื่อให้สามารถวิเคราะห์รูปแบบเหตุการณ์อื่น ๆ ที่เกิดขึ้นตามมาได้อย่างสมบูรณ์ โดยสามารถแบ่งรูปแบบเหตุการณ์ได้เป็น 2 ประเภท ได้แก่ การรับส่งข้อมูลระหว่างอุปกรณ์อย่างปกติสมบูรณ์ และการรับส่งข้อมูลที่ผิดปกติระหว่างอุปกรณ์

3.2.2 ข้อมูลธุรกรรมการรับส่งข้อมูลอย่างปกติสมบูรณ์

ข้อมูลธุรกรรมที่เกิดขึ้นโดยทั่วไปในกรณีการสื่อสารแบบปกติที่สรรพสิ่งต่าง ๆ สามารถรับส่งข้อมูลได้อย่างสมบูรณ์จากสรรพสิ่งต้นทางถึงสรรพสิ่งปลายทาง เมื่อสรรพสิ่งต้นทางส่งข้อมูลออกไป สรรพสิ่งต้นทางก็จะบันทึกข้อมูลธุรกรรมไว้ว่าได้ส่งข้อมูลออกไปที่สรรพสิ่งต้นทางเอง เมื่อข้อมูลจากสรรพสิ่งต้นทางมาถึงเน็ตพาย เน็ตพายจะทำหน้าที่ในการกระจายข้อมูลไปยังสรรพสิ่งปลายทางที่ต้องการจะส่งข้อมูลไป ซึ่งในขณะเดียวกันเน็ตพายจะบันทึกธุรกรรมว่าได้รับข้อมูลจากสรรพสิ่งต้นทางและกำลังส่งข้อมูลดังกล่าวไปยังสรรพสิ่งปลายทาง หากสรรพสิ่งปลายทางที่ได้รับข้อมูลที่ส่งมาจากเน็ตพาย สรรพสิ่งปลายทางจะบันทึกข้อมูลธุรกรรมว่าได้รับข้อมูลแล้ว ซึ่งสรรพสิ่งปลายทางจะตอบกลับไปยังเน็ตพายเพื่อยืนยันว่าสรรพสิ่งปลายทางได้รับข้อมูลอย่างสมบูรณ์ภายในเวลาที่กำหนด ทำให้เน็ตพายสามารถปิดการบันทึกธุรกรรมสำหรับข้อมูลนี้ว่าสรรพสิ่งปลายทางได้รับข้อมูลจากสรรพสิ่งต้นทางไปยังสรรพสิ่งปลายทางได้อย่างสมบูรณ์ ดังแสดงในรูปที่ 7



รูปที่ 7 การรับส่งข้อมูลระหว่างอุปกรณ์อย่างสมบูรณ์



รูปที่ 8 การวิเคราะห์ธุรกรรมการรับส่งข้อมูลระหว่างอุปกรณ์อย่างสมบูรณ์

หากในมุมมองของข้อมูลธุรกรรม เมื่อสรรพสิ่งต้นทางส่งข้อมูลมายังเน็ตพาย ในส่วนของข้อมูลธุรกรรมของสรรพสิ่งต้นทางจะเก็บข้อมูลการส่งข้อมูลออกไป และเน็ตพายจะบันทึกข้อมูลธุรกรรมเมื่อรับข้อมูลจากสรรพสิ่งต้นทางว่าสรรพสิ่งต้นทางได้มีการส่งข้อมูลออกมาแล้ว เมื่อเน็ตพายส่งต่อข้อมูลไปยังสรรพสิ่งปลายทาง การบันทึกธุรกรรมจะรอการตอบกลับจากสรรพสิ่งปลายทาง หากสรรพสิ่งปลายทางได้รับข้อมูลแล้ว สรรพสิ่งปลายทางจะตอบกลับมายังเน็ตพายเพื่อบันทึกว่าสรรพสิ่งปลายทางได้รับข้อมูลแล้ว สรรพสิ่งปลายทางจะบันทึกข้อมูลธุรกรรมว่าได้รับข้อมูลจากสรรพสิ่งต้นทางแล้วที่ตัวสรรพสิ่งเช่นกัน ดังนั้นจะพบว่าในกรณีการตรวจสอบการส่งข้อมูลที่สมบูรณ์ระหว่างสรรพสิ่งสามารถตรวจสอบจากข้อมูลธุรกรรมที่เน็ตพายก็เพียงพอ เพราะหากมีการบันทึกว่าสรรพสิ่งปลายทางได้รับข้อมูลที่เน็ตพายแล้ว แสดงว่าการส่งข้อมูลสามารถส่งได้อย่างสมบูรณ์ ดังแสดงในรูปที่ 8

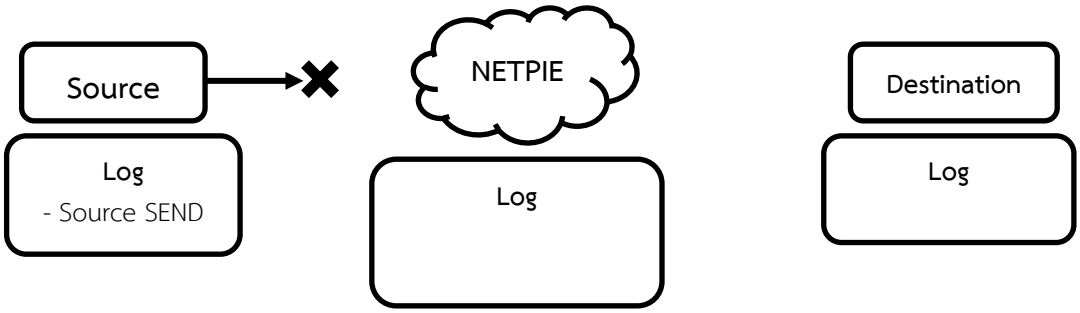
3.2.3 ข้อมูลธุรกรรมการรับส่งข้อมูลที่สมบูรณ์แต่ล่าช้า

ข้อมูลธุรกรรมนี้เป็นรูปแบบเหตุการณ์ที่ข้อมูลสามารถส่งจากสรรพสิ่งต้นทางไปยังสรรพสิ่งปลายทางได้อย่างสมบูรณ์แต่ใช้ระยะเวลาการส่งข้อมูลมากกว่าเวลาการเปลี่ยนแปลงของข้อมูลทางการแพทย์ ซึ่งมีการเปลี่ยนแปลงข้อมูลทุก ๆ 1 วินาที โดยใช้การตรวจสอบจากผลต่างของเวลาการส่งข้อมูลจากสรรพสิ่งต้นทางกับเวลาการรับข้อมูลจากสรรพสิ่งปลายทาง ถ้าพบว่าผลต่างของเวลาการส่งข้อมูลดังกล่าวใช้เวลามากกว่า 1 วินาที แสดงว่าข้อมูลที่สื่อสารเกิดความล่าช้าจึงบันทึกข้อมูลธุรกรรมจากเหตุการณ์นี้

3.2.4 ข้อมูลธุรกรรมการรับส่งข้อมูลที่ไม่สมบูรณ์

ข้อมูลธุรกรรมประเภทนี้จะเป็นเหตุการณ์ที่เกิดขึ้นหากการรับส่งข้อมูลระหว่างอุปกรณ์ไม่สมบูรณ์ โดยเมื่อส่งข้อมูลจากสรรพสิ่งต้นทางแล้วแต่สรรพสิ่งปลายทางไม่ได้รับข้อมูล ซึ่งสามารถแบ่งออกได้ 2 กรณี ได้แก่ ข้อมูลการสื่อสารสูญหายระหว่างสรรพสิ่งต้นทางกับเน็ตพายและข้อมูลการสื่อสารสูญหายระหว่างเน็ตพายกับสรรพสิ่งปลายทาง โดยมีรายละเอียดดังนี้

ข้อมูลการสื่อสารสูญหายระหว่างสรรพสิ่งต้นทางกับเน็ตพาย เป็นการส่งข้อมูลจากสรรพสิ่งต้นทางไปยังปลายทาง แต่ข้อมูลสูญหาย ในส่วนของการส่งข้อมูลจากสรรพสิ่งต้นทางไปยังเน็ตพาย โดยรูปแบบนี้จะมีข้อมูลธุรกรรมว่าอุปกรณ์ต้นทางได้ส่งข้อมูลออกไปแล้วที่ตัวอุปกรณ์ แต่ที่เน็ตพายและสรรพสิ่งปลายทางยังไม่มีธุรกรรมข้อมูลการได้รับข้อมูลจากสรรพสิ่งต้นทางดังแสดงในรูปที่ 9

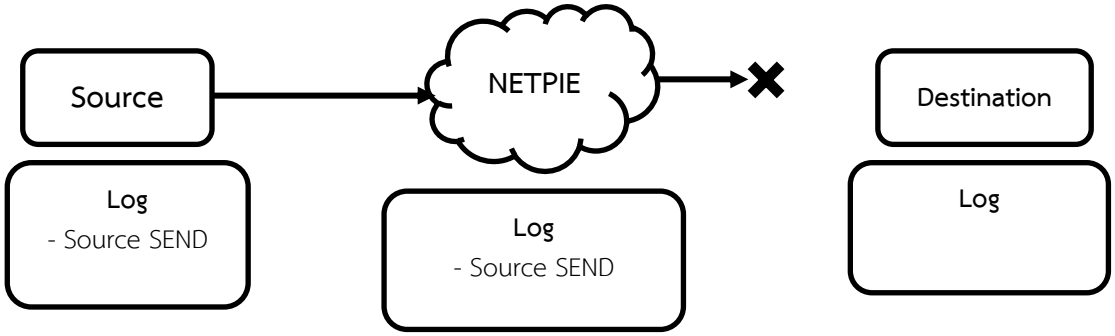


รูปที่ 9 การส่งข้อมูลสูญหายระหว่างส่งจากสรรพสิ่งต้นทางไปยังเน็ตพาย

หากมองในมุมมองของข้อมูลธุรกรรม เมื่อสรรพสิ่งต้นทางส่งข้อมูลออกไปยังเน็ตพายในส่วนของข้อมูลธุรกรรมของสรรพสิ่งต้นทางจะเก็บข้อมูลการส่งข้อมูลออกไป แต่เมื่อเน็ตพายไม่ได้รับข้อมูลเนื่องจากข้อมูลเกิดการสูญหายระหว่างทางจากสรรพสิ่งต้นทางมายังเน็ตพาย จึงทำให้ข้อมูลธุรกรรมที่เน็ตพายและสรรพสิ่งปลายทางไม่มีเหตุการณ์เกิดขึ้น จะพบว่าในกรณีข้อมูลเกิดการสูญหายระหว่างสรรพสิ่งต้นทางไปยังเน็ตพายจะพบการบันทึกข้อมูลธุรกรรมเพียงที่การบันทึก

ธุรกรรมที่สรรพสิ่งต้นทางเท่านั้น ทำให้กรณีนี้จำเป็นต้องให้สรรพสิ่งต้นทางมีการบันทึกข้อมูลธุรกรรมที่ตัวอุปกรณ์ด้วย

ข้อมูลการสื่อสารสูญหายระหว่างเน็ตพายกับสรรพสิ่งปลายทางเป็นการส่งข้อมูลจากสรรพสิ่งต้นทางไปยังปลายทาง แต่ข้อมูลสูญหาย ในส่วนของการส่งข้อมูลจากเน็ตพายไปยังสรรพสิ่งปลายทาง โดยรูปแบบนี้จะมีข้อมูลธุรกรรมว่าสรรพสิ่งต้นทางได้ส่งข้อมูลออกไปแล้วที่ตัวอุปกรณ์และเน็ตพาย แต่ที่สรรพสิ่งปลายทางไม่มีธุรกรรมเกี่ยวกับการได้รับข้อมูลจากอุปกรณ์ต้น ดังแสดงในรูปที่ 10

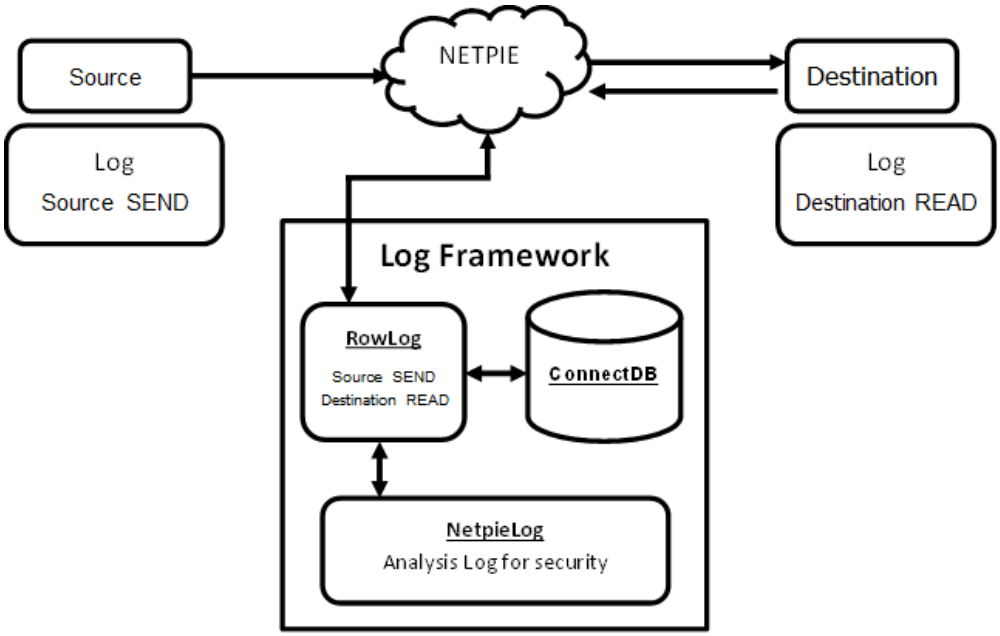


รูปที่ 10 การส่งข้อมูลสูญหายระหว่างส่งจากเน็ตพายไปยังสรรพสิ่งปลายทาง

หากมองในมุมมองของข้อมูลธุรกรรม เมื่อสรรพสิ่งต้นทางส่งข้อมูลออกไปยังเน็ตพาย ในส่วนของข้อมูลธุรกรรมของสรรพสิ่งต้นทางจะเก็บข้อมูลการส่งข้อมูลออกไป และที่เน็ตพายจะบันทึกข้อมูลธุรกรรมเมื่อรับข้อมูลจากสรรพสิ่งต้นทางว่าสรรพสิ่งต้นทางได้มีการส่งข้อมูลออกมาแล้ว และเมื่อเน็ตพายจะส่งต่อข้อมูลไปยังสรรพสิ่งปลายทาง การบันทึกธุรกรรมจะรอการตอบกลับจากสรรพสิ่งปลายทาง ซึ่งในกรณีนี้ข้อมูลจะเกิดการสูญหายระหว่างการส่งข้อมูลจากเน็ตพายไปยังสรรพสิ่งปลายทาง จึงทำให้ไม่มีการตอบรับไปยังเน็ตพาย ทำให้ข้อมูลธุรกรรมไม่ได้รับการบันทึกเกี่ยวกับการรับข้อมูลทั้งที่เน็ตพายและตัวสรรพสิ่งปลายทาง ในกรณีที่การตรวจสอบการส่งข้อมูลแล้วเกิดข้อมูลสูญหายระหว่างเน็ตพายกับสรรพสิ่งปลายทาง เน็ตพายจะไม่ได้รับการตอบรับจากสรรพสิ่งปลายทางเพื่อบันทึกธุรกรรมเกี่ยวกับความสำเร็จในการส่งข้อมูลในระยะเวลาที่กำหนด จึงสามารถวิเคราะห์ได้จากข้อมูลธุรกรรมที่เน็ตพาย เพราะในเหตุการณ์ปกติเน็ตพายเมื่อได้รับข้อมูลจะส่งต่อให้อุปกรณ์ทันทีและรอการตอบกลับภายในระยะเวลาที่กำหนด หากในข้อมูลธุรกรรมที่เน็ตพายมีเพียงการบันทึกการส่งข้อมูลมาจากอุปกรณ์ต้นทาง แต่ไม่มีการบันทึกการได้รับข้อมูลที่สรรพสิ่งปลายทางในระยะเวลาที่กำหนดก็สามารถสรุปได้ว่าข้อมูลสูญหายระหว่างการส่งข้อมูลจากเน็ตพายไปยังสรรพสิ่งปลายทาง

3.2.5 การวิเคราะห์ความผิดปกติ

ระบบบันทึกธุรกรรมสำหรับการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตมีรูปแบบที่ประกอบด้วยข้อมูลธุรกรรมที่จัดเก็บจากส่วนกลางของเน็ตพาย การรวบรวมข้อมูลธุรกรรมจากแต่ละอุปกรณ์มารวมกัน เพื่อใช้ในการวิเคราะห์แบบเทียบเคียงระหว่างข้อมูลธุรกรรมจากเน็ตพายและข้อมูลธุรกรรมรายอุปกรณ์ เพื่อหาความสอดคล้องกันและตรวจสอบความผิดปกติ ดังนั้น ระบบต้องมีส่วนของการจัดเก็บข้อมูลการสื่อสารระหว่างแต่ละอุปกรณ์ในเวลาล่าสุด เพื่อตรวจสอบหาอุปกรณ์ใหม่ที่มีการเชื่อมต่อไปยังอุปกรณ์ในระบบนอกเหนือจากการสื่อสารระหว่างอุปกรณ์เดิม ซึ่งจะมีโครงสร้างระบบภาพรวมดังแสดงในรูปที่ 11



รูปที่ 11 ภาพรวมระบบวิเคราะห์ธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต

ทั้งนี้สรุปได้ว่ากระบวนการตรวจสอบความผิดปกติในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตเบื้องต้นจะพิจารณาจากลำดับการส่งข้อมูลทั้งนี้จะเกิดจากการลงหมายเลขชุดข้อมูลที่ส่ง (Order ID) หากมีการส่งมายังเน็ตพายตามลำดับจำนวนเต็ม จะถือว่าข้อมูลส่งปกติ แต่หากมีการข้ามหมายเลขข้อมูลไม่เป็นไปตามลำดับนั้น หมายถึงมีบางชุดข้อมูลสูญหายไป โดยอาจสรุปจำนวนชุดข้อมูลที่สูญหายไปจากผลต่างระหว่างหมายเลขชุดข้อมูลปัจจุบันกับชุดข้อมูลล่าสุดที่ได้รับ แต่หากพบว่าชุดข้อมูลล่าสุดที่ได้รับคือหมายเลข 0 จะสามารถสรุปได้ว่าอุปกรณ์อาจทำการรีสตาร์ทการเชื่อมต่อ และหากหมายเลขชุดข้อมูลที่ได้รับไม่ถูกส่งมาตามลำดับหรือได้รับหมายเลขซ้ำกันในขณะที่ข้อมูลภายในไม่เหมือนกัน นั้นสรุปได้ว่าอาจมีการส่งข้อมูลซ้ำซ้อนในสื่อสารหรืออาจมีผู้ไม่หวังดีบุกรุกเข้ามาระหว่างการสื่อสารและพยายามปลอมแปลงการส่งข้อมูล

3.3 การจัดเก็บข้อมูลธุรกรรม

กระบวนการตรวจสอบธุรกรรมในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตซึ่งมีการสื่อสารตลอดเวลา หากจัดเก็บข้อมูลธุรกรรมทั้งหมดจะได้ข้อมูลมากเกินความจำเป็น จึงควรมีกระบวนการวิเคราะห์สรุปข้อมูลธุรกรรมก่อนจัดเก็บในระบบ โดยมุ่งเน้นเกี่ยวกับประเด็นด้านความปลอดภัยในการสื่อสารเท่านั้น เพื่อตรวจสอบสิ่งที่เกิดขึ้นในการสื่อสารระหว่างสรรพสิ่งโดยสามารถบอกรายละเอียดว่าผู้ใช้เป็นใคร สั่งผ่านอุปกรณ์ใด เวลาเกิดเหตุการณ์ และมีลักษณะเหตุการณ์อย่างไร ทั้งนี้รูปแบบข้อมูลธุรกรรมที่บันทึกจะมีการจัดหมวดหมู่ของเหตุการณ์ที่เกิดขึ้นจากการวิเคราะห์สิ่งที่เกิดขึ้นในการสื่อสารโดยอ้างอิงจากการกระบวนการยืนยันตัวตนของผู้ใช้งานและอุปกรณ์ รวมถึงความสัมพันธ์ของผู้ใช้งานกับอุปกรณ์เป็นหลัก เพื่อวิเคราะห์การบุกรุกของผู้ไม่หวังดีที่จะเข้ามาในระบบสื่อสาร จึงต้องมีการบันทึกข้อมูลสถานะต่าง ๆ ของสรรพสิ่งเพื่อให้สามารถตรวจสอบได้จากข้อมูลพื้นฐานในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตโดยไม่ล่วงละเมิดข้อมูลทางการแพทย์ที่บรรจุอยู่ในชุดข้อมูลซึ่งเป็นการละเมิดความส่วนตัวของผู้ป่วยซึ่งเป็นเจ้าของข้อมูล

ตารางที่ 2 ข้อมูลการบันทึกธุรกรรมทั้งหมด

Field	Data collected
ID	หมายเลขของเหตุการณ์
order	หมายเลขข้อมูลของสรรพสิ่ง
topic	หัวข้อของการสื่อสารของเหตุการณ์
source_device	ชื่ออุปกรณ์ที่ส่งข้อมูลของเหตุการณ์
des_device	ชื่ออุปกรณ์ที่รับข้อมูลของเหตุการณ์
source_stamp	วันเวลาที่ส่งข้อมูลจากสรรพสิ่งต้นทาง
des_stamp	วันเวลาที่เน็ตพายส่งข้อมูลออกไปยังสรรพสิ่งปลายทาง
netpie_stamp	วันเวลาที่เน็ตพายได้รับข้อมูลจากสรรพสิ่งต้นทาง
netpie_sent	วันเวลาที่เน็ตพายส่งข้อมูลไปยังสรรพสิ่งปลายทาง
username	บัญชีผู้ใช้ที่ส่งข้อมูล
patient	หมายเลขประจำตัวผู้ป่วย
location	สถานที่ที่ส่งข้อมูล
datasize	ขนาดข้อมูล

ข้อมูลพื้นฐานในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตประกอบด้วย หมายเลขลำดับข้อมูลที่ส่งออก วันเวลาที่ส่งข้อมูล หัวข้อการสื่อสาร ชื่ออุปกรณ์ที่ส่งข้อมูล ชื่อของอุปกรณ์ที่ต้องการให้รับข้อมูล ชื่อบัญชีผู้ใช้งานที่ส่งข้อมูล ขนาดข้อมูลรวม และหมายเลขอ้างอิงตัวผู้ป่วยในการยืนยันว่าเป็นข้อมูลของผู้ป่วยคนดังกล่าวอย่างแท้จริง ซึ่งจากข้อมูลพื้นฐานดังกล่าวที่ส่งมาจากจากสรรพสิ่งผ่านเน็ตพาย สามารถออกแบบรูปแบบการบันทึกธุรกรรมสำหรับการวิเคราะห์ความผิดปกติทั้งหมดได้ดังตารางที่ 2 ซึ่งบันทึกในฐานข้อมูล RowLog โดยเป็นข้อมูลธุรกรรมเหตุการณ์ทั้งหมดที่เกิดขึ้นในการสื่อสาร ซึ่งไม่ได้ผ่านการวิเคราะห์ จากภาพรวมระบบวิเคราะห์ฯ (แสดงในรูปที่ 11) มีฐานข้อมูลสำหรับบันทึกผลของการวิเคราะห์ข้อมูลธุรกรรมด้านความปลอดภัยที่เกิดจากการวิเคราะห์ข้อมูล RowLog ทันทีที่มีการบันทึกใหม่และเก็บข้อมูลเฉพาะข้อมูลที่มีความผิดปกติไว้อย่างถาวร โดยเก็บข้อมูลธุรกรรมดังกล่าวไว้ในฐานข้อมูล NetpieLog ตามรูปแบบโครงสร้างในตารางที่ 3 ซึ่งจะเป็นธุรกรรมที่เก็บเฉพาะข้อมูลธุรกรรมที่มีความสำคัญและเหตุการณ์ความผิดปกติด้านความปลอดภัยที่วิเคราะห์ได้จากข้อมูลธุรกรรมการสื่อสารทั้งหมด

ตารางที่ 3 ข้อมูลการบันทึกธุรกรรมที่ผิดปกติ

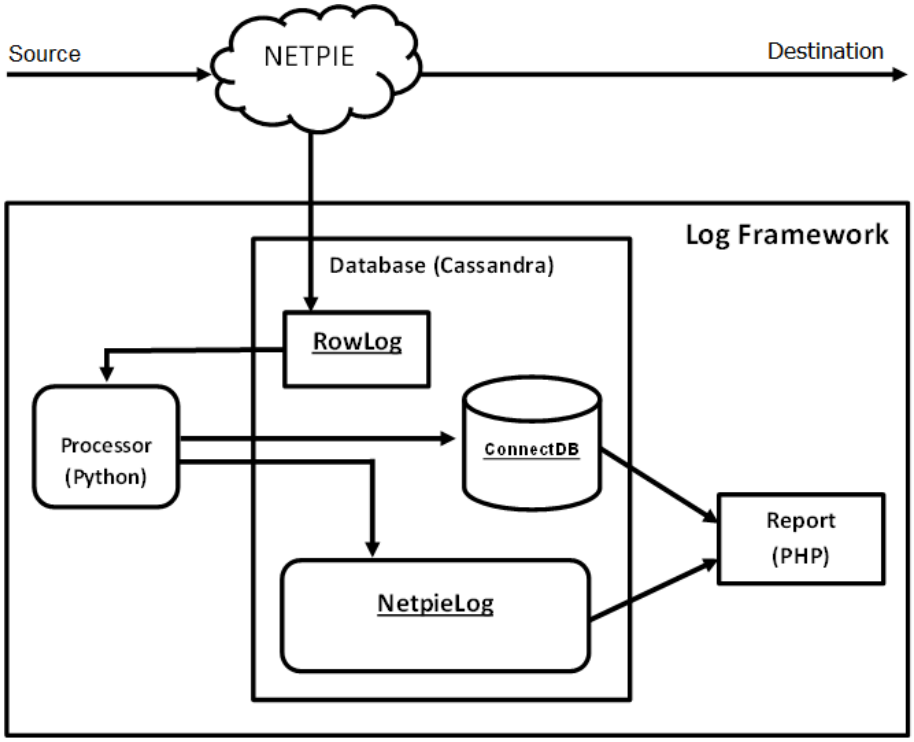
Field	**Data collected**
ID	หมายเลขของเหตุการณ์
DateStamp	วันเวลาของเหตุการณ์ที่เกิดขึ้น
Username	บัญชีผู้ใช้ที่ส่งข้อมูล
source_device	ชื่ออุปกรณ์ที่การส่งข้อมูลของเหตุการณ์
dest_device	ชื่ออุปกรณ์ที่การับข้อมูลของเหตุการณ์
Topic	หัวข้อของการสื่อสารของเหตุการณ์
Detail	รายละเอียดของเหตุการณ์
Type	ประเภทของข้อมูลธุรกรรมที่บันทึก

3.3.1 ระบบฐานข้อมูล

เนื่องจากรูปแบบฐานข้อมูลการบันทึกธุรกรรมในระบบส่วนใหญ่จะเพิ่มข้อมูลทันทีที่เกิดเหตุการณ์ขึ้นในระบบ แต่เนื่องจากการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตมีการสื่อสารตลอดเวลาและมีจำนวนมาก จึงต้องใช้ฐานข้อมูลที่มีคุณสมบัติในการจัดการข้อมูลได้ในปริมาณมากและสามารถรองรับการเพิ่มข้อมูลจำนวนมากทันทีที่มีการสื่อสาร จากคุณสมบัติฐานข้อมูลดังกล่าวจึงได้เลือกฐานข้อมูลแบบโนเอสคิวแอลในการจัดการฐานข้อมูล ทั้งนี้ได้เลือกฐานข้อมูลโนเอสคิวแอลที่เลือกใช้คือ Apache Cassandra [27] ซึ่งเป็นฐานข้อมูลที่มีประสิทธิภาพในการเขียนข้อมูลเป็น

จำนวนมาก เหมาะสมกับการใช้งานสำหรับเก็บข้อมูลธุรกรรมเพื่อลดข้อจำกัดในการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตที่มีปริมาณมาก อีกทั้งฐานข้อมูลชนิดนี้สามารถปรับขนาดและมีความพร้อมใช้งานที่มีประสิทธิภาพสูงในการทำงานเชิงเส้นและความทนทานต่อข้อผิดพลาดในฮาร์ดแวร์หรือโครงสร้างพื้นฐาน ภาษาในการควบคุมฐานข้อมูลมีความใกล้เคียงภาษาเอสคิวแอล

โครงสร้างฐานข้อมูลธุรกรรมใน Apache Cassandra สำหรับการบันทึกธุรกรรมที่มีปริมาณมากและอ่านข้อมูลตลอดเวลา จะทำงานร่วมกับส่วนประมวลผลข้อมูลธุรกรรมเพื่อวิเคราะห์หาความผิดปกติจากฐานข้อมูล RowLog ซึ่งพัฒนาด้วยภาษาไพทอน (Python) เพื่อประมวลผลค้นหาความผิดปกติต่าง ๆ ด้วยข้อมูลธุรกรรมพื้นฐานที่สรรพสิ่งส่งมาโดยไม่ล่วงละเมิดความเป็นส่วนตัวของผู้ป่วยที่เป็นเจ้าของข้อมูล อีกทั้งแสดงรายงานธุรกรรมทั้งหมดที่เกิดขึ้นโดยเฉพาะส่วนข้อมูลธุรกรรมความผิดปกติสำหรับการสื่อสารในรูปแบบหน้าเว็บไซต์ที่พัฒนาด้วยภาษาพีเอ็ชพี (PHP) เพื่อให้ง่ายต่อการเข้าถึงจากผู้ดูแลระบบและลดข้อจำกัดด้านอุปกรณ์รวมถึงระบบปฏิบัติการสำหรับการเข้าอ่านข้อมูลแสดงผลการติดตามธุรกรรม รูปที่ 12 แสดงส่วนประกอบของระบบบันทึกธุรกรรม

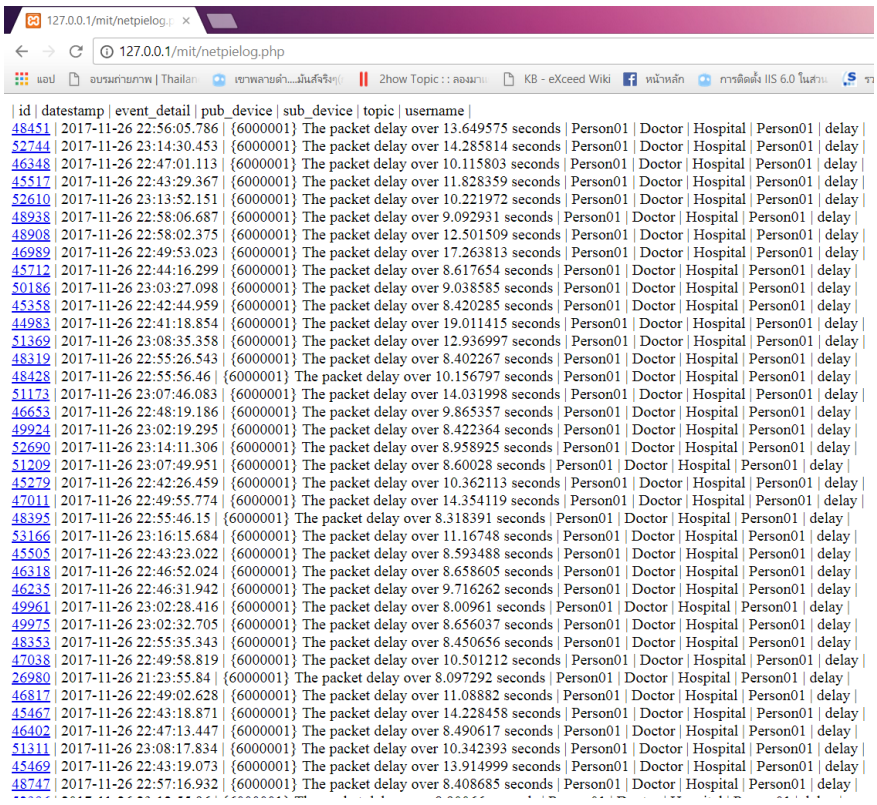


รูปที่ 12 ส่วนประกอบระบบบันทึกธุรกรรม

จากรูปที่ 12 แสดงให้เห็นถึงส่วนประกอบภายในระบบบันทึกธุรกรรมซึ่งแบ่งออกเป็น 3 ส่วน ได้แก่ ส่วนบันทึกข้อมูลธุรกรรม ส่วนประมวลผลธุรกรรม และส่วนรายงานผลการประมวลผลธุรกรรม เมื่อมีการสื่อสารข้อมูลผ่านเน็ตพาย ระบบจะเริ่มบันทึกธุรกรรมทั้งหมดที่ฐานข้อมูล RowLog และจะประมวลผลธุรกรรมใหม่ดังกล่าวกับธุรกรรมก่อนหน้าใน RowLog ด้วยส่วนประมวลผล (Processor) หากพบการเชื่อมต่อระหว่างอุปกรณ์ที่ไม่เคยมีการสื่อสารกัน ส่วนประมวลผลจะบันทึกธุรกรรมที่ ConnectDB เมื่อมีการจับคู่สรรพสิ่งใหม่ แต่หากพบการเชื่อมต่อที่ผิดปกติอื่น ๆ เช่นการส่งข้อมูลไม่เป็นไปตามลำดับ หรือมีข้อมูลในการสื่อสารสูญหาย ส่วนประมวลผลจะบันทึกผลการวิเคราะห์ความผิดปกติที่ NetpieLog เนื่องจากการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตมีการเชื่อมต่อกันตลอดเวลาและมีจำนวนมากเกินความจำเป็น แต่หากต้องการติดตามความผิดปกติของธุรกรรม ระบบจะแสดงผลข้อมูลจาก NetpieLog และ ConnectDB ออกมาในรูปแบบเว็บไซต์ เพื่อให้ง่ายต่อการติดตามความผิดปกติที่เกิดขึ้นได้จากอุปกรณ์ต่าง ๆ

ส่วนรายงานการแสดงเหตุการณ์ความผิดปกติที่เกิดขึ้นในการสื่อสารข้อมูลระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตจะมีลักษณะดังรูปที่ 13 ซึ่งทำให้ผู้ดูแลระบบสามารถดูเหตุการณ์ความผิดปกติที่เกิดขึ้นได้ทันทีโดยไม่ต้องประมวลผลวิเคราะห์ข้อมูลใหม่ในแต่ละครั้งและสามารถเชื่อมโยงรายละเอียดธุรกรรมเหตุการณ์ดังกล่าวได้ผ่านข้อมูลซึ่งบรรจุใน RowLog โดยสืบค้นได้จากข้อมูลหมายเลขธุรกรรม

ทั้งนี้ในส่วนระบบประมวลผลที่พัฒนาด้วยภาษาไพทอนและระบบรายงานธุรกรรมที่พัฒนาด้วยพีเอ็ชพีต้องติดตั้งส่วนเสริมในการเชื่อมต่อกับฐานข้อมูล Apache Cassandra เพื่อให้รองรับเครื่องมือการพัฒนาเหล่านี้



รูปที่ 13 ตัวอย่างหน้ารายงานแสดงข้อมูลธุรกรรมความผิดปกติที่พบ

3.3.2 กระบวนการเข้ารหัสข้อมูล

เนื่องจากการบันทึกข้อมูลธุรกรรมเหตุการณ์ในระบบการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต เป็นกระบวนการในการตรวจสอบความปลอดภัยที่เกิดขึ้นว่าเป็นไปตามวัตถุประสงค์ของผู้ใช้งานอย่างถูกต้อง โดยไม่มีการสลับข้อมูลหรือแอบอ้างระหว่างการสื่อสารควบคุมสรรพสิ่งผ่านอินเตอร์เน็ตซึ่งเป็นช่องทางการสื่อสารสาธารณะ เพื่อสร้างความน่าเชื่อถือในการนำแนวคิดการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตมาใช้งานจริงมากยิ่งขึ้นโดยเฉพาะทางการแพทย์ อีกทั้งสามารถติดตามความผิดปกติที่เกิดขึ้นในการสื่อสาร เพื่อตรวจสอบรูปแบบกิจกรรมการรับส่งข้อมูลว่ามาจากใคร ด้วยอุปกรณ์อะไร และดำเนินการอะไรกับสรรพสิ่ง เช่น ติดตามกระบวนการควบคุมการเปิดปิดไฟฟ้าในบ้านอัจฉริยะจากแนวคิดการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตด้วยโทรศัพท์มือถือว่ามาจากผู้ใช้งานที่มีสิทธิ์ในการเข้าถึงการควบคุมการเปิดปิดไฟฟ้าในบ้านอัจฉริยะหลังนั้นจริงหรือไม่ และด้วยอุปกรณ์อะไร จากเดิมการควบคุมการเปิดปิดไฟฟ้าผ่านอินเตอร์เน็ตนั้นสรรพสิ่งที่ใช้ในการรับคำสั่งการสื่อสารควบคุมการเปิดปิดไฟฟ้าไม่เหมาะสำหรับการบันทึกข้อมูลธุรกรรมการสื่อสารที่เกิดขึ้น ทั้งในด้านของหน่วยประมวลผล หน่วยความจำ และหน่วยการจัดการพลังงานในอุปกรณ์ เนื่องจากเป็นระบบประมวลผลขนาดเล็ก จึงทำให้มีความเสี่ยงที่ผู้ไม่หวังดีสามารถกระทำการใด ๆ ในการแอบอ้างเพื่อเข้ามาควบคุมการสั่งการควบคุมการเปิดปิดไฟฟ้าได้ ทำ

ให้การประยุกต์แนวคิดการสื่อสารระหว่างสรรพสิ่งขาดความน่าเชื่อถือ อีกทั้งไม่สามารถรู้ถึงสถานะปัจจุบันของอุปกรณ์ควบคุมการเปิดเปิดไฟฟ้าว่าอยู่ในสถานะเปิดหรือปิดอยู่ในขณะนั้น

กระบวนการในการบันทึกธุรกรรมในการสื่อสารระหว่างสรรพสิ่งจะใช้การเข้ารหัสข้อมูลคำสั่งด้วยกุญแจประจำตัวของบัญชีผู้ใช้งานและกุญแจประจำตัวของอุปกรณ์ที่ใช้ส่งข้อมูล เพื่อนำข้อมูลชุดนี้ไปยืนยันตัวตนที่ตัวกลางของการสื่อสารระหว่างสรรพสิ่งโดยการถอดรหัสข้อมูลด้วยชุดกุญแจถอดรหัสของบัญชีผู้ใช้งานและกุญแจถอดรหัสของอุปกรณ์ที่ใช้ส่งข้อมูลที่ถูกเก็บไว้ในฐานข้อมูลสำหรับการยืนยันตัวตนโดยใช้หมายเลขบัญชีผู้ใช้งานและหมายเลขอุปกรณ์ที่ใช้ส่งข้อมูลในการค้นหากุญแจสำหรับถอดรหัส ทำให้ข้อมูลมีความปลอดภัยจากการสลับเปลี่ยนและแอบอ้างในการสื่อสารระหว่างสรรพสิ่ง เนื่องจากกุญแจสำหรับการเข้ารหัสอยู่ที่สรรพสิ่งและกุญแจสำหรับถอดรหัสอยู่ที่ตัวกลางของการสื่อสารเท่านั้น โดยสรรพสิ่งต้องมีการลงทะเบียนยืนยันตัวตนด้วยกระบวนการโอออท (OAuth) กับตัวกลางการสื่อสารไว้ก่อนแล้ว

จากกระบวนการดังกล่าว การบันทึกข้อมูลธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตที่นำเสนอจะมีความน่าเชื่อถือมากขึ้น อีกทั้ง สามารถป้องกันการบิดเบือนข้อมูลธุรกรรมจากผู้ไม่หวังดีโดยกระบวนการยืนยันตัวตน เนื่องจากการบันทึกธุรกรรมสำหรับการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตนั้นจะมีลักษณะพิเศษ กล่าวคือ สรรพสิ่งที่สื่อสารจะเป็นอุปกรณ์ประมวลผลขนาดเล็กที่มีการรับส่งข้อมูลตลอดเวลาผ่านอินเตอร์เน็ตซึ่งเป็นโพรโทคอลสาธารณะ ทำให้สรรพสิ่งมีความเสี่ยงที่จะมีผู้ไม่หวังดีโจรกรรมข้อมูลหรือลักลอบควบคุมสรรพสิ่งโดยไม่ได้รับอนุญาต ดังนั้นรูปแบบการบันทึกธุรกรรมจะต้องบอกถึงการรับส่งข้อมูลจากใคร ด้วยสรรพสิ่งใด และเวลาใด เป็นต้น

การตรวจสอบความผิดปกติที่เกิดขึ้นในการสื่อสาร จำเป็นต้องใช้ข้อมูลว่าสรรพสิ่งรับส่งข้อมูลจากใครซึ่งสามารถอ้างอิงได้จากบัญชีผู้ใช้ เนื่องจากการที่หนึ่งสรรพสิ่งใช้งานจากหลายบัญชีผู้ใช้ หรือหนึ่งบัญชีผู้ใช้ใช้งานหลายสรรพสิ่ง

3.4 กระบวนการจัดเก็บข้อมูลธุรกรรม

กระบวนการยืนยันตัวตนเพื่อบันทึกข้อมูลธุรกรรมการควบคุมสรรพสิ่งผ่านอินเตอร์เน็ตควรมีการตรวจสอบว่าผู้ใช้เป็นใคร และใช้งานจากอุปกรณ์อะไร แล้วจึงมาหาความสัมพันธ์อีกครั้งหนึ่งว่าผู้ใช้กับอุปกรณ์ที่ใช้ควบคุมน่าเชื่อถือหรือไม่ ทั้งนี้การบันทึกข้อมูลธุรกรรมควรดำเนินการอย่างปลอดภัย เพราะหากผู้ไม่หวังดีสามารถติดตามข้อมูลธุรกรรมกิจกรรมในระบบได้อาจทำให้ผู้ไม่หวังดีสามารถปลอมแปลงตัวตนเพื่อควบคุมสรรพสิ่งต่าง ๆ ได้เช่นกัน ดังนั้นการรับส่งข้อมูลการควบคุมสรรพสิ่งผ่านทางอินเตอร์เน็ต ควรมีการเข้ารหัสข้อมูลจากการยืนยันตัวตนของผู้ใช้งานก่อนโดยใช้กุญแจของผู้ใช้งาน ทั้งนี้ผู้ใช้งานต้องลงทะเบียนกับส่วนการยืนยันตัวตนของระบบบันทึกธุรกรรมพร้อมกับแนบหมายเลขบัญชีผู้ใช้ล่วงหน้าแล้ว จากนั้นจึงนำข้อมูลที่ถูกเข้ารหัสจาก

บัญชีผู้ใช้มาเข้ารหัสด้วยหมายเลขอุปกรณ์ที่ใช้ควบคุมสรรพสิ่งอีกครั้งหนึ่งพร้อมกับแนบหมายเลขอุปกรณ์ที่ใช้งานไปด้วยดังรูปที่ 14

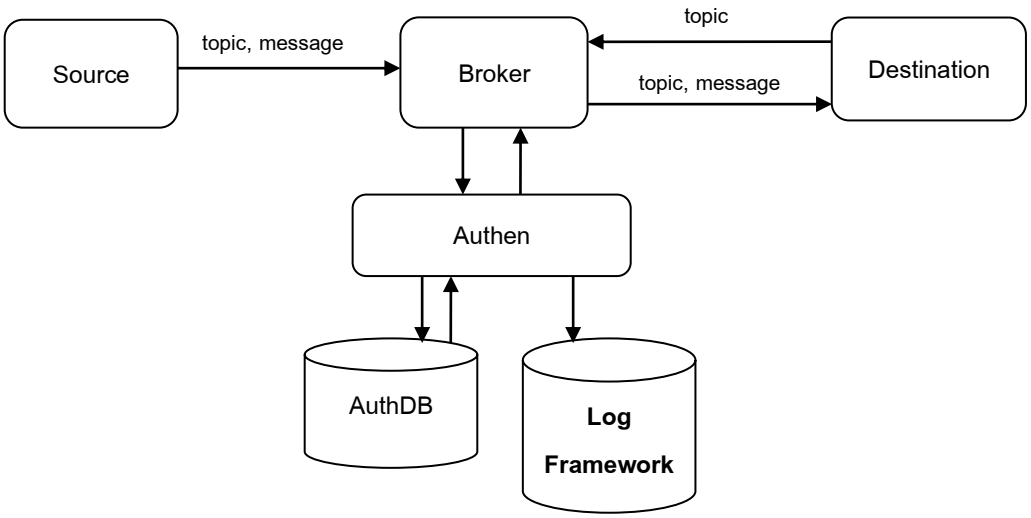
จากนั้นจึงนำข้อมูลที่ถูกเข้ารหัสส่งไปยังตัวกลางในการสื่อสาร (Broker) เพื่อทำการยืนยันตัวตนและคัดแยกข้อมูลเพื่อส่งข้อมูลไปยังสรรพสิ่ง โดยข้อมูลจะถูกส่งไปยัง Authen ในการยืนยันตัวตนของอุปกรณ์ที่สั่งการจากข้อมูล DeviceID ที่แนบมาตามรูปที่ 15 เพื่อค้นหากุญแจในการถอดรหัสจาก AuthDB ซึ่งหากค้นหากุญแจของอุปกรณ์เจอจากฐานข้อมูลดังรูปที่ 16 จะสามารถยืนยันตัวตนได้ว่ามาจากอุปกรณ์ตัวใด

เมื่อถอดรหัสจากหมายเลขอุปกรณ์เพื่อยืนยันตัวอุปกรณ์ได้แล้ว จะต้องยืนตัวตนของผู้ใช้งานจาก UserID ซึ่งคือหมายเลขผู้ใช้ที่แนบมาด้วย เพื่อนำไปค้นหาในฐานข้อมูล AuthDB อีกครั้งหนึ่งในการหากุญแจถอดรหัสข้อมูลอีกขั้นที่แนบมา ทำให้สามารถยืนยันตัวตนของผู้ใช้งานได้เช่นกัน โดยจะนำข้อมูลธุรกรรมดังกล่าวมาบันทึกในส่วนของ LogDB เพื่อใช้สำหรับการบันทึกข้อมูลธุรกรรมที่เชื่อถือได้

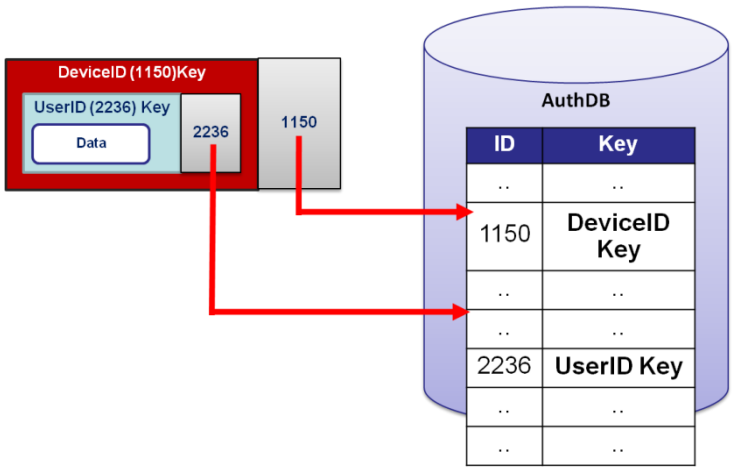
เมื่อทำการยืนยันตัวตนของผู้ใช้และอุปกรณ์ได้แล้ว จะพบกับข้อมูลที่ใช้ในการสื่อสารและหัวข้อในการสื่อสารเพื่อให้ Broker จัดการส่งข้อมูลไปยังสรรพสิ่งปลายทางที่ร้องขอข้อมูลที่สนใจในหัวข้อมูลเดียวกัน ข้อมูลที่จะส่งไปยังสรรพสิ่งปลายทางจะถูกแนบหมายเลขผู้ใช้งานและอุปกรณ์ที่ใช้ควบคุมไปด้วย เพื่อสร้างความน่าเชื่อถือในการสื่อสารว่าข้อมูลที่ถูกส่งมาได้รับการยืนยันตัวตนแล้ว อีกทั้งจะถูกเข้ารหัสจากกุญแจสรรพสิ่งปลายทางที่ร้องขอดังรูปที่ 17 ซึ่งนำมาจาก AuthDB ซึ่งเป็นกุญแจที่มาจากการลงทะเบียนของสรรพสิ่งไว้ก่อนหน้านี้แล้ว เพื่อป้องกันการดักจับข้อมูลซึ่งสรรพสิ่งปลายทางจะสามารถถอดรหัสได้จากกุญแจที่ตัวเองมีอยู่แล้วในการอ่านข้อมูล ทั้งนี้สรรพสิ่งปลายทางจะได้รับข้อมูลจากผู้ใช้ รวมถึงข้อมูลว่าผู้ใช้ใดเป็นคนส่ง และส่งจากอุปกรณ์อะไรให้สร้างความน่าเชื่อถือให้กับการสื่อสารในการใช้งานด้านต่าง ๆ ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

DeviceIDPub [UserID [Topic , Message] , UserID] , DeviceIDPub

รูปที่ 14 แนวคิดการเข้ารหัสข้อมูลเพื่อส่งข้อมูลจาก Publisher ไปยัง Broker



รูปที่ 15 โครงสร้างแนวคิดการยืนยันตัวตนสำหรับการบันทึกธุรกรรม



รูปที่ 16 แนวคิดการยืนยันตัวตนจากข้อมูลที่เข้ารหัสในฐานข้อมูล AuthDB

DeviceSub [Topic , Message , UserID , DeviceIDPub] , DeviceSub

รูปที่ 17 แนวคิดการเข้ารหัสข้อมูลเพื่อส่งข้อมูลจาก Broker ไปยัง Subscriber

3.5 การทดสอบระบบ

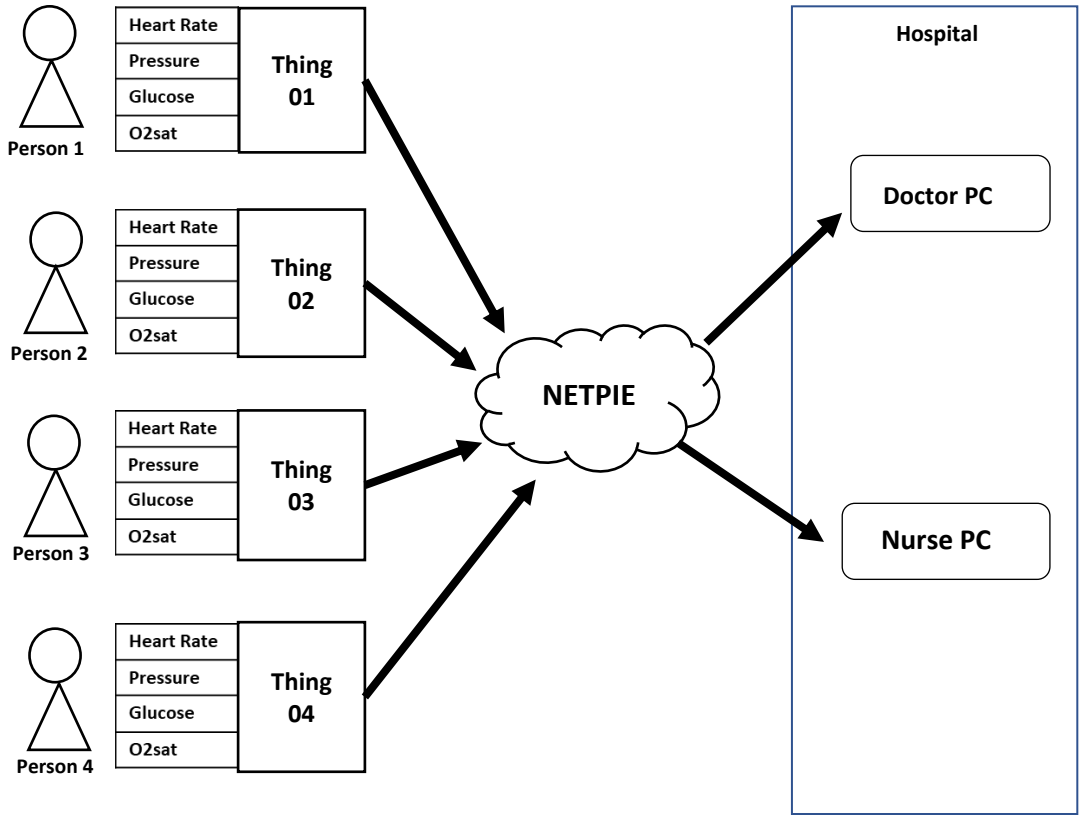
กระบวนการบันทึกธุรกรรมระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตในกรณีข้อมูลสุขภาพส่วนบุคคลซึ่งจำเป็นต้องมีการติดตามเรื่องความปลอดภัยในการรับส่งข้อมูลเป็นอย่างสูง เนื่องจากเป็นข้อมูลความลับส่วนบุคคลที่สามารถสร้างความเสียหายต่อเจ้าของข้อมูลได้ โดยทั้งนี้มุ่งเน้นเหตุการณ์ในการติดตามข้อมูลสุขภาพของผู้ป่วยจากอุปกรณ์วัดค่าที่สามารถเชื่อมต่ออินเตอร์เน็ตเพื่อส่งข้อมูลมายังโรงพยาบาลเพื่อให้แพทย์วินิจฉัยผู้ป่วยในกรณีที่ต้องติดตามอย่างใกล้ชิดได้ตลอดเวลา การออกแบบกรณีเหตุการณ์จำลองการสื่อสารระหว่างอุปกรณ์ที่วัดค่าจากผู้ป่วยไปยังโรงพยาบาลแสดงดังรูปที่ 18 ซึ่งเป็นการสื่อสารระหว่างอุปกรณ์วัดข้อมูลสุขภาพของผู้ป่วยแต่ละคน

โดยข้อมูลที่บันทึกจะมาจากอุปกรณ์วัดค่า 4 ชนิด ได้แก่ การวัดอัตราการเต้นของหัวใจ การวัดความดันโลหิต การวัดระดับน้ำตาล และการวัดระดับออกซิเจน ทั้งนี้ข้อมูลจากอุปกรณ์วัดค่าทั้ง 4 ชนิด จะถูกส่งผ่านสรรพสิ่ง (Thing) เพียง 1 ชิ้น ซึ่งจะเป็นสรรพสิ่งของผู้ป่วยคนดังกล่าว การส่งข้อมูลจะส่งข้อมูลผ่านเครือข่ายอินเตอร์เน็ตภายในพื้นที่มหาวิทยาลัยสงขลานครินทร์ อำเภอหาดใหญ่ จังหวัดสงขลา และใช้งานเน็ตพายปกติ ส่วนสรรพสิ่งซึ่งรับข้อมูลจะอยู่ที่โรงพยาบาลราษฎร์ยินดี อำเภอหาดใหญ่ จังหวัดสงขลา เพื่อเป็นการจำลองลักษณะช่องทางสื่อสารข้อมูลที่เป็นอยู่จริงในสภาพปัจจุบัน

จากเหตุการณ์จำลองดังกล่าวทุกอุปกรณ์ที่มีการรับส่งข้อมูล จะมีการจัดเก็บข้อมูลธุรกรรมการดำเนินการของแต่ละอุปกรณ์ไว้ในอุปกรณ์ และมีการปรับข้อมูลธุรกรรมของแต่ละอุปกรณ์มารวมอยู่ที่ศูนย์กลางเพื่อให้เป็นรูปแบบโครงสร้างเดียวกัน โดยอ้างอิงจากกระบวนการที่ใช้สื่อสารของเน็ตพายซึ่งมีการกำหนดปลายทางเป็นชื่ออุปกรณ์หรือหัวข้อที่ใช้ในการสื่อสาร อย่างไรก็ตาม เมื่อข้อมูลธุรกรรมมาอยู่รวมกันจะทำให้ข้อมูลที่เข้ามามีปริมาณที่มากและมีแนวโน้มที่จะเพิ่มขึ้นเรื่อย ๆ จึงต้องมีการบริหารจัดการข้อมูลที่ดี เพื่อใช้ในการวิเคราะห์อย่างมีประสิทธิภาพ โดยต้องคัดกรองข้อมูลที่ไม่จำเป็นออกหรือสรุปข้อมูลที่มีช่วงข้อมูลที่มีปริมาณเกินความจำเป็นและเก็บเฉพาะส่วนที่สรุปไว้เพื่อการวิเคราะห์ในครั้งต่อไป ดังนั้นจึงต้องอาศัยการนำแนวคิดการจัดการข้อมูลขนาดใหญ่ (Big data) มาช่วยในการวิเคราะห์ข้อมูลธุรกรรมในลักษณะนี้ซึ่งมีการเคลื่อนไหวของข้อมูลจำนวนมากซึ่งจะรายงานออกมาในรูปแบบดังรูปที่ 19

จากรูปแบบการบันทึกข้อมูลธุรกรรมของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตโดยผ่านผู้ให้บริการเน็ตพาย จึงต้องมีการประเมินเพื่อประสิทธิภาพในการบันทึกธุรกรรมระหว่างสรรพสิ่งในการสื่อสารด้านสาธารณสุขซึ่งความครบถ้วนสมบูรณ์ของข้อมูลมีความสำคัญ เพื่อให้ข้อมูลที่จัดเก็บสามารถใช้งานได้ ข้อมูลจากอุปกรณ์วัดค่าทางการแพทย์อาจจะมีข้อจำกัดในการอ่านค่าข้อมูลดังแสดงไว้ในหัวข้อ 3.1 อีกทั้งการสื่อสารข้อมูลสุขภาพในความเป็นจริงสามารถมีการสื่อสารระหว่างเซ็นเซอร์จากผู้ป่วยแต่ละคนส่งไปยังอุปกรณ์อ่านผลของแพทย์ พยาบาล และญาติของ

ผู้ป่วยได้หลากหลายรูปแบบตามสิทธิ์ที่เจ้าของข้อมูลกำหนด ทำให้การวัดผลประสิทธิภาพการตรวจสอบข้อมูลธุรกรรมอาจแปรผันตามปริมาณการสื่อสาร ดังนั้นเพื่อทดลองหาประสิทธิภาพการบันทึกธุรกรรมและตรวจสอบความผิดปกติที่เกิดขึ้นในการสื่อสารข้อมูลทางการแพทย์ระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต จึงกำหนดการทดลองให้อยู่ในสภาพแวดล้อมเดียวกันในรูปแบบมีปริมาณผู้ป่วยมากกว่าหนึ่งคนส่งข้อมูลไปให้แพทย์หนึ่งคนผ่านเน็ตพายภายใต้สภาพแวดล้อมเดียวกัน ในการทดสอบระบบจึงมีการทดลองที่ 1 และ 2 เพื่อหาอัตราการรับส่งข้อมูลและปริมาณข้อมูลที่เหมาะสมในการใช้เพื่อการบันทึกธุรกรรม



รูปที่ 18 ออกแบบการจำลองเหตุการณ์สื่อสารข้อมูลสุขภาพระหว่างผู้ป่วยกับโรงพยาบาล

การทดลองที่ 1 ทำการทดลองเพื่อหาอัตราการรับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม โดยมีวัตถุประสงค์เพื่อหาอัตราการรับส่งข้อมูลระหว่างสรรพสิ่งต้นทางผ่านเครือข่ายอินเตอร์เน็ตไปยังเน็ตพายและกลับมายังสรรพสิ่งปลายทาง ภายใต้สภาวะแวดล้อมในพื้นที่อำเภอหาดใหญ่ จังหวัดสงขลา โดยจำนวนสรรพสิ่งต้นทางมี 5 แบบ ได้แก่ 1, 2, 4, 8 และ 16 ชิ้น ส่วนขนาดข้อมูลคงที่ขนาด 56 ไบต์ แต่ละสรรพสิ่งส่งข้อมูลจำนวน 1000 ชุด และสรรพสิ่งปลายทางมีจำนวน 1 ชิ้น ทั้งนี้

ระยะห่างระหว่างการส่งข้อมูลจะเปลี่ยนแปลงโดยมีการส่งข้อมูลทุก 1 วินาที 500 มิลลิวินาที 250 มิลลิวินาที และ 125 มิลลิวินาที

การทดลองที่ 2 ทำการทดลองเพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย โดยมีวัตถุประสงค์เพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารข้อมูลระหว่างสรรพสิ่งต้นทางผ่านเครือข่ายอินเตอร์เน็ตไปยังเน็ตพายและกลับมายังสรรพสิ่งปลายทาง ภายใต้สภาวะแวดล้อมในพื้นที่อำเภอหาดใหญ่ จังหวัดสงขลา โดยจำนวนสรรพสิ่งต้นทางมี 16 ชิ้น แต่ละสรรพสิ่งส่งข้อมูลจำนวน 1000 ชุด สรรพสิ่งปลายทางมีจำนวน 1 ชิ้น ทั้งนี้ ระยะห่างระหว่างการส่งข้อมูลเป็น 250 มิลลิวินาที และขนาดของข้อมูลโดยเริ่มจาก 1 Bytes แล้วจึงเพิ่มขนาดครั้งละสองเท่าเป็น 2, 4, 8, 16, 24, 36, 64, 128, 256, 512, 1024, 2048, 4096, 8192 และ 16392 ไบต์ เพื่อหาขนาดข้อมูลที่ทำให้เกิดความล่าช้าเกิน 1 วินาที

id	nouns	datasize	location	netpie_stamp	patient	pub_device	pub_stamp	sub_device	sub_stamp	topic	username
440656	169464	12	Room43	2018-06-15 10:12:55.962+0000	6000002	Cardiac Monitoring A02	2018-06-15 10:13:52.600+0000	DoctorPC	2018-06-15 10:12:55.962+0000	heartrate	Person02
127510	60302	12	Room43	2018-06-15 02:34:54.895+0000	6000002	Cardiac Monitoring A02	2018-06-15 02:35:49.268+0000	DoctorPC	2018-06-15 02:34:54.895+0000	heartrate	Person02
247398	104689	12	Room43	2018-06-15 05:40:33.783+0000	6000002	Cardiac Monitoring A02	2018-06-15 05:41:29.074+0000	DoctorPC	2018-06-15 05:40:33.783+0000	heartrate	Person02
439904	169237	2	Room43	2018-06-15 10:11:52.687+0000	6000001	Cardiac Monitoring A01	2018-06-15 10:11:58.219+0000	DoctorPC	2018-06-15 10:11:52.687+0000	o2sat	Person01
230562	44597	2	Home01	2018-06-15 05:16:57.823+0000	6000101	Portable Monitoring A01	2018-06-15 05:19:26.741+0000	DoctorPC	2018-06-15 05:16:57.823+0000	heartrate	PersonA
239658	102657	2	Room43	2018-06-15 05:29:43.402+0000	6000001	Cardiac Monitoring A01	2018-06-15 05:29:47.768+0000	DoctorPC	2018-06-15 05:29:43.402+0000	heartrate	Person01
389757	152499	2	Room43	2018-06-15 09:00:56.660+0000	6000001	Cardiac Monitoring A01	2018-06-15 09:01:01.910+0000	DoctorPC	2018-06-15 09:00:56.660+0000	heartrate	Person01
583817	219531	12	Room43	2018-06-15 13:44:04.918+0000	6000002	Cardiac Monitoring A02	2018-06-15 13:45:02.593+0000	DoctorPC	2018-06-15 13:44:04.918+0000	heartrate	Person02
602967	225653	2	Room43	2018-06-15 14:11:00.749+0000	6000001	Cardiac Monitoring A01	2018-06-15 14:11:07.283+0000	DoctorPC	2018-06-15 14:11:00.749+0000	glucose	Person01
61995	31826	3	Room43	2018-06-15 00:29:58.296+0000	6000001	Cardiac Monitoring A01	2018-06-15 00:30:01.398+0000	DoctorPC	2018-06-15 00:29:58.296+0000	heartrate	Person01
341498	136380	2	Room43	2018-06-15 07:52:36.453+0000	6000001	Cardiac Monitoring A01	2018-06-15 07:52:40.753+0000	DoctorPC	2018-06-15 07:52:36.453+0000	heartrate	Person01
353952	140517	2	Room43	2018-06-15 08:10:07.383+0000	6000001	Cardiac Monitoring A01	2018-06-15 08:10:12.419+0000	DoctorPC	2018-06-15 08:10:07.383+0000	heartrate	Person01
138540	63996	12	Room43	2018-06-15 02:50:21.584+0000	6000002	Cardiac Monitoring A02	2018-06-15 02:51:16.035+0000	DoctorPC	2018-06-15 02:50:21.584+0000	heartrate	Person02
486142	184652	12	Room43	2018-06-15 11:17:00.879+0000	6000002	Cardiac Monitoring A02	2018-06-15 11:17:57.827+0000	DoctorPC	2018-06-15 11:17:00.879+0000	heartrate	Person02
107309	54371	2	Room43	2018-06-15 02:05:10.032+0000	6000001	Cardiac Monitoring A01	2018-06-15 02:05:13.535+0000	DoctorPC	2018-06-15 02:05:10.032+0000	pressure	Person01
425893	164534	12	Room43	2018-06-15 09:52:06.403+0000	6000002	Cardiac Monitoring A02	2018-06-15 09:53:02.940+0000	DoctorPC	2018-06-15 09:52:06.403+0000	heartrate	Person02
99354	50421	2	Room43	2018-06-15 01:48:26.442+0000	6000001	Cardiac Monitoring A01	2018-06-15 01:48:29.875+0000	DoctorPC	2018-06-15 01:48:26.442+0000	pressure	Person01
181153	23957	2	Home01	2018-06-15 03:50:23.490+0000	6000101	Portable Monitoring A01	2018-06-15 03:52:52.039+0000	DoctorPC	2018-06-15 03:50:23.490+0000	heartrate	PersonA
110362	54562	12	Room43	2018-06-15 02:10:54.750+0000	6000002	Cardiac Monitoring A02	2018-06-15 02:11:48.991+0000	DoctorPC	2018-06-15 02:10:54.750+0000	heartrate	Person02
158669	71700	2	Room43	2018-06-15 03:18:33.991+0000	6000001	Cardiac Monitoring A01	2018-06-15 03:18:37.807+0000	DoctorPC	2018-06-15 03:18:33.991+0000	pressure	Person01
220067	41093	2	Home01	2018-06-15 05:02:15.402+0000	6000101	Portable Monitoring A01	2018-06-15 05:04:44.259+0000	DoctorPC	2018-06-15 05:02:15.402+0000	pressure	PersonA
160318	72250	2	Room43	2018-06-15 03:20:53.857+0000	6000001	Cardiac Monitoring A01	2018-06-15 03:20:57.684+0000	DoctorPC	2018-06-15 03:20:53.857+0000	heartrate	Person01
595404	169455	2	Home01	2018-06-15 14:00:20.829+0000	6000101	Portable Monitoring A01	2018-06-15 14:02:51.953+0000	DoctorPC	2018-06-15 14:00:20.829+0000	pressure	PersonA
604754	226538	12	Room43	2018-06-15 14:13:32.176+0000	6000002	Cardiac Monitoring A02	2018-06-15 14:14:29.986+0000	DoctorPC	2018-06-15 14:13:32.176+0000	heartrate	Person02
185920	80786	2	Room43	2018-06-15 03:57:04.282+0000	6000001	Cardiac Monitoring A01	2018-06-15 03:57:08.256+0000	DoctorPC	2018-06-15 03:57:04.282+0000	heartrate	Person01
405393	157723	2	Room43	2018-06-15 09:23:04.880+0000	6000001	Cardiac Monitoring A01	2018-06-15 09:23:10.219+0000	DoctorPC	2018-06-15 09:23:04.880+0000	heartrate	Person01
386237	96863	2	Home01	2018-06-15 08:55:59.617+0000	6000101	Portable Monitoring A01	2018-06-15 08:58:29.462+0000	DoctorPC	2018-06-15 08:55:59.617+0000	pressure	PersonA
145501	12081	2	Home01	2018-06-15 03:00:06.430+0000	6000101	Portable Monitoring A01	2018-06-15 03:02:34.783+0000	DoctorPC	2018-06-15 03:00:06.430+0000	pressure	PersonA
189954	82123	2	Room43	2018-06-15 04:02:44.202+0000	6000001	Cardiac Monitoring A01	2018-06-15 04:02:48.204+0000	DoctorPC	2018-06-15 04:02:44.202+0000	o2sat	Person01
275880	114633	2	Room43	2018-06-15 06:20:27.605+0000	6000001	Cardiac Monitoring A01	2018-06-15 06:20:32.184+0000	DoctorPC	2018-06-15 06:20:27.605+0000	o2sat	Person01
51051	26351	2	Room43	2018-06-15 00:06:58.989+0000	6000001	Cardiac Monitoring A01	2018-06-15 00:07:01.995+0000	DoctorPC	2018-06-15 00:06:58.989+0000	heartrate	Person01
524543	145604	2	Home01	2018-06-15 12:20:23.415+0000	6000101	Portable Monitoring A01	2018-06-15 12:22:54.120+0000	DoctorPC	2018-06-15 12:20:23.415+0000	glucose	PersonA
604399	172479	2	Home01	2018-06-15 14:13:01.463+0000	6000101	Portable Monitoring A01	2018-06-15 14:15:32.642+0000	DoctorPC	2018-06-15 14:13:01.463+0000	pressure	PersonA
77594	39614	2	Room43	2018-06-15 01:02:40.555+0000	6000001	Cardiac Monitoring A01	2018-06-15 01:02:43.794+0000	DoctorPC	2018-06-15 01:02:40.555+0000	pressure	Person01

รูปที่ 19 ตัวอย่างข้อมูลธุรกรรมของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตทั้งหมด

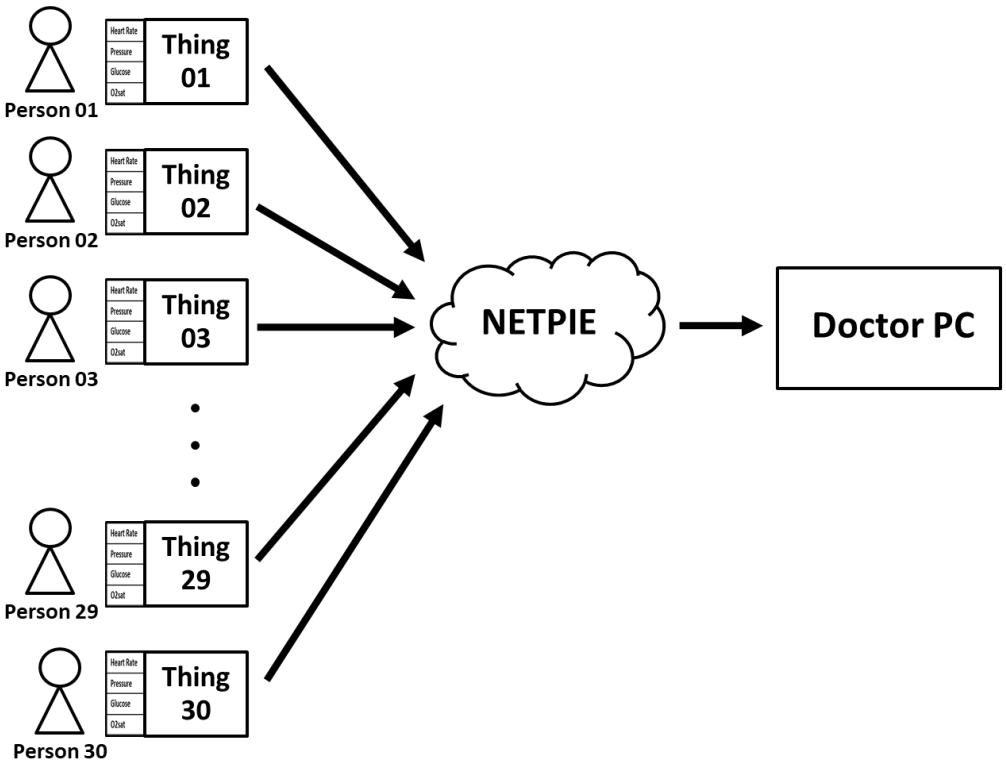
เมื่อได้อัตราการรับส่งข้อมูลและขนาดข้อมูลที่เหมาะสมจากการทดลองที่ 1 และ 2 ตามลำดับแล้ว ผลดังกล่าวจะถูกนำไปใช้ในการทดลองที่ 3 ซึ่งเป็นการจำลองการบันทึกข้อมูลธุรกรรม ซึ่งรูปแบบการทดลองจะติดตั้งอุปกรณ์ส่งข้อมูลทางการแพทย์ (Source) กับผู้ป่วยจำนวน 30 คน ผู้ป่วยแต่ละคนจะมีอุปกรณ์ทางการแพทย์จำนวน 4 ชิ้น และผู้ป่วยแต่ละคนจะมีสรรพสิ่งจำนวน 1 ชิ้น รวมทั้งสิ้น 30 สรรพสิ่ง เพื่อทำหน้าที่ส่งข้อมูล เป็นเวลา 24 ชั่วโมง ผ่านเน็ตพาย มายังคอมพิวเตอร์ของแพทย์ที่โรงพยาบาล จำนวน 1 เครื่อง โดยกำหนดให้รูปแบบตัวอย่างข้อมูลการสื่อสารในการทดลองนี้ จะส่งค่าผลการวัดข้อมูลสัญญาณชีพต่าง ๆ (Vital sign) ของอุปกรณ์ทั้ง 4 ชิ้น ดังแสดงในรูปที่ 20

ทั้งนี้ จำนวนผู้ป่วย 30 คน อ้างอิงจากขนาดจำนวนเตียงของโรงพยาบาลชุมชนขนาดเล็กที่สุด (F3) ซึ่งจะมีจำนวนเตียงน้อยกว่า 30 เตียง และจำนวนแพทย์ของโรงพยาบาลขนาดดังกล่าว จำนวน 1 คน [18] โดยมีรูปแบบการทดลองแบ่งออกเป็น 4 รูปแบบ ได้แก่

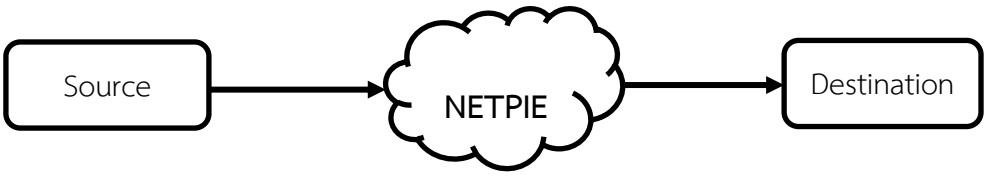
- วัดค่าผู้ป่วย 30 คนเป็นเวลา 24 ชั่วโมง โดยไม่บันทึกธุรกรรม ดังรูปที่ 21
- วัดค่าผู้ป่วย 30 คนเป็นเวลา 24 ชั่วโมง โดยบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น ดังรูปที่ 22
- วัดค่าผู้ป่วย 30 คนเป็นเวลา 24 ชั่วโมง โดยบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น ดังรูปที่ 23
- วัดค่าผู้ป่วย 30 คนเป็นเวลา 24 ชั่วโมง โดยบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด ดังรูปที่ 24

รูปแบบการออกแบบการทดลองโดยอ้างอิงจากรูปแบบการวัดค่าผู้ป่วย 30 คน เป็นเวลา 24 ชั่วโมง โดยบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด กำหนดให้ผู้ป่วย 1 คนได้รับการติดตามข้อมูลสุขภาพจากเซ็นเซอร์วัดค่าสุขภาพ 4 ชิ้น กระบวนการทดสอบประสิทธิภาพการตรวจจับธุรกรรมความผิดปกติที่เกิดขึ้นในการสื่อสารระหว่างสรรพสิ่งด้วยเน็ตพาย โดยกำหนดให้การทดลองทุกอุปกรณ์จะมีการบันทึกธุรกรรมของตนเองในการสื่อสาร เพื่อนำมาเปรียบเทียบพฤติกรรมการสื่อสารเพื่อหาการสูญหายของข้อมูลธุรกรรมระหว่างการสื่อสารของสรรพสิ่งด้วยเน็ตพาย

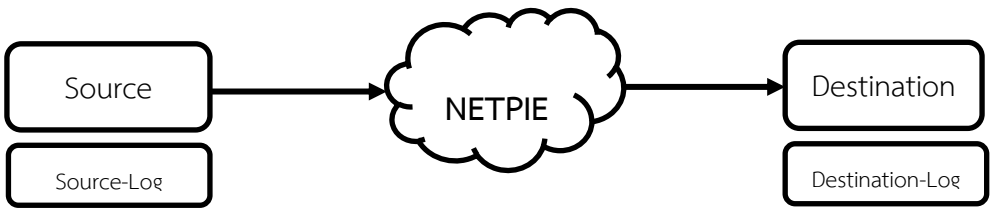
ในการออกแบบการทดลอง จะกำหนดให้เน็ตพายล็อก (NETPIE-log) เป็นเสมือนส่วนหนึ่งของเน็ตพาย (NETPIE) และจะบันทึกข้อมูลธุรกรรมทั้งหมดที่เน็ตพายได้รับหรือส่งออกนั้นคือจะไม่มีข้อมูลสูญหายระหว่างเน็ตพายและเน็ตพายล็อก แผนผังการสื่อสารระหว่างสรรพสิ่งแสดงดังรูปที่ 25 และ 26



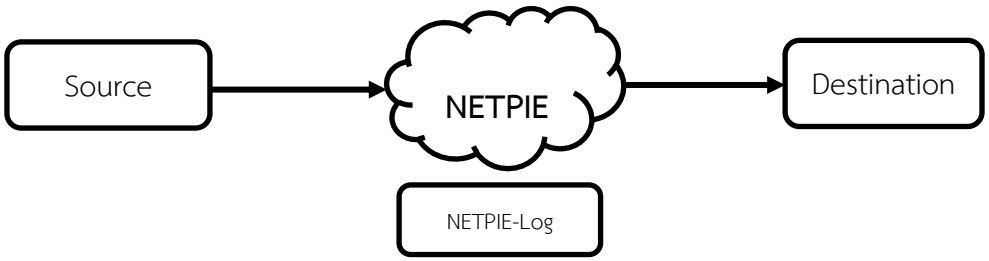
รูปที่ 20 รูปแบบภาพรวมการทดลองบันทึกธุรกรรมทางการแพทย์ในสภาพแวดล้อมของเน็ตพาย



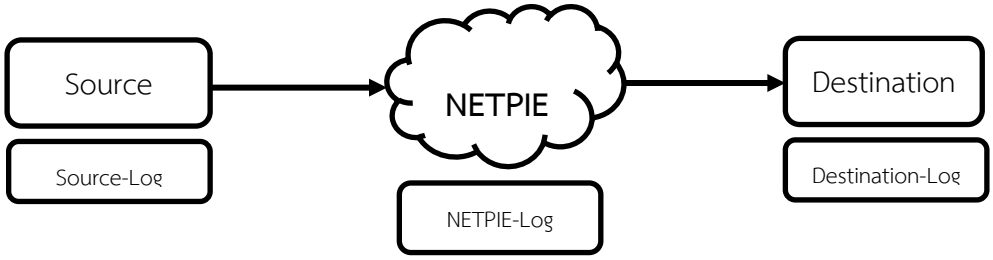
รูปที่ 21 รูปแบบการวัดค่าผู้ป่วยโดยไม่บันทึกธุรกรรม



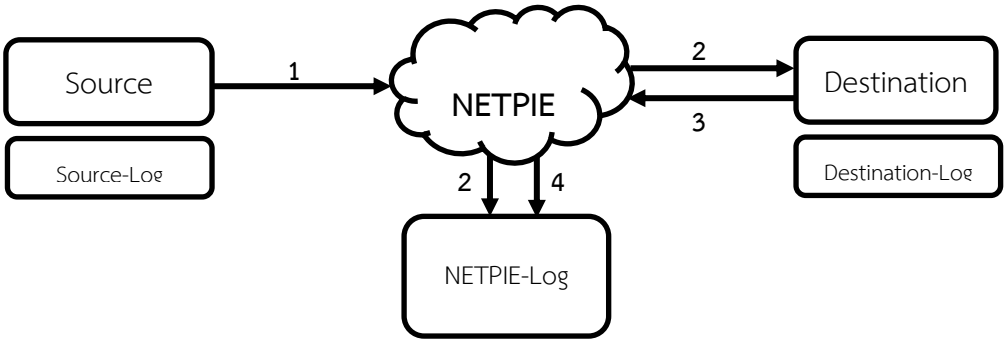
รูปที่ 22 รูปแบบการผู้ป่วยโดยบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น



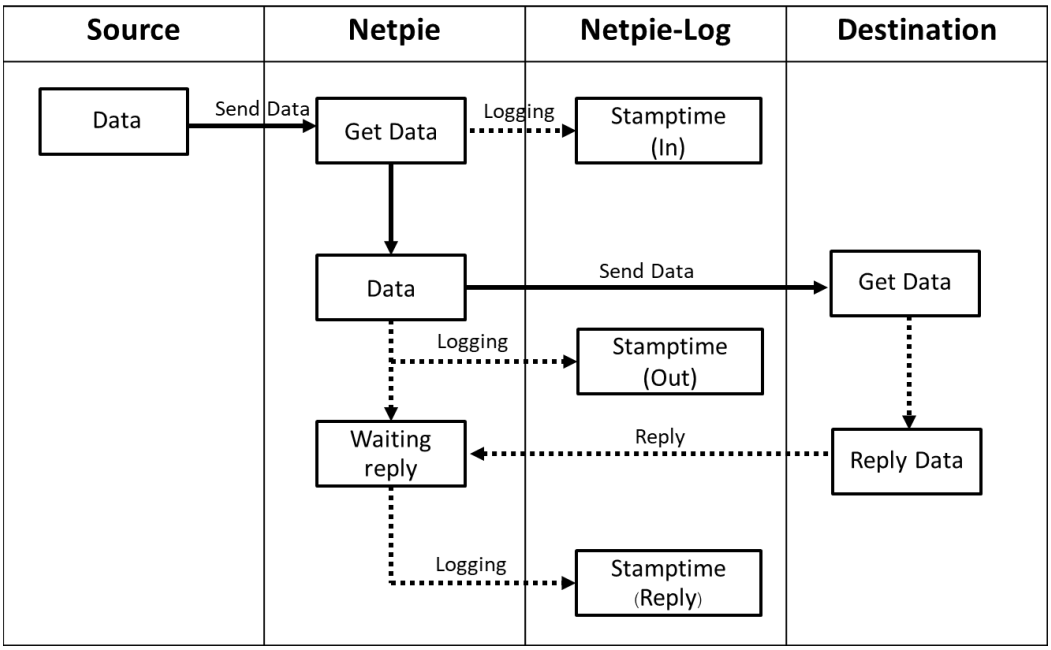
รูปที่ 23 รูปแบบการวัดค่าผู้ป่วยโดยบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น



รูปที่ 24 รูปแบบการวัดค่าผู้ป่วยโดยบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด



รูปที่ 25 รูปแบบการบันทึกธุรกรรมในระหว่างการสื่อสารของสรรพสิ่ง



รูปที่ 26 รูปแบบการบันทึกธุรกรรมในระหว่างการสื่อสารของสรรพสิ่ง

ลำดับขั้นตอนการบันทึกข้อมูลธุรกรรมในการสื่อสารจากการบันทึกเวลาเริ่มต้นจากสรรพสิ่งต้นทาง (Source) ส่งข้อมูลไปยังเน็ตพาย (NETPIE) และจัดเก็บในล็อกต้นทาง (Source-Log) เมื่อเน็ตพายได้รับข้อมูลจากสรรพสิ่งต้นทาง เน็ตพายจะทำการลงเวลาและบันทึกข้อมูลในเน็ตพายล็อก ในขณะเดียวกันก็จะส่งข้อมูลจากเน็ตพายไปยังสรรพสิ่งปลายทาง (Destination) ในเวลาเดียวกัน ซึ่งหากสรรพสิ่งปลายทางได้รับข้อมูลจะทำการบันทึกข้อมูลที่ได้รับไว้ที่ล็อกปลายทาง (Destination-Log) และตอบกลับมายังเน็ตพาย เมื่อเน็ตพายได้รับข้อมูลการตอบกลับจากสรรพสิ่งปลายทางแล้ว เน็ตพายบันทึกว่า สรรพสิ่งปลายทางได้รับข้อมูลแล้วลงในเน็ตพายล็อก เพื่อให้ผู้ดูแลระบบสามารถวิเคราะห์ข้อมูลการสื่อสารทั้งหมดได้จากเน็ตพายล็อก

จากการจำลองสุ่มข้อมูลทดแทนเซ็นเซอร์วัดค่าข้อมูลสุขภาพ โดยส่วนใหญ่ข้อมูลที่เซ็นเซอร์จะวัดเป็นข้อมูลลักษณะตัวเลข 3 หลักและมีทศนิยม 2 ตำแหน่ง ยกเว้นข้อมูลความดันที่มีรูปแบบข้อมูลเฉพาะในลักษณะจำนวนเต็ม 2 จำนวนขั้นด้วยเครื่องหมายทับ ซึ่งขนาดข้อมูลในการส่งแต่ละครั้งมีขนาดข้อมูลไม่เกิน 1 กิโลไบต์ ในการส่งข้อมูลจากสรรพสิ่งต้นทางตามลำดับการทำงานของอุปกรณ์แต่ละตัวจะทำงานดังตารางที่ 4 และ 5 ตัวอย่างข้อมูลของผู้ป่วยซึ่งใช้ในการทดลองที่ 3 แสดงไว้ในภาคผนวก ก

ตาราง 4 ตารางเวลาการเริ่มส่งข้อมูลของสรรพสิ่งทั้ง 30 อุปกรณ์เป็นเวลาอุปกรณ์ละ 24 ชั่วโมง

เวลาเริ่มทำงาน	เวลาสิ้นสุด	อุปกรณ์ที่ทำงาน
08/08/2018 – 20:00	09/08/2018 – 20:00	P.01, P.02
08/08/2018 – 21:00	09/08/2018 – 21:00	P.03, P.04
08/08/2018 – 22:00	09/08/2018 – 22:00	P.05, P.06
08/08/2018 – 23:00	09/08/2018 – 23:00	P.07, P.08
09/08/2018 – 00:00	10/08/2018 – 00:00	P.09, P.10
09/08/2018 – 01:00	10/08/2018 – 01:00	P.11, P.12
09/08/2018 – 02:00	10/08/2018 – 02:00	P.13, P.14
09/08/2018 – 03:00	10/08/2018 – 03:00	P.15, P.16
09/08/2018 – 04:00	10/08/2018 – 04:00	P.17, P.18
09/08/2018 – 05:00	10/08/2018 – 05:00	P.19, P.20
09/08/2018 – 06:00	10/08/2018 – 06:00	P.21, P.22
09/08/2018 – 07:00	10/08/2018 – 07:00	P.23, P.24
09/08/2018 – 08:00	10/08/2018 – 08:00	P.25, P.26
09/08/2018 – 09:00	10/08/2018 – 09:00	P.27, P.28
09/08/2018 – 10:00	10/08/2018 – 10:00	P.29, P.30

3.6 การวิเคราะห์ข้อมูล

จากการทดลองทั้ง 3 รูปแบบ ซึ่งได้แก่ การทดสอบเพื่อหาอัตราการรับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม การทดสอบเพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย และการทดสอบบันทึกธุรกรรมทางการแพทย์ในสภาพแวดล้อมของเน็ตพาย เพื่อหารูปแบบสภาพแวดล้อมสำหรับการบันทึกธุรกรรมระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตที่เหมาะสมกับรูปแบบข้อมูลทางการแพทย์ด้วยเน็ตพาย แต่เนื่องจากข้อมูลทางการแพทย์มีลักษณะการรับส่งข้อมูลทุก ๆ 1 วินาที จึงต้องวิเคราะห์หารูปแบบความถี่ในการสื่อสาร จำนวนสรรพสิ่ง และขนาดข้อมูลที่เน็ตพายสามารถรองรับการสื่อสารที่มีการเปลี่ยนแปลงของข้อมูลทุก ๆ 1 วินาทีได้ดังนี้

3.6.1 การวิเคราะห์อัตรารับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม

โดยวิเคราะห์จากการทดลองส่งข้อมูลขนาด 56 ไบต์ ซึ่งเป็นข้อมูลตัวเลขจำนวนเต็มจากสรรพสิ่งผู้ป่วยไปยังสรรพสิ่งของแพทย์ในจำนวนอัตราส่วนระหว่างสรรพสิ่ง 1:1, 2:1, 4:1, 8:1

และ 16:1 ส่งข้อมูลทุก ๆ 1 วินาที ด้วยชุดข้อมูลทั้ง 1,000 ชุดข้อมูลเท่ากัน จากนั้นจึงเพิ่มความเร็วในการส่งข้อมูลทุก ๆ 500 มิลลิวินาที 250 มิลลิวินาที และ 125 มิลลิวินาทีในสภาพแวดล้อมการทดลองเดียวกัน และวิเคราะห์หาข้อมูลการสื่อสารว่าเริ่มเกิดการสูญหายในความถี่การส่งข้อมูลที่เท่าไหร่ เพื่อใช้ความถี่การสื่อสารสูงสุดสำหรับข้อมูลทางการแพทย์ด้วยเน็ตพาย สำหรับการทดลองหาขนาดข้อมูลในการสื่อสาร

3.6.2 การวิเคราะห์ขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย

เมื่อวิเคราะห์ได้ผลลัพธ์การวิเคราะห์หาความถี่การสื่อสารสูงสุดสำหรับข้อมูลทางการแพทย์ด้วยเน็ตพายจากการวิเคราะห์ทดลองในข้อที่ 3.6.1 สามารถใช้ความถี่สูงสุดในการสื่อสารนี้สำหรับการทดลองหาขนาดข้อมูลสูงสุดที่สามารถส่งจากสรรพสิ่งของผู้ป่วยไปยังสรรพสิ่งของแพทย์ผ่านเน็ตพายได้ โดยเริ่มจากข้อมูลขนาด 1 ไบต์ แล้วเพิ่มขนาดครั้งละสองเท่าเป็นขนาด 2, 4, 8, 16, 24, 36, 64, 128, 256, 512, 1024, 2048, 4096, 8192 และ 16392 ไบต์ เพื่อหาขนาดข้อมูลสูงสุดสำหรับการสื่อสารที่ทำให้เกิดความล่าช้าเกิน 1 วินาที จากการส่งข้อมูลทุก ๆ 250 มิลลิวินาทีผ่านเน็ตพาย

3.6.3 การวิเคราะห์ผลการบันทึกธุรกรรมทางการแพทย์ผ่านเน็ตพาย

เนื่องจากการหาสภาพแวดล้อมการสื่อสารที่เหมาะสม ได้แก่ ระยะเวลาระหว่างการส่งแต่ละครั้งที่สูงสุดที่เป็นไปได้ในการสื่อสาร และขนาดข้อมูลสูงสุดสำหรับข้อมูลทางการแพทย์ด้วยเน็ตพาย จากการวิเคราะห์การทดลองในข้อที่ 3.6.1 และ 3.6.2 เพื่อใช้รูปแบบสภาพแวดล้อมที่เหมาะสมกับการสื่อสารหารูปแบบการบันทึกธุรกรรมที่เหมาะสมในการสื่อสารระหว่างสรรพสิ่งด้วยเน็ตพายสำหรับข้อมูลด้านการแพทย์ โดยแบ่งออกเป็น 4 รูปแบบการทดลอง ได้แก่ การส่งแบบไม่บันทึกธุรกรรม การส่งแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น การส่งแบบบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น และการส่งแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด โดยการวิเคราะห์จะประกอบด้วยการส่งข้อมูลแบบปกติ และการส่งข้อมูลที่มีการกำหนดข้อผิดพลาดในการส่งข้อมูล เพื่อทำการวิเคราะห์หาประสิทธิภาพในการตรวจจับความผิดปกติของการสื่อสาร และการหาประสิทธิภาพการทำงานในสภาพแวดล้อมที่เสมือนจริง

ตาราง 5 ตารางแผนการเริ่มส่งข้อมูลของสรรพสิ่งทั้ง 30 อุปกรณ์เป็นเวลาอุปกรณ์ละ 24 ชั่วโมง

	08/08/2018				09/08/2018																								10/08/2018									
	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10
P.01																																							
P.02																																							
P.03																																							
P.04																																							
P.05																																							
P.06																																							
P.07																																							
P.08																																							
P.09																																							
P.10																																							
P.11																																							
P.12																																							
P.13																																							
P.14																																							
P.15																																							
P.16																																							
P.17																																							
P.18																																							
P.19																																							
P.20																																							
P.21																																							
P.22																																							
P.23																																							
P.24																																							
P.25																																							
P.26																																							
P.27																																							
P.28																																							
P.29																																							
P.30																																							

บทที่ 4
ผลการทดลองและวิเคราะห์ผล

การทดสอบเพื่อหาประสิทธิภาพของการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตแบ่งเป็น 3 การทดลอง ได้แก่ การทดลองเพื่อหาอัตราการรับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม การทดลองเพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย และการทดลองบันทึกธุรกรรมทางการแพทย์ในสภาพแวดล้อมจริงในพื้นที่อำเภอหาดใหญ่ จังหวัดสงขลา

4.1 การทดสอบเพื่อหาอัตราการรับส่งข้อมูลด้วยเน็ตพายที่เหมาะสม

การทดลองนี้มีวัตถุประสงค์เพื่อหาอัตราการรับส่งข้อมูลระหว่างสรรพสิ่งต้นทางผ่านเครือข่ายอินเตอร์เน็ตไปยังเน็ตพายและกลับมายังสรรพสิ่งปลายทาง ภายใต้สภาวะแวดล้อมในพื้นที่อำเภอหาดใหญ่ จังหวัดสงขลา โดยจำนวนสรรพสิ่งต้นทางมี 5 แบบ ได้แก่ 1, 2, 4, 8 และ 16 ชิ้น ส่วนขนาดข้อมูลคงที่ขนาด 56 ไบต์ แต่ละสรรพสิ่งส่งข้อมูลจำนวน 1000 ชุด และสรรพสิ่งปลายทางมีจำนวน 1 ชิ้น ทั้งนี้ ระยะห่างระหว่างการส่งข้อมูลจะเปลี่ยนแปลงโดยมีการส่งข้อมูลทุก 1 วินาที 500 มิลลิวินาที 250 มิลลิวินาที และ 125 มิลลิวินาที ผลการทดลองแสดงในตารางที่ 6 – 9 ตามลำดับ

จากผลการทดลองแสดงในตารางที่ 6 พบว่าข้อมูลสามารถส่งจากสรรพสิ่งต้นทางมายังสรรพสิ่งปลายทางโดยไม่สูญหายแม้กรณีเดียว และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 66 มิลลิวินาที โดยระยะเวลาสูงสุดที่ 375 มิลลิวินาที และระยะเวลาต่ำสุดที่ 62 มิลลิวินาที

จากผลการทดลองแสดงในตารางที่ 7 และ 8 พบว่าข้อมูลสามารถส่งจากสรรพสิ่งต้นทางมายังสรรพสิ่งปลายทางทุก 500 มิลลิวินาที และ 250 มิลลิวินาที ไม่พบการสูญหายแม้กรณีเดียว และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 76 มิลลิวินาที โดยระยะเวลาสูงสุดที่ 391 มิลลิวินาที ในกรณีส่งทุก 500 มิลลิวินาที และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 74 มิลลิวินาที โดยระยะเวลาสูงสุดที่ 297 มิลลิวินาที ในกรณีส่งทุก 250 มิลลิวินาที

จากผลการทดลองแสดงในตารางที่ 9 ซึ่งส่งข้อมูลทุก 125 มิลลิวินาที พบว่าข้อมูลเกิดการสูญหายเป็นจำนวนมาก อีกทั้งการรับส่งข้อมูลไปยังปลายทางยังเกิดความล่าช้าเป็นระยะเวลาเฉลี่ย 593 มิลลิวินาที ซึ่งเป็นระยะเวลาจากต้นทางถึงปลายทางสูงสุดที่ 5 วินาที และต่ำสุดที่ 47 มิลลิวินาที

ตาราง 6 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 1 วินาที

Frequency 1 Second	Device 16:1	Device 8:1	Device 4:1	Device 2:1	Device 1:1
Average	0.066 s	0.075 s	0.066 s	0.065 s	0.066 s
Max	0.375 s	0.265 s	0.281 s	0.250 s	0.281 s
Min	0.062 s	0.062 s	0.062 s	0.062 s	0.062 s
Number of data	16000	8000	4000	2000	1000
Delay Packet	0	0	0	0	0
Loss Packet	0	0	0	0	0
% Delay Packet	0.00%	0.00%	0.00%	0.00%	0.00%
% Loss Packet	0.00%	0.00%	0.00%	0.00%	0.00%

ตาราง 7 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 500 มิลลิวินาที

Frequency 500 millisecond	Device 16:1	Device 8:1	Device 4:1	Device 2:1	Device 1:1
Average	0.076 s	0.071 s	0.069 s	0.066 s	0.065 s
Max	0.391 s	0.282 s	0.281 s	0.266 s	0.266 s
Min	0.062 s	0.061 s	0.055 s	0.054 s	0.062 s
Number of data	16000	8000	4000	2000	1000
Delay Packet	0	0	0	0	0
Loss Packet	0	0	0	0	0
% Delay Packet	0.00%	0.00%	0.00%	0.00%	0.00%
% Loss Packet	0.00%	0.00%	0.00%	0.00%	0.00%

ตาราง 8 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 250 มิลลิวินาที

Frequency 250 millisecond	Device 16:1	Device 8:1	Device 4:1	Device 2:1	Device 1:1
Average	0.074 s	0.073 s	0.070 s	0.067 s	0.065 s
Max	0.282 s	0.297 s	0.250 s	0.250 s	0.235 s
Min	0.062 s	0.062 s	0.062 s	0.062 s	0.062 s
Number of data	16000	8000	4000	2000	1000
Delay Packet	0	0	0	0	0
Loss Packet	0	0	0	0	0
% Delay Packet	0.00%	0.00%	0.00%	0.00%	0.00%
% Loss Packet	0.00%	0.00%	0.00%	0.00%	0.00%

ตาราง 9 ผลการทดสอบการรับส่งข้อมูลด้วยการส่งข้อมูลทุก 125 มิลลิวินาที

Frequency 125 millisecond	Device 16:1	Device 8:1	Device 4:1	Device 2:1	Device 1:1
Average	0.593 s	0.326 s	0.232 s	0.175 s	0.183 s
Max	4.930 s	2.481 s	1.870 s	1.448 s	1.081 s
Min	0.052 s	0.047 s	0.052 s	0.053 s	0.062 s
Number of data	8484	5149	2804	1401	742
Delay Packet	1892	526	140	23	1
Loss Packet	7516	2851	1192	599	258
% Delay Packet	22.30%	10.22%	4.99%	1.64%	0.13%
% Loss Packet	88.59%	55.37%	42.51%	42.76%	34.77%

จากผลการทดลองข้างต้น ระยะห่างระหว่างการส่งข้อมูลที่ไม่พบการสูญหายของข้อมูลคือ 250 มิลลิวินาที ตารางที่ 10 สรุปผลการทดลองของการส่งข้อมูลทุก 250 มิลลิวินาทีเพื่อใช้ในการอ้างอิง เพื่อการวิเคราะห์เชิงลึกถึงการสูญหายของข้อมูลในช่วงเวลาต่าง จึงทำการทดลองเพิ่มโดยการส่งข้อมูลทุก 250 มิลลิวินาที จากสรรพสิ่งต้นทางจำนวน 16 ชิ้นมายังสรรพสิ่งปลายทางจำนวน 1 ชิ้น โดยใช้ข้อมูลขนาด 56 ไบต์และส่งเป็นระยะเวลา 24 ชั่วโมง ผลการทดลองแสดงในตารางที่ 11 เพื่อค้นหาจำนวนข้อมูลที่เกิดความล่าช้าในช่วงเวลาต่างๆ ของวันทั้ง 24 ชั่วโมง โดยการหาผลต่างของเวลาการส่งจากสรรพสิ่งต้นทางกับเวลาการรับจากสรรพสิ่งปลายทางและหาชุดข้อมูลที่ส่วนต่างของเวลามากกว่า1 วินาที เพื่อค้นหาจำนวนชุดข้อมูลที่เกิดความล่าช้าในการสื่อสารในแต่ละชั่วโมง ซึ่งในแต่ละชั่วโมงจะมีจำนวนข้อมูลทั้งสิ้น 230,400 ข้อมูล เนื่องจากแต่ละสรรพสิ่งส่งข้อมูล 4 ข้อมูลทุก 1 วินาที เป็นจำนวน 1 ชั่วโมง และมีทั้งสิ้น 16 สรรพสิ่ง

จากผลการทดสอบแสดงในตารางที่ 11 พบว่าข้อมูลไม่มีการสูญหายแต่ข้อมูลมีการล่าช้าเกินกว่า 1 วินาที ต่ำกว่าร้อยละ 0.08 โดยพื้นที่แถบสีแดงในตารางคือช่วงเวลาที่มีจำนวนข้อมูลล่าช้ามากกว่า 10 ชุดข้อมูล โดยปริมาณข้อมูลล่าช้ากว่า 1 วินาทีในช่วง 1 ชั่วโมง จำนวนสูงสุด คือ 176 ข้อมูล คิดเป็นร้อยละ 0.076 และปริมาณข้อมูลล่าช้ากว่า 1 วินาทีทั้ง 24 ชั่วโมงมีจำนวนทั้งสิ้น 626 ข้อมูล คิดเป็นร้อยละ 0.27 จากการทดลองสรุปได้ว่าความสำเร็จในการส่งข้อมูลจะแปรผันตามช่วงเวลาของอินเตอร์เน็ต เนื่องจากการทดลองในช่วงเวลาและความเร็วที่แตกต่างกันของอินเตอร์เน็ตส่งผลให้เกิดการหน่วงในการรับส่งข้อมูลเล็กน้อย ดังนั้น การทดสอบระบบควรดำเนินการให้ครบทั้ง 24 ชั่วโมง เพื่อให้ได้ผลการทดสอบที่ครอบคลุมสภาวะการใช้งานระบบเครือข่าย

ตาราง 10 ตารางผลการทดลองจำนวนอุปกรณ์การส่งข้อมูลทุก ๆ 250 มิลลิวินาที

Sources	Time (ms)		
	average	*maximum*	*minimum*
16	66	375	62
8	75	265	62
4	66	281	62
2	65	250	62
1	66	234	62

ตาราง 11 ตารางแสดงผลภาพรวมของสรรพสิ่งที่ 16 ชิ้น ในการส่งข้อมูลในแต่ละชั่วโมง

เวลา	จำนวนข้อมูลที่เกิดความล่าช้า	คิดเป็นร้อยละ
01:00	0	0.00000
02:00	2	0.00087
03:00	5	0.00217
04:00	0	0.00000
05:00	0	0.00000
06:00	1	0.00043
07:00	3	0.00130
08:00	15	0.00651
09:00	11	0.00477
10:00	176	0.07639
11:00	42	0.01823
12:00	11	0.00477

เวลา	จำนวนข้อมูลที่เกิดความล่าช้า	คิดเป็นร้อยละ
13:00	60	0.02604
14:00	176	0.07639
15:00	42	0.01823
16:00	11	0.00477
17:00	37	0.01606
18:00	9	0.00391
19:00	11	0.00477
20:00	3	0.00130
21:00	6	0.00260
22:00	0	0.00000
23:00	5	0.00217
24:00	0	0.00000

4.2 การทดสอบเพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารด้วยเน็ตพาย

การทดลองนี้มีวัตถุประสงค์เพื่อหาขนาดข้อมูลที่เหมาะสมสำหรับการสื่อสารข้อมูลระหว่างสรรพสิ่งต้นทางผ่านเครือข่ายอินเตอร์เน็ตไปยังเน็ตพายและกลับมายังสรรพสิ่งปลายทางภายใต้สภาวะแวดล้อมในพื้นที่อำเภอหาดใหญ่ จังหวัดสงขลา โดยจำนวนสรรพสิ่งต้นทางมี 16 ชิ้น แต่ละสรรพสิ่งส่งข้อมูลจำนวน 1000 ชุด สรรพสิ่งปลายทางมีจำนวน 1 ชิ้น ทั้งนี้ ระยะห่างระหว่างการส่งข้อมูลเป็น 250 มิลลิวินาที และขนาดของข้อมูลโดยเริ่มจาก 1 Bytes แล้วจึงเพิ่มขนาดครั้งละสองเท่าเป็น 2, 4, 8, 16, 24, 36, 64, 128, 256, 512, 1024, 2048, 4096, 8192 และ 16392 ไบต์ เพื่อหาขนาดข้อมูลที่ทำให้เกิดความล่าช้าเกิน 1 วินาที ผลการทดลองแสดงในตารางที่ 12

ตาราง 12 ตารางผลการเปรียบเทียบเวลากับขนาดข้อมูล

ขนาดข้อมูล	ระยะเวลาการรับส่งเฉลี่ย
1 Bytes	97 ms
2 Bytes	76 ms
4 Bytes	73 ms
8 Bytes	72 ms
16 Bytes	72 ms
32 Bytes	70 ms
64 Bytes	71 ms
128 Bytes	72 ms
256 Bytes	74 ms
512 Bytes	77 ms
1024 Bytes	89 ms
2048 Bytes	99 ms
4096 Bytes	191 ms
8196 Bytes	1.25 s
16392 Bytes	4.75 s

จากผลการทดลองแสดงในตารางที่ 12 พบว่าข้อมูลขนาด 4096 ไบต์ (4 กิโลไบต์) หรือต่ำกว่า สามารถถูกส่งจากสรรพสิ่งต้นทางผ่านเครือข่ายอินเตอร์เน็ตและเน็ตพาย กลับมายังสรรพสิ่งปลายทางได้โดยไม่มีการสูญหายและใช้ระยะเวลาต่ำกว่า 1 วินาที แต่ขนาดข้อมูลตั้งแต่ 8196 ไบต์ (8 กิโลไบต์) ขึ้นไป จะทำให้การส่งข้อมูลไปยังปลายทางเกิดความล่าช้าเกิน 1 วินาที

จากผลการทดลองที่ 1 และ 2 สามารถสรุปได้ว่าการรับส่งข้อมูลของสรรพสิ่งผ่านเน็ตพายในสภาพแวดล้อมจำลองจากเครื่องมือวัดทางการแพทย์พบว่าข้อจำกัดของการรับส่งข้อมูลภายใต้สภาพแวดล้อมนี้จะสามารถส่งข้อมูลสูงสุดทุก 250 มิลลิวินาที โดยส่งจากสรรพสิ่งต้นทางจำนวน 16 ชิ้นมายังสรรพสิ่งปลายทางจำนวน 1 ชิ้น โดยใช้ข้อมูลขนาดไม่เกิน 4096 ไบต์ หรือ 4 กิโลไบต์ ซึ่งเป็นสภาพแวดล้อมสูงสุดที่สามารถส่งข้อมูลได้สำเร็จและไม่เกิดความล่าช้าในการส่งไปยังปลายทาง จากรูปแบบเครื่องมือวัดทางการแพทย์พื้นฐานมีการส่งข้อมูลส่วนใหญ่ทุก 1 วินาที และมีขนาดข้อมูลไม่เกิน 1 กิโลไบต์ [28] ยกเว้นเครื่องมือที่มีการตอบสนองด้วยความถี่สูง ได้แก่ การวัดค่าคลื่นหัวใจหรือคลื่นสมอง เป็นต้น ซึ่งเครื่องมือวัดที่สำรวจจากหอผู้ป่วยหนัก (ICU) พบอุปกรณ์ตรวจวัดประมาณไม่เกิน 10 อุปกรณ์ ดังนั้นการประยุกต์ใช้การสื่อสารระหว่างสรรพสิ่งผ่าน

อินเตอร์เน็ตทางการแพทย์เหมาะสำหรับการวัดค่าข้อมูลสุขภาพที่มีความถี่ต่ำในเบื้องต้น ได้แก่ ระดับน้ำตาล ความดัน ชีพจร อุณหภูมิร่างกาย เป็นต้น

4.3 การทดสอบบันทึกธุรกรรมทางการแพทย์ในสภาพแวดล้อมของเน็ตพาย

การทดลองระบบโดยการจำลองสถานการณ์ของผู้ป่วยจำนวน 30 คน แต่ละคนมีสรรพสิ่ง 1 ชิ้น ซึ่งเชื่อมต่อกับอุปกรณ์เซ็นเซอร์วัดค่าสุขภาพผู้ป่วยจำนวน 4 ชนิด โดยสรรพสิ่งของผู้ป่วยทั้ง 30 คน จะส่งข้อมูลค่าที่วัดได้ผ่านเครือข่ายอินเตอร์เน็ตและเน็ตพายไปยังคอมพิวเตอร์ของแพทย์ที่โรงพยาบาล โดยขนาดของข้อมูลเฉลี่ยที่ 2 กิโลไบต์ เป็นระยะเวลา 24 ชั่วโมง โดยการส่งข้อมูลทุก 250 มิลลิวินาที ตามรูปแบบชนิดข้อมูลสุขภาพที่วัดค่า (ภาคผนวก ก แสดงตัวอย่างข้อมูลที่ส่งออกโดยสรรพสิ่ง) แต่ละสรรพสิ่งส่งข้อมูลทั้งสิ้น 345,600 ชุดเท่ากัน แต่ช่วงเวลาในการส่งข้อมูลแตกต่างกันดังแสดงไว้ในตารางที่ 5 การทดลองแบ่งเป็น 4 รูปแบบ ได้แก่ การส่งแบบไม่บันทึกธุรกรรม การส่งแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น การส่งแบบบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น และการส่งแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด ตารางที่ 13-16 แสดงผลการทดลองทั้ง 4 รูปแบบ

จากผลการทดลองการส่งแบบไม่บันทึกธุรกรรมแสดงในตารางที่ 13 พบว่าข้อมูลสามารถส่งจากสรรพสิ่งต้นทางมายังสรรพสิ่งปลายทางโดยไม่มีการสูญหาย แต่พบการล่าช้าจำนวน 1,468 ชุดข้อมูลจาก 10,368,000 ชุดข้อมูล คิดเป็นร้อยละ 0.014 และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 0.2713 วินาที โดยระยะเวลาสูงสุดที่ 3.539 วินาที

จากผลการทดลองการบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้นแสดงในตารางที่ 14 พบว่าข้อมูลสามารถส่งจากสรรพสิ่งต้นทางมายังสรรพสิ่งปลายทางโดยไม่มีการสูญหาย แต่พบการล่าช้าจำนวน 2,633 ชุดข้อมูลจาก 10,368,000 ชุดข้อมูล คิดเป็นร้อยละ 0.025 และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 0.4854 วินาที โดยระยะเวลาสูงสุดที่ 8.074 วินาที

จากผลการทดลองการส่งแบบบันทึกธุรกรรมเฉพาะที่เน็ตพายแสดงในตารางที่ 15 พบว่าข้อมูลสามารถส่งจากสรรพสิ่งต้นทางมายังสรรพสิ่งปลายทางโดยไม่มีการสูญหาย แต่พบการล่าช้าจำนวน 4,920 ชุดข้อมูลจาก 10,368,000 ชุดข้อมูล คิดเป็นร้อยละ 0.047 และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 0.4934 วินาที โดยระยะเวลาสูงสุดที่ 9.641 วินาที

ตาราง 13 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบไม่บันทึกธุรกรรม

measurement	Things (second)									
	1	2	3	4	5	6	7	8	9	10
average	0.093	0.096	0.11	0.96	0.184	0.121	0.126	0.229	0.13	0.433
max	1.35	1.01	0.648	0.742	1.472	1.041	1.712	1.127	0.698	1.683
min	0.012	0.017	0.042	0.057	0.016	0.027	0.008	0.026	0.007	0.034
Delay	2	1	0	0	59	3	10	8	0	4
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0006	0.0003	0.0000	0.0000	0.0171	0.0009	0.0029	0.0023	0.0000	0.0012
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	11	12	13	14	15	16	17	18	19	20
average	0.138	0.138	0.372	0.119	0.104	0.104	0.41	0.232	0.792	0.42
max	1.363	0.882	2.113	1.371	1.38	0.837	1.211	3.539	2.05	0.772
min	0.088	0.042	0.053	0.019	0.006	0.005	0.009	0.056	0.096	0.003
Delay	19	0	104	19	17	0	17	914	16	0
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0055	0.0000	0.0301	0.0055	0.0049	0.0000	0.0049	0.2645	0.0046	0.0000
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	21	22	23	24	25	26	27	28	29	30	**Total**
average	0.138	0.138	0.372	0.119	0.104	0.104	0.41	0.232	0.792	0.42	**0.2713**
max	0.867	1.363	0.882	2.113	1.371	1.38	0.837	1.211	3.539	0.698	**3.539**
min	0.007	0.088	0.002	0.053	0.019	0.006	0.005	0.009	0.056	0.096	**0.002**
Delay	0	211	0	14	25	6	0	12	7	0	**1468**
Lost	0	0	0	0	0	0	0	0	0	0	**0**
%delay	0.0000	0.0611	0.0000	0.0041	0.0072	0.0017	0.0000	0.0035	0.0020	0.0000	**0.0142**
%loss	0	0	0	0	0	0	0	0	0	0	**0**

ตาราง 14 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่ง

measurement	Things (second)									
	1	2	3	4	5	6	7	8	9	10
average	0.406	0.403	0.389	0.403	0.317	0.379	0.373	0.37	0.169	0.37
max	1.592	1.926	0.849	0.988	1.002	1.835	2.136	1.852	0.809	2.014
min	0.047	0.069	0.152	0.103	0.052	0.036	0.037	0.038	0.011	0.057
Delay	78	22	0	0	1	36	226	35	0	210
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0226	0.0064	0.0000	0.0000	0.0003	0.0104	0.0654	0.0101	0.0000	0.0608
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	11	12	13	14	15	16	17	18	19	20
average	0.361	0.361	0.119	0.38	0.396	0.395	0.898	0.267	0.821	0.794
max	1.782	0.971	1.441	1.488	1.929	0.768	1.308	8.074	1.465	0.914
min	0.096	0.036	0.07	0.039	0.021	0.009	0.009	0.059	0.026	0.026
Delay	198	0	8	11	190	0	196	726	198	0
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0573	0.0000	0.0023	0.0032	0.0550	0.0000	0.0567	0.2101	0.0573	0.0000
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	21	22	23	24	25	26	27	28	29	30	**Total**
average	0.361	0.761	0.519	0.38	0.696	0.695	0.898	0.267	0.821	0.794	**0.4854**
max	0.849	2.014	1.782	0.971	1.441	1.488	1.929	0.768	1.308	2.014	**8.074**
min	0.009	0.057	0.096	0.006	0.07	0.039	0.021	0.009	0.009	0.059	**0.006**
Delay	0	112	83	0	53	74	66	0	17	93	**2633**
Lost	0	0	0	0	0	0	0	0	0	0	**0**
%delay	0.0000	0.0324	0.0240	0.0000	0.0153	0.0214	0.0191	0.0000	0.0049	0.0269	**0.0254**
%loss	0	0	0	0	0	0	0	0	0	0	**0**

ตาราง 15 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบบันทึกธุรกรรมเฉพาะเน็ตพาย

measurement	Things (second)									
	1	2	3	4	5	6	7	8	9	10
average	0.505	0.512	0.505	0.495	0.513	0.501	0.488	0.492	0.501	0.514
max	5.656	3.505	3.3	3.547	7.156	3.565	3.338	9.127	2.404	3.796
min	0.016	0.032	0.036	0.033	0.026	0.028	0.026	0.054	0.031	0.02
Delay	59	54	219	207	223	77	218	199	82	196
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0171	0.0156	0.0634	0.0599	0.0645	0.0223	0.0631	0.0576	0.0237	0.0567
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	11	12	13	14	15	16	17	18	19	20
average	0.482	0.506	0.486	0.522	0.505	0.499	0.489	0.443	0.487	0.477
max	3.78	3.73	3.635	3.746	3.818	3.812	3.918	3.755	5.063	2.891
min	0.019	0.037	0.022	0.021	0.027	0.027	0.033	0.049	0.024	0.044
Delay	194	212	184	190	174	174	176	174	27	160
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0561	0.0613	0.0532	0.0550	0.0503	0.0503	0.0509	0.0503	0.0078	0.0463
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	21	22	23	24	25	26	27	28	29	30	**Total**
average	0.461	0.482	0.506	0.486	0.522	0.505	0.499	0.489	0.443	0.487	**0.4934**
max	4.593	9.641	8.064	3.068	3.503	4.624	0.381	3.918	3.752	5.066	**9.641**
min	0.02	0.019	0.037	0.022	0.021	0.027	0.027	0.033	0.049	0.024	**0.016**
Delay	162	59	196	194	212	184	190	174	174	176	**4920**
Lost	0	0	0	0	0	0	0	0	0	0	**0**
%delay	0.0469	0.0171	0.0567	0.0561	0.0613	0.0532	0.0550	0.0503	0.0503	0.0509	**0.0475**
%loss	0	0	0	0	0	0	0	0	0	0	**0**

ตาราง 16 ตารางแสดงผลการเวลาการสื่อสารในการทดลองแบบบันทึกธุรกรรมทุกส่วน

measurement	Things (second)									
	1	2	3	4	5	6	7	8	9	10
average	0.963	1.037	1.01	1.017	0.992	1.016	0.979	1.048	0.975	1.031
max	4.528	3.641	1.195	5.097	7.661	2.389	6.701	3.995	2.986	3.964
min	0.023	0.003	0.011	0.001	0.014	0.003	0.004	0.005	0.001	0.011
Delay	108	455	419	444	173	432	379	152	381	410
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.0313	0.1317	0.1212	0.1285	0.0501	0.1250	0.1097	0.0440	0.1102	0.1186
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	11	12	13	14	15	16	17	18	19	20
average	0.995	0.951	1.022	0.995	1.018	0.996	0.974	0.994	1.051	1.037
max	5.086	6.922	5.154	8.795	4.864	4.778	1.002	7.506	6.374	1.451
min	0.008	0.001	0.003	0.001	0.007	0.005	0.002	0.049	0.005	0.001
Delay	401	374	364	355	346	360	332	49	298	304
Lost	0	0	0	0	0	0	0	0	0	0
%delay	0.1160	0.1082	0.1053	0.1027	0.1001	0.1042	0.0961	0.0142	0.0862	0.0880
%loss	0	0	0	0	0	0	0	0	0	0
measurement	Things (second)									
	21	22	23	24	25	26	27	28	29	30	**Total**
average	0.963	0.995	0.951	1.022	0.995	1.018	0.996	0.974	0.994	1.051	**1.002**
max	5.086	6.922	5.154	8.795	4.864	4.778	2.002	7.506	6.374	1.451	**8.795**
min	0.002	0.008	0.001	0.003	0.001	0.007	0.005	0.002	0.049	0.001	**0.001**
Delay	110	401	374	364	355	346	360	332	49	298	**9525**
Lost	0	0	0	0	0	0	0	0	0	0	**0**
%delay	0.0318	0.1160	0.1082	0.1053	0.1027	0.1001	0.1042	0.0961	0.0142	0.0862	**0.0919**
%loss	0	0	0	0	0	0	0	0	0	0	**0**

จากผลการทดลองการส่งแบบบันทึกธุรกรรมทุกที่แสดงในตารางที่ 16 พบว่าข้อมูลสามารถส่งจากสรรพสิ่งต้นทางมายังสรรพสิ่งปลายทางโดยไม่มีการสูญหาย แต่พบการล่าช้าจำนวน 9,525 ชุดข้อมูลจาก 10,368,000 ชุดข้อมูล คิดเป็นร้อยละ 0.091 และระยะเวลาการส่งข้อมูลถึงปลายทางเฉลี่ย 1.002 วินาที โดยระยะเวลาสูงสุดที่ 8.785 วินาที

สรุปผลการจำลองส่งข้อมูลจากผู้ป่วยจำนวน 30 คน ในระยะเวลา 24 ชั่วโมง โดยผู้ป่วยแต่ละคนจะส่งข้อมูลจากเซ็นเซอร์ทางการแพทย์จำนวน 4 ชนิดแบบสุ่ม ผ่านระบบเครือข่ายอินเตอร์เน็ตและเน็ตพายไปยังเครื่องคอมพิวเตอร์ของแพทย์ในโรงพยาบาล โดยข้อมูลถูกส่งทุก 250 มิลลิวินาที ดังนั้น แต่ละสรรพสิ่งจะส่งข้อมูลจำนวนทั้งสิ้น 345,600 ชุด ซึ่งผลการทดลองทั้ง 4 รูปแบบพบกว่าข้อมูลทั้งหมดถูกส่งไปถึงสรรพสิ่งปลายทางโดยไม่มีการสูญหาย แต่พบความล่าช้าในการสื่อสาร และความล่าช้าดังกล่าวเกิดในช่วงเวลาเดียวกัน และความล่าช้าของข้อมูลในระยะเวลาใกล้เคียงกัน เนื่องจากปัจจัยของผู้ให้บริการอินเตอร์เน็ต อย่างไรก็ตาม การบันทึกข้อมูลธุรกรรมทุกที่ส่งผลต่อระยะเวลาในการส่งข้อมูล โดยได้ระยะเวลาเฉลี่ยเกิน 1 วินาทีเล็กน้อย

ข้อมูลปริมาณพื้นที่สำหรับเก็บข้อมูลธุรกรรมของการทดลองทั้ง 4 รูปแบบ แสดงในตารางที่ 17 ทั้งนี้ ข้อมูลทั้งหมดที่ส่งในการทดลองนี้มีขนาด 20.736 กิกะไบต์ จากผลการทดลองพบว่าการบันทึกธุรกรรมเฉพาะที่สรรพสิ่งใช้พื้นที่เก็บข้อมูลจำนวน 84.54 เมกะไบต์ คิดเป็นร้อยละ 0.41 โดยแบ่งเป็นส่วนที่เก็บในสรรพสิ่งต้นทางจำนวน 16.14 เมกะไบต์ คิดเป็นร้อยละ 0.07 ส่วนที่เก็บในสรรพสิ่งปลายทางจำนวน 68.4 เมกะไบต์ คิดเป็นร้อยละ 0.33 ส่วนการบันทึกธุรกรรมเฉพาะที่เน็ตพายใช้พื้นที่เก็บข้อมูลจำนวน 42 เมกะไบต์ คิดเป็นร้อยละ 0.20 และหากบันทึกธุรกรรมทั้งที่สรรพสิ่งและที่เน็ตพายจะใช้พื้นที่รวมทั้งสิ้น 126.54 เมกะไบต์ คิดเป็นร้อยละ 0.61 จะเห็นได้ว่าพื้นที่สำหรับเก็บข้อมูลในการบันทึกธุรกรรมมีขนาดเล็กกว่าร้อยละ 1 ของข้อมูลทั้งหมดในการสื่อสาร

ตาราง 17 ตารางสรุประยะเวลาการสื่อสารของการทดลองแต่ละแบบ

Case	average time	size of log (Source)	size of log (Netpie)	size of log (Destination)	Size Total
ไม่บันทึกธุรกรรม	0.271	-	-	-	0 MB
บันทึกธุรกรรมเฉพาะที่สรรพสิ่ง	0.485	16.14 MB	-	68.4 MB	84.54 MB
บันทึกธุรกรรมเฉพาะเน็ตพาย	0.493	-	42 MB	-	42 MB
บันทึกธุรกรรมทุกส่วน	1.002	16.14 MB	42 MB	68.4 MB	126.54 MB

จากผลการทดสอบในสภาพแวดล้อมปกติพบว่า การบันทึกธุรกรรมในกรณีมีการบันทึกธุรกรรมทุกส่วนมีการล่าช้าเกิน 1 วินาทีเล็กน้อย อย่างไรก็ตาม ข้อมูลทำการส่งทุก 0.25 วินาที ส่งผลให้ปริมาณข้อมูลที่สามารถใช้งานได้ของแพทย์ในช่วง 1 วินาทีมีทั้งสิ้น 4 ชุด เป็นการเสริมความ

มั่นคงในประเด็นการส่งข้อมูลมากกว่า 1 ชุด ในส่วนของพื้นที่เก็บข้อมูลพบว่าพื้นที่สำหรับบันทึกข้อมูลธุรกรรมใช้พื้นที่น้อยกว่าร้อยละ 1 ข้อปริมาณข้อมูลในการสื่อสาร

การทดสอบระบบบันทึกข้อมูลธุรกรรมชุดที่สอง ทำการทดลองโดยการจำลองเหตุการณ์ผิดปกติเข้าไปในระบบ โดยการสุ่มสร้างเหตุการณ์ข้อมูลสูญหายในแต่ละช่วงเวลากำหนดให้ในแต่ละช่วงเวลาทุกสรรพสิ่งจะเกิดการสูญหายของข้อมูลเท่ากัน ในส่วนนี้จำนวนชุดข้อมูลที่สรรพสิ่งต้นทางต้องมากกว่าจำนวนสรรพสิ่งปลายทางเพราะข้อมูลที่ส่งมาจากสรรพสิ่งต้นทางจะเกิดการสูญหายจากการจำลองในการทดลองนี้ ทั้งนี้ การสุ่มจำนวนข้อมูลที่เกิดการสูญหายในทุกสรรพสิ่งต้นทางจากผู้ป่วยทั้ง 30 คนเท่า ๆ กันในแต่ละชั่วโมง เป็นเวลาสรรพสิ่งละ 24 ชั่วโมง โดยการส่งข้อมูลทุก 250 มิลลิวินาทีผ่านเน็ตพายเช่นเดิม ซึ่งใช้รูปแบบการบันทึกธุรกรรมทุกส่วนในการตรวจสอบข้อมูลสูญหาย เนื่องจากเป็นรูปแบบการบันทึกธุรกรรมในทุกส่วนของการสื่อสาร ได้แก่ สรรพสิ่งต้นทาง สรรพสิ่งปลายทาง และเน็ตพาย จึงทำให้สามารถตรวจสอบการสูญหายของข้อมูลได้ครบถ้วนหากเกิดเหตุการณ์ ตารางที่ 18 แสดงข้อมูลการสุ่มสร้างเหตุการณ์สูญหายของข้อมูลและผลการทดลอง

จากผลการทดลองในตารางที่ 18 พบว่าจำนวนการสูญหายของชุดข้อมูลที่ธุรกรรมในแต่ละสรรพสิ่งตรวจพบมีความใกล้เคียงกับค่าตั้งต้นของข้อมูลการสูญหายที่กำหนดในแต่ละชั่วโมง โดยคิดเป็นร้อยละ 96.33 ของการทดลองสำหรับการบันทึกธุรกรรมในทุกส่วนของการสื่อสาร

กระบวนการตรวจสอบความผิดปกติในการบันทึกธุรกรรมการสื่อสารสามารถตรวจสอบจากลำดับชุดข้อมูลและช่วงเวลาในการสื่อสารซึ่งเป็นข้อมูลพื้นฐานสำหรับระบบเครือข่ายซึ่งเหมาะสมสำหรับใช้ในการสื่อสารระหว่างสรรพสิ่งทางการแพทย์ผ่านอินเตอร์เน็ตที่ต้องการน่าเชื่อถือในการสื่อสารและสามารถแก้ไขปัญหาการสูญหายของการสื่อสารได้หากตรวจพบ ดังนั้นการทดลองต่อไปนี้จะเน้นการทดสอบความผิดปกติอื่น ได้แก่ การส่งข้อมูลที่เกิดความล่าช้า ข้อมูลที่เกิดสูญหายก่อนถึงเน็ตพาย และข้อมูลที่เกิดสูญหายหลังจากเน็ตพายส่งข้อมูล และอาจรวมถึงกรณีการบุกรุกจากผู้ไม่หวังดีที่พยายามแทรกแซงการสื่อสารระหว่างสรรพสิ่งที่อาจเกิดขึ้น เช่น กรณีพยายามข้อมูลการสื่อสารซ้ำ และการพยายามปลอมแปลงข้อมูลการสื่อสารโดยจะมีรูปแบบข้อมูลที่ส่งจะไม่เป็นไปตามลำดับ

ตาราง 18 ตารางจำนวนข้อมูลธุรกรรมที่พบการสูญหายของข้อมูลการสื่อสารในแต่ละชั่วโมงและแต่ละสรรพสิ่งใน 24 ชั่วโมง

Hours / Things	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**Sum**
Setup Lost Packet	**21**	**27**	**29**	**33**	**23**	**29**	**29**	**32**	**33**	**33**	**33**	**32**	**33**	**32**	**32**	**32**	**32**	**31**	**32**	**31**	**32**	**35**	**24**	**17**	**717**
P.01	21	27	29	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	32	35	24	17	**717**
P.02	21	27	29	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	32	11	18	19	**689**
P.03	21	27	29	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	32	13	18	19	**691**
P.04	21	27	29	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	32	11	18	19	**689**
P.05	21	27	30	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	32	35	18	20	**715**
P.06	21	27	30	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	33	35	18	19	**715**
P.07	21	27	29	33	23	29	29	33	33	33	33	32	33	32	32	32	32	31	32	31	33	35	23	19	**720**
P.08	21	27	29	33	23	29	29	32	33	33	33	32	33	32	32	32	32	31	32	31	33	35	24	21	**722**
P.09	21	27	29	33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**717**
P.10	21	27	29	33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**717**
P.11		27	29	33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**696**
P.12		27	29	33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**696**
P.13			29	33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**669**
P.14			29	33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**669**
P.15				33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**640**
P.16				33	23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**640**
P.17					23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**607**
P.18					23	29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**607**
P.19						29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**584**
P.20						29	29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**584**
P.21							29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**555**
P.22							29	32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**555**
P.23								32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**526**
P.24								32	33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**526**
P.25									33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**494**
P.26									33	33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**494**
P.27										33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**461**
P.28										33	33	32	33	31	32	32	32	31	32	31	33	35	24	17	**461**
P.29											33	32	33	31	32	32	32	31	32	31	33	35	24	17	**428**
P.30											33	32	33	31	32	32	32	31	32	31	33	35	24	17	**428**

การทดลองเพื่อตรวจสอบข้อมูลธุรกรรมหากเกิดความผิดปกติในการสื่อสารต่าง ๆ ใช้รูปแบบการทดลองการบันทึกธุรกรรมระหว่างสรรพสิ่งในทุกส่วน จากสรรพสิ่งผู้ป่วย 30 ชิ้นที่เชื่อมต่อกับอุปกรณ์เซ็นเซอร์วัดค่าสุขภาพผู้ป่วยจำนวน 4 ชนิด โดยแต่ละสรรพสิ่งจะส่งข้อมูลไปยังสรรพสิ่งปลายทาง 1 ชิ้น เป็นเวลาสรรพสิ่งละ 24 ชั่วโมง โดยการส่งข้อมูลทุก 250 มิลลิวินาที ผ่านเน็ตพาย ใช้การสุ่มจำลองกรณีความผิดปกติจากการสื่อสารในแต่ละสรรพสิ่งทั้ง 30 สรรพสิ่ง ประกอบด้วย กรณีเกิดความล่าช้าในการสื่อสาร 20 ครั้งต่อสรรพสิ่ง รวมทั้งหมดเป็น 600 ครั้ง การสุ่มจำลองกรณีข้อมูลสูญหายก่อนเน็ตพาย 15 ครั้งต่อสรรพสิ่ง รวมทั้งหมดเป็น 450 ครั้ง การสุ่มจำลองกรณีข้อมูลสูญหายหลังเน็ตพาย 15 ครั้งต่อสรรพสิ่ง รวมทั้งหมดเป็น 450 ครั้ง การสุ่มจำลองกรณีข้อมูลถูกส่งซ้ำ 2 ครั้งต่อสรรพสิ่ง รวมทั้งหมดเป็น 60 ครั้ง และข้อมูลถูกส่งอย่างไม่เป็นลำดับซึ่งเกิดจากพฤติกรรมของผู้ไม่หวังดี 2 ครั้งต่อสรรพสิ่ง รวมทั้งหมดเป็น 60 ครั้ง โดยผลการทดสอบประสิทธิภาพการตรวจจับความผิดปกติที่เกิดขึ้นของธุรกรรมแสดงในตารางที่ 19

ตาราง 19 ตารางแสดงการตรวจพบกรณีความผิดปกติในการสื่อสารจากการทดลองด้วยธุรกรรม

รูปแบบข้อมูล	ความผิดปกติที่กำหนด	การตรวจพบ			**% ที่ตรวจพบ**	
		ที่กำหนด	ที่ไม่ได้กำหนด	ทั้งหมด	ที่กำหนด	ที่ไม่ได้กำหนด
ข้อมูลที่เกิดความล่าช้า	600	600	2044	2644	100%	100%
ข้อมูลที่เกิดสูญหายก่อน NETPIE	450	450	0	450	100%	0%
ข้อมูลที่เกิดสูญหายหลัง NETPIE	450	450	0	450	100%	0%
ข้อมูลถูกส่งซ้ำ	60	60	0	60	100%	0%
ข้อมูลถูกส่งอย่างไม่เป็นลำดับ	60	60	0	60	100%	0%

จากผลการทดลองแสดงในตารางที่ 19 สามารถสรุปการทดลองการตรวจจับสรรพสิ่งผ่านอินเตอร์เน็ตด้วยการบันทึกธุรกรรมในทุกส่วนของอุปกรณ์ในแต่ละกรณี ระบบสามารถตรวจจับความผิดปกติได้ทุกกรณีที่สร้างขึ้น อีกทั้งสามารถตรวจจับความล่าช้าในการสื่อสารในสภาพใช้งานจริง ซึ่งเกิดขึ้นจากความล่าช้าของอินเตอร์เน็ตของแต่ละอุปกรณ์เป็นช่วงเวลา

ตารางที่ 20 สรุปผลการทดลองการทดสอบบันทึกธุรกรรมจากเซ็นเซอร์วัดค่าร่างกาย 4 ชิ้นต่อผู้ป่วย 1 คน ของผู้ป่วยจำนวน 30 คน ด้วยการส่งข้อมูลทุก 250 มิลลิวินาที ส่งข้อมูลไปยังคอมพิวเตอร์แพทย์ที่โรงพยาบาลด้วยเน็ตพายด้วยกระบวนการบันทึกธุรกรรมทั้ง 4 แบบ ได้แก่ แบบไม่บันทึกธุรกรรม แบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น บันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น และแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด พบว่าทุกรูปแบบที่มีการบันทึกธุรกรรมสามารถตรวจสอบพบการเชื่อมต่อใหม่และความล่าช้าในการสื่อสารของสรรพสิ่งได้ทั้งหมด แต่รูปแบบการตรวจสอบหาการสูญหายของข้อมูลมีความละเอียดในการตรวจพบแตกต่างไป

ซึ่งการบันทึกธุรกรรมที่สรรพสิ่งต่าง ๆ อย่างเดียว จะสามารถตรวจพบการสูญหายของข้อมูลได้ที่สรรพสิ่งปลายทาง ทั้งนี้จะไม่สามารถระบุรูปแบบการสูญหายของข้อมูลได้ว่าสูญหายจากสรรพสิ่งต้นทางส่งถึงเน็ตพายหรือหลังจากเน็ตพายส่งถึงสรรพสิ่งปลายทาง โดยหากมีการบันทึกธุรกรรมที่เน็ตพายจะสามารถตรวจพบได้ว่าข้อมูลเกิดการสูญหายในส่วนนี้

ทั้งนี้ผลสรุปของการตรวจสอบธุรกรรมของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ต จากสรรพสิ่งจำนวน 30 อุปกรณ์ แต่ละสรรพสิ่งเชื่อมต่ออุปกรณ์ทางการแพทย์จำนวน 4 ชิ้น ส่งข้อมูลด้วยการส่งข้อมูลทุก 250 มิลลิวินาที โดยมีการบันทึกธุรกรรมในทุกสรรพสิ่งได้แก่ การบันทึกธุรกรรมที่ต้นทาง (Source-Log) บันทึกธุรกรรมที่เน็ตพาย (NETPIE-Log) และบันทึกธุรกรรมที่ปลายทาง (Destination-Log) พบว่าสามารถตรวจพบความผิดปกติของการสื่อสารได้ที่เน็ตพาย และสรรพสิ่งปลายทางได้ทันที แต่จะทราบเพียงเกิดการสูญหายของข้อมูลที่ส่งมาจากสรรพสิ่งต้นทางถึงปลายทาง แต่ธุรกรรมที่สรรพสิ่งปลายทางจะไม่สามารถวิเคราะห์ได้ว่าข้อมูลเกิดการสูญหายที่ก่อนหรือหลังผ่านเน็ตพาย ซึ่งหากต้องการทราบว่าข้อมูลสูญหายก่อนหรือหลังผ่านเน็ตพายจะต้องวิเคราะห์จากธุรกรรมของเน็ตพายเท่านั้น (NETPIE-Log)

ขนาดของพื้นที่จัดเก็บข้อมูลธุรกรรมในการสื่อสารรูปแบบนี้มีขนาดทั้งหมด 652.74 เมกะไบต์ต่อวัน โดยแบ่งออกเป็น 3 ส่วน ได้แก่ ขนาดธุรกรรมของแต่ละสรรพสิ่งต้นทาง 16.14 เมกะไบต์ ซึ่งในการทดลองนี้มี 30 สรรพสิ่ง รวมทั้งสิ้น 484.20 เมกะไบต์ ขนาดธุรกรรมของเน็ตพาย 42 เมกะไบต์ และขนาดธุรกรรมของสรรพสิ่งปลายทาง 126.54 เมกะไบต์ แต่เนื่องจากรูปแบบการบันทึกธุรกรรมของเน็ตพายใช้ฐานข้อมูล Apache Cassandra บริหารจัดการจัดการข้อมูลธุรกรรม จึงทำให้ข้อมูลธุรกรรมทั้งหมดมีขนาดที่น้อยกว่าขนาดธุรกรรมของสรรพสิ่งปลายทางซึ่งมีการบันทึกข้อมูลที่เท่ากัน

ตาราง 20 ผลการทดลองการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตทั้ง 4 แบบ

		Source	NETPIE	Destination	Log Size
แบบไม่บันทึกธุรกรรม	สามารถตรวจการเชื่อมต่อใหม่				
	สามารถตรวจข้อมูลสูญหาย				
	สามารถตรวจข้อมูลหาย ก่อน NETPIE				
	สามารถตรวจข้อมูลหาย หลัง NETPIE				
	สามารถตรวจความความล่าช้า ของข้อมูล				
	ขนาดพื้นที่ธุรกรรม	-	-	-	0 MB
	ระยะเวลาการสื่อสาร	-	-	-	0.2 s
แบบบันทึกธุรกรรม เฉพาะที่สรรพสิ่งเท่านั้น	สามารถตรวจการเชื่อมต่อใหม่			/	
	สามารถตรวจข้อมูลสูญหาย			/	
	สามารถตรวจข้อมูลหาย ก่อน NETPIE				
	สามารถตรวจข้อมูลหาย หลัง NETPIE				
	สามารถตรวจความความล่าช้า ของข้อมูล			/	
	ขนาดพื้นที่ธุรกรรม	16.14 MB	-	68.4 MB	84.54 MB
	ระยะเวลาการสื่อสาร	-	-	0.224 s	0.224 s
บันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น	สามารถตรวจการเชื่อมต่อใหม่		/		
	สามารถตรวจข้อมูลสูญหาย		/		
	สามารถตรวจข้อมูลหาย ก่อน NETPIE		/		
	สามารถตรวจข้อมูลหาย หลัง NETPIE		/		
	สามารถตรวจความความล่าช้า ของข้อมูล		/		
	ขนาดพื้นที่ธุรกรรม	-	42 MB	-	42 MB
	ระยะเวลาการสื่อสาร	-	0.582 s	-	0.582 s
บันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด	สามารถตรวจการเชื่อมต่อใหม่		/	/	
	สามารถตรวจข้อมูลสูญหาย		/	/	
	สามารถตรวจข้อมูลหาย ก่อน NETPIE		/		
	สามารถตรวจข้อมูลหาย หลัง NETPIE		/		
	สามารถตรวจความความล่าช้า ของข้อมูล		/	/	
	ขนาดพื้นที่ธุรกรรม	16.14 MB	42 MB	68.4 MB	126.54 MB
	ระยะเวลาการสื่อสาร	-	0.589 s	0.245 s	0.834 s

ดังนั้นหากต้องการข้อมูลธุรกรรมที่สามารถบอกได้ถึงการสูญหายของข้อมูลว่าเกิดจากก่อนเข้ามาถึงเน็ตพายหรือหลังจากออกจากเน็ตพายไปแล้ว อีกทั้งข้อมูลความผิดปกติในการสื่อสารที่เกิดขึ้นและการเชื่อมต่อใหม่ของสรรพสิ่ง การบันทึกธุรกรรมที่เน็ตพายอย่างเดียวจะเหมาะสมที่สุด เพราะใช้พื้นที่ในการจัดเก็บไม่มากเมื่อเทียบกับการจัดเก็บธุรกรรมในทุกสรรพสิ่ง แต่สามารถตรวจสอบความผิดปกติในการสื่อสารที่เกิดขึ้นต้องติดตามจากธุรกรรมของเน็ตพายตลอดเวลาเช่นกัน

4.4 แนวทางการประยุกต์ใช้ระบบบันทึกธุรกรรมที่นำเสนอ

รูปแบบการบันทึกธุรกรรมเฉพาะที่เน็ตพายระหว่างการสื่อสารสรรพสิ่งผ่านอินเตอร์เน็ตสำหรับข้อมูลทางการแพทย์นั้น เพียงพอสำหรับการตรวจสอบความผิดปกติที่เกิดจากความไม่สมบูรณ์ของการสื่อสาร อีกทั้งขนาดในการจัดเก็บข้อมูลที่ได้รับการบริหารจัดการด้านฐานข้อมูล Apache Cassandra ซึ่งรองรับการเขียนและอ่านข้อมูลที่มีปริมาณมากในรูปแบบธุรกรรมและได้รับการควบคุมผ่านตัวกลางการสื่อสาร จึงทำให้สรรพสิ่งไม่ต้องใช้พื้นที่จัดเก็บข้อมูลธุรกรรมสำหรับสรรพสิ่งที่ต้องสื่อสารกัน เนื่องจากบางสรรพสิ่งอาจเป็นอุปกรณ์ประมวนผลขนาดเล็ก ทำให้ประสิทธิภาพในการประมวนผลและบันทึกข้อมูลจำนวนอาจไม่เหมาะสม

ดังนั้นรูปแบบการบันทึกธุรกรรมเฉพาะที่เน็ตพายจะสามารถรองรับความหลากหลายของรูปแบบสรรพสิ่งที่ใช้ในการสื่อสาร โดยไม่จำเป็นต้องใช้หน่วยประมวนผลและหน่วยความจำที่มีขนาดใหญ่สำหรับการบันทึกธุรกรรมในแต่ละสรรพสิ่งที่อาจใช้สำหรับอ่านค่าข้อมูลสุขภาพเพียงอย่างเดียว ตัวอย่างเช่น อุปกรณ์เซ็นเซอร์วัดค่าสุขภาพร่างกายผู้ป่วย ซึ่งอาจเชื่อมต่อเซ็นเซอร์เหล่านั้นกับเน็ตพายเพื่อส่งข้อมูลให้แพทย์ติดตามได้ทันที เนื่องจากอุปกรณ์เซ็นเซอร์จะส่งข้อมูลที่วัดค่าได้ไปยังเน็ตพายเพียงอย่างเดียว โดยเน็ตพายจะทำหน้าที่บันทึกธุรกรรมและตรวจสอบความผิดปกติที่ศูนย์กลางได้จากหน่วยประมวนผล โดยสามารถตรวจสอบความผิดปกติต่าง ๆ ได้แก่ การตรวจสอบการเชื่อมต่อใหม่ของสรรพสิ่ง การตรวจสอบความล่าช้าของข้อมูลการสื่อสาร การสูญหายของข้อมูลก่อนและหลังเน็ตพาย เป็นต้น

การทดลองนี้เป็นการนำรูปแบบการสื่อสารข้อมูลทางการแพทย์ระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตด้วยเน็ตพายสำหรับโรงพยาบาลชุมชนขนาดเล็กสุด (F3) โดยรองรับผู้ป่วยขนาด 30 เตียง และมีแพทย์ดูแล 1 คน โดยให้สรรพสิ่งที่วัดค่าสุขภาพต่าง ๆ ของผู้ป่วยแต่ละคนส่งข้อมูลทุก 0.25 วินาที เป็นเวลา 24 ชั่วโมง ซึ่งหากในการใช้งานสำหรับโรงพยาบาลขนาดใหญ่จะต้องคำนึงถึงปริมาณข้อมูลที่สมดุลกับอินเตอร์เน็ตในแต่ละช่วงเวลาเพื่อไม่ให้เกิดความล่าช้าในการสื่อสาร อีกทั้งปริมาณขนาดพื้นที่จัดเก็บข้อมูลธุรกรรมที่มีขนาดเพิ่มขึ้นตามจำนวนเตียงผู้ป่วยและเวลาที่ใช้ในการ

สื่อสาร ทั้งนี้ข้อมูลธุรกรรมการสื่อสารในฐานข้อมูล RowLog ซึ่งเป็นการจัดเก็บข้อมูลการสื่อสารแต่ละสรรพสิ่งทั้งหมดตลอดเวลา ทำให้ข้อมูลในส่วนนี้จะมีขนาดที่เพิ่มขึ้นเป็นจำนวนมากที่สุด

อย่างไรก็ตามหากข้อมูลธุรกรรมทั้งหมดในการสื่อสารได้รับการประมวนผลค้นหาความผิดปกติในการสื่อสารเพื่อบันทึกเฉพาะเหตุการณ์ผิดปกติลงในฐานข้อมูล Netpielog แล้ว และพบว่าอายุของข้อมูลธุรกรรมดังกล่าวมากกว่า 90 วันจากปัจจุบัน [29] ซึ่งเป็นช่วงเวลาที่ได้รับการยอมรับว่าเป็นระยะเวลาที่ไม่เป็นปัจจุบันสำหรับการติดตามเฝ้าระวังเหตุการณ์ ทั้งนี้สามารถที่จะลบข้อมูลธุรกรรมการสื่อสารในส่วนของ RowLog ที่มีอายุข้อมูลมากกว่า 90 วันแล้วได้ เพื่อแก้ปัญหาสำหรับการจัดสรรพื้นที่จัดเก็บข้อมูลธุรกรรมที่ไม่เพียงพอกับทรัพยากรที่มีอยู่ ในขณะที่ข้อมูลธุรกรรมการสื่อสารเพิ่มปริมาณมากขึ้นตามระยะเวลาการใช้งานและจำนวนสรรพสิ่งที่เชื่อมต่อสื่อสารที่มากขึ้นเช่นกันในอนาคต

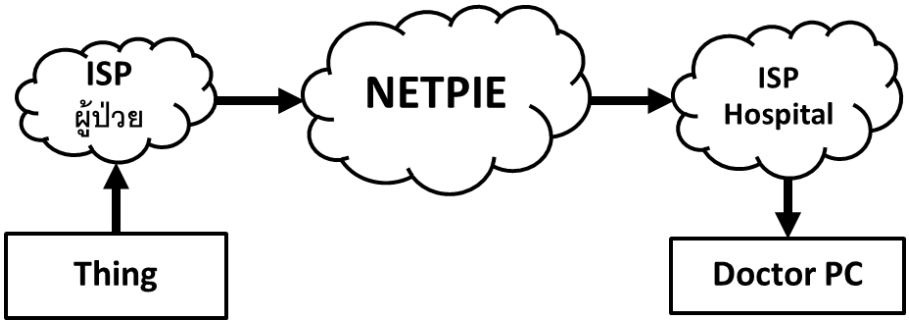
บทที่ 5
บทสรุปและข้อเสนอแนะ

ระบบบันทึกข้อมูลธุรกรรมระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตสำหรับข้อมูลทางการแพทย์ เป็นระบบสำหรับการติดตามความครบถ้วนสมบูรณ์ในการสื่อสารของสรรพสิ่งผ่านอินเตอร์เน็ตซึ่งเป็นโพรโทคอลสาธารณะ เพื่อให้เกิดความน่าเชื่อถือและความมั่งคงในการสื่อสารข้อมูลต่าง ๆ ระหว่างสรรพสิ่งโดยเฉพาะข้อมูลทางการแพทย์ ที่ต้องการความน่าเชื่อถือและความต่อเนื่องสำหรับการสื่อสาร โดยทั่วไปข้อมูลสุขภาพพื้นฐานนั้นก็คือข้อมูลสัญญาณชีพ (Vital signs) ซึ่งเป็นข้อมูลที่มีการเปลี่ยนแปลงอย่างน้อยทุก 1 วินาที ทำให้การสื่อสารข้อมูลลักษณะนี้ต้องมีการส่งข้อมูลอย่างน้อย 1 วินาทีตลอดเวลา เพื่อให้แพทย์หรือผู้ที่สิทธิ์สามารถติดตามข้อมูลได้อย่างต่อเนื่องขณะดำเนินการรักษา

การทดลองบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตนั้นใช้ตัวอย่างผู้ให้บริการสื่อสารระหว่างสรรพสิ่ง คือ เน็ตพาย (Netpie) โดยกำหนดให้มีการบันทึกธุรกรรมการสื่อสารทั้งหมดของแต่ละสรรพสิ่งในฐานข้อมูลส่วน RowLog และประมวนผลเพื่อค้นหาเฉพาะความผิดปกติในการสื่อสารมาบันทึกในฐานข้อมูล NetpieLog เท่านั้น เพื่อให้ผู้ดูแลระบบสามารถติดตามความผิดปกติที่เกิดขึ้นจากหน้ารายงานได้ทันทีโดยไม่ต้องประมวนผลใหม่ทุกครั้งเมื่อแสดงรายงาน โดยมีรูปแบบการทดลองเป็น 3 ส่วน ได้แก่ การทดลองเพื่อหาอัตราการส่งข้อมูลของเน็ตพาย การทดลองเพื่อหาขนาดข้อมูลที่เหมาะสมในการสื่อสาร และการทดลองหาประสิทธิภาพการบันทึกธุรกรรมแบบต่าง ๆ เป็นต้น ซึ่งรูปแบบการบันทึกธุรกรรมที่ใช้ในการทดลองเพื่อหาประสิทธิภาพการตรวจสอบความผิดปกติในการสื่อสารนั้นมี 4 รูปแบบ คือ รูปแบบไม่บันทึกธุรกรรม รูปแบบธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น รูปแบบบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น รูปแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด เป็นต้น

จากการทดลองการส่งข้อมูลจากเซ็นเซอร์วัดค่าสุขภาพผู้ป่วยทั้ง 30 ชิ้นผ่านเน็ตพายไปยังคอมพิวเตอร์ของแพทย์ที่โรงพยาบาลเป็นเวลา 24 ชั่วโมงด้วยการส่งข้อมูลทุก ๆ 250 มิลลิวินาทีด้วยข้อมูลขนาดเฉลี่ย 56 ไบต์ตามรูปแบบชนิดข้อมูลสุขภาพที่วัดค่าโดยแบ่งออกเป็น 4 รูปแบบได้แก่ แบบไม่บันทึกธุรกรรม แบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น บันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น และแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด ได้ผลลัพธ์ของการบันทึกธุรกรรมของการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตในรูปแบบต่าง ๆ ซึ่งพบว่าเครือข่ายอินเตอร์เน็ตที่สรรพสิ่งต้นทางและสรรพสิ่งปลายทางเชื่อมต่อไม่ได้อยู่ภายใต้เครือข่ายเดียวกัน โดยแต่ละสรรพสิ่งจะเชื่อมต่อกับผู้ให้บริการอินเตอร์เน็ตของตนเอง ดังนั้นประสิทธิภาพของเครือข่ายอินเตอร์เน็ต

ในแต่ละสรรพสิ่ง จึงเป็นปัจจัยที่ส่งผลต่อความเร็วในการสื่อสารเช่นกันนอกเหนือข้อจำกัดด้านประสิทธิภาพการสื่อสารของเน็ตพาย จากโครงสร้างเครือข่ายการสื่อสารระหว่างสรรพสิ่งผ่านเน็ตพายดังรูปที่ 27



รูปที่ 27 โครงสร้างเครือข่ายของแต่ละสรรพสิ่งที่เชื่อมต่อเน็ตพาย

แต่ในกรณีการตรวจสอบการสูญหายของข้อมูลหลังจากเน็ตพายส่งถึงสรรพสิ่งปลายทางจากการบันทึกธุรกรรมที่เน็ตพายอย่างเดียว จะสามารถพบข้อมูลสูญหายได้ก็ต่อเมื่อสรรพสิ่งปลายทางไม่มีการตอบกลับเมื่อได้รับข้อมูล ดังนั้นหมายความว่าการบันทึกธุรกรรมที่เน็ตพายเพียงอย่างเดียว จะไม่สามารถรู้ได้ทันทีหากเกิดการสูญหายหลังจากเน็ตพายส่งถึงสรรพสิ่งปลายทาง ซึ่งต้องรอจนถึงระยะเวลาหนึ่งเมื่อเน็ตพายส่งข้อมูลไปยังสรรพสิ่งปลายทางแล้วไม่มีการตอบกลับมา หรือสรรพสิ่งปลายทางตอบกลับมาด้วยข้อมูลใหม่ที่ไม่เป็นไปตามลำดับของข้อมูลที่ส่งไป ดังนั้นหากต้องการความสมบูรณ์ในการตรวจพบการสูญหายของข้อมูลได้ทันที จึงควรมีการบันทึกธุรกรรมทั้งที่สรรพสิ่งและเน็ตพายประกอบกัน แต่ทั้งนี้พื้นที่ในการจัดเก็บข้อมูลธุรกรรมของระบบโดยรวมก็จะมีปริมาณมากขึ้นด้วยเช่นกัน โดยปริมาณพื้นที่ในการจัดเก็บธุรกรรมที่เน็ตพายเพียงอย่างเดียวจะมีปริมาณข้อมูลที่ครบถ้วนทั้งหมด และผลจากการตรวจพบความผิดปกติจากการสื่อสารทั้งหมดในการสื่อสารซึ่งใช้สถาปัตยกรรมฐานข้อมูลรูปแบบ Apache Cassandra สำหรับบริหารจัดการข้อมูลซึ่งมีคุณสมบัติในการบันทึกข้อมูลที่มีปริมาณมาก ทำให้มีความเหมาะสมในการใช้จัดเก็บข้อมูลธุรกรรมต่าง ๆ จึงทำให้พื้นที่จัดเก็บข้อมูลมีขนาดน้อยกว่ารูปแบบฐานข้อมูลทั่วไปในปริมาณข้อมูลที่เท่ากัน ซึ่งในการบันทึกธุรกรรมที่สรรพสิ่งขนาดเล็ก ได้แก่ เซ็นเซอร์วัดค่า อุปกรณ์ฝังตัว และไมโครคอลโทรเลอร์ จะไม่สามารถใช้รูปแบบสถาปัตยกรรมแบบ Apache Cassandra ได้ เนื่องจากหน่วยประมวลผลมีขนาดเล็กจึงไม่สามารถประมวลผลฐานข้อมูลแบบโนเอสคิวแอลได้ ทั้งนี้การตรวจสอบบันทึกที่อุปกรณ์ต่าง ๆ จะส่งผลต่อระยะเวลาการสื่อสารที่เพิ่มขึ้นอีกด้วย เพราะต้องมีการตรวจสอบความผิดปกติข้อมูลของการสื่อสารต่าง ๆ

5.1 สรุปผลการบันทึกธุรกรรมการสื่อสารระหว่างสรรพสิ่งแบบต่าง ๆ

รูปแบบการบันทึกธุรกรรมต่าง ๆ จึงมีข้อดีข้อเสียที่แตกต่างกันและมีรูปแบบความเหมาะสมในการใช้งานที่แตกต่างกันไปดังต่อไปนี้

5.1.1 สรุปผลการแบบไม่บันทึกธุรกรรม

แบบไม่บันทึกธุรกรรม จะไม่สามารถตรวจสอบความผิดปกติของการสื่อสารได้ทุกรูปแบบ แต่จะเป็นการสื่อสารที่มีความรวดเร็วที่สุด เพราะไม่มีการตรวจสอบข้อมูลในการสื่อสาร เหมาะกับการสื่อสารระหว่างสรรพสิ่งที่ไม่ต้องการความปลอดภัยและความน่าเชื่อถือในการสื่อสาร

5.1.2 สรุปผลการแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น

แบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น เหมาะกับการบันทึกธุรกรรมที่สนใจเฉพาะความสมบูรณ์ในการสื่อสารไปยังสรรพสิ่งปลายทาง ซึ่งสามารถตรวจจับความผิดปกติของธุรกรรมได้ทันทีจากลำดับของข้อมูลที่รับส่งและระยะห่างของเวลาส่งจากสรรพสิ่งต้นกับเวลารับที่สรรพสิ่งปลายทางโดยข้อมูลธุรกรรมจะถูกเก็บแยกส่วนกันที่สรรพสิ่งต่าง ๆ ทำให้สามารถดูความผิดปกติที่เกิดขึ้นได้ตามสิ่งที่เกิดขึ้นในแต่ละสรรพสิ่ง ซึ่งเหมาะกับรูปแบบการสื่อสารของสรรพสิ่งที่ไม่มีความสัมพันธ์กันและต้องการติดตามความผิดปกติที่การขึ้นกับสรรพสิ่งปลายทางเท่านั้น เพราะรูปแบบนี้จะใช้ระยะเวลาในการสื่อสารน้อยที่สุดในรูปแบบการตรวจสอบและบันทึกข้อมูลธุรกรรมต่าง ๆ แต่จะไม่สามารถลงรายละเอียดความผิดปกติได้ชัดเจนว่าความผิดปกติเกิดขึ้นที่การสื่อสารส่วนใดบ้าง ซึ่งจะพบเพียงว่าเปิดความผิดปกติขึ้นและรายงานได้เฉพาะแต่ละสรรพสิ่งเท่านั้น

5.1.3 สรุปผลการแบบบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น

บันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น เป็นรูปแบบที่สามารถลงรายละเอียดได้ชัดเจนว่าเกิดความผิดปกติที่การสื่อสารส่วนใด โดยสามารถเห็นความผิดปกติเป็นภาพรวมได้จากการบันทึกในฐานข้อมูลธุรกรรมเดียวกัน ซึ่งทำให้ขนาดของข้อมูลธุรกรรมมีขนาดน้อยที่สุดในรูปแบบการตรวจสอบและบันทึกข้อมูลธุรกรรมต่าง ๆ แต่ระยะเวลาการสื่อสารจะมากกว่าแบบบันทึกธุรกรรมเฉพาะที่สรรพสิ่งเท่านั้น เพราะในส่วนการตรวจสอบข้อมูลความผิดปกติที่เน็ตพายซึ่งเป็นตัวกลางในการสื่อสารจะมีการตรวจสอบทุกข้อมูลของแต่ละสรรพสิ่งที่เข้ามาทั้งหมด และในส่วนของการตรวจสอบการสูญหายหลังจากเน็ตพายส่งถึงสรรพสิ่งปลายทางจะต้องรอข้อมูลตอบกลับจากสรรพสิ่งปลายทางเป็นระยะเวลาหนึ่ง ซึ่งการบันทึกข้อมูลธุรกรรมที่เน็ตพายเท่านั้นจะเหมาะสมกับการสื่อสารในลักษณะที่ทุกสรรพสิ่งต้องการความปลอดภัยและความน่าเชื่อถือในการสื่อสาร แต่ไม่สนใจความรวดเร็วในการรายงานผลความผิดปกติ เนื่องจากรูปแบบการบันทึกธุรกรรมนี้มีการตรวจสอบและบันทึกธุรกรรมที่เน็ตพาย ซึ่งเป็นส่วนกลางในการสื่อสารทั้งหมดเพียงอย่างเดียว จึงทำให้ต้องใช้ระยะเวลาการประมวลผล และการตอบรับจากสรรพสิ่งปลายทางหากส่งข้อมูลถึงปลายทางสำเร็จ

ทุกครั้ง การบันทึกธุรกรรมในลักษณะนี้จึงไม่เหมาะกับรูปแบบการสื่อสารที่ต้องการติดตามความผิดปกติแบบรายงานผลทันทีที่แต่ละสรรพสิ่งต่าง ๆ

5.1.4 สรุปผลการแบบบันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด

บันทึกธุรกรรมที่เน็ตพายและสรรพสิ่งทั้งหมด เป็นรูปแบบการบันทึกธุรกรรมในทุกส่วนของการสื่อสารตั้งแต่สรรพสิ่งต้นทาง สรรพสิ่งปลายทาง และที่ตัวกลางการสื่อสารได้แก่ เน็ตพาย ทำให้การบันทึกธุรกรรมในรูปแบบนี้จะต้องตรวจสอบความผิดปกติในทุกส่วนของการสื่อสาร จึงทำให้ใช้เวลาในการตรวจสอบความผิดปกติของธุรกรรมมากที่สุด แต่ไม่ส่งผลต่อความล่าช้าและความผิดพลาดในการสื่อสาร อีกทั้งข้อมูลธุรกรรมที่บันทึกจะได้รับการบันทึกในทุกส่วนของการสื่อสารโดยมีมุมมองในการบันทึกธุรกรรมที่แตกต่างกันออกไป เช่น ธุรกรรมของแต่ละสรรพสิ่งจะบันทึกข้อมูลการสื่อสารที่ได้รับหรือส่งข้อมูลออกไปเท่านั้น ซึ่งหากเกิดความผิดพลาดในการสื่อสารระหว่างสรรพสิ่งนั้น ๆ ก็จะถูกบันทึกความผิดพลาดดังกล่าวในธุรกรรมของแต่ละสรรพสิ่งทันที และธุรกรรมของเน็ตพายจะบันทึกข้อมูลธุรกรรมของทุกสรรพสิ่งที่สื่อสารผ่านเน็ตพาย โดยจะสามารถตรวจสอบความผิดปกติในการสื่อสารจากสรรพสิ่งหนึ่งไปยังอีกสรรพสิ่งหนึ่งได้ทันที ซึ่งทำให้การตรวจสอบการสูญหายของสรรพสิ่งต้นทางไปยังปลายทางสามารถตรวจสอบแบ่งออกได้เป็น 2 ส่วน คือ ข้อมูลสูญหายระหว่างสรรพสิ่งต้นทางไปยังเน็ตพาย จะสามารถตรวจสอบและรายงานความผิดปกติได้ทันทีในธุรกรรมของเน็ตพาย และข้อมูลสูญหายระหว่างเน็ตพายไปยังสรรพสิ่งปลายทางจะสามารถตรวจสอบได้ทันทีที่ธุรกรรมของสรรพสิ่งปลายทาง แต่หากต้องการตรวจสอบการสูญหายของข้อมูลระหว่างเน็ตพายไปยังสรรพสิ่งปลายทางที่ธุรกรรมของเน็ตพาย จะต้องรอการหมดเวลาการตอบกลับหากข้อมูลส่งถึงสรรพสิ่งปลายทางได้สำเร็จ ซึ่งถ้าหมดเวลาการสื่อสารแล้วสรรพสิ่งปลายทางยังไม่ตอบกลับมายังเน็ตพาย ธุรกรรมที่เน็ตพายจะสรุปว่าข้อมูลสูญหายระหว่างเน็ตพายไปยังสรรพสิ่งปลายทาง ซึ่งธุรกรรมที่เน็ตพายจะรายงานผลได้ช้ากว่าธุรกรรมที่สรรพสิ่งปลายทางในกรณีนี้ ดังนั้นการบันทึกธุรกรรมในรูปแบบนี้จะสามารถตรวจสอบรูปแบบธุรกรรมได้ทั้งหมด และสามารถรายงานผลได้ทันทีในทุกกรณีความผิดปกติของการสื่อสาร เนื่องจากมีการบันทึกธุรกรรมในทุกสรรพสิ่งและตัวกลางการสื่อสาร โดยผู้ดูแลระบบสามารถตรวจสอบติดตามการสื่อสารและความผิดปกติได้ทั้งภาพรวมและแต่ละสรรพสิ่งเพื่อวิเคราะห์ได้อย่างสมบูรณ์ยิ่งขึ้น แต่อย่างไรก็ตามการบันทึกธุรกรรมในรูปแบบนี้ต้องมีการตรวจสอบข้อมูลในทุกส่วนที่มีการสื่อสารและบันทึกข้อมูลธุรกรรมลงในแต่ละส่วนการสื่อสาร ตามมุมมองของส่วนที่บันทึกธุรกรรมต่าง ๆ จึงทำให้ระยะเวลาการตรวจสอบและใช้พื้นที่การจัดเก็บข้อมูลธุรกรรมโดยรวมทั้งระบบมากที่สุดในรูปแบบการบันทึกธุรกรรมทั้ง 4 กรณี การบันทึกธุรกรรมในรูปแบบนี้จึงเหมาะกับการบันทึกธุรกรรมที่ต้องการความครบถ้วนของข้อมูล

เพื่อต้องการตรวจสอบความผิดพลาดของการสื่อสารในทุกส่วนและรายงานผลได้ทันที โดยไม่มีข้อจำกัดด้านพื้นที่การจัดเก็บข้อมูลในแต่ละส่วนและความล่าช้าที่เพิ่มขึ้นในการสื่อสาร

ทั้งนี้รูปแบบการบันทึกธุรกรรมระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตที่เหมาะสม จะต้องพิจารณาจากข้อจำกัดต่าง ๆ ในระบบการสื่อสารเรื่องพื้นที่การจัดเก็บข้อมูลและความเร็วการสื่อสาร ซึ่งใน 4 รูปแบบการบันทึกธุรกรรมจะมีข้อดีข้อเสียในแต่ละรูปแบบที่แตกต่างกันไป ดังนั้นการใช้รูปแบบการบันทึกธุรกรรมที่เหมาะสมกับระบบการสื่อสารและข้อจำกัดจะส่งผลในการบันทึกธุรกรรมในระบบมีประสิทธิภาพและความแม่นยำในการตรวจสอบมากยิ่งขึ้น ซึ่งในกรณีศึกษาซึ่งใช้การสื่อสารระหว่างสรรพสิ่งในการสื่อสารข้อมูลสุขภาพ ซึ่งต้องเน้นความรวดเร็วในการสื่อสารและความละเอียดในการตรวจสอบความผิดปกติในการสื่อสาร อีกทั้งข้อจำกัดด้านพื้นที่จัดเก็บข้อมูลในแต่ละสรรพสิ่งจึงเหมาะสมกับการบันทึกธุรกรรมเฉพาะที่เน็ตพายเท่านั้น เพราะมีความครบถ้วนในการตรวจสอบความผิดปกติอย่างละเอียดในระยะเวลาในการตรวจสอบความผิดปกติระดับกลาง โดยตรวจสอบเฉพาะเน็ตพายเท่านั้นซึ่งเป็นตรวจสอบการสื่อสารระหว่างสรรพสิ่งทั้งหมด โดยใช้พื้นที่จัดเก็บธุรกรรมเฉพาะเน็ตพายเท่านั้น ทำให้พื้นที่จัดเก็บข้อมูลธุรกรรมไม่มากเกินไป สามารถควบคุมพื้นที่การจัดเก็บข้อมูลได้ด้วยฐานข้อมูลสถาปัตยกรรม Apache Cassandra ซึ่งเป็นที่รองรับการอ่านเขียนเป็นจำนวนมากและไม่ต้องจัดเก็บข้อมูลธุรกรรมที่สรรพสิ่งอื่น ๆ โดยการตรวจสอบข้อมูลธุรกรรมนี้จะไม่ล่วงละเมิดภายในเนื้อหาข้อมูล ซึ่งเป็นข้อมูลด้านการแพทย์และสาธารณสุขที่ให้ความสำคัญกับประเด็นความลับของผู้ป่วยเพราะสามารถพิจารณาได้จากข้อมูลพื้นฐานของการสื่อสารเท่านั้น

5.2 ข้อเสนอแนะ

แนวทางการพัฒนาสำหรับการบันทึกธุรกรรมระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตสำหรับข้อมูลทางการแพทย์ให้สมบูรณ์นั้นความมั่นคงข้อมูลเป็นสิ่งสำคัญ ในการออกแบบระบบธุรกรรมนี้เป็นการตรวจสอบความครบถ้วนสมบูรณ์ในการสื่อสารกรณีต่าง ๆ เช่น การตรวจหาสรรพสิ่งที่เชื่อมต่อเข้ามาใหม่ การสูญหายของข้อมูล และความล่าช้าของการสื่อสาร เท่านั้น แต่การบันทึกธุรกรรมในงานนี้ ยังไม่ครอบคลุมถึงการตรวจสอบประเด็นความปลอดภัยอื่น ๆ ที่เกิดจากการโจมตีและบุกรุกโดยผู้ไม่หวังดี ซึ่งเป็นอีกประเด็นหนึ่งที่ส่งผลต่อความน่าเชื่อถือในการสื่อสารข้อมูลทางการแพทย์ จึงควรมีระบบธุรกรรมการตรวจสอบการโจมตีและโจรกรรมข้อมูลจากผู้ไม่หวังดีเพิ่มเติม เพื่อความสมบูรณ์ในการตรวจสอบความมั่งคงปลอดภัยในการสื่อสารระหว่างสรรพสิ่งผ่านอินเตอร์เน็ตสำหรับข้อมูลทางด้านการแพทย์ ซึ่งให้ความสำคัญกับความเป็นส่วนตัวและความน่าเชื่อถือของข้อมูลสุขภาพของผู้ป่วยเป็นหลัก สำหรับการใช้งานด้านการสื่อสารเพื่อดำเนินการรักษาอย่างมีประสิทธิภาพโดยไม่ละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ป่วย

บรรณานุกรม

[1] S. Madakam, "Internet of things: Smart things," International Journal of Future Computer and Communication, vol. 4, no. 4, pp. 250–253, 2015.

[2] J. Djurica, "Internet of Things Offers Great Opportunities and Much Risk," ISACA JOURNAL, vol. 2, 2015.

[3] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of things: Perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481–2501, Jun. 2014.

[4] R. Costa and A. Pinto, "A framework for the secure storage of data generated in the IoT," in Ambient Intelligence - Software and Applications. Springer Science + Business Media, 2015, pp. 175–182.

[5] H. Jiang, F. Shen, S. Chen, K.-C. Li, and Y.-S. Jeong, "A secure and scalable storage system for aggregate data in IoT," Future Generation Computer Systems, vol. 49, pp. 133–141, Aug. 2015.

[6] S. Al-Fedaghi and F. Mahdi, "Events classification in log audit," International journal of Network Security & Its Applications, vol. 2, no. 2, pp. 58–73, Apr. 2010.

[7] "MQTT," 2014. [Online]. Available: http://mqtt.org/. [Accessed: Jul. 15, 2016].

[8] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S — A publish/subscribe protocol for wireless sensor networks," pp. 791–798, Jan. 2010.

[9] S. Lee, H. Kim, D. Hong, and H. Ju, "Correlation Analysis of MQTT Loss and Delay According to QoS Level," The International Conference on Information Networking 2013 (ICOIN), pp. 714–717, Jan. 2013.

[10] "NETPIE, Network platform for Internet of everything," 2015. [Online]. Available: https://netpie.io/. [Accessed: Jul. 16, 2016].

[11] "Cloudmqtt, A globally distributed MQTT broker". [Online]. Available: https://www.cloudmqtt.com/. [Accessed: Jul. 16, 2016].

[12] I. LogMeIn and A. rights reserved, "Xively by LogMeIn: IoT platform for connected devices" 2003. [Online]. Available: https://www.xively.com/. [Accessed: Jul. 20, 2016].

บรรณานุกรม (ต่อ)

[13] "IBM Bluemix - the cloud platform to accelerate innovation on both sides of the firewall". [Online]. Available: http://www.ibm.com/cloud-computing/bluemix/. [Accessed: Jul. 16, 2016].

[14] S. Al-Fedaghi and F. Mahdi, "Events classification in log audit," International journal of Network Security & Its Applications, vol. 2, no. 2, pp. 58–73, Apr. 2010.

[15] V. Alagar, A. Alsaig, O. Ormandjieva and K. Wan, " Context-based Security and Privacy for Healthcare IoT," 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 122–128, Apr. 2018.

[16] D. Hardt, "RFC 6749 - The OAuth 2.0 Authorization Framework", Tools.ietf.org, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749. [Accessed: Mar. 7, 2018]

[17] Czanik, P. (2018). Reliable IoT event logging with syslog-ng. [Online] Opensource.com. Available: https://opensource.com/article/18/3/logging-iot-events-syslog-ng [Accessed Jun. 25, 2018].

[18] G. Gandelman, L. Cunningham and M. Snyder, "Vital Signs (Body Temperature, Pulse Rate, Respiration Rate, Blood Pressure) - Health Encyclopedia - University of Rochester Medical Center", Urmc.rochester.edu, 2018. [Online]. Available: https://www.urmc.rochester.edu/encyclopedia/content.aspx?ContentTypeID=85&ContentID=P00866. [Accessed: 03- Apr- 2019]

[19] "จำนวนสถานพยาบาลจำแนกตามประเภท", Thcc.or.th, 2015. [Online]. Available: http://thcc.or.th/download/Number%20of%20hospital%20290558.pdf. [Accessed: May. 7, 2019].

[20] A. Sheth, “Transforming Big Data into Smart Data: Deriving value via harnessing Volume, Variety, and Velocity using semantic techniques and technologies,” 2014 IEEE 30th International Conference on Data Engineering, 2014.

[21] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, A. Bouabdallah. “A Systemic Approach for IoT Security”. IEEE. DCOSS, 2013, Boston, United States. pp.351-355, 2013

บรรณานุกรม (ต่อ)

[22] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 59–64, Oct. 2004.

[23] V. C. Sekhar and M. Sarvabhatla, "Security in wireless sensor networks with public key techniques," pp. 1–16, Jan. 2012.

[24] P. Sookpimontree and S. Kungpisdan, "Authentication Protocol on Wireless Sensor Networks Based on Hybrid Cryptographic Technique," International Computer Science and Engineering Conference (ICSEC), 2013.

[25] N. E. Petroulakis, I. G. Askoxylakis, and T. Tryfonas, "Life-logging in smart environments: Challenges and security threats," 2012 IEEE International Conference on Communications (ICC), pp. 5680–5684, Jun. 2012.

[26] Timeanddate.com. (2019). UTC – Coordinated Universal Time. [online] Available : https://www.timeanddate.com/time/aboututc.html [Accessed Jul. 25, 2017].

[27] V. Mishra, “NoSQL: Cassandra Basics,” Beginning Apache Cassandra Development, pp. 1–26, 2014.

[28] J. Kim, “Energy-Efficient Dynamic Packet Downloading for Medical IoT Platforms,” IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 1653–1659, 2015.

[29] W. Johnson, "Predicting log removal performance of membrane systems using in-situ integrity testing", Filtration & Separation, vol. 35, no. 1, pp. 26-29, 1998.

[30] F. Provost and T. Fawcett, “Data Science and its Relationship to Big Data and Data-Driven Decision Making,” Big Data, vol. 1, no. 1, pp. 51–59, 2013.

ภาคผนวก ก
ตัวอย่างข้อมูลทางการแพทย์ที่ส่งออกจากสรรพสิ่งของผู้ป่วย

ตัวอย่างข้อมูลทางการแพทย์ที่ส่งออกจากสรรพสิ่งของผู้ป่วย

จากรูปที่ 28 เป็นตัวอย่างของข้อมูลทางการแพทย์ที่วัดค่าได้จากเซ็นเซอร์ทางการแพทย์ทั้ง 4 ชนิด ได้แก่ เซ็นเซอร์วัดอัตราการเต้นของหัวใจ (Heart Rate) เซ็นเซอร์วัดความดัน (Pressure) เซ็นอเซอร์วัดระดับออกซิเจนในเลือด (O2sat) และเซ็นเซอร์วัดระดับน้ำตาล (Glucose) ด้วยสรรพสิ่งของผู้ป่วยคนที่ 1 ส่งข้อมูลออกไปยังเน็ตพายเพื่อส่งข้อมูลไปยังสรรพสิ่งของแพทย์ผู้ติดตามการรักษาผ่านอินเตอร์เน็ตทุก 0.25 วินาที

```
i,typedata,msg,user,stamp,hn,pub_device,sub_device,location,topic
0,publish,96,Person01,8/8/2018 20:00:16.852,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
1,publish,84,Person01,8/8/2018 20:00:17.129,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
2,publish,94,Person01,8/8/2018 20:00:17.430,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
3,publish,94,Person01,8/8/2018 20:00:17.682,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
4,publish,71,Person01,8/8/2018 20:00:17.983,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
5,publish,76,Person01,8/8/2018 20:00:18.284,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
6,publish,71,Person01,8/8/2018 20:00:18.585,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
7,publish,84,Person01,8/8/2018 20:00:18.837,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
8,publish,90,Person01,8/8/2018 20:00:19.140,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
9,publish,82,Person01,8/8/2018 20:00:19.443,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
10,publish,85,Person01,8/8/2018 20:00:19.745,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
11,publish,86,Person01,8/8/2018 20:00:19.998,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
12,publish,70,Person01,8/8/2018 20:00:20.301,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
13,publish,93,Person01,8/8/2018 20:00:20.604,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
14,publish,77,Person01,8/8/2018 20:00:20.907,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
15,publish,98,Person01,8/8/2018 20:00:21.160,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
16,publish,72,Person01,8/8/2018 20:00:21.463,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
17,publish,74,Person01,8/8/2018 20:00:21.766,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
18,publish,70,Person01,8/8/2018 20:00:22.069,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
19,publish,74,Person01,8/8/2018 20:00:22.322,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
20,publish,77,Person01,8/8/2018 20:00:22.625,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
21,publish,74,Person01,8/8/2018 20:00:22.928,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
22,publish,92,Person01,8/8/2018 20:00:23.231,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
23,publish,89,Person01,8/8/2018 20:00:23.495,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
24,publish,84,Person01,8/8/2018 20:00:23.798,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
25,publish,93,Person01,8/8/2018 20:00:24.101,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
26,publish,100,Person01,8/8/2018 20:00:24.404,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
27,publish,82,Person01,8/8/2018 20:00:24.657,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
28,publish,81,Person01,8/8/2018 20:00:24.960,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
29,publish,78,Person01,8/8/2018 20:00:25.263,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
30,publish,79,Person01,8/8/2018 20:00:25.566,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
31,publish,83,Person01,8/8/2018 20:00:25.828,6000001,Portable Monitoring A01,DoctorPC,Room301,glucose
32,publish,74,Person01,8/8/2018 20:00:26.131,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
33,publish,75,Person01,8/8/2018 20:00:26.434,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
34,publish,90,Person01,8/8/2018 20:00:26.737,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
35,publish,74,Person01,8/8/2018 20:00:26.990,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
36,publish,73,Person01,8/8/2018 20:00:27.293,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
37,publish,93,Person01,8/8/2018 20:00:27.596,6000001,Portable Monitoring A01,DoctorPC,Room301,heartrate
38,publish,94,Person01,8/8/2018 20:00:27.900,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
39,publish,86,Person01,8/8/2018 20:00:28.154,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
40,publish,70,Person01,8/8/2018 20:00:28.457,6000001,Portable Monitoring A01,DoctorPC,Room301,o2sat
41,publish,79,Person01,8/8/2018 20:00:28.760,6000001,Portable Monitoring A01,DoctorPC,Room301,pressure
```

รูปที่ 28 ตัวอย่างข้อมูลทางการแพทย์ที่ส่งออกจากสรรพสิ่งของผู้ป่วย

ภาคผนวก ข
ตัวอย่างส่วนข้อมูลธุรกรรมสำหรับเน็ตพายในฐานข้อมูล

```
id,nouns,datasize,location,netpie_stamp,patient,pub_device,pub_stamp,sub_device,sub_stamp,topic,username
222731,34518,2,Room318,2018-08-09 06:54:59.159+0000,6000018,Portable Monitoring A18,2018-08-09 06:54:24.068+0000,DoctorPC,2018-08-09 06:54:59.159+0000,heartrate,Person18
222732,70236,2,Room312,2018-08-09 06:54:59.414+0000,6000012,Portable Monitoring A12,2018-08-09 06:54:20.978+0000,DoctorPC,2018-08-09 06:54:59.414+0000,heartrate,Person12
222733,34550,2,Room317,2018-08-09 06:54:59.680+0000,6000017,Portable Monitoring A17,2018-08-09 06:54:20.508+0000,DoctorPC,2018-08-09 06:54:59.680+0000,pressure,Person17
222734,94095,2,Room307,2018-08-09 06:54:59.922+0000,6000007,Portable Monitoring A07,2018-08-09 06:54:22.626+0000,DoctorPC,2018-08-09 06:54:59.922+0000,pressure,Person07
222735,129838,2,Room304,2018-08-09 06:55:00.173+0000,6000004,Portable Monitoring A04,2018-08-09 06:54:21.324+0000,DoctorPC,2018-08-09 06:55:00.173+0000,heartrate,Person04
222736,46449,2,Room316,2018-08-09 06:55:00.429+0000,6000016,Portable Monitoring A16,2018-08-09 06:54:19.337+0000,DoctorPC,2018-08-09 06:55:00.429+0000,glucose,Person16
222737,82196,2,Room309,2018-08-09 06:55:00.695+0000,6000009,Portable Monitoring A09,2018-08-09 06:54:19.312+0000,DoctorPC,2018-08-09 06:55:00.695+0000,o2sat,Person09
222738,22626,3,Room319,2018-08-09 06:55:00.933+0000,6000019,Portable Monitoring A19,2018-08-09 06:54:17.963+0000,DoctorPC,2018-08-09 06:55:00.933+0000,heartrate,Person19
222739,58313,2,Room313,2018-08-09 06:55:01.190+0000,6000013,Portable Monitoring A13,2018-08-09 06:54:21.010+0000,DoctorPC,2018-08-09 06:55:01.190+0000,o2sat,Person13
222740,58383,2,Room314,2018-08-09 06:55:01.441+0000,6000014,Portable Monitoring A14,2018-08-09 06:54:22.495+0000,DoctorPC,2018-08-09 06:55:01.441+0000,o2sat,Person14
222741,46489,2,Room315,2018-08-09 06:55:01.699+0000,6000015,Portable Monitoring A15,2018-08-09 06:54:20.472+0000,DoctorPC,2018-08-09 06:55:01.699+0000,pressure,Person15
222742,106017,2,Room305,2018-08-09 06:55:01.948+0000,6000005,Portable Monitoring A05,2018-08-09 06:54:22.930+0000,DoctorPC,2018-08-09 06:55:01.948+0000,heartrate,Person05
222743,22635,2,Room320,2018-08-09 06:55:02.203+0000,6000020,Portable Monitoring A20,2018-08-09 06:54:20.222+0000,DoctorPC,2018-08-09 06:55:02.203+0000,o2sat,Person20
222744,70295,2,Room311,2018-08-09 06:55:02.456+0000,6000011,Portable Monitoring A11,2018-08-09 06:54:20.891+0000,DoctorPC,2018-08-09 06:55:02.456+0000,pressure,Person11
222745,82196,2,Room310,2018-08-09 06:55:02.710+0000,6000010,Portable Monitoring A10,2018-08-09 06:54:19.137+0000,DoctorPC,2018-08-09 06:55:02.710+0000,heartrate,Person10
222746,105974,2,Room306,2018-08-09 06:55:02.966+0000,6000006,Portable Monitoring A06,2018-08-09 06:54:17.912+0000,DoctorPC,2018-08-09 06:55:02.966+0000,pressure,Person06
222747,129842,2,Room302,2018-08-09 06:55:03.217+0000,6000002,Portable Monitoring A02,2018-08-09 06:54:20.014+0000,DoctorPC,2018-08-09 06:55:03.217+0000,heartrate,Person02
222748,117893,2,Room303,2018-08-09 06:55:03.471+0000,6000003,Portable Monitoring A03,2018-08-09 06:54:21.884+0000,DoctorPC,2018-08-09 06:55:03.471+0000,heartrate,Person03
222749,94068,2,Room308,2018-08-09 06:55:03.725+0000,6000008,Portable Monitoring A08,2018-08-09 06:54:19.681+0000,DoctorPC,2018-08-09 06:55:03.725+0000,pressure,Person08
222750,34519,2,Room318,2018-08-09 06:55:03.979+0000,6000018,Portable Monitoring A18,2018-08-09 06:54:24.371+0000,DoctorPC,2018-08-09 06:55:03.979+0000,pressure,Person18
222751,70237,2,Room312,2018-08-09 06:55:04.234+0000,6000012,Portable Monitoring A12,2018-08-09 06:54:21.280+0000,DoctorPC,2018-08-09 06:55:04.234+0000,heartrate,Person12
222752,34551,2,Room317,2018-08-09 06:55:04.491+0000,6000017,Portable Monitoring A17,2018-08-09 06:54:20.810+0000,DoctorPC,2018-08-09 06:55:04.491+0000,pressure,Person17
222753,94096,2,Room307,2018-08-09 06:55:04.741+0000,6000007,Portable Monitoring A07,2018-08-09 06:54:22.928+0000,DoctorPC,2018-08-09 06:55:04.741+0000,glucose,Person07
222754,129839,2,Room304,2018-08-09 06:55:04.994+0000,6000004,Portable Monitoring A04,2018-08-09 06:54:21.627+0000,DoctorPC,2018-08-09 06:55:04.994+0000,pressure,Person04
222755,46450,2,Room316,2018-08-09 06:55:05.246+0000,6000016,Portable Monitoring A16,2018-08-09 06:54:19.639+0000,DoctorPC,2018-08-09 06:55:05.246+0000,heartrate,Person16
222756,82197,2,Room309,2018-08-09 06:55:05.501+0000,6000009,Portable Monitoring A09,2018-08-09 06:54:19.613+0000,DoctorPC,2018-08-09 06:55:05.501+0000,o2sat,Person09
222757,22627,2,Room319,2018-08-09 06:55:05.754+0000,6000019,Portable Monitoring A19,2018-08-09 06:54:18.265+0000,DoctorPC,2018-08-09 06:55:05.754+0000,o2sat,Person19
222758,58314,2,Room313,2018-08-09 06:55:06.008+0000,6000013,Portable Monitoring A13,2018-08-09 06:54:21.312+0000,DoctorPC,2018-08-09 06:55:06.008+0000,pressure,Person13
222759,58384,3,Room314,2018-08-09 06:55:06.262+0000,6000014,Portable Monitoring A14,2018-08-09 06:54:22.798+0000,DoctorPC,2018-08-09 06:55:06.262+0000,heartrate,Person14
222760,46490,2,Room315,2018-08-09 06:55:06.521+0000,6000015,Portable Monitoring A15,2018-08-09 06:54:20.774+0000,DoctorPC,2018-08-09 06:55:06.521+0000,heartrate,Person15
222761,106018,2,Room305,2018-08-09 06:55:06.770+0000,6000005,Portable Monitoring A05,2018-08-09 06:54:23.232+0000,DoctorPC,2018-08-09 06:55:06.770+0000,o2sat,Person05
222762,22636,2,Room320,2018-08-09 06:55:07.023+0000,6000020,Portable Monitoring A20,2018-08-09 06:54:20.525+0000,DoctorPC,2018-08-09 06:55:07.023+0000,heartrate,Person20
222763,70296,2,Room311,2018-08-09 06:55:07.278+0000,6000011,Portable Monitoring A11,2018-08-09 06:54:21.193+0000,DoctorPC,2018-08-09 06:55:07.278+0000,glucose,Person11
222764,82197,2,Room310,2018-08-09 06:55:07.532+0000,6000010,Portable Monitoring A10,2018-08-09 06:54:19.439+0000,DoctorPC,2018-08-09 06:55:07.532+0000,pressure,Person10
222765,105975,2,Room306,2018-08-09 06:55:07.785+0000,6000006,Portable Monitoring A06,2018-08-09 06:54:18.215+0000,DoctorPC,2018-08-09 06:55:07.785+0000,glucose,Person06
222766,129843,2,Room302,2018-08-09 06:55:08.040+0000,6000002,Portable Monitoring A02,2018-08-09 06:54:20.317+0000,DoctorPC,2018-08-09 06:55:08.040+0000,heartrate,Person02
222767,117894,2,Room303,2018-08-09 06:55:08.295+0000,6000003,Portable Monitoring A03,2018-08-09 06:54:22.187+0000,DoctorPC,2018-08-09 06:55:08.295+0000,heartrate,Person03
222768,94069,2,Room308,2018-08-09 06:55:08.550+0000,6000008,Portable Monitoring A08,2018-08-09 06:54:19.983+0000,DoctorPC,2018-08-09 06:55:08.550+0000,o2sat,Person08
222769,34520,2,Room318,2018-08-09 06:55:08.804+0000,6000018,Portable Monitoring A18,2018-08-09 06:54:24.674+0000,DoctorPC,2018-08-09 06:55:08.804+0000,glucose,Person18
222770,70238,2,Room312,2018-08-09 06:55:09.058+0000,6000012,Portable Monitoring A12,2018-08-09 06:54:21.583+0000,DoctorPC,2018-08-09 06:55:09.058+0000,glucose,Person12
222771,34552,2,Room317,2018-08-09 06:55:09.318+0000,6000017,Portable Monitoring A17,2018-08-09 06:54:21.112+0000,DoctorPC,2018-08-09 06:55:09.318+0000,pressure,Person17
222772,94097,2,Room307,2018-08-09 06:55:09.570+0000,6000007,Portable Monitoring A07,2018-08-09 06:54:23.231+0000,DoctorPC,2018-08-09 06:55:09.570+0000,glucose,Person07
222773,129840,3,Room304,2018-08-09 06:55:09.821+0000,6000004,Portable Monitoring A04,2018-08-09 06:54:21.929+0000,DoctorPC,2018-08-09 06:55:09.821+0000,glucose,Person04
```

รูปที่ 29 ตัวอย่างข้อมูลธุรกรรมในฐานข้อมูล RowLog

```
id,datestamp,topic,username,event_detail,pub_device,sub_device,type
158240,2018-08-09 01:59:57.480+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158241,2018-08-09 01:59:57.833+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158242,2018-08-09 01:59:58.119+0000,Room314,Person14,{6000014} Portable Monitoring A14 -> DoctorPC is new connection!,Portable Monitoring A14,DoctorPC,connect
158243,2018-08-09 02:00:19.008+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158244,2018-08-09 02:00:19.071+0000,Room301,Person01,{6000001} Delay Packet 1.3 Second ,Portable Monitoring A01,DoctorPC,delay
158245,2018-08-09 02:00:20.074+0000,Room313,Person13,{6000013} Portable Monitoring A13 -> DoctorPC is new connection!,Portable Monitoring A13,DoctorPC,connect
158246,2018-08-09 02:02:57.150+0000,Room310,Person10,{6000010} Delay Packet 1.354 Second ,Portable Monitoring A10,DoctorPC,delay
158247,2018-08-09 02:02:57.156+0000,Room306,Person06,{6000006} Delay Packet 1.354 Second ,Portable Monitoring A06,DoctorPC,delay
158248,2018-08-09 02:02:57.391+0000,Room305,Person05,{6000005} Delay Packet 1.354 Second ,Portable Monitoring A05,DoctorPC,delay
158249,2018-08-09 02:02:57.637+0000,Room314,Person14,{6000014} Delay Packet 1.354 Second ,Portable Monitoring A14,DoctorPC,delay
158250,2018-08-09 02:02:57.637+0000,Room300,Person00,{6000000} Delay Packet 1.3 Second ,Portable Monitoring A00,DoctorPC,delay
158251,2018-08-09 02:02:57.895+0000,Room307,Person07,{6000007} Delay Packet 1.354 Second ,Portable Monitoring A07,DoctorPC,delay
158252,2018-08-09 02:02:58.141+0000,Room311,Person11,{6000011} Delay Packet 1.354 Second ,Portable Monitoring A11,DoctorPC,delay
158253,2018-08-09 02:02:58.396+0000,Room302,Person02,{6000002} Delay Packet 1.355 Second ,Portable Monitoring A02,DoctorPC,delay
158254,2018-08-09 02:02:58.650+0000,Room309,Person09,{6000009} Delay Packet 1.355 Second ,Portable Monitoring A09,DoctorPC,delay
158255,2018-08-09 02:02:58.748+0000,Room301,Person01,{6000001} Delay Packet 1.3 Second ,Portable Monitoring A01,DoctorPC,delay
158256,2018-08-09 02:02:58.904+0000,Room301,Person01,{6000001} Delay Packet 1.370 Second ,Portable Monitoring A01,DoctorPC,delay
158257,2018-08-09 02:02:59.159+0000,Room308,Person08,{6000008} Delay Packet 1.354 Second ,Portable Monitoring A08,DoctorPC,delay
158258,2018-08-09 02:02:59.421+0000,Room303,Person03,{6000003} Delay Packet 1.355 Second ,Portable Monitoring A03,DoctorPC,delay
158259,2018-08-09 02:02:59.672+0000,Room312,Person12,{6000012} Delay Packet 1.355 Second ,Portable Monitoring A12,DoctorPC,delay
158260,2018-08-09 02:02:59.929+0000,Room304,Person04,{6000004} Delay Packet 1.355 Second ,Portable Monitoring A04,DoctorPC,delay
158261,2018-08-09 02:02:59.984+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158262,2018-08-09 02:03:00.172+0000,Room313,Person13,{6000013} Delay Packet 1.355 Second ,Portable Monitoring A13,DoctorPC,delay
158263,2018-08-09 02:03:01.054+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158264,2018-08-09 02:03:02.298+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158265,2018-08-09 02:03:03.380+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158266,2018-08-09 02:03:04.640+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158267,2018-08-09 02:03:05.692+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158268,2018-08-09 02:03:06.651+0000,Room300,Person00,{6000000} Delay Packet 1.3 Second ,Portable Monitoring A00,DoctorPC,delay
158269,2018-08-09 02:03:08.022+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158270,2018-08-09 02:03:09.311+0000,Room300,Person00,{6000000} Delay Packet 1.5 Second ,Portable Monitoring A00,DoctorPC,delay
158271,2018-08-09 02:03:10.327+0000,Room300,Person00,{6000000} Delay Packet 1.378 Second ,Portable Monitoring A00,DoctorPC,delay
158272,2018-08-09 02:03:10.406+0000,Room301,Person01,{6000001} Delay Packet 1.3 Second ,Portable Monitoring A01,DoctorPC,delay
158273,2018-08-09 02:03:11.630+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158274,2018-08-09 02:03:12.672+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158275,2018-08-09 02:03:13.663+0000,Room300,Person00,{6000000} Delay Packet 1.3 Second ,Portable Monitoring A00,DoctorPC,delay
158276,2018-08-09 02:03:15.005+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158277,2018-08-09 02:03:15.995+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158278,2018-08-09 02:03:17.052+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158279,2018-08-09 02:03:18.320+0000,Room300,Person00,{6000000} Delay Packet 1.4 Second ,Portable Monitoring A00,DoctorPC,delay
158280,2018-08-09 02:03:19.328+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
158281,2018-08-09 02:03:20.357+0000,Room300,Person00,{6000000} Delay Packet 1.3 Second ,Portable Monitoring A00,DoctorPC,delay
158282,2018-08-09 02:03:21.641+0000,Room301,Person01,{6000001} Delay Packet 1.4 Second ,Portable Monitoring A01,DoctorPC,delay
```

รูปที่ 30 ตัวอย่างข้อมูลธุรกรรมในฐานข้อมูล NetpieLog

```
id,username,pub_device,sub_device,timediff,u_date
1,Person00,Portable Monitoring A00,DoctorPC,23,2018-08-08 13:44:55.832+0000
74106,Person01,Portable Monitoring A01,DoctorPC,25,2018-08-08 20:00:01.703+0000
74109,Person04,Portable Monitoring A04,DoctorPC,26,2018-08-08 20:00:02.360+0000
74113,Person02,Portable Monitoring A02,DoctorPC,25,2018-08-08 20:00:02.832+0000
110665,Person03,Portable Monitoring A03,DoctorPC,27,2018-08-08 21:00:01.738+0000
159127,Person05,Portable Monitoring A05,DoctorPC,28,2018-08-08 21:59:59.656+0000
159202,Person06,Portable Monitoring A06,DoctorPC,24,2018-08-08 22:00:04.020+0000
231380,Person07,Portable Monitoring A07,DoctorPC,29,2018-08-08 22:59:59.163+0000
231450,Person08,Portable Monitoring A08,DoctorPC,25,2018-08-08 23:00:02.153+0000
326917,Person09,Portable Monitoring A09,DoctorPC,26,2018-08-09 00:00:01.054+0000
326932,Person10,Portable Monitoring A10,DoctorPC,25,2018-08-09 00:00:01.568+0000
446807,Person12,Portable Monitoring A12,DoctorPC,27,2018-08-09 00:59:59.262+0000
446829,Person11,Portable Monitoring A11,DoctorPC,27,2018-08-09 00:59:59.771+0000
590458,Person14,Portable Monitoring A14,DoctorPC,29,2018-08-09 01:59:57.862+0000
591405,Person13,Portable Monitoring A13,DoctorPC,28,2018-08-09 02:00:19.841+0000
757841,Person15,Portable Monitoring A15,DoctorPC,28,2018-08-09 02:59:56.505+0000
758018,Person16,Portable Monitoring A16,DoctorPC,27,2018-08-09 03:00:00.014+0000
949143,Person18,Portable Monitoring A18,DoctorPC,32,2018-08-09 03:59:55.352+0000
949340,Person17,Portable Monitoring A17,DoctorPC,28,2018-08-09 03:59:58.791+0000
1100956,Person20,Portable Monitoring A20,DoctorPC,28,2018-08-09 04:59:59.091+0000
1101081,Person19,Portable Monitoring A19,DoctorPC,26,2018-08-09 05:00:01.118+0000
```

รูปที่ 31 ตัวอย่างข้อมูลธุรกรรมในฐานข้อมูล ConnectDB

ภาคผนวก ค
งานวิจัยที่ได้รับการตีพิมพ์

2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE)

Logging mechanism for Internet of Things: A Case Study of Patient Monitoring System

Piyawat Maneenual
Management of Information Technology
Prince of Songkla University
Hat Yai, Songkhla, Thailand
5810121044@email.psu.ac.th

Sangsuree Vasupongayya
Department of Computer Engineering
Prince of Songkla University
Hat Yai, Songkhla, Thailand
sangsuree.v@psu.ac.th

***Abstract*— A logging mechanism for NETPIE in the patient medical device monitoring task is proposed in this work. The logging mechanism aims to collect the communication log between things and NETPIE such that any communication issue or any attack can be detected. There are three main components in the proposed logging mechanism including the raw data, the analysis part, and the final result. The raw data is approximately less than 256 bytes per each communication. The raw data will be analyzed to generate the final result which will contain only the suspicion events including communication issue (i.e., packet lost) and possible attack (i.e., reply attack). The cost of the proposed mechanism includes an extra communication per each communication path and a storage space for the collected data at NETPIE, and things.**

Keywords—NETPIE, packet lost, log analysis, Apache Cassandra

I. Introduction

NETPIE [1] is a network platform for Internet of everything developed by a group of researchers at NECTEC, Thailand. Developers can use the network platform provided by NETPIE to connect things and to communicate between things. The main advantage of NETPIE includes ease of uses and a real-time feature. By installing the NETPIE library on the support devices, the platform will allow things to be communicated with each other within a defined scope. The security of NETPIE is achieved through the use of three pieces of information including APPID, KEY, and SECRET. APPID is the name of the application while the KEY and the SECRET are the two specific information of your applications that must be kept secret. The platform will generate a token so that things under an application with the correct information can communicate with each other.

Nowadays, the number of people own wearable devices for collecting their health related information has been increasing both inside the healthcare facility and at home in order to analyze the patient behavior [2-3]. The network platform for Internet of everything such as NETPIE can be utilized for such situations. However, the security and the privacy of the user data can be a big issue [4-10].

Logging is a crucial part of information security [11-14]. Log data allows all parties to analyze the system in order to verify a valid transaction or to detect a suspicion activity in the system. For a dense communication environment such as NETPIE, however, a logging system can significantly increase the number of messages inside the system. This work aims to propose a logging mechanism for home-stay patients and medical-facility-stay patients. Both types of patients are connected with some medical monitoring devices that are sending the information via NETPIE over a public Internet.

The remaining of the paper is organized as follow. Section II lists the patient monitoring system requirements while Section III provides the proposed logging mechanism. Section IV shows the experimental results while Section V gives that discussions. Lastly, Section VI provides the conclusion.

II. Patient Monitoring System Requirements

Typical patient monitoring devices in a healthcare facility include heart rate, Electrocardiograph (ECG or EKG), pulse, body temperature, blood pressure, sugar level, infusion pump, and syringe pump. Most basic medical monitoring devices send out the data at the rate of 1 second and the data size is less than 1KB [15]. The fact is true for most basic medical monitoring devices, except high frequency devices such as EKG and Electroencephalography (EEG). Thus, Internet of Things (IoT) is better applied on low frequency response devices such as body temperature, pulse, blood pressure, sugar level and respiratory rate.

In addition to the healthcare facility setting, there are patients of non-communicable diseases (NCDs) which are usually home-stay patient. These patients can also utilize some patient monitoring devices. World health organization (WHO) classifies NCDs as one of the major cause of deaths. For example, 63% of deaths occurred in 2009 were caused by NCDs. In Thailand, 73% of deaths occurred in 2009 were caused by NCDs [16]. The top six diseases in NCDs that cause the most deaths include diabetes mellitus, cardiovascular and cerebrovascular disease, emphysema, cancer, hypertension and obesity. Typical patient's monitory devices used by NCDs patients include heart rate, blood pressure, respiratory rate and sugar level.

III. Proposed Logging System

The proposed logging system is designed based on the real usage scenarios presented in subsection A. The architecture of the proposed logging mechanism is presented in subsection B.

A. Scenarios

All communications under NETPIE can be grouped into 4 scenarios including new-connection, complete, lost-before-NETPIE, and lost-after-NETPIE. The details of each scenario is as follow.

- New-connection scenario means that the device is connected to the system for the first time. In this case, a database of device connections maybe used to collect the device that connects with the system. However, a database of connection could delay the initial connection process of the device. Fig. 1 shows

978–1–5386–5538–2/18/$31.00 ©2018 IEEE

the New-connection situation. Fig. 2 shows the connection information collected by the system.

- Complete scenario means that the devices successfully send and receive their data. Fig. 3 shows the complete scenario. In this case, the source device knows what has been sent and the destination device must receive the data in order to conclude that the communication is completed. Thus, the log data will show both the source site and the destination site.
- Lost-before-NETPIE scenario means that the device is sending the data but the data is lost between the device and NETPIE. Fig. 4 shows the Lost-before-NETPIE scenario. In this case, the logging mechanism at NETPIE will not have any information. Thus, the logging mechanism must be implemented at the source device in order to record the sending event from the source.
- Lost-after-NETPIE scenario means that the source device is successfully sending the data to the NETPIE. However, the data is not received at the destination device as shown in Fig. 5. In this case, the logging mechanism at NETPIE does contain the sending information but the data is not reaching the destination. Thus, the logging mechanism must be implemented at the destination device in order to record the receiving event from the destination.

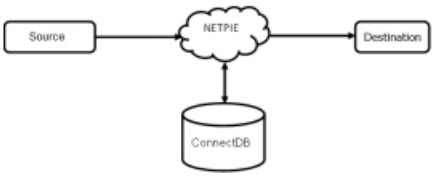


Fig. 1. New-connection scenario

Source	Destination	Time
DeviceA	DeviceB	09/04/2560 01:36
DeviceC	DeviceB	02/04/2560 01:20
DeviceB	DeviceD	03/04/2560 04:48

Fig. 2. Sample connection information collected by the proposed system

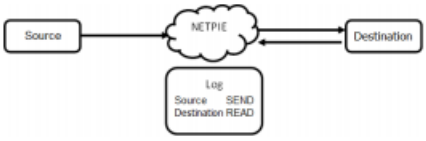


Fig. 3. Complete scenario

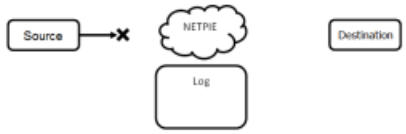


Fig. 4. Lost-before-NETPIE scenario

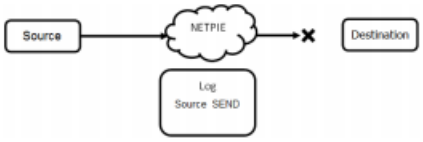


Fig. 5. Lost-after-NETPIE scenario

B. Architecture of the Proposed Logging Mechanism

According to the four communication scenarios of NETPIE framework presented in the previous section, Fig. 6 shows the architecture of the proposed logging mechanism. There is a logging mechanism on each device in order to collect the send or receive event. The log framework includes the main logging data (RawLog), the connection data (ConnectDB), and the analysis part (NetpieLog).

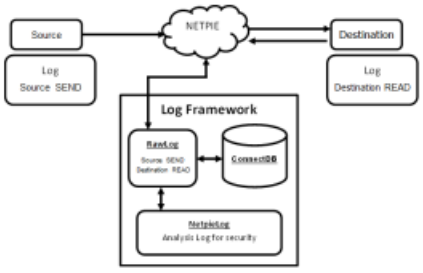


Fig. 6. Atchitecture of the Proposed logging mechanism

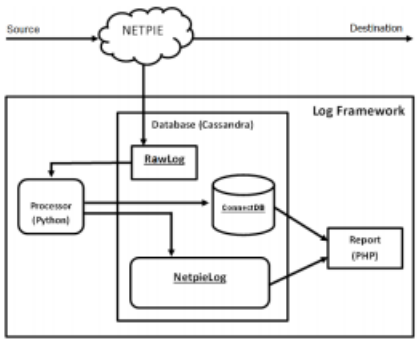


Fig. 7. Proposed logging mechanism details

Inside the main logging mechanism, there are three-step processes as shown in Fig. 7. RawLog, NetpieLog and ConnectDB are stored on Apache Cassandra [17-18]. The pre-processing is written in Python and the Report is produced as a web format using PHP. When the data is sent from the source to the destination, the logging data will be stored on the RawLog before it is being pre-process in order to be stored on the ConnectDB for the New-connection scenario and on the NetpieLog. However, only an abnormal scenario such as the Lost-before-NETPIE or the Lost-after-NETPIE event will be stored on the NetpieLog. The Report will be generated from the information stored on the ConnectDB and the NetpieLog.

C. Log Format

For any IoT communication, the data is dense by nature. Thus, the logging mechanism must select necessary information to be collected in order to reduce the volume of the stored data. According to the proposed mechanism architecture presented previously, there are two sets of data to be collected including the RawLog and the NetpieLog. The RawLog data contains 13 fields as shown in Table I. The NetpieLog data contains 8 fields as shown in Table II.

TABLE I. RAWLOG DATA

Field	Data Collected
ID	Event ID
order	Order id of the packet in the event
topic	Topic of the event
source_device	Source device information
des_device	Destination device information
source_stamp	Date/time the data is sent from the source
des_stamp	Date/time the data is received by the destination
netpie_stamp	Date/time the data reached NETPIE from the source
netpie_sent	Date/time the data is sent by NETPIE to the destination
username	The user who initiates the communication
patient	Information of patient
location	Location of the communication
datasize	Size of the data in bytes

The RawLog data is the raw data collected from the communication. The raw data will then be processed by the pre-processor in order to extract the abnormal event to be recorded on the NetpieLog, while the new connection event will be recorded on the ConnectDB.

The NetpieLog data is a post-processed data from the raw data stored on the RawLog. This way, the pre-processing of the data can be delayed if the communication performance is at a critical level. Therefore, the proposed logging mechanism will be able to make way to support a peak communication level when it is needed.

TABLE II. NETPIELOG DATA

Field	Data Collected
ID	Event ID
DateStamp	Date/time the data is generated
Username	User who initiates the communication
source_device	Source device information
dest_device	Destination device information
Topic	Topic of the event
Detail	Event details
Type	▪ Warning : packet lost issues ▪ Alert : possible attacks

D. Log Analysis

The communication starts from the source device sending its message together with the message order id to NETPIE. The RawLog will record the sending of a message from the source device. Next, NETPIE will forward the message to the destination device. If the destination device completely received the message, the device will send the notification to NETPIE so that NETPIE can record the receiving of a message from the destination device. This case is the complete scenario as shown in Fig. 3. Thus, the data from the RawLog can be analyzed in order to follow the path of each packet. If the whole path is presented in the RawLog then the packet is sent successfully and completely.

However, the communication over the RawLog can be affected by many factors. To analyze the Lost-before-NETPIE scenario (shown in Fig. 4), the data in the RawLog of each source device will be checked in the order that the data is recorded inside the RawLog. If the difference of the order id of the current and the previous messages is larger than 1, there is a message lost. However, if the last packet is the message that is lost, it cannot be detected by this method. Therefore, the local log at the source device can solve such issues because the local log at the source device can be compared with the RawLog in order to analyze the last packet lost case.

To analyze the Lost-after-NETPIE scenario (shown in Fig. 5), the data in the RawLog of each destination device will be checked in the order that the data is recorded inside the RawLog. If there is no notification of receiving of any message, it is possible that the message is lost. However, the message might reach the destination device but the notification of receiving of message is lost instead. This way, the local log at the destination device can solve such issues because the local log at the destination device can be compared with the data recorded on the RawLog in order to analyze such issue.

Another possible attack that can be analyzed from the data recorded on the RawLog is the replay attack. That is, any difference of the message order id that is less than 1 indicates the possibility of the replay attack. This event must be investigated fast such as sending an alert to the administrator [1]. The event will be recorded on the NetpieLog as Alert while the Lost-before-NETPIE and the Lost-after-NETPIE event will be recorded on the NetpieLog as Warning. The normal event will be omitted from the NetpieLog in order to save the space. However, the RawLog

data will not be deleted but the data must be moved out to another storage after the data analysis is completed.

IV. Experimental Results

To evaluate the possibility of using NETPIE for patient monitoring tasks, we conduct a preliminary experiment on the connection performance by sending the data from the Internet to NETPIE and recording the performance. Fig. 8 shows the patient monitoring scenario in the experiment. According to the scenario presented in Fig. 8, it is possible that the logging mechanism must be able to handle both the data from home-stay devices and healthcare facility devices. Three basic experiments to evaluate the current environment are conducted in this work.

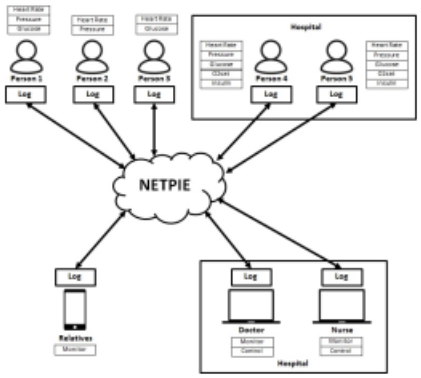


Fig. 8. Patient monitoring scenario

A. Varying the Number of Monitoring Devices

The first experiment focuses on the number of monitoring and displaying devices. According to the scenario presented in Fig. 8, there are multiple monitoring devices that can send their data to a single display device. Thus, the first experiment varies the number of monitoring devices from 1, 2, 4, 8, and 16 and fixes the number of displaying device to 1. The maximum number of monitoring devices in a healthcare facility is 10. Therefore, 16 devices in this experiment is a large enough number. The data of 64B is sent from the monitoring devices in Songkhla province of Thailand via the common Internet provider to the NETPIE server located in the middle part of Thailand and back to the displaying device in Songkhla province. Each monitoring device will send its data at the rate of 1 packet per second. The packet size is 64B. The data is sent for 10 hours.

The resulting communication time is presented in Table III. The communication time is the time when the data is sent until the time when the data is received at the displaying device. According to the data presented in Table III, all five cases can successfully send and receive the data within 1s and there is no data lost. Unexpectedly, the average communication time of 8:1 case is higher than that of the 16:1 while the maximum communication time of 8:1 is lower than that of the 16:1 case. Thus, this result might be an effect of the underlying traffic on the communication channel.

TABLE III. Communication Time of Various Number of Monitoring Devices

#sources	Time (ms)		
	average	*maximum*	*minimum*
16	66	375	62
8	75	265	62
4	66	281	62
2	65	250	62
1	66	234	62

Next, the monitoring device will send the data at a higher frequency.

B. Varying the data sending rate

The second experiment focuses on the rate at which the monitoring device sends its data. According to the literature [15], typical monitoring devices send the data at the rate of 1s. Thus, this experiment varies the rate from 1s, 500ms, 250ms, and 125ms. There are 16 monitoring devices and 1 display device. The data size is 64B. The data is sent for 10 hours.

The resulting communication rate is shown in Table IV. At the 125ms rate, 88.6% of data is lost while there is no data lost at 250ms, 500ms and 1s rates. Interestingly, the maximum communication time of 250ms (282ms) is smaller than that of the 1s (375ms) while the average communication time of 250ms (74ms) is larger than that of the 1s (66ms). Moreover, both the average and the maximum communication time of 250ms are better than its counterpart of 500ms.

TABLE IV. Communication Time of Various Data Sending Rate

Rate	%loss	Time (ms)		
		average	*max*	*min*
1s	0%	66	375	62
500ms	0%	76	391	62
250ms	0%	74	282	62
125ms	88.6%	593	4,930	62

Next, the data packet size will be increased in order to analyze the performance.

C. Varying the data size

The third experiment focuses on the size of the data packet sent by the monitoring devices. According to the literature [15], typical monitoring devices send the data of size less than 1KB. Thus, this experiment varies the size of the data from 64B, 128B, 256B, 512B, 1KB, 2KB, 4KB, 8KB and 16KB. There are 16 monitoring devices and 1 display device. Each monitoring device send 1 packet every 250ms. The data is sent for 10 hours.

The resulting communication time is presented in Table V. According to the average time shown in Table V, the round trip time will exceed 1s when the data size is larger than 4KB.

TABLE V. COMMUNICATION TIME OF VARIOUS DATA SIZE

Data size	Average time (ms)
64B	71.25
128B	72.44
256B	73.56
512B	76.77
1KB	89.31
2KB	99.13
4KB	191.44
8KB	1,244.38
16KB	4,954.56

V. DISCUSSIONS

To achieve the logging mechanism as proposed, there is a time and space requirement. Section A gives a discussion on an extra communication cost while Section B gives a discussion on an extra storage cost. In addition, Section C gives a discussion on an extra computational cost.

A. Communication Cost

The communication cost can be classified into two cases. First, the one-way communication means that the source device is sending the information to the destination device and the destination device does not send any response back to the source device. For this case, the proposed logging mechanism requires an extra packet for every communication. That is, the notification of receiving the message sending by the destination device once the packet is completely received. Under the current NETPIE communication environment (i.e., without any logging mechanism), each communication will consist of 2 parts, including the packet from the source to NETPIE and the packet from NETPIE to the destination. Under the proposed system, there is an extra packet which is the notification of packet receiving at the destination to be sent to the proposed logging mechanism.

Second, the two-way communication means that the source device is sending the information to the destination device and the destination device must send some response back to the source device. For this case, the proposed logging mechanism will track the communication as two communication from different sources. However, the event ID and the order ID from the RawLog will be used for identifying the whole communication path from the source to the destination and the destination back to the source.

B. Storage Cost

The storage requirement consists of two parts. First, the storage space is required at the NETPIE in order to store the ConnectDB data, the RawLog data and the NetpieLog data. Each record on the RawLog and the NetpieLog takes approximately less than 256 bytes, while each record on the ConnectDB takes approximately 64 bytes. Therefore, the space requirement is achievable with the current storage technology.

Second, the storage space at the source device and the destination device in order to store the local log data. This requirement is also an extra requirement. The requirement can be achieved by several methods such as a storage point for many things in the same area in order to reduce the space requirement on the actual devices. Since each thing is a patient monitoring device which may be connected to the Internet via a gateway point. The gateway point can be used as the local log storage.

C. Computational Cost

The computational cost of the proposed logging mechanism is an extra cost because the RawLog must be analyzed to extract the event details of each event in the system. In addition, there is an additional cost of transferring any required local log data from the local gateway storage to the main analysis framework when it is needed. This case will require when the RawLog data cannot resolve the issue such as the last packet lost discussed previously. However, this event will not be a regular activity since the information from the local gateway storage will be needed in some specific cases in order to verifying the suspicion events detected by the main analysis framework as described previously.

VI. CONCLUSIONS

A logging mechanism for Internet of things on the patient medical device monitoring applications is proposed in this work. The underlining framework is NETPIE which is a network communication framework for Internet of everything. The logging mechanism aims to capture four basic scenarios of communication including new, complete, Lost-before-NETPIE and Lost-after-NETPIE scenarios. The format of the raw data, namely RawLog, to be collected at the main logging framework is described. The RawLog data will be analyzed in order to generate the result, namely NetpieLog. Only communication issue and a possible attack will be recorded in the NetpieLog to reduce the space requirement. There is a local log at each thing in order to further analyze some situations. However, the local log data is not required to be checked until it is an issue in order to reduce the time and communication cost created by the logging mechanism.

Based on the literatures [15], the data must be completely sent and received every second and the data size of 4KB is large enough to send the data from the patient monitoring devices. Our preliminary results show that the data can be sent at the rate of 1 packet every 250 milliseconds from 16 devices to one single destination. The evaluation environment is a regular Internet speed from Songkhla province to NETPIE and back. Since each patient will have approximately less than 10 monitoring devices, 16 devices will cover the case study requirement. Based on the preliminary results, the proposed logging mechanism has a potential to be used for logging information of patient monitoring scenarios.

Future work includes evaluating the proposed mechanism on a workload capturing from a real situation both the home-stay monitoring case and medical-facility-stay monitoring case on the performance, the space and the computational time.

REFERENCES

[1] "NETPIE, Network platform for Internet of everything," 2015. [Online]. Available: https://netpie.io/. Accessed: Jul. 16, 2016.

[2] E. A. Alkeem, C. Y. Yeun, and M. J. Zemerly, "Security and privacy framework for ubiquitous healthcare IoT devices," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015.

[3] S. Lavanya, G. Lavanya, and J. Divyabharathi, "Remote prescription and i-Home healthcare based on IoT," 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), 2017.

[4] S. Madakam, "Internet of things: Smart things," International Journal of Future Computer and Communication, vol. 4, no. 4, pp. 250–253, 2015.

[5] J. Djurica, "Internet of Things Offers Great Opportunities and Much Risk," ISACA JOURNAL, vol. 2, 2015.

[6] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of things: Perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481–2501, Jun. 2014.

[7] R. Costa and A. Pinto, "A framework for the secure storage of data generated in the IoT," in Ambient Intelligence - Software and Applications. Springer Science + Business Media, 2015, pp. 175–182.

[8] H. Jiang, F. Shen, S. Chen, K.-C. Li, and Y.-S. Jeong, "A secure and scalable storage system for aggregate data in IoT," Future Generation Computer Systems, vol. 49, pp. 133–141, Aug. 2015.

[9] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in Internet of things: A survey," 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017.

[10] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[11] S. Al-Fedaghi and F. Mahdi, "Events classification in log audit," International journal of Network Security & Its Applications, vol. 2, no. 2, pp. 58–73, Apr. 2010.

[12] A. Jain, T. Padiya, and M. Bhise, "Log based method for faster IoT queries," 2017 IEEE Region 10 Symposium (TENSYMP), 2017.

[13] S. Shaikh and V. Chitre, "Healthcare monitoring system using IoT," 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017.

[14] N. Azmi and L. M. Kamarudin, "Enabling IoT: Integration of wireless sensor network for healthcare application using Waspmote," 2017.

[15] J. Kim, "Energy-Efficient Dynamic Packet Downloading for Medical IoT Platforms," IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 1653–1659, 2015.

[16] Thai Health Promotion Foundation, "NCDs (Non-Communicable diseases)," unpublished.

[17] L. B. Dias, M. Holanda, R. C. Huacarpuma, and R. T. D. S. Jr, "NoSQL Database Performance Tuning for IoT Data - Cassandra Case Study," Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, 2018.

[18] V. Mishra, "NoSQL: Cassandra Basics," Beginning Apache Cassandra Development, pp. 1–26, 2014.

ORAL PRESENTATION

presented to

Piyawat Maneenual and Sangsuree Vasupongayya

for the paper entitled

Logging mechanism
for Internet of Things: A Case Study of Patient Monitoring System

in The 15th International Joint Conference on Computer Science and Software Engineering (JCSSE2018)
11 - 13 July 2018, Faculty of ICT, Mahidol University, Nakhon Pathom, Thailand

Jarernsri Mitrpanont

(Assoc. Prof. Dr. Jarernsri Mitrpanont)
General Chair
Dean, Faculty of ICT, Mahidol University

ประวัติผู้เขียน

ชื่อ สกุล นายปิยวัฒน์ มณีนวล

รหัสประจำตัวนักศึกษา 5810121044

วุฒิการศึกษา

วุฒิ	ชื่อสถาบัน	ปีที่สำเร็จการศึกษา
วิศวกรรมศาสตรบัณฑิต (สาขาวิชาวิศวกรรมคอมพิวเตอร์)	มหาวิทยาลัยสงขลานครินทร์	2557

ตำแหน่งและสถานที่ทำงาน

นักพัฒนาระบบสารสนเทศ บริษัท โรงพยาบาลราษฎร์ยินดี จำกัด (มหาชน)

การตีพิมพ์เผยแพร่ผลงาน

1. P. Maneenual & S. Vasupongayya, "External Auditing Module for Secure Personal Health Record Framework", Proc. the 19th ITC-CSCC, Phuket, Thailand, July 1-4, 2014.
2. P. Maneenual and S. Vasupongayya, "Logging mechanism for Internet of Things: A Case Study of Patient Monitoring System", Proceeding of the 15th International Joint Conference on Computer Science and Software Engineering (JCSSE2018), Nakhon Pathom, Thailand, 11-13 July 2018. DOI: 10.1109/JCSSE.2018.8457390