SAC-01-005

การออกแบบและพัฒนาระบบการสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัวสำหรับระบบเพาะเลี้ยงปูนาแบบน้ำหมุนเวียนโดยใช้การเข้ารหัส ChaCha20

Design and Development of Privacy-Preserving Data Communication for Recirculating Rice Field Crab Farming Systems Using ChaCha20 Encryption

วุฒิชัย ปวงมณี[1*] รติ วงษ์สถาน[2] และ สรจักร ปารมี[3]
Wutthichai Puangmanee[1*] Rati Wongsathan[2] and Sorrajuk Paramee[3]
สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยนอร์ท-เชียงใหม่[1, 3]
สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยนอร์ท-เชียงใหม่[2]
Department of Computer Engineering, Faculty of Engineering and Technology, North-Chiang MaiUniversity[1, 3]
Department of Electrical Engineering, Faculty of Engineering and Technology, North-Chiang Mai University[2]
e-mail: wutthichai@northcm.ac.th[1], rati@northcm.ac.th[2], sorrajuk7237@gmail.com[3]

บทคัดย่อ

การวิจัยนี้เป็นการวิจัยสำหรับการออกแบบและพัฒนา โดยมีวัตถุประสงค์เพื่อ (1) ออกแบบและพัฒนาการสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัวสำหรับการเพาะเลี้ยงปูนาแบบน้ำหมุนเวียนโดยใช้เทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things: IoT) ร่วมกับอัลกอริทึม ChaCha20 (2) เปรียบเทียบประสิทธิภาพของการเข้ารหัสข้อมูลด้วย ChaCha20 กับวิธีการเข้ารหัสแบบเดิมในด้านเวลาในการประมวลผล การใช้ทรัพยากร และความปลอดภัยของข้อมูล โดยกลุ่มตัวอย่างที่ใช้ในการวิจัย ได้แก่ ข้อมูลจากเซนเซอร์ในระบบเพาะเลี้ยงแบบน้ำหมุนเวียน ประกอบด้วยข้อมูลอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง (pH) ปริมาณออกซิเจนละลาย (DO) และค่าความขุ่นของน้ำ โดยใช้บอร์ดไมโครคอนโทรลเลอร์ ESP32 ส่งข้อมูลผ่านเครือข่ายไร้สาย (Wi-Fi) ไปยังคลาว์ดเซิร์ฟเวอร์ โดยใช้อัลกอริทึม ChaCha20 สำหรับเข้ารหัสข้อมูลก่อนการรับส่งข้อมูล โดยทำการบันทึกข้อมูลแบบทันทีทันใด (Real Time) จากนั้นทำการวิเคราะห์ข้อมูล และเปรียบเทียบเวลาในการประมวลผล ผลการวิจัยพบว่าสามารถเข้ารหัสและรับส่งข้อมูลได้อย่างปลอดภัย โดยอัลกอริทึม ChaCha20 ใช้เวลาในการเข้ารหัสเฉลี่ย 1.25 มิลลิวินาทีต่อแพ็กเก็ต เร็วกว่าวิธีการเข้ารหัสแบบ AES-256 ร้อยละ 32.4 และใช้หน่วยความจำลดลงร้อยละ 18.7 ซึ่งเหมาะสมกับอุปกรณ์ที่ใช้เทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่งที่มีข้อจำกัดในด้านพลังงานและทรัพยากรสำหรับการประมวลผล

คำสำคัญ: การเข้ารหัสข้อมูล อินเทอร์เน็ตทุกสรรพสิ่ง ระบบเพาะเลี้ยงสัตว์น้ำแบบหมุนเวียน เซนเซอร์ไร้สาย

Abstract

This research is a design and development study aimed at (1) designing and developing a privacy-preserving data communication system for recirculating rice field crab farming using Internet of Things (IoT) technology integrated with the ChaCha20 encryption algorithm, and (2) comparing the performance of ChaCha20 with conventional encryption methods in terms of processing time, resource utilization, and data security. The samples used in this study consisted of sensor data collected from a recirculating aquaculture system, including water temperature, pH, dissolved oxygen (DO), and turbidity. An ESP32 microcontroller board was employed to transmit data via a Wi-Fi network to a cloud server. The ChaCha20 algorithm was implemented to encrypt data prior to transmission. The sensor data were collected and stored in real time, followed by data analysis and evaluation of encryption performance. The results showed that the proposed system was able to securely encrypt and transmit sensor data. ChaCha20 achieved an average encryption time of 1.25 milliseconds per packet, which was 32.4% faster than AES-256. In addition, memory consumption was reduced by 18.7% compared with AES-256. These findings indicate that ChaCha20 is a suitable encryption algorithm for privacy-preserving IoT communication, particularly for resource-constrained devices with limited energy and computational capabilities.

Keywords: Data Encryption, Internet of Things, Recirculating Aquaculture Systems, Wireless sensor

บทนำ

ปัจจุบันการเพาะเลี้ยงสัตว์น้ำมีบทบาทสำคัญต่อการสร้างความมั่นคงทางอาหารและการพัฒนาเศรษฐกิจของหลายประเทศ ซึ่งปูนาเป็นสัตว์น้ำที่มีความสำคัญต่อวิถีชีวิตและการบริโภคของประชาชนในหลายพื้นที่ของประเทศไทย เนื่องจากมีโปรตีนที่มีคุณค่าทางโภชนาการสูงและสามารถนำไปแปรรูปเป็นขนม (จีระนันท์ วงศ์วทัญญู และคณะ, 2567) หรือผลิตภัณฑ์อาหารได้หลากหลาย (นิภาศักดิ์ คงงาม และคณะ, 2561) ปัจจุบันปริมาณปูนาในธรรมชาติมีแนวโน้มลดลงอย่างต่อเนื่องจากการเปลี่ยนแปลงสภาพแวดล้อม การใช้สารเคมีทางการเกษตร และการจับมาบริโภค ส่งผลให้การเพาะเลี้ยงปูนากลายเป็นทางเลือกสำคัญในการเพิ่มผลผลิตและสร้างรายได้ให้แก่เกษตรกร แต่การเพาะเลี้ยงปูนายังคงประสบปัญหาด้านการควบคุมคุณภาพน้ำ การเปลี่ยนแปลงของอุณหภูมิ ค่าความเป็นกรด-ด่าง และปริมาณออกซิเจนละลายน้ำ ซึ่งส่งผลโดยตรงต่ออัตราการรอดชีวิต (วิจิตรตา อรรถสาร และคณะ, 2567) การเจริญเติบโตและประสิทธิภาพการผลิต ดังนั้นการเพาะเลี้ยงแบบน้ำหมุนเวียน (Recirculating Aquaculture System: RAS) จึงเป็นอีกวิธีหนึ่งสำหรับการเพาะเลี้ยงสัตว์น้ำที่สามารถช่วยควบคุมสภาพแวดล้อม (นิชนันท์ ชูเกิด และคณะ, 2568) ลดอัตราการตาย การใช้น้ำ และเพิ่มประสิทธิภาพการผลิตได้อย่างมีประสิทธิภาพ (Timmons et al., 2018) ซึ่งปัจจุบันการประยุกต์ใช้เทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things: IoT) ในระบบเพาะเลี้ยงสัตว์น้ำอัจฉริยะ (Smart Aquaculture) ช่วยให้สามารถติดตามและควบคุมปัจจัยด้านคุณภาพน้ำแบบทันทีทันใด (Real time) ผ่านเซนเซอร์ต่าง ๆ เช่น อุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง (pH) ปริมาณออกซิเจนละลายน้ำ (Dissolved Oxygen: DO) และค่าความขุ่นของน้ำ โดยข้อมูลดังกล่าวสามารถส่งผ่านเครือข่ายไร้สายไปยังฐานข้อมูลบนคลาวด์เพื่อวิเคราะห์และใช้ในการตัดสินใจ (Jawad et al., 2017) ส่งผลให้ผู้เลี้ยงสามารถบริหารจัดการระบบการเพาะเลี้ยงได้อย่างมีประสิทธิภาพ ซึ่งการรับส่งข้อมูลระหว่างอุปกรณ์ และฐานข้อมูลบนคลาวด์ผ่านเครือข่ายอินเทอร์เน็ตก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) และความเป็นส่วนตัวของข้อมูล (Data Privacy) ข้อมูลที่ถูกส่งจากเซนเซอร์อาจถูกดักจับ ปลอมแปลง หรือเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ซึ่งอาจส่งผลให้ข้อมูลเกิดความคลาดเคลื่อนและนำไปสู่การแสดงผลหรือนำไปใช้สำหรับการตัดสินใจที่ผิดพลาดในการบริหารจัดการข้อมูลสำหรับการเพาะ (Sicari et al., 2015) จากปัญหาดังที่กล่าวมามีความสำคัญอย่างมากในการพัฒนาและออกแบบอุปกรณ์เซนเซอร์ไร้สาย (Wireless sensor) เนื่องจากอุปกรณ์ส่วนใหญ่มีข้อจำกัดด้านพลังงาน หน่วยความจำ และความเร็วในการประมวลผล ซึ่งส่งผลให้ไม่สามารถใช้กลไกและขั้นตอนในการเข้ารหัสที่ซับซ้อนและใช้ทรัพยากรสูงได้ (Alaba et al., 2017)

ดังนั้นคณะผู้วิจัยจึงเกิดแนวคิดการพัฒนาอัลกอริทึมการเข้ารหัสข้อมูลเพื่อรองรับอุปกรณ์เซนเซอร์ไร้สายที่มีทรัพยากรจำกัดด้วยอัลกอริทึม ChaCha20 ซึ่งเป็นอัลกอริทึมการเข้ารหัสแบบสตรีม (Stream Cipher) ที่พัฒนาโดย Daniel J. Bernstein และได้รับการยอมรับอย่างกว้างขวางในด้านความปลอดภัยและประสิทธิภาพการทำงาน โดยใช้วิธีทางคณิตศาสตร์พื้นฐาน ได้แก่ การบวก (Addition) การทำ XOR (Exclusive OR) และการหมุนตำแหน่งของบิต (Bit Rotation) ซึ่งทำให้สามารถประมวลผลได้รวดเร็วและใช้ทรัพยากรต่ำกว่าอัลกอริทึมแบบการเข้ารหัสแบบสมมาตร (Advanced Encryption Standard: AES) ในอุปกรณ์ที่ไม่มีอุปกรณ์อื่นๆ สำหรับช่วยในการประมวลผลการเข้ารหัส (Nir & Langley, 2018) ด้วยเหตุผลนี้การใช้ลกอริทึม ChaCha20 มาประยุกต์ใช้ในการเข้ารหัสข้อมูลในการส่งข้อมูลสำหรับระบบเพาะเลี้ยงปูนาแบบน้ำหมุนเวียนจึงเป็นวีการที่สามารถช่วยเพิ่มความปลอดภัยและความเป็นส่วนตัวของข้อมูล และในขณะเดียวกันยังสามารถช่วยให้ประสิทธิภาพการทำงานของอุปกรณ์เซนเซอร์ไร้สายที่มีข้อจำกัดด้านทรัพยากร สามารถทำงานได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

1. ออกแบบและพัฒนาการสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัวสำหรับการเพาะเลี้ยงปูนาแบบน้ำหมุนเวียนโดยใช้เทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things: IoT) ร่วมกับอัลกอริทึม ChaCha20
2. เปรียบเทียบประสิทธิภาพของการเข้ารหัสข้อมูลด้วย ChaCha20 กับวิธีการเข้ารหัสแบบเดิมในด้านเวลาในการประมวลผล การใช้ทรัพยากร และความปลอดภัยของข้อมูล

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยและพัฒนา (Research and Development: R&D) มีวัตถุประสงค์เพื่อออกแบบและพัฒนาการสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัวสำหรับการเพาะเลี้ยงปูนาแบบน้ำหมุนเวียน โดยประยุกต์ใช้อัลกอริทึม ChaCha20 สำหรับการเข้ารหัสข้อมูลบนอุปกรณ์เซนเซอร์ไร้สาย ก่อนการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตไปยังฐานข้อมูลบนคลาวด์ (Firebase

Realtime Database) โดยการดำเนินการวิจัยได้พัฒนาโปรแกรมบนบอร์ดไมโครคอนโทรลเลอร์ ESP32 การพัฒนาโปรแกรมสำหรับการถอดรหัสและแสดงผลข้อมูลแบบทันทีทันใดผ่านเว็บแอปพลิเคชัน รวมถึงการประเมินประสิทธิภาพการทำงานด้านความถูกต้องของข้อมูลและเวลาในการประมวลผล โดยข้อมูลที่ใช้ในการวิจัยประกอบด้วย ข้อมูลจากเซนเซอร์ตรวจวัดคุณภาพน้ำในถังระบบน้ำหมุนเวียน ได้แก่ ค่าความเป็นกรด-ด่าง ค่าปริมาณออกซิเจนในน้ำ และค่าความขุ่นของน้ำ โดยค่าอุณหภูมิน้ำ จะวัดในบ่อเลี้ยงเพียงจุดเดียว ซึ่งทำการเก็บรวบรวมแบบเวลาจริง (Real-Time) ผ่านบอร์ด ESP32 ที่เชื่อมต่ออินเทอร์เน็ตแล้วนำข้อมูลที่ได้เข้าสู่กระบวนการเข้ารหัส ส่งผ่านเครือข่ายอินเทอร์เน็ตไปยังคลาวด์ และทำการถอดรหัสเพื่อนำไปวิเคราะห์และเปรียบเทียบประสิทธิภาพของระบบ โดยรายละเอียดของวิธีดำเนินการวิจัย ประกอบด้วย การออกแบบระบบ เครื่องมือที่ใช้ในการวิจัย วิธีการรวบรวมข้อมูล ขั้นตอนการดำเนินการทดลอง และการวิเคราะห์ข้อมูล ซึ่งนำเสนอในหัวข้อต่อไป

1. การออกแบบระบบ

การออกแบบระบบที่นำเสนอในงานวิจัยนี้ได้รับการออกแบบให้เป็นระบบตรวจวัดและสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัวสำหรับระบบเพาะเลี้ยงปูนาแบบน้ำหมุนเวียน โดยประยุกต์ใช้เทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่ง ร่วมกับอัลกอริทึมการเข้ารหัส ChaCha20 เพื่อเพิ่มความปลอดภัยของข้อมูลระหว่างการรับส่งข้อมูลจากอุปกรณ์ตรวจวัดไปยังฐานข้อมูลบนคลาวด์ โครงสร้างของระบบแบ่งออกเป็น 4 ส่วนหลัก ได้แก่ (1) ส่วนตรวจวัดข้อมูล (2) ส่วนประมวลผลและเข้ารหัสข้อมูล (3) ส่วนสื่อสารข้อมูลและ (4) ส่วนจัดเก็บและแสดงผลข้อมูล แสดงภาพรวมการทำงานดังภาพที่ 1

ภาพที่ 1 ภาพรวมการทำงานของอุปกรณ์เซนเซอร์ไร้สายในการส่งข้อมูลและประมวลผล

จากภาพที่ 1 ข้อมูลประกอบด้วยค่าจากเซนเซอร์สำหรับตรวจวัดคุณภาพน้ำ ได้แก่ เซนเซอร์วัดอุณหภูมิน้ำ เซนเซอร์วัดค่าความเป็นกรด-ด่าง (pH) เซนเซอร์วัดปริมาณออกซิเจนละลายน้ำ และเซนเซอร์วัดค่าความขุ่นของน้ำ โดยเซนเซอร์ทั้งหมดเชื่อมต่อกับบอร์ดไมโครคอนโทรลเลอร์ ESP32 เพื่ออ่านค่าจากเซนเซอร์ จากนั้นจะทำการเข้ารหัสข้อมูลประกอบ วันและเวลาที่บันทึกข้อมูล และรหัสอุปกรณ์ (Device ID) จากนั้นข้อมูลจะถูกเข้ารหัสด้วยอัลกอริทึม ChaCha20 โดยใช้กุญแจลับ (Secret Key) และค่า Nonce ก่อนส่งผ่านเครือข่ายอินเทอร์เน็ต เพื่อป้องกันการดักจับหรือแก้ไขข้อมูลระหว่างการสื่อสาร ข้อมูลที่ผ่านการเข้ารหัสแล้วจะถูกส่งไปยังคลาวด์จัดเก็บข้อมูล จากนั้นข้อมูลจะถูกนำไปแสดงผลผ่านเว็บแอปพลิเคชันหรือแดชบอร์ดที่ออกแบบและพัฒนาขึ้นมาเพื่อแสดงผลสำหรับผู้ใช้งานสามารถติดตามสถานะคุณภาพน้ำแบบเรียลทันทีทันใด รวมทั้งสามารถนำข้อมูลไปใช้สำหรับวิเคราะห์แนวโน้มและสนับสนุนการตัดสินใจในการบริหารจัดการการเพาะเลี้ยงปูนาได้ และเพื่อประเมินประสิทธิภาพวิธีการที่เสนอคณะผู้วิจัยได้มีการเปรียบเทียบการเข้ารหัสข้อมูลด้วยอัลกอริทึม ChaCha20 กับอัลกอริทึม AES-256 โดยใช้ตัวชี้วัด ได้แก่ เวลาในการเข้ารหัส (Encryption Time) การใช้หน่วยความจำ (Memory Usage) การใช้หน่วยประมวลผล (CPU Usage) และอัตราความสำเร็จของการรับส่งข้อมูล (Packet Delivery Success Rate) เพื่อแสดงให้เห็นถึงความเหมาะสมของอัลกอริทึม ChaCha20 สำหรับอุปกรณ์เซนเซอร์ไร้สายที่มีข้อจำกัดด้านทรัพยากรในการประมวลผล

2. เครื่องมือที่ใช้ในการวิจัย

2.1 ฮาร์ดแวร์

- บอร์ดไมโครคอนโทรลเลอร์ ESP32 ทำหน้าที่รับข้อมูลจากเซนเซอร์ ประมวลผลการเข้ารหัสข้อมูลด้วยอัลกอริทึม ChaCha20 และส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตไปยังฐานข้อมูลบนคลาวด์
- เซนเซอร์ตรวจวัดคุณภาพน้ำ ประกอบด้วย
    - เซนเซอร์วัดอุณหภูมิน้ำ (Water Temperature Sensor)

- เซนเซอร์วัดค่าความเป็นกรด-ด่าง (pH Sensor)
- เซนเซอร์วัดปริมาณออกซิเจนละลายน้ำ (Dissolved Oxygen: DO Sensor)
- เซนเซอร์วัดค่าความขุ่นของน้ำ (Turbidity Sensor)

- บ่อเพาะเลี้ยงปูนาแบบน้ำหมุนเวียน (Recirculating Rice Field Crab Farming System) ประกอบด้วย บ่อเลี้ยงปูนา ระบบหมุนเวียนน้ำ ปั๊มน้ำ ระบบกรองน้ำ และระบบเติมอากาศ ซึ่งใช้เป็นพื้นที่ทดลองในการเก็บข้อมูลจริง
- อุปกรณ์เครือข่ายไร้สาย (Wi-Fi Router) ใช้สำหรับเชื่อมต่อ ESP32 เพื่อรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต

2.2 ซอฟต์แวร์

- โปรแกรม Arduino IDE สำหรับเขียนโปรแกรมและอัปโหลดโปรแกรมลงบนบอร์ด ESP32
- ระบบฐานข้อมูลบนคลาว์ด สำหรับจัดเก็บข้อมูลจากอุปกรณ์เซนเซอร์ไร้สาย
- เว็บแอปพลิเคชันหรือแดชบอร์ดสำหรับแสดงผลข้อมูลคุณภาพน้ำแบบทันทีทันใด

3. วิธีการรวบรวมข้อมูล

การวิจัยครั้งนี้ดำเนินการรวบรวมข้อมูลจากบ่อเพาะเลี้ยงปูนาแบบน้ำหมุนเวียน ที่ติดตั้งอุปกรณ์ตรวจวัดคุณภาพน้ำโดยใช้บอร์ดไมโครคอนโทรลเลอร์ ESP32 เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตและเชื่อมต่อกับเซนเซอร์ตรวจวัดคุณภาพน้ำ ประกอบด้วย เซนเซอร์วัดอุณหภูมิน้ำ เซนเซอร์วัดค่าความเป็นกรด-ด่าง เซนเซอร์วัดปริมาณออกซิเจนละลายน้ำ และเซนเซอร์วัดค่าความขุ่นของน้ำ เพื่อเก็บข้อมูลและส่งไปยังระบบฐานข้อมูลบนคลาว์ด จากนั้นแสดงผลข้อมูลคุณภาพน้ำบนเว็บแอปพลิเคชันที่ได้ทำการออกแบบไว้ต่อไป โดยขั้นตอนต่างๆ มีดังนี้

- ก่อนเริ่มการเก็บข้อมูล ได้ทำการตรวจสอบและสอบเทียบ (Calibration) เซนเซอร์ทุกตัวตามคู่มือของผู้ผลิต เพื่อให้ค่าที่วัดได้มีความถูกต้องและเชื่อถือได้ จากนั้นอ่านค่าจากเซนเซอร์ในช่วงเวลาที่กำหนดทุก 10 นาที พร้อมกำหนดวันและเวลาที่บันทึกข้อมูล
- ข้อมูลที่ได้จากเซนเซอร์จะถูกเข้ารหัสด้วยอัลกอริทึม ChaCha20 ภายใน ESP32 ก่อนส่งผ่านเครือข่าย Wi-Fi ไปยังฐานข้อมูลบนคลาว์ด เพื่อป้องกันการดักจับหรือแก้ไขข้อมูลระหว่างการสื่อสาร
- การทดลองแบ่งออกเป็น 2 กรณี ได้แก่ (1) การรับส่งข้อมูลด้วยอัลกอริทึม ChaCha20 และ (2) การรับส่งข้อมูลด้วยอัลกอริทึม AES-256 เพื่อใช้เป็นข้อมูลอ้างอิงในการเปรียบเทียบประสิทธิภาพ โดยทั้งสองกรณีใช้ชุดข้อมูลจากเซนเซอร์เดียวกัน ภายใต้สภาพแวดล้อมและเงื่อนไขการทดลองเดียวกัน เพื่อลดปัจจัยที่อาจส่งผลต่อผลการทดลอง
- ข้อมูลที่รวบรวมได้ประกอบด้วย ค่าอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง ค่าปริมาณออกซิเจนละลายน้ำ และค่าความขุ่นของน้ำ รวมถึงข้อมูลด้านประสิทธิภาพของระบบ ได้แก่ เวลาในการเข้ารหัส (Encryption Time) เวลาในการถอดรหัส (Decryption Time) การใช้หน่วยความจำ (Memory Usage) การใช้หน่วยประมวลผล (CPU Usage) อัตราการรับส่งข้อมูล (Throughput) และอัตราความสำเร็จในการรับส่งข้อมูล (Packet Delivery Success Rate)
- หลังจากเสร็จสิ้นการรวบรวมข้อมูล จะนำข้อมูลทั้งหมดมาวิเคราะห์ด้วยสถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) และค่าร้อยละ (Percentage) พร้อมเปรียบเทียบประสิทธิภาพระหว่างอัลกอริทึม ChaCha20 และอัลกอริทึม AES-256 เพื่อประเมินความแตกต่างทั้งสองอัลกอริทึม

4. ขั้นตอนการดำเนินการทดลอง

การทดลองสำหรับงานวิจัยนี้ ได้กำหนดเป็นช่วงเวลาในการวัดเพื่อติดตามประสิทธิภาพในการทำงานของระบบกรองสำหรับระบบน้ำหมุนเวียนด้วย โดยขนาดขอบ่อในการเพาะเลี้ยงปูนาที่ใช้ในการทดลอง กว้าง 250 เซนติเมตร ยาว 265 เซนติเมตร และระดับน้ำสูงประมาณ 7 เซนติเมตร แสดงตัวอย่างดังภาพที่ 2

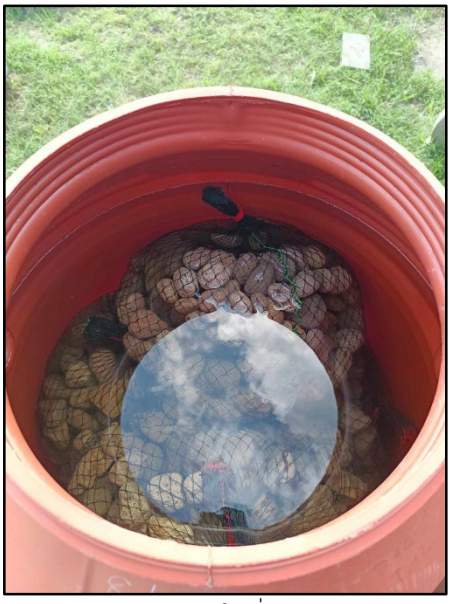
ภาพที่ 2 ขนาดของเพาะเลี้ยงปูนาที่ใช้ในการทดลอง

การออกแบบระบบน้ำหมุนเวียนในการวิจัยนี้จะเน้นการให้น้ำที่ใช้งานกลับแล้วสามารถนำมาใช้ใหม่ได้เพื่อลดการสูญเสียและเพิ่มประสิทธิภาพของระบบ น้ำที่ใช้งานจะถูกนำกลับมาสู่ระบบหลังจากใช้แล้ว โดยมีการทำความสะอาดและปรับสภาพน้ำเพื่อให้มีคุณภาพที่เหมาะสมสำหรับการใช้งานต่อไป โดยขั้นตอนการกรองของถังกรองทั้ง 4 ใบ แสดงตัวอย่างภาพที่ 3 จากภาพ โดยการออกแบบระบบกรองน้ำทั้ง 4 ถัง ใช้วัสดุกรองแตกต่างกันเพื่อให้เหมาะสมกับหน้าที่ของแต่ละขั้นตอน โดยถังใบที่ 1 ใส่แปรงพู่ (Filter Brush) ความยาวประมาณ 50 เซนติเมตร สำหรับดักตะกอน เศษอาหารหรือเศษวัสดุที่มีขนาดใหญ่ ลดการอุดตันสำหรับถังใบที่ 2 และเพิ่มพื้นที่สัมผัสสำหรับจุลินทรีย์เกาะอาศัย ถังใบที่ 2 ใช้แผ่นใยกรองสังเคราะห์ (Filter Mat) ซึ่งมีโครงสร้างเส้นใยละเอียดช่วยกรองตะกอนแขวนลอยและสิ่งสกปรกขนาดเล็ก พร้อมเป็นแหล่งยึดเกาะของจุลินทรีย์ที่ช่วยย่อยสลายสารอินทรีย์ ถังใบที่ 3 เป็นถังเติมอากาศ โดยใช้หัวกระจายอากาศเพื่อเพิ่มปริมาณออกซิเจนละลายในน้ำ โดยจะส่งเสริมการทำงานของจุลินทรีย์แบบใช้ออกซิเจนและช่วยปรับปรุงคุณภาพน้ำก่อนเข้าสู่ขั้นตอนสุดท้าย ถังใบที่ 4 ใช้วัสดุกรองชีวภาพประเภทหินพัมมิซ (Pumice) บรรจุในถุงตาข่าย ซึ่งมีพื้นที่ผิวสูงและมีรูพรุนจำนวนมาก ทำหน้าที่เป็นแหล่งอาศัยของจุลินทรีย์สำหรับกระบวนการบำบัดทางชีวภาพ ช่วยลดแอมโมเนียสารอินทรีย์ และเพิ่มความเสถียรของคุณภาพน้ำก่อนนำน้ำกลับมาใช้ในระบบหมุนเวียนอีกครั้ง

(ก) ถังใบที่ 1

(ข) ถังใบที่ 2

(ค) ถังใบที่ 3



(ง) ถังใบที่ 4

ภาพที่ 3 วัสดุที่บรรจุในถังทั้ง 4 ใบของระบบน้ำหมุนเวียน

ขั้นตอนการวัดค่าความเป็นกรด-ด่างในน้ำและปริมาณออกซิเจนละลายในบ่อ โดยมีการปรับเทียบค่าของเครื่องมือที่ใช้วัดก่อนแล้ว โดยทำการเปรียบเทียบการวัดค่าความเป็นกรด-ด่างถังใบที่ 1 ที่ดูดน้ำจากบ่อเลี้ยงโดยใช้ปั๊มน้ำ และถังใบที่ 4 น้ำที่จะนำกลับไปยังบ่อเลี้ยง โดยถังใบที่ 1 ค่าความเป็นกรด-ด่างที่วัดได้ 7.18 และถังใบที่ 4 ค่าความเป็นกรด-ด่างที่วัดได้ 7.08 และเมื่อ เวลาผ่านไป 3 ชั่วโมง เปรียบเทียบค่าความเป็นกรด-ด่างและปริมาณออกซิเจนละลาย (DO) ดังภาพที่ 4 ซึ่งค่าความเป็นกรด-ด่าง ที่วัดได้ต่างกันอยู่ที่ 0.1

(ก) วัดค่าความเป็นกรด-ด่าง ถังใบที่ 1

(ข) วัดค่าความเป็นกรด-ด่าง ถังใบที่ 4

ภาพที่ 4 วัดค่าความเป็นกรด-ด่าง เปรียบเทียบถังใบที่ 1 กับถังใบที่ 4

อัลกอริทึม ChaCha20

การออกแบบและพัฒนาระบบการสื่อสารข้อมูลที่ปลอดภัยในบทความนี้ใช้อัลกอริทึมการเข้ารหัสแบบ ChaCha20 สำหรับการป้องกันข้อมูลของเซนเซอร์ที่วัดได้จากอุปกรณ์ที่ออกแบบไปยังฐานข้อมูลบนคลาวด์โดยอัลกอริทึม ChaCha20 มีความปลอดภัยสูงและประมวลผลได้รวดเร็ว ซึ่งเหมาะสำหรับการนำมาใช้กับอุปกรณ์เซนเซอร์ไร้สายที่มีทรัพยากรจำกัด โดยขั้นตอนการทำงานของอัลกอริทึม ChaCha20 จะใช้คีย์ขนาด 256 บิต (256-bit Secret Key) ร่วมกับค่าตัวเลขที่ใช้เพียงครั้งเดียว (Number Used Once) ขนาด 96 บิต และตัวนับบล็อกขนาด 32 บิต เพื่อสร้างกุญแจสำหรับการเข้ารหัส (Keystream) ที่แตกต่างกันในแต่ละแพ็กเก็ตข้อมูลที่ส่ง โดยเริ่มจากสร้างเมทริกซ์สถานะ (State Matrix) ขนาด 4 × 4 ที่ประกอบด้วยค่าคงที่จำนวน 4 ค่า กุญแจลับจำนวน 8 ค่า ตัวนับ (Counter) จำนวน 1 ค่า และค่าตัวเลขที่ใช้เพียงครั้งเดียวจำนวน 3 ค่า ดังสมการที่ 1

$$S_0 = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 \\ k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ ctr & n_0 & n_1 & n_2 \end{bmatrix} \tag{1}$$

จากนั้นนำเมทริกซ์ที่สร้างทำการคำนวณจำนวน 20 รอบ (หรือ 10 Double Rounds) ซึ่งแต่ละรอบ ประกอบด้วยการคำนวณแบบ Column Quarter Round และ Diagonal Quarter Round โดยใช้การดำเนินการทางคณิตศาสตร์ ได้แก่ การบวกแบบ Modulo 2^{32} การดำเนินการ XOR และการหมุนบิตทางซ้าย (Left Rotation)

$$\begin{aligned} a &= a + b, \quad d = d \oplus a, \quad d \text{ Œ } 16 \\ c &= c + d, \quad b = b \oplus c, \quad b \text{ Œ } 12 \\ a &= a + b, \quad d = d \oplus a, \quad d \text{ Œ } 8 \\ c &= c + d, \quad b = b \oplus c, \quad b \text{ Œ } 7 \end{aligned} \tag{2}$$

เมื่อครบทั้ง 20 รอบ จะนำผลลัพธ์มาบวกกับเมทริกซ์เริ่มต้นเพื่อสร้าง Keystream ขนาด 512 บิต จากนั้นนำ Keystream ไปดำเนินการแบบ Exclusive OR (XOR) กับข้อมูลต้นฉบับ (Plaintext) เพื่อสร้างข้อมูลเข้ารหัส (Ciphertext) ดังสมการ

$$CT = PT \oplus KS \tag{3}$$

โดยค่าที่ PT คือ ข้อมูลต้นฉบับจากเซนเซอร์ KS คือ ค่า Keystream ที่สร้างจาก ChaCha20 และ CT คือ ข้อมูลที่ถูกเข้ารหัสแล้ว สำหรับงานวิจัยนี้ข้อมูลที่ได้รับจากเซนเซอร์ประกอบด้วยค่าอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง ค่าปริมาณออกซิเจนละลายน้ำ ค่าความขุ่นของน้ำ และเวลาที่บันทึกข้อมูล ซึ่งถูกจัดเก็บเป็นแพ็กเก็ตข้อมูลก่อนเข้ารหัสด้วยอัลกอริทึม ChaCha20 แล้วจึงส่งผ่านเครือข่ายไร้สายเชื่อมต่ออินเทอร์เน็ตไปยังฐานข้อมูลบนคลาวด์สำหรับจัดเก็บข้อมูล โดยหลังจากเข้ารหัสข้อมูลในแต่ละแพ็กเก็ตระบบจะเพิ่มค่าการนับ (Counter) ทีละ 1 เพื่อให้ Keystream ที่สร้างขึ้นแตกต่างกันทุกครั้ง ช่วยลดความเสี่ยงจากการนำกุญแจเข้ารหัสกลับมาใช้ซ้ำและเพิ่มความปลอดภัยในการสื่อสารข้อมูล

Algorithm 1: Secure Sensor Data Transmission Using ChaCha20 Encryption

Require:

K : 256-bit Secret Key

N : 96-bit Nonce

C : Counter

S : Sensor Set

= {Temperature, pH, DO, Turbidity}

Ensure:

Secure transmission to Cloud

```
Initialize IoT Node
Initialize ChaCha20(K, N, C)
repeat
    for each sensor si ∈ S do
        Di ⟵ Read(si)
    end for
    Packet ⟵ Serialize(D1, D2, D3, D4, Timestamp)
    Ciphertext ⟵ ChaCha20(Packet, K, N, C)
    Send Ciphertext via Wi-Fi
    Wait ACK
    if Timeout then
        Retransmit Ciphertext
    end if
    C ⟵ C + 1
until System Shutdown
return
```

Algorithm 2: ChaCha20 decryption algorithm

Require: K ∈ {0,1} ^ 256,
N ∈ {0,1} ^ 96,
C ∈ {0,1} ^ 32,
CT ∈ {0,1}*

Ensure: PT = ChaCha20-Decrypt (K, N, C, CT)

```
IM ⟵ Init (K, N, C)
for x ⟵ 0 to (|CT|/512) – 1 do
    OM ⟵ IM
    for j ⟵ 0 to 9 do
        OM[0,4,8,12]  ⟵ QR(OM[0,4,8,12])
        OM[1,5,9,13]  ⟵ QR(OM[1,5,9,13])
        OM[2,6,10,14] ⟵ QR(OM[2,6,10,14])
        OM[3,7,11,15] ⟵ QR(OM[3,7,11,15])
        OM[0,5,10,15] ⟵ QR(OM[0,5,10,15])
        OM[1,6,11,12] ⟵ QR(OM[1,6,11,12])
        OM[2,7,8,13]  ⟵ QR(OM[2,7,8,13])
        OM[3,4,9,14]  ⟵ QR(OM[3,4,9,14])
    end for
    S ⟵ Serialize(OM + IM)
    for z ⟵ 0 to 511 do
        PT[512x+z] ⟵ CT[512x+z] ⊕ S[z]
    end for
    IM[12] ⟵ IM[12] + 1
end for
return PT
```

โดย Algorithm 2 แสดงขั้นตอนการถอดรหัสข้อมูลของอัลกอริทึม ChaCha20 โดยเริ่มจากการสร้าง Initial State Matrix จากกุญแจลับ (Secret Key) ขนาด 256 บิต ค่า Nonce ขนาด 96 บิต และตัวนับ (Counter) ขนาด 32 บิต จากนั้นดำเนินการ Quarter Round จำนวน 20 รอบ (10 Double Rounds) เพื่อสร้าง Keystream ซึ่งมีค่าเหมือนกับที่ใช้ในขั้นตอนการเข้ารหัส เมื่อได้ Keystream แล้ว จะนำไปดำเนินการ XOR กับข้อมูลที่เข้ารหัส (Ciphertext) เพื่อกู้คืนข้อมูลต้นฉบับ (Plaintext) หลังจากประมวลผลครบหนึ่งบล็อก Counter จะถูกเพิ่มค่า 1 เพื่อสร้าง Keystream สำหรับบล็อกถัดไป กระบวนการดังกล่าวดำเนินการจนกว่าจะถอดรหัสข้อมูลครบทุกแพ็กเก็ต

วิธีการวัดประเมินการเข้ารหัส

เพื่อประเมินประสิทธิภาพของอัลกอริทึม ChaCha20 ในการเข้ารหัสข้อมูล งานวิจัยนี้ได้วัดเวลาในการเข้ารหัส (Encryption Time) โดยใช้ตัวจับเวลาที่มีอยู่ในไมโครคอนโทรลเลอร์บอร์ด ESP32 ผ่านฟังก์ชัน esp_timer_get_time() ซึ่งให้ความละเอียดในการวัดไมโครวินาที (Microsecond Precision) โดยขั้นตอนการวัดเริ่มจากการบันทึกเวลาเริ่มต้น (T_{start}) ทันที ก่อนเรียกใช้ฟังก์ชัน ChaCha20_Encrypt() เพื่อเข้ารหัสแพ็กเก็ตข้อมูล จากนั้นเมื่อกระบวนการเข้ารหัสเสร็จสมบูรณ์ จะบันทึกเวลาสิ้นสุด (T_{end}) และคำนวณเวลาในการเข้ารหัสจากผลต่างของเวลาทั้ง 2 ค่า จากสูตรคำนวณ $T_{enc} = T_{end} - T_{start}$ โดยทำการแปลงหน่วยจากไมโครวินาทีเป็นมิลลิวินาทีด้วยการหารด้วย 1,000 เพื่อให้สามารถเปรียบเทียบผลได้ง่าย ข้อมูลที่ใช้ในการทดลองเป็นแพ็กเก็ตข้อมูลจากเซนเซอร์ที่วัดได้ ประกอบด้วยค่าอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง ค่าปริมาณออกซิเจนละลายในน้ำ ค่าความขุ่น และข้อมูลเวลาที่บันทึก

(Timestamp) ซึ่งมีขนาดเฉลี่ยประมาณ 96 ไบต์ จากนั้นนำผลลัพธ์ที่ได้มาคำนวณหาค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation: S.D) และค่าต่ำสุด–สูงสุดของเวลาในการเข้ารหัส เพื่อใช้เปรียบเทียบกับอัลกอริทึม AES-256 ในเงื่อนไขเช่นเดียวกัน ทั้งนี้การวัดเวลาจะครอบคลุมเฉพาะกระบวนการเข้ารหัสเท่านั้น โดยไม่รวมเวลาในการอ่านค่าจากเซนเซอร์ การสร้างแพ็กเก็ตข้อมูลการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต เพื่อให้สามารถประเมินประสิทธิภาพของอัลกอริทึม ChaCha20 ได้อย่างถูกต้องและเปรียบเทียบกับอัลกอริทึม AES-256

ผลการวิจัย

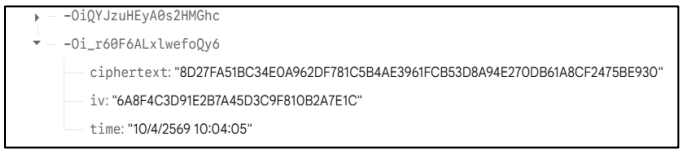
การประเมินประสิทธิภาพของการสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัว โดยใช้อัลกอริทึม ChaCha20 สำหรับการเข้ารหัสข้อมูลก่อนส่งผ่านเครือข่ายอินเทอร์เน็ต การประเมินประสิทธิภาพครอบคลุมด้านการเข้ารหัสข้อมูล ความเร็วในการประมวลผล การใช้ทรัพยากรของไมโครคอนโทรลเลอร์ และประสิทธิภาพในการรับส่งข้อมูลแบบทันทีทันใด เพื่อพิจารณาความเหมาะสมของอัลกอริทึมที่ใช้สำหรับการออกการเข้านหัสข้อมูลที่มีความปลอดภัยและข้อจำกัดด้านการประมวลผล หน่วยความจำ และการใช้พลังงาน โดยใช้บอร์ด ESP32 ซึ่งเชื่อมต่อกับเซนเซอร์ตรวจวัดคุณภาพน้ำ ได้แก่ เซนเซอร์วัดอุณหภูมิ เซนเซอร์วัดค่าความเป็นกรด-ด่าง เซนเซอร์วัดปริมาณออกซิเจนละลายในน้ำ และเซนเซอร์วัดค่าความขุ่นของน้ำ โดยการวางตำแหน่งของเซนเซอร์สำหรับการวัดค่าในถังใบที่ 1 และถังใบที่ 4 สำหรับการทดลองแสดงดังภาพที่ 5

(ก) **(ข)**

ภาพที่ 5 ตัวอย่างการติดตั้งเซนเซอร์ในการวัด (ก) ถังใบที่ 1 (ข) ถุงใบที่ 4

ข้อมูลจากเซนเซอร์ถูกจัดรูปแบบเป็นแพ็กเก็ตก่อนเข้าสู่กระบวนการเข้ารหัสด้วยอัลกอริทึม ChaCha20 และส่งผ่านเครือข่ายอินเทอร์เน็ตไปยังฐานข้อมูลบนคลาว์ดเพื่อจัดเก็บข้อมูล โดยได้เปรียบเทียบอัลกอริทึม ChaCha20 กับอัลกอริทึม AES-256 ซึ่งเป็นมาตรฐานการเข้ารหัสข้อมูลที่ได้รับความนิยมอย่างแพร่หลาย โดยใช้ตัวชี้วัดหลัก ได้แก่ เวลาในการเข้ารหัส (Encryption Time) เวลาในการถอดรหัส (Decryption Time) การใช้หน่วยความจำ (Heap Memory Usage) การใช้ทรัพยากรของหน่วยประมวลผล (CPU Usage) อัตราการรับส่งข้อมูล (Throughput) ตัวอย่างข้อมูลทีส่งไปยังฐานข้อมูลบนคลาว์ดเมื่อทำการเข้ารหัสข้อมูลแล้ว ดังตัวอย่างภาพที่ 5

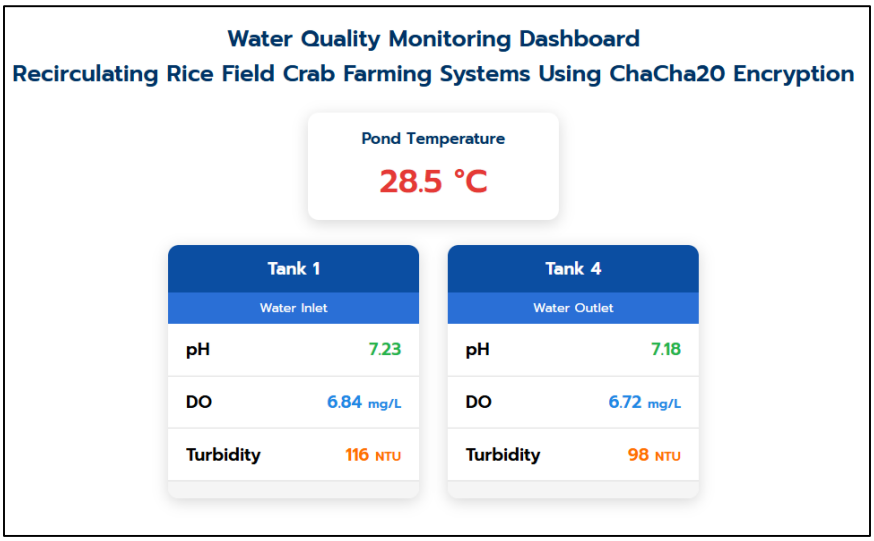
(ก)



(ข)

ภาพที่ 5 ตัวอย่างข้อมูลที่เข้ารหัสจัดเก็บในฐานข้อมูลบนคลาว์ด (Firebase Realtime Database) (ก) เข้ารหัสด้วยอัลกอริทึม ChaCha20 (ข) เข้ารหัสด้วยอัลกอริทึม AES-256

จากข้อมูลดังกล่าวจะเห็นว่าฐานข้อมูลบนคลาว์ด ไม่ได้เก็บข้อมูลจากเซนเซอร์โดยตรง แต่เก็บเฉพาะข้อมูลที่เข้ารหัสแล้ว (Ciphertext) จึงไม่สามารถทราบค่าจริงของอุณหภูมิ ค่าอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง ค่าปริมาณออกซิเจนละลายในน้ำ และค่าความขุ่นของน้ำ มีค่าเท่าไหร่ซึ่งจะสามารถทราบได้โดยการงานงานในส่วนของแดชบอร์ดแสดงผลคุณภาพน้ำ ดังตัวอย่างภาพที่ 6



ภาพที่ 6 แดชบอร์ดแสดงผลคุณภาพน้ำแบบเวลาจริงโดยใช้การเข้ารหัสและถอดรหัสด้วยอัลกอริทึม ChaCha20

ภาพที่ 6 แสดงหน้าจอแดชบอร์ดสำหรับติดตามคุณภาพน้ำของระบบเพาะเลี้ยงปูนาแบบน้ำหมุนเวียน (Recirculating Rice Field Crab Farming System) แบบเวลาจริง โดยแสดงค่าอุณหภูมิของบ่อเลี้ยง (Pond Temperature) จำนวน 1 ค่า และแสดงค่าคุณภาพน้ำของ ถังน้ำเข้า (Tank 1: Water Inlet) และ ถังน้ำออก (Tank 4: Water Outlet) ซึ่งประกอบด้วยค่าความเป็นกรด-ด่าง ปริมาณออกซิเจนละลายในน้ำ และค่าความขุ่นของน้ำ ข้อมูลทั้งหมดถูกส่งจากบอร์ด ESP32 หลังผ่านกระบวนการเข้ารหัสด้วยอัลกอริทึม ChaCha20 ไปจัดเก็บในฐานข้อมูลบนคลาว์ด จากนั้นจึงถอดรหัสและแสดงผลผ่านเว็บเบราว์เซอร์แบบเวลาจริง เพื่อช่วยให้ผู้ใช้งานสามารถติดตามและเปรียบเทียบคุณภาพน้ำระหว่างน้ำเข้าและน้ำออกได้อย่างสะดวกและปลอดภัย

(ก) (ข)

ภาพที่ 7 ตัวอย่างกราฟแสดงข้อมูลเปรียบเทียบคุณภาพน้ำ (ก) แสดงค่าความเป็นกรด-ด่าง (pH) ระหว่างถัง 1 น้ำเข้าและถัง 4 น้ำออก (ข) กราฟเปรียบเทียบค่าอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง (pH) ปริมาณออกซิเจนละลาย (DO) และค่าความขุ่นของน้ำ ระหว่างถัง 1 น้ำเข้าและถัง 4 น้ำออก

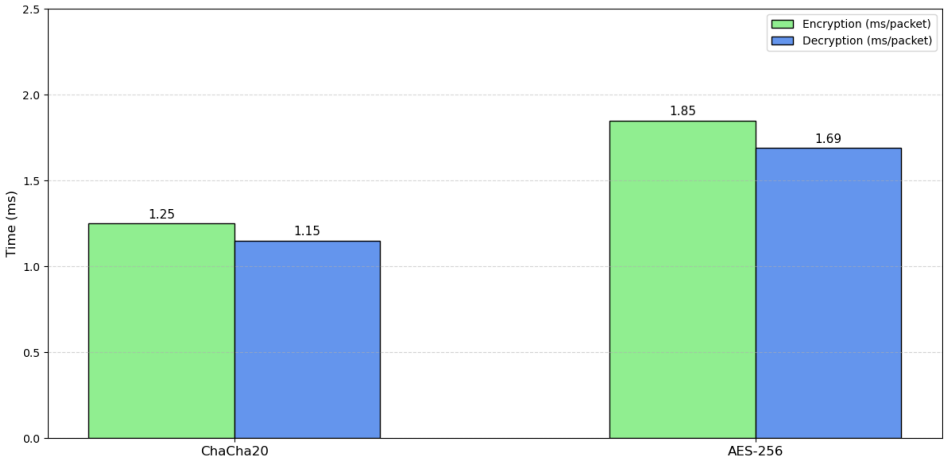
ภาพที่ 7 แสดงผลการเปรียบเทียบข้อมูลคุณภาพน้ำแบบเวลาจริงระหว่าง ถัง 1 น้ำเข้า (Tank 1) และ ถัง 4 น้ำออก (Tank 4) โดยภาพที่ 7(ก) แสดงการเปรียบเทียบแนวโน้มของค่าความเป็นกรด-ด่าง (pH) ซึ่งพบว่าค่าของทั้งสองถังมีการเปลี่ยนแปลงเพียงเล็กน้อยและอยู่ในช่วงที่เหมาะสมต่อการเพาะเลี้ยงปูนา ส่วนภาพที่ 7(ข) แสดงแนวโน้มของตัวแปรคุณภาพน้ำทั้ง 4 ค่า ได้แก่ อุณหภูมิ (Temperature) ค่าความเป็นกรด-ด่าง (pH) ปริมาณออกซิเจนละลายในน้ำ (DO) และค่าความขุ่นของน้ำ (Turbidity) โดยข้อมูลจากทั้งสองถังมีแนวโน้มสอดคล้องกันตลอดช่วงเวลาการทดลอง แสดงให้เห็นว่าระบบสามารถติดตามและแสดงผลข้อมูลคุณภาพน้ำแบบเวลาจริงได้อย่างต่อเนื่อง พร้อมทั้งช่วยให้ผู้ใช้งานสามารถเปรียบเทียบคุณภาพน้ำระหว่างน้ำเข้าและน้ำออกเพื่อประเมินประสิทธิภาพของระบบเพาะเลี้ยงแบบน้ำหมุนเวียนได้อย่างมีประสิทธิภาพ ผลการทดลองแสดงให้เห็นว่าอัลกอริทึม ChaCha20 มีประสิทธิภาพในการเข้ารหัสและถอดรหัสข้อมูลสูงกว่าอัลกอริทึม AES-256 โดยสามารถลดเวลาในการประมวลผล ลดการใช้หน่วยความจำ และลดภาระการทำงานของหน่วยประมวลผลได้อย่างมีนัยสำคัญ ส่งผลให้ระบบสามารถรับส่งข้อมูลจากเซนเซอร์ไปยังฐานข้อมูลบนคลาวด์ได้เร็วกว่า

ตารางที่ 1
เปรียบเทียบผลการทดลองโดยใช้บอร์ด ESP32 ในการเข้ารหัสข้อมูล

Performance Metric	ChaCha20 (Mean)	ChaCha20 (S.D)	AES-256 (Mean)	AES-256 (S.D)	Improvement (%)
Encryption Time (ms/packet)	1.25	0.08	1.85	0.11	32.4
Decryption Time (ms/packet)	1.15	0.07	1.69	0.10	31.8
Heap Memory Usage (Bytes)	**24,312**	312	**29,862**	387	18.7
CPU Usage (%)	38.6	2.1	52.1	2.8	25.9
Throughput (KB/s)	73.0	4.7	49.3	3.6	48.1
Power Consumption (mA)	128.3	4.3	142.7	5.2	10.1

ผลการเปรียบเทียบจากข้อมูลตารางที่ 1 พบว่าการใช้อัลกอริทึม ChaCha20 ใช้หน่วยความจำ Heap เฉลี่ย 24,312 ไบต์ น้อยกว่า AES-256 ซึ่งใช้ 29,862 ไบต์ หรือคิดเป็นการลดลงประมาณร้อยละ 18.7 นอกจากนี้อัลกอริทึม ChaCha20 ยังใช้ทรัพยากรของหน่วยประมวลผลประมาณร้อยละ 38.6 ขณะที่ AES-256 ใช้ประมาณร้อยละ 52.1 ซึ่งส่งผลให้สามารถลดภาระการทำงานของไมโครคอนโทรลเลอร์ได้ประมาณร้อยละ 25.9 โดยในด้านอัตราการรับส่งข้อมูล พบว่าอัลกอริทึม ChaCha20 มีค่าปริมาณของข้อมูลที่

ถูกประมาลผล (Throughput) เฉลี่ย 73.0 KB/s สูงกว่า AES-256 ซึ่งมีค่า 49.3 KB/s โดยคิดเป็นการเพิ่มขึ้นประมาณร้อยละ 48.1 ขณะที่การใช้พลังงานเฉลี่ยของอัลกอริทึม ChaCha20 อยู่ที่ 128.3 mA ต่ำกว่า AES-256 ซึ่งใช้พลังงานถึง 142.7 mA หรือประหยัดการใช้พลังงานได้ประมาณร้อยละ 10.1 จึงส่งผลให้การใช้อัลกอริทึม ChaCha20 มีความเหมาะสมอย่างมากสำหรับการนำมาประยุกต์ใช้ในการออกแบบที่ต้องทำงานต่อเนื่องเป็นเวลานานและมีข้อจำกัดด้านพลังงาน



ภาพที่ 8 เปรียบเทียบเวลาเฉลี่ยในการเข้ารหัสและถอดรหัสข้อมูลของอัลกอริทึม ChaCha20 และอัลกอริทึม AES-256

จากภาพที่ 8 แสดงผลการเปรียบเทียบเวลาเฉลี่ยในการเข้ารหัสและถอดรหัสข้อมูลระหว่างอัลกอริทึม ChaCha20 และอัลกอริทึม AES-256 บนบอร์ด ESP32 โดยพบว่าอัลกอริทึม ChaCha20 ใช้เวลาในการเข้ารหัสเฉลี่ย 1.25 มิลลิวินาทีต่อแพ็กเก็ต และเวลาในการถอดรหัสเฉลี่ย 1.15 มิลลิวินาทีต่อแพ็กเก็ต ซึ่งต่ำกว่าอัลกอริทึม AES-256 ที่ใช้เวลาในการเข้ารหัสเฉลี่ย 1.85 มิลลิวินาทีต่อแพ็กเก็ต และเวลาในการถอดรหัสเฉลี่ย 1.69 มิลลิวินาทีต่อแพ็กเก็ต แสดงให้เห็นว่าอัลกอริทึม ChaCha20 มีประสิทธิภาพในการประมวลผลที่สูงกว่า และเหมาะสำหรับอุปกรณ์ IoT ที่มีข้อจำกัดด้านทรัพยากรและต้องการการสื่อสารข้อมูลแบบเวลาจริง

สรุปผลการวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบและพัฒนาการเข้ารหัสข้อมูลแบบรักษาความเป็นส่วนตัวโดยใช้อัลกอริทึม ChaCha20 สำหรับการเข้ารหัสข้อมูลจากเซนเซอร์ที่สัดได้จากการตรวจวัดคุณภาพน้ำประกอบด้วย ค่าอุณหภูมิน้ำ ค่าความเป็นกรด-ด่าง ปริมาณออกซิเจนละลายในน้ำ และค่าความขุ่นของน้ำ โดยข้อมูลถูกจัดเก็บในรูปแบบแพ็กเก็ตและเข้ารหัสข้อมูล ผลการทดลองสามารถเข้ารหัสในการส่งข้อมูล และถอดรหัสข้อมูลได้อย่างถูกต้อง โดยข้อมูลที่ได้รับหลังการถอดรหัสมีความถูกต้องตรงกับข้อมูลต้นฉบับ ผลการประเมินประสิทธิภาพด้านการประมวลผลพบว่าอัลกอริทึม ChaCha20 ใช้เวลาในการเข้ารหัส และถอดรหัสน้อยกว่าอัลกอริทึม AES-256 จากผลการวิจัยสามารถสรุปได้ว่า วิธีการที่ใช้สามารถเพิ่มความปลอดภัยของข้อมูลจากเซนเซอร์ได้อย่างมีประสิทธิภาพ และรองรับการทำงานแบบทันทีทันใด โดยไม่ก่อให้เกิดการทำงานสำหรับการประมวลผลมากจนทำให้อุปกรณ์ไม่สามารถทำงานได้

การอภิปรายผล

ผลการวิจัยการประยุกต์ใช้อัลกอริทึม ChaCha20 สำหรับการเข้ารหัสข้อมูลจากเซนเซอร์ในระบบเพาะเลี้ยงแบบน้ำหมุนเวียนสามารถเพิ่มความปลอดภัยของข้อมูลได้โดยไม่ส่งผลกระทบต่อประสิทธิภาพของระบบสื่อสาร เนื่องจากอัลกอริทึม ChaCha20 เป็นอัลกอริทึมประเภท Stream Cipher ที่สร้างกระแสกุญแจ (Keystream) จากการทำงานของฟังก์ชัน Quarter Round ซึ่งอาศัยเพียงการดำเนินการทางคณิตศาสตร์พื้นฐานโดยไม่ใช้การคำนวณที่ซับซ้อนเหมือนกับอัลกอริทึมแบบการเข้ารหัสแบบสมมาตร จึงทำให้อัลกอริทึม ChaCha20 ใช้เวลาในการประมวลผลน้อยกว่าและเหมาะสำหรับอุปกรณ์ฝังตัวที่มีข้อจำกัดด้านทรัพยากร จากผลการทดลองพบว่าอัลกอริทึม ChaCha20 ใช้เวลาในการเข้ารหัสเฉลี่ย 1.25 มิลลิวินาทีต่อแพ็กเก็ต และใช้เวลาในการถอดรหัสเฉลี่ย 1.15 มิลลิวินาทีต่อแพ็กเก็ต ซึ่งต่ำกว่าอัลกอริทึม AES-256 ที่ใช้เวลาเฉลี่ย 1.85 และ 1.69 มิลลิวินาทีต่อแพ็กเก็ต ตามลำดับ โดยอัลกอริทึม AES-256 ต้องใช้การคำนวณหลายรอบตามขั้นตอนและกระบวนการที่ประกอบไปด้วยขั้นตอน SubBytes, ShiftRows, MixColumns และ

AddRoundKey ส่งผลให้ต้องใช้รอบการประมวลผลมากกว่า ซึ่งผลการวิจัยนี้สอดคล้องกับ Daniel J. Bernstein ผู้พัฒนาอัลกอริทึม ChaCha ซึ่งระบุว่าอัลกอริทึม ChaCha20 ได้รับการออกแบบให้มีความปลอดภัยเทียบเท่าหรือสูงกว่า Salsa20 พร้อมทั้งเพิ่มประสิทธิภาพในการประมวลผลบนแพลตฟอร์มด้านซอฟต์แวร์ ทำให้เหมาะสำหรับอุปกรณ์ที่มีทรัพยากรจำกัด (Bernstein et al., 2008) นอกจากนี้ผลการทดลองยังสอดคล้องกับมาตรฐาน RFC 8439 ซึ่งกำหนดให้อัลกอริทึม ChaCha20 ใช้กุญแจขนาด 256 บิต ร่วมกับ Nonce ขนาด 96 บิต และ Counter ขนาด 32 บิต เพื่อป้องกันการใช้ Keystream ซ้ำ และเพิ่มความปลอดภัยของข้อมูลในระหว่างการรับส่งผ่านเครือข่าย โดยในงานวิจัยนี้ได้กำหนดให้แต่ละแพ็กเก็ตมีค่า Nonce และ Counter ที่ไม่ซ้ำกัน ส่งผลให้ข้อมูลที่เข้ารหัสแต่ละครั้งมี Ciphertext แตกต่างกัน แม้ว่าข้อมูลต้นฉบับจะเหมือนกันก็ตาม ซึ่งสอดคล้องกับข้อกำหนดมาตรฐานด้านความปลอดภัย และผลการวิจัยยังสอดคล้องกับงานของ Langley และคณะ, 2018 ซึ่งเป็นผู้ร่วมจัดทำ RFC 8439 โดยระบุว่าอัลกอริทึม ChaCha20 มีประสิทธิภาพสูงกว่า AES ในอุปกรณ์ที่ไม่มีฮาร์ดแวร์หรืออุปกรณ์เสริม อย่างเช่น เครื่องคอมพิวเตอร์ ช่วยในเข้ารหัส ผลการวิจัยสนับสนุนว่าอัลกอริทึม ChaCha20 เป็นอัลกอริทึมที่เหมาะสมสำหรับการออกแบบและพัฒนาอุปกรณ์เซนเซอร์ไร้สายในการการสื่อสารข้อมูลที่มีข้อจำกัดด้านทรัพยากร เนื่องจากสามารถรักษาความปลอดภัยของข้อมูลได้ตามมาตรฐาน พร้อมทั้งมีประสิทธิภาพในการประมวลผล ใช้หน่วยความจำที่มีจำกัดได้และรองรับการรับส่งข้อมูลแบบทันทีทันใดได้อย่างมีประสิทธิภาพ จึงมีศักยภาพในการประยุกต์ใช้กับการพัฒนาระบบเครือข่ายเซนเซอร์ไร้สายที่ต้องการความปลอดภัยในการรักษาความลับของข้อมูลได้

ข้อเสนอแนะ

งานวิจัยนี้สามารถพัฒนาระบบการสื่อสารข้อมูลแบบรักษาความเป็นส่วนตัวโดยใช้อัลกอริทึม ChaCha20 ได้อย่างมีประสิทธิภาพ ซึ่งผลการทดลองแสดงให้เห็นว่าสามารถเข้ารหัสและถอดรหัสข้อมูลได้ถูกต้อง อย่างไรก็ตามงานวิจัยยังมีข้อจำกัดบางประการที่ควรนำไปพัฒนาในการศึกษาครั้งต่อไป ดังนี้

1) การประเมินประสิทธิภาพยังจำกัดอยู่บนบอร์ด ESP32 เท่านั้น ซึ่งเป็นบอร์ดไมโครคอนโทรลเลอร์ที่ได้รับความนิยมในการนำมาพัฒนาอุปกรณ์เซนเซอร์ไร้สาย ดังนั้นผลการทดลองอาจแตกต่างเมื่อประยุกต์ใช้กับบอร์ดไมโครคอนโทรลเลอร์ประเภทอื่น โดยการศึกษาต่อไปควรเปรียบเทียบประสิทธิภาพของกับบอร์ดบอร์ดไมโครคอนโทรลเลอร์อื่นที่มีความเร็วในการประมวลผลที่แตกต่างกัน

2) การประเมินผลยังอยู่ภายใต้เครือข่ายไร้สาย การศึกษาครั้งต่อไปควรประเมินบนเครือข่ายสื่อสารประเภทอื่น เช่น LoRaWAN, NB-IoT หรือ 5G รวมถึงการทดสอบภายใต้สภาวะเครือข่ายที่มีโอกาสสูญเสียแพ็กเกต (Packet Loss)

3) ควรพัฒนาระบบวิเคราะห์ข้อมูลร่วมกับการรักษาความปลอดภัยของข้อมูล ในอนาคตสามารถต่อยอดระบบโดยผสานกับเทคนิคด้านปัญญาประดิษฐ์ (Artificial Intelligence: AI) หรือการเรียนรู้ของเครื่อง (Machine Learning: ML) เพื่อวิเคราะห์แนวโน้มคุณภาพน้ำ คาดการณ์ความเสี่ยงต่อการเกิดโรค หรือควบคุมระบบหมุนเวียนน้ำอัตโนมัติ พร้อมทั้งรักษาความปลอดภัยของข้อมูลด้วยอัลกอริทึม ChaCha20 หรือ ChaCha20-Poly1305 ซึ่งจะช่วยยกระดับเพาะเลี้ยงสู่การเป็นระบบเกษตรอัจฉริยะ (Smart Aquaculture) อย่างสมบูรณ์

สรุปข้อเสนอแนะ

จากข้อจำกัดของงานวิจัยการศึกษาครั้งต่อไปควรมุ่งเน้นการเพิ่มความสมบูรณ์ของระบบทั้งด้านความมั่นคงปลอดภัยและการวิเคราะห์ข้อมูลอัจฉริยะ เพื่อให้ระบบสามารถนำไปประยุกต์ใช้งานในฟาร์มเพาะเลี้ยงสัตว์น้ำและระบบเกษตรอัจฉริยะได้อย่างมีประสิทธิภาพ มีความปลอดภัย และรองรับการใช้งานในระดับอุตสาหกรรมได้ในอนาคต

เอกสารอ้างอิง

จีระนันท์ วงศ์วทัญญ, ปิยฉัตร ทองแพง, เมธี ไชยหา และอภิญญา ภูมิสายดอน. (2567). การพัฒนาผลิตภัณฑ์ข้าวเกรียบปูนาปรุงรส. *วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏศรีสะเกษ*, *4*(1), 45–54.

นิชนันท์ ชูเกิด, พุทธพร พุ่มโรจน์ และสุขสันต์ ขำคง. (2568). ผลของระบบการเพาะเลี้ยงแบบน้ำหมุนเวียนต่อค่าโลหิตวิทยา คุณภาพน้ำและสมรรถนะการเจริญเติบโตของปลานิลแดง (Oreochromis niloticus X O. mossambicus). *วารสารเกษตรพระวรุณ มหาวิทยาลัยราชภัฏมหาสารคาม*, *22*(1), 67–77.

นิภาศักดิ์ คงงาม, ประภัสรา ศิริขันธ์แสง และเฉลา สำราญดี .(2561). ความหลากหลายของการใช้ประโยชน์จากปูนา ของชุมชนในพื้นที่บริเวณแนวเทือกเขาพนมดงรัก. *วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏสุรินทร์*, *20*(2), 229-241.

วิจิตรตา อรรถสาร, อดิเทพชัยย์การณ์ ภาชนะวรรณ, จิราวรรณ คำธร และอนวัทย์ ผาลี. (2567). การเลี้ยงปูนาพันธุ์ Esanthelphusa dugasti ที่เสริมด้วยเปลือกไข่ เพื่อเพิ่มประสิทธิภาพการเจริญเติบโตและอัตราการรอดตาย. *วารสารวิจัยและส่งเสริมวิชาการเกษตร*, *41*(1), 65–73.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. http://doi.org/10.1016/j.jnca.2017.04.002

Bernstein, D. J., Robshaw, M., & Billet, O. (2008). *New stream cipher designs*. Springer-Verlag.

Jawad, H. M, Nordin, R., Gharghan, S. K., Jawad, A. M., & Ismail, M. (2017). Energy-efficient wireless sensor networks for precision agriculture: A review. *Sensors*, *17*(8), 1781. https://doi.org/10.3390/s17081781

Langley, A., Hamburg, M., & Turner, S. (2018). *RFC 8439: ChaCha20 and Poly1305 for IETF Protocols*. n.p.

Nir, Y., & Langley, A. (2018). ChaCha20 and Poly1305 for IETF protocols. *RFC*, 8439, 1-46.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead, *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

Timmons, M., Guerdat, T., & Vinci, B. (2018). *Recirculating aquaculture* (4th ed.). n.p.