การออกแบบและพัฒนาสมาร์ตดิจิทัลแพลตฟอร์มระบบจัดเก็บและแลกเปลี่ยนข้อมูล สำหรับระบบบัญชาการและควบคุมของกองทัพอากาศ โดยใช้เทคโนโลยีบล็อกเชน

The Design and Development of a Smart Digital Data Storage and Exchange Platform for the Air Force Command and Control Systems Using Blockchain Technology

ธนกฤต เพ็งเคียน (Thanakrit Pengkian)* ประสงค์ ปราณีตพลกรัง (Prasong Praneetpolgrang)**
และพายัพ ศิรินาม (Payap Sirinam)**

Received: October 26, 2023
Revised: September 27, 2024
Accepted: October 2, 2024

*ผู้นิพนธ์ประสานงาน: ธนกฤต เพ็งเคียน (Thanakrit Pengkian) อีเมล: intelligent.it4@gmail.com

DOI:10.14416/j.it.2026.v1.004

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบและพัฒนาสมาร์ตดิจิทัลแพลตฟอร์มระบบจัดเก็บและแลกเปลี่ยนข้อมูลสำหรับระบบบัญชาการและควบคุมของกองทัพอากาศโดยใช้เทคโนโลยีบล็อกเชน ซึ่งระบบบัญชาการและควบคุมเป็นระบบที่มุ่งเน้นกรรมวิธีและข้อมูลในการจัดการและควบคุมดำเนินงานหรือกิจกรรม ทั้งนี้รวมถึงการตัดสินใจในสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็ว หรือในสภาวะที่มีความซับซ้อนและไม่แน่นอน ทั้งหมดนี้จำเป็นต้องมีการแลกเปลี่ยนข้อมูลที่รวดเร็วและปลอดภัย ดังนั้น งานวิจัยนี้จึงได้สร้างสถาปัตยกรรมของแพลตฟอร์ม ที่มีการนำเอาบล็อกเชนมาใช้เพื่อจัดเก็บและแลกเปลี่ยนข้อมูล เพื่อเพิ่มขีดความสามารถในการปกป้องข้อมูล และเสริมสร้างความปลอดภัยในการแลกเปลี่ยนข้อมูล โดยการทดสอบการส่งข้อมูลขนาดใหญ่ผ่านสมาร์ตคอนแทร็กต์พบว่า ระบบสามารถจัดการกับข้อมูลขนาดต่างๆ ได้อย่างดี อย่างไรก็ตาม เมื่อขนาดของข้อมูลเพิ่มขึ้น เวลาประมวลผลก็เพิ่มขึ้นเช่นกัน โดยข้อมูลขนาดใหญ่ที่สุด 20 MB ใช้เวลาในการประมวลผลเฉลี่ย 1.175 วินาที อย่างไรก็ตาม ผลลัพธ์จากงานวิจัยนี้จะทำให้กองทัพอากาศมีแพลตฟอร์มเป็นของตนเองสำหรับบัญชาการและควบคุมให้การทำงานเป็นไปได้อย่างเข้มแข็งและมีประสิทธิภาพสูง ซึ่งจะเป็นการบูรณาการเทคโนโลยีสมัยใหม่ให้เข้ากับบริบททางทหารอันส่งผลให้เป็นเทคโนโลยีป้องกันประเทศ ที่อยู่บนพื้นฐานของภูมิปัญญาไทยที่สามารถพึ่งพาตนเองได้

คำสำคัญ: บล็อกเชน แพลตฟอร์ม ระบบบัญชาการและควบคุม

Abstract

Research objectives are to design and develop a smart digital data storage and exchange platform for the Air Force's command and control system using the blockchain. This system focuses on process in managing data and controlling operations or activities. This also includes executing decisions under rapid changing situations or in conditions that are far more complex and uncertain. All of these require a fast and secure exchange of data. Then, the research has created an architectural platform that uses blockchain to store and exchange data. Moreover, to enhance data protection capabilities and strengthen the security of data exchange, large data transmissions were tested via smart contracts. The results showed that the system can handle data of various sizes effectively. However, as the data size increases, the processing time also increases, with the largest data size of 20 MB taking an average of 1.175 seconds to process. The research result provides the Air Force platform for command and control to work with full strength and high efficiency. This will integrate new technology with the military context, transcending into defense technology, based on the concept of Thai invention aiming to be self-sufficient.

Keywords: Blockchain, Platform, Command and Control.

** สาขาวิชาเทคโนโลยีป้องกันประเทศ สำนักบัณฑิตศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช*

** Defense Technology Program, The Graduate School of Navaminda Kasatriyadhiraj Royal Air Force Academy.*

*** กองการศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช*

*** Academic Faculty, Navaminda Kasatriyadhiraj Royal Air Force Academy.*

1. บทนำ

จากยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ. 2561-2580) หนึ่งในประเด็นสำคัญมากที่ได้รับการเน้นย้ำคือเรื่องของเทคโนโลยีสารสนเทศและการสื่อสารหรือดิจิทัลที่มีการพัฒนาอย่างรวดเร็ว ซึ่งทำให้เกิดภัยคุกคามในมิติไซเบอร์ที่หลากหลาย ไม่ว่าจะเป็นการจารกรรมข้อมูล หรือการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ ที่ส่งผลกระทบต่อข้อมูลหรือโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ ทั้งนี้ หลายประเทศได้มีการจัดตั้งหน่วยงานเฉพาะเพื่อรับผิดชอบเรื่องนี้โดยตรง อย่างไรก็ตาม กองทัพอากาศยังต้องมุ่งมั่นในการพัฒนาขีดความสามารถด้านไซเบอร์ของตนเอง เพื่อให้มีความพร้อมในการตอบสนองต่อภัยคุกคามทางไซเบอร์ และพัฒนาระบบเครือข่ายคอมพิวเตอร์ให้มีความแข็งแกร่ง และปลอดภัยมากยิ่งขึ้น

เทคโนโลยีบล็อกเชนถือเป็นอีกหนึ่งทางเลือกในการพัฒนาระบบเครือข่ายคอมพิวเตอร์ของกองทัพอากาศเนื่องจากเป็นเทคโนโลยีที่มีการประมวลผลและจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology: DLT) [1] โดยใช้วิทยาการเข้ารหัสลับ (Cryptography) ร่วมกับกลไกความเห็นพ้อง (Consensus) ในการบันทึกข้อมูล และกระจายการจัดเก็บข้อมูลชุดเดียวกันไว้หลายแห่ง (Distributed Ledgers) ด้วยคุณสมบัติเหล่านี้ทำให้บล็อกเชนได้รับการยอมรับว่าเป็นเทคโนโลยีที่มีความปลอดภัยสูง ช่วยป้องกันการรั่วไหลของข้อมูลได้ จึงได้มีการนำมาประยุกต์ใช้กับการตรวจสอบความถูกต้องของข้อมูลในด้านอื่น ๆ เช่น เมืองอัจฉริยะ [2], [3] อินเทอร์เน็ตประสานสรรพสิ่ง [4], [5] การดูแลสุขภาพ [6], [7] เป็นต้น

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

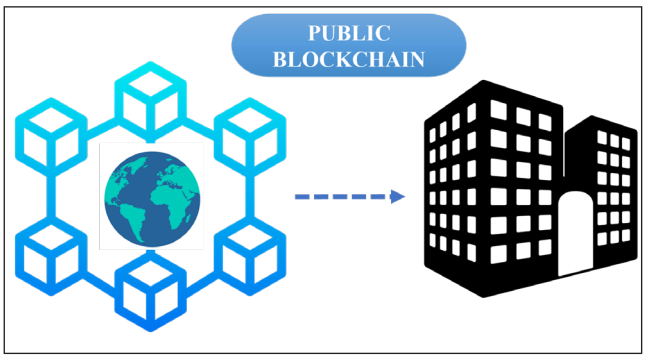
2.1 เทคโนโลยีบล็อกเชน

บล็อกเชน เป็นเทคโนโลยีการจัดเก็บข้อมูลแบบ ฐานข้อมูลใช้ร่วม (Shared Database) โดยเป็นรูปแบบการบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านั้นไม่อาจที่จะเปลี่ยนแปลงหรือแก้ไขได้ ผู้ใช้งานทุกคนจะได้เห็นข้อมูลชุดเดียวกันทั้งหมด โดยใช้หลักการของวิทยาการเข้ารหัสลับ จุดเริ่มต้นของเทคโนโลยีบล็อกเชน เกิดขึ้นครั้งแรกในปี 2008 โดยการนำเสนอของ "Satoshi Nakamoto" [8] เป็นการนำเสนอแนวคิดเกี่ยวกับการสร้างแพลตฟอร์ม (Platform) ที่สร้างความปลอดภัยในการแลกเปลี่ยนเงินสกุลดิจิทัลที่มีชื่อว่า "Bitcoin" ในปัจจุบันเทคโนโลยีบล็อกเชนนอกจากจะใช้ในการซื้อขายแลกเปลี่ยนสกุลเงินดิจิทัลแล้วยังมีการนำมาใช้งานกับธุรกิจต่าง ๆ อีกมากมายซึ่งจะเรียกว่า แอปพลิเคชันแบบกระจาย (Decentralized Applications) [9], [10]

2.1.1 ประเภทของบล็อกเชน

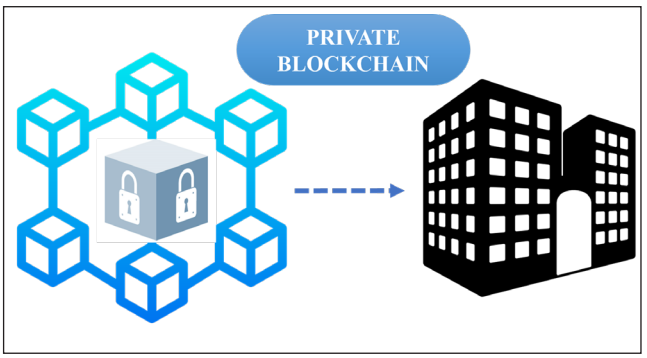
บล็อกเชนแบ่งออกได้เป็น 3 ประเภท [11] โดยพิจารณาจากข้อกำหนด ในการเข้าร่วมเป็นสมาชิกของเครือข่าย คือ บล็อกเชนแบบเปิดสาธารณะ (Public Blockchain) บล็อกเชนแบบปิดหรือแบบส่วนตัว (Private Blockchain) และบล็อกเชนแบบเฉพาะกลุ่ม (Consortium Blockchain)

บล็อกเชนแบบเปิดสาธารณะ คือบล็อกเชนวงเปิดที่อนุญาตให้ทุกคนเข้าใช้งานไม่ว่าจะเป็นการอ่าน หรือการทำธุรกรรมต่าง ๆ ได้อย่างอิสระโดยไม่จำเป็นต้องขออนุญาต หรือรู้จักในอีกชื่อคือ Permissionless Blockchain ดังภาพที่ 1



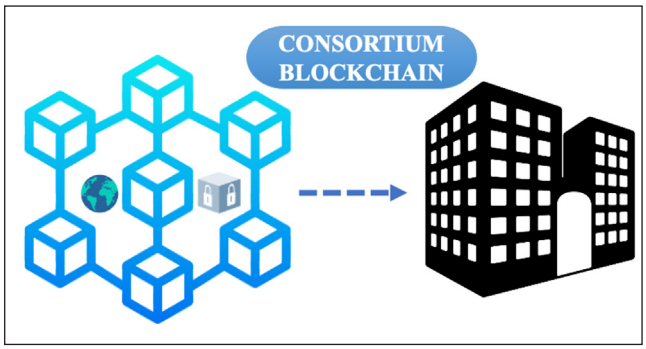
ภาพที่ 1 บล็อกเชนแบบเปิดสาธารณะ

บล็อกเชนแบบปิดหรือแบบส่วนตัว คือ บล็อกเชนวงปิดที่เข้าใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น [12] ซึ่งส่วนใหญ่ถูกสร้างขึ้นเพื่อใช้งานภายในองค์กร ดังนั้น ข้อมูลการทำธุรกรรมต่าง ๆ จะถูกจำกัดอยู่เฉพาะภายในเครือข่ายที่ประกอบไปด้วยสมาชิกที่ได้รับอนุญาตเท่านั้น ดังภาพที่ 2



ภาพที่ 2 บล็อกเชนแบบปิด

บล็อกเชนแบบเฉพาะกลุ่ม คือบล็อกเชนที่เปิดให้ใช้งานได้เฉพาะกลุ่มเท่านั้น โดยเป็นการผสมผสานแนวคิดระหว่างบล็อกเชนแบบเปิดสาธารณะ และบล็อกเชนแบบปิด [13] ซึ่งส่วนมากเป็นการรวมตัวกันขององค์กรที่มีลักษณะธุรกิจเหมือนกันและต้องมีการแลกเปลี่ยนข้อมูลระหว่างกันอย่างสม่ำเสมออยู่แล้ว มาร่วมตัวกันตั้งวงบล็อกเชนขึ้นมา ทั้งนี้ เนื่องจากธุรกรรมและข้อมูลที่จัดเก็บเป็นข้อมูลที่เป็นความลับหรือข้อมูลส่วนตัวภายในองค์กรอันส่งผลให้องค์กรไม่สามารถเปิดเผยข้อมูลดังกล่าวทั้งหมดแก่สาธารณชนได้ ด้วยเหตุนี้ ผู้เข้าร่วมบล็อกเชนเฉพาะกลุ่มจำเป็นต้องได้รับการอนุญาตจากผู้ดูแลระบบ จึงจะเข้าใช้งานได้ เช่น เครือข่ายระหว่างธนาคารที่ใช้ในการแลกเปลี่ยนข้อมูลการทำธุรกรรม หรือแลกเปลี่ยนสินทรัพย์ภายในกลุ่มของธนาคาร [14], [15] เช่น Japanese Bank และ R3CEV ดังภาพที่ 3



ภาพที่ 3 *บล็อกเชนเฉพาะกลุ่ม*

กล่าวโดยสรุป เทคโนโลยีบล็อกเชนคือ ลำดับของบล็อกหรือกลุ่มระเบียนธุรกรรมซึ่งในแต่ละกลุ่มระเบียนได้ใช้วิธีการเข้ารหัสเพื่อเชื่อมข้อมูลเข้าเป็นกลุ่มระเบียนที่เปลี่ยนรูปไม่ได้ ทั้งในรายละเอียดจะเป็นการแลกเปลี่ยนและกระจายบัญชีธุรกรรมอิเล็กทรอนิกส์กับผู้ที่เกี่ยวข้องในเครือข่าย ซึ่งข้อมูลจะถูกบันทึกถาวร เปลี่ยนแปลงไม่ได้ อีกทั้ง ยังมีกลไกในการป้องกันการแก้ไขรายการข้อมูลจากธุรกรรมใด ๆ ไม่ให้ผิดเพี้ยนไปจากต้นฉบับ ทำให้ระบบคอมพิวเตอร์ในเครือข่ายสามารถรักษาความสมบูรณ์ถูกต้องของข้อมูลต้นฉบับเอาไว้ได้ ปกติจะใช้สถาปัตยกรรมข้อมูลแบบกระจายมีการจัดการกระบวนการโดยใช้เครือข่ายคอมพิวเตอร์ในระดับเดียวกัน (Peer-to-Peer Network) ที่ป้องกันความล้มเหลวของจุดใดจุดหนึ่งได้ ที่สำคัญคือหากต้องการจะทำการปรับปรุงเปลี่ยนแปลง และตรวจสอบความถูกต้องของข้อมูลทั้งหมดก็ทำได้ในเวลาเดียวกัน เทคโนโลยีบล็อกเชนอาจจะเป็นส่วนเสริมสำหรับโลกอนาคตที่มีทั้งรูปแบบรวมศูนย์ และแบบกระจาย นั่นคือแนวคิดที่อาจส่งเสริมการพัฒนาระบบสังคมขนาดใหญ่ที่มีทั้งรูปแบบดั้งเดิมและแบบที่มีนวัตกรรม ดังนั้น ปัจจุบันจึงเป็นช่วงเวลาที่เทคโนโลยีบล็อกเชน จะอยู่ในระบบสังคมขนาดใหญ่ที่มีทั้งแบบรวมศูนย์และแบบกระจายได้

2.2 แพลตฟอร์ม

แพลตฟอร์ม (Platform) คือ สภาวะแวดล้อมที่ประกอบด้วยฮาร์ดแวร์ และซอฟต์แวร์ของระบบ ซึ่งวางไว้กว้าง ๆ และเปิดให้ผู้อื่นเข้ามาพัฒนาต่อยอดงานของตนเองได้ ทำหน้าที่เป็นตัวกลางระหว่างผู้ใช้บริการและผู้ให้บริการเข้ามาดำเนินงานของตนเองได้ อีกทั้งสร้างโมเดลงานของตนเองได้ [16]

2.3 การเข้ารหัสข้อมูล

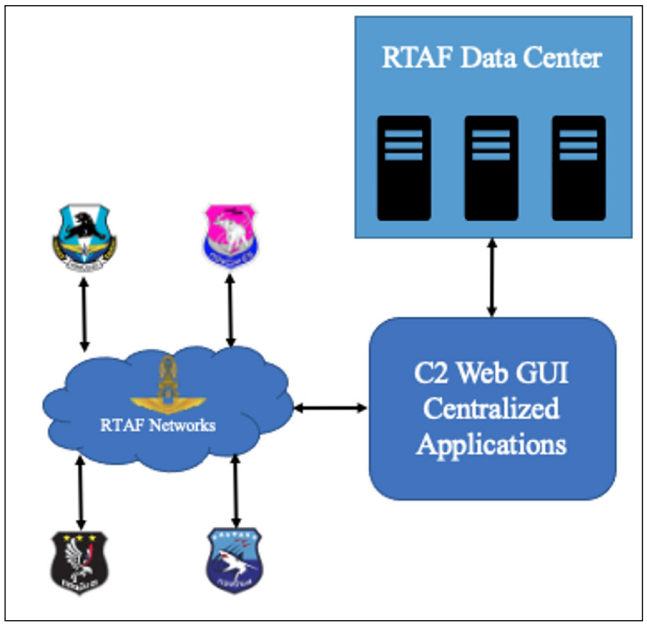
การเข้ารหัสข้อมูลสามารถแบ่งออกเป็นสองประเภทหลัก คือ การเข้ารหัสแบบสมมาตร (Symmetric Encryption) และการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) [17], [18] การเข้ารหัสแบบสมมาตรใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัสข้อมูล กุญแจนี้จะถูกเก็บเป็นความลับและใช้ร่วมกันระหว่างผู้ส่งและผู้รับ เช่น การเข้ารหัส AES (Advanced Encryption Standard) ซึ่งมีความปลอดภัยสูงและใช้กันอย่างแพร่หลาย ขณะที่การเข้ารหัสแบบอสมมาตรใช้คู่กุญแจสาธารณะและกุญแจส่วนตัว กุญแจสาธารณะใช้ในการเข้ารหัสข้อมูล และกุญแจส่วนตัวใช้ในการถอดรหัสข้อมูล เช่น การเข้ารหัส RSA (Rivest-Shamir-Adleman) ซึ่งมีความปลอดภัยสูงและเหมาะสำหรับการแลกเปลี่ยนกุญแจและการปกป้องข้อมูลที่ต้องการความมั่นคงในระดับสูง

2.4 ระบบบัญชาการและควบคุม

ระบบบัญชาการและควบคุม (Command and Control Systems) คือ ระบบที่ใช้ในการส่งคำสั่ง และข้อมูลในกระบวนการตัดสินใจระหว่างหน่วยต่าง ๆ [19] ในองค์กรหรือหน่วยงานทางทหาร ระบบนี้ช่วยในการประสานงานและการจัดการทรัพยากรในการดำเนินการต่าง ๆ ผ่านระบบเครือข่ายคอมพิวเตอร์ของกองทัพอากาศ ดังภาพที่ 4

ระบบบัญชาการและควบคุมใช้สำหรับการประสานงานและการควบคุมการดำเนินการทางทหารทั้งการป้องกันการโจมตี หรือการสนับสนุนในภารกิจต่าง ๆ ประกอบด้วยส่วนประกอบหลัก ๆ ดังนี้

2.4.1 Command คือ ส่วนที่เกี่ยวข้องกับการตัดสินใจ



ภาพที่ 4 แสดงการเชื่อมต่อข้อมูลระบบบัญชาการและควบคุมของกองทัพอากาศ

และการสั่งการ ได้แก่ การวางแผน การกำหนดยุทธศาสตร์ การสั่งการให้กำลังทหารดำเนินการตามแผน

2.4.2 Control คือ ส่วนที่เกี่ยวข้องกับการควบคุมและการประสานงาน เพื่อให้แน่ใจว่าการดำเนินการไปในทิศทางที่ถูกต้อง และสอดคล้องกับแผน

2.4.3 Communication คือ ส่วนที่เกี่ยวข้องกับการสื่อสารระหว่างหน่วยต่าง ๆ ในระบบ เช่น การส่งข้อมูล การส่งคำสั่ง การแลกเปลี่ยนข้อมูลที่จำเป็น

2.4.4 Intelligence คือ ส่วนที่เกี่ยวข้องกับการจัดหา การวิเคราะห์ และการแบ่งปันข้อมูลข่าวกรอง ที่ช่วยในการตัดสินใจ

2.4.5 Technology คือ อุปกรณ์และเทคโนโลยีที่ใช้ในระบบ เช่น วิทยุ ดาวเทียม ระบบคอมพิวเตอร์ ซอฟต์แวร์ และเครือข่ายคอมพิวเตอร์

2.5 งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่ผ่านมาพบว่า เทคโนโลยีบล็อกเชน นอกจากจะใช้ในการแลกเปลี่ยนสกุลเงินดิจิทัลแล้ว พบว่าเทคโนโลยีนี้สามารถนำมาใช้ประยุกต์ใช้กับงานด้านอื่น ๆ ได้ โดยมีรายละเอียดดังนี้

Arvind Panwar [20] ได้ทำการวิจัยเรื่อง "A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake" ผลการวิจัยพบว่า การใช้บล็อกเชนได้เพิ่มความปลอดภัยและความน่าเชื่อถือ ในการจัดการข้อมูล PHR บล็อกเชนจะทำหน้าที่เป็น Ledger ที่ไม่สามารถแก้ไขได้ นั่นหมายความว่าข้อมูลที่ถูกบันทึกเข้าสู่ระบบแล้วจะไม่ถูกเปลี่ยนแปลงหรือลบล้างได้ อีกทั้ง การใช้สัญญาสมาร์ตหรือสมาร์ตคอนแทร็กต์ (Smart Contract) ในการจัดการอนุญาตและควบคุมการเข้าถึงข้อมูล สมาร์ตคอนแทร็กต์ช่วยให้กำหนดเงื่อนไข และกฎในการเข้าถึงข้อมูลได้อย่างเป็นรูปธรรม และทำให้การจัดการข้อมูลมีความโปร่งใสและปลอดภัยมากขึ้น

Ulfah Nadiya [21] ได้ทำการวิจัยเรื่อง "Blockchain-based Secure Data Storage for Door Lock System" ผลการวิจัยพบว่า การนำบล็อกเชนมาประยุกต์ใช้ในงานเกี่ยวกับการยืนยันใบหน้าเป็นวิธีที่สร้างความน่าเชื่อถือ เนื่องจากข้อมูลที่ถูกจัดเก็บลงในบล็อกเชนไม่อาจเปลี่ยนแปลงได้

วรวุฒิ บัวทองจันทร์ [22] ได้พัฒนา "ต้นแบบการอนุวัติการจัดการระบบบริการสหกรณ์ร้านค้าดิจิทัลในประเทศไทยด้วยการประยุกต์ใช้บล็อกเชน" ผู้วิจัยได้ประยุกต์ใช้เทคโนโลยีบล็อกเชนในการพัฒนาต้นแบบระบบบริการสหกรณ์ร้านค้าดิจิทัล ผลการวิจัยพบว่า ระบบบริการสหกรณ์ร้านค้าดิจิทัลในประเทศไทยมีความน่าเชื่อถือเมื่อประยุกต์ใช้บล็อกเชนในการดำเนินการกับข้อมูลธุรกรรมในส่วนจัดเก็บของระบบบริการสหกรณ์ร้านค้าดิจิทัล ทำให้ระบบบริการสหกรณ์ร้านค้าดิจิทัลมีความถูกต้องด้านข้อมูลธุรกรรม อีกทั้งข้อมูลของระบบบริการมีความมั่นคงปลอดภัย นอกจากนั้น ยังช่วยให้สหกรณ์ร้านค้าดิจิทัลตรวจสอบข้อมูลธุรกรรมในที่จัดเก็บได้ได้อย่างสะดวกและมีประสิทธิภาพ

Zhuohao et al. [23] ได้ทำการวิจัยเรื่อง “A Blockchain-Based Auditable Semi-Asynchronous Federated Learning for Heterogeneous Clients" ผลการวิจัยพบว่า ระบบการเรียนรู้แบบรวมศูนย์ที่ใช้บล็อกเชนเพื่อเพิ่มความโปร่งใสและความสามารถในการตรวจสอบได้ในกระบวนการแลกเปลี่ยนโมเดลการเรียนรู้ร่วมกัน (Federated Learning: FL) ในสภาพแวดล้อมที่มีอุปกรณ์ที่หลากหลาย โดยระบบ BASA-FL (Blockchain-based Auditable Semi-Asynchronous Federated Learning) ใช้สมาร์ตคอนแทร็กต์เพื่อประสานงานและบันทึกกระบวนการแลกเปลี่ยนโมเดลการเรียนรู้ร่วมกัน นอกจากนี้ ระบบยังมีการประเมินและให้รางวัลตามการมีส่วนร่วมของผู้ใช้ ทำให้สามารถจัดการกับปัญหาความแตกต่างของอุปกรณ์และเพิ่มประสิทธิภาพในการเรียนรู้ร่วมกัน ผลการทดลอง

แสดงให้เห็นว่าระบบ BASA-FL สามารถปรับปรุงประสิทธิภาพในการแลกเปลี่ยนโมเดลและการตรวจสอบความถูกต้องได้อย่างมีประสิทธิภาพ

Barbaria et al. [24] ได้ทำการวิจัยเรื่อง "Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks" ผลการวิจัยพบว่า การใช้เครือข่ายแบบกระจายศูนย์ที่ใช้เทคโนโลยีบล็อกเชนในการแบ่งปันข้อมูลผู้ป่วย โดยเน้นการรักษาความเป็นส่วนตัวและการจัดการความยินยอมของผู้ป่วยในการแชร์ข้อมูล ระบบที่พัฒนาขึ้นใช้ Hyperledger Blockchain เพื่อเสริมความปลอดภัยและความโปร่งใสในการแลกเปลี่ยนข้อมูลทางการแพทย์ นอกจากนี้ยังพัฒนาโมเดลการจัดการข้อมูลที่รวมการควบคุมการเข้าถึงและการตรวจสอบการใช้ข้อมูลผ่านสมาร์ตคอนแทร็กต์ ผลการวิจัยแสดงให้เห็นว่าเทคโนโลยีบล็อกเชนสามารถเพิ่มความปลอดภัย ความโปร่งใส และความเชื่อถือในการจัดการข้อมูลผู้ป่วยได้อย่างมีประสิทธิภาพ

Pawar P et al. [25] ได้ทำการวิจัยเรื่อง "HealthChain a Blockchain-based Personal Health Information Management System" ซึ่งเป็นระบบการจัดการข้อมูล สุขภาพส่วนบุคคลโดยใช้เทคโนโลยีบล็อกเชน ผลการวิจัยพบว่า eHealthChain เพิ่มความปลอดภัย ความโปร่งใส และความสามารถในการจัดการข้อมูลสุขภาพจากอุปกรณ์ IoT ทางการแพทย์ ระบบนี้ประกอบด้วยชั้นบล็อกเชนสำหรับเก็บข้อมูล ชั้นอุปกรณ์ IoT สำหรับรวบรวมข้อมูลสุขภาพ ชั้นแอปพลิเคชันสำหรับแลกเปลี่ยนข้อมูลสุขภาพ และชั้นอะแดปเตอร์ที่เชื่อมต่อชั้นต่าง ๆ ผลการวิจัย แสดงให้เห็นว่า eHealthChain ช่วยให้ผู้ใช้ควบคุมการเก็บรวบรวม การจัดเก็บ และการแชร์ข้อมูลสุขภาพได้อย่างสมบูรณ์ โดยใช้ Hyperledger Fabric เพื่อความปลอดภัยและความเป็นส่วนตัวของข้อมูลสุขภาพ

Sejong Lee et al. [26] ได้ทำการวิจัยเรื่อง "Searchable Blockchain-Based Healthcare Information Exchange System to Enhance Privacy Preserving and Data Usability" ผลการวิจัยพบว่า ระบบแลกเปลี่ยนข้อมูลสุขภาพที่ใช้เทคโนโลยีบล็อกเชนเพื่อเพิ่มความปลอดภัยและความสามารถในการใช้ข้อมูลโดยใช้การเข้ารหัสแบบ Searchable Encryption และการเข้ารหัสแบบ Homomorphic Encryption เพื่อให้ผู้ใช้สามารถค้นหาและใช้ข้อมูลสุขภาพที่เข้ารหัสอยู่ได้อย่างมีประสิทธิภาพ ผลการทดลองแสดงให้เห็นว่าระบบที่พัฒนาขึ้นนี้สามารถลดความเสี่ยงจากการละเมิดความเป็นส่วนตัว และเพิ่มความสามารถในการใช้งานของข้อมูลสุขภาพได้อย่างดี

Mohammad Wizid et al. [27] ได้ทำการวิจัยเรื่อง "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things" ผลการวิจัยพบว่า ในอนาคตการสร้างระบบการสื่อสารที่ปลอดภัยด้วยบล็อกเชนสำหรับอินเทอร์เน็ตของสรรพสิ่งอัจฉริยะ (IoIT) โดยเน้นที่การจัดการคีย์การยืนยันตัวตน และการป้องกันข้อมูลจากการโจมตีต่าง ๆ เช่น การโจมตีแบบ replay, MITM, และการปลอมแปลงตัว ระบบที่นำเสนอมีการใช้บล็อกเชนเพื่อเพิ่มความปลอดภัย ความโปร่งใส และการกระจายตัวของข้อมูล และยังเสนอแนวทางวิจัยในอนาคตเพื่อพัฒนากลไกการเข้ารหัสที่มีประสิทธิภาพมากขึ้น เพื่อตอบสนองความต้องการของระบบ IoIT

3. วิธีดำเนินการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบ และพัฒนาสมาร์ตดิจิทัลแพลตฟอร์มระบบจัดเก็บ และแลกเปลี่ยนข้อมูลสำหรับระบบบัญชาการ และควบคุมของกองทัพอากาศ โดยใช้เทคโนโลยีบล็อกเชน เป็นการวิจัยและพัฒนา (Research and Development) ในบทความนี้จะกล่าวถึง ขั้นตอนการวิจัยโดยใช้วิธีดำเนินการตามวงจรการพัฒนาระบบ (System Development Life Cycle: SDLC) มีรายละเอียดดังนี้

3.1 ศึกษาและรวบรวมข้อมูล

จากการศึกษาข้อมูล สรุปได้ดังนี้

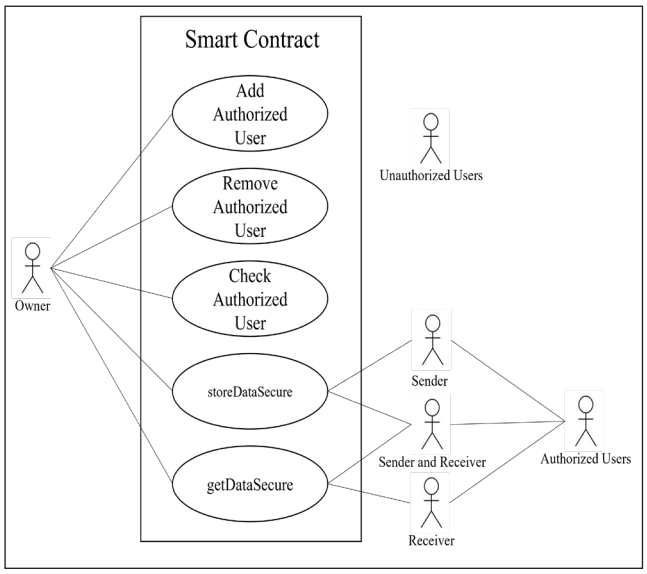
3.1.1 เทคโนโลยีที่นำมาใช้พัฒนาระบบ ผู้วิจัยได้เลือกใช้ Hyperledger Fabric Blockchain เป็นบล็อกเชนแบบส่วนตัวที่เขียนคำสั่งต่าง ๆ ให้ทำงานในรูปแบบแอปพลิเคชันแบบกระจาย (Decentralized Applications) [28], [29] รวมถึงการทดสอบในสภาวะที่ผู้วิจัยสามารถควบคุมได้

3.1.2 ภาษาที่ใช้ในการพัฒนา ผู้วิจัยได้เลือกใช้ภาษา JavaScript ในการพัฒนาสมาร์ตคอนแทร็กต์ และใช้ PHP Laravel Framework, JavaScript ในการพัฒนาแพลตฟอร์ม

3.2 การวิเคราะห์และออกแบบระบบ

การวิเคราะห์และออกแบบระบบระบบจัดเก็บ และแลกเปลี่ยนข้อมูลสำหรับระบบบัญชาการและควบคุมของกองทัพอากาศ โดยใช้เทคโนโลยีบล็อกเชน เป็นขั้นตอนที่จัดทำขึ้นเพื่อให้มั่นใจว่าระบบดังกล่าวจะมีความปลอดภัย โปร่งใส และมีประสิทธิภาพ โดยมีรายละเอียดดังนี้

3.2.1 การวิเคราะห์ฟังก์ชันการทำงานของสัญญาสมาร์ตหรือสมาร์ตคอนแทร็กต์ [30] เพื่อระบุฟังก์ชันการทำงานต่าง ๆ และช่วยในการกำหนดขอบเขตและความต้องการของระบบ เขียนเป็นแผนภาพยูสเคส (Use Case Diagram) ได้ดังภาพที่ 5



ภาพที่ 5 *Use Case Diagram การทำงานของระบบ*

จากภาพที่ 5 แสดงแผนภาพยูสเคสฟังก์ชันการทำงานของระบบที่เชื่อมต่อกับสมาร์ตคอนแทร็กต์ โดยจะแบ่ง Actors ออกเป็น 3 กลุ่ม คือ Owner คือ เจ้าของระบบ Authorized Users คือ ผู้ใช้ที่ได้รับอนุญาตจาก Owner และ Unauthorized Users คือผู้ที่ไม่ได้รับอนุญาต ดังตารางที่ 1

ตารางที่ 1 *แสดงสิทธิ์การใช้งานสมาร์ตคอนแทร็กต์*

Function	Owner	Authorized Users			Unauthorized Users
		Sender and Receiver	Sender	Receiver	
AddAuthorized	✓	×	×	×	×
RemoveAuthorized	✓	×	×	×	×
CheckAuthorized	✓	×	×	×	×
storeDataSecure	✓	✓	✓	×	×
getDataSecure	✓	✓	×	✓	×

จากตารางที่ 1 แสดงสิทธิ์การใช้งานฟังก์ชัน อธิบายได้ดังนี้

1) ฟังก์ชันเพิ่มผู้ใช้ที่ได้รับอนุญาต (Add Authorized User) เข้าในเครือข่ายบล็อกเชน ผู้ที่ใช้ฟังก์ชันนี้ได้ คือ เจ้าของระบบ (Owner) เท่านั้น

2) ฟังก์ชันลบผู้ใช้ที่ได้รับอนุญาต (Remove Authorized User) ผู้ที่ใช้ฟังก์ชันนี้ได้ คือเจ้าของระบบ (Owner) เท่านั้น

3) ฟังก์ชันตรวจสอบผู้ใช้ที่ได้รับอนุญาต (Check Authorized User) ผู้ที่ใช้ฟังก์ชันนี้ได้ คือเจ้าของระบบ (Owner) เท่านั้น

4) ฟังก์ชันส่งข้อมูล (storeDataSecure) ผู้ที่ใช้ฟังก์ชันนี้ได้จะต้องเป็นผู้ใช้ที่ได้รับอนุญาต (Authorized Users) ที่ได้รับสิทธิ์ Sender และ Sender and Receiver เท่านั้น

5) ฟังก์ชันรับข้อมูล (getDataSecure) ผู้ที่ใช้ฟังก์ชันนี้ได้จะต้องเป็นผู้ใช้ที่ได้รับอนุญาต ที่ได้รับสิทธิ์ Receiver และ Sender and Receiver เท่านั้น

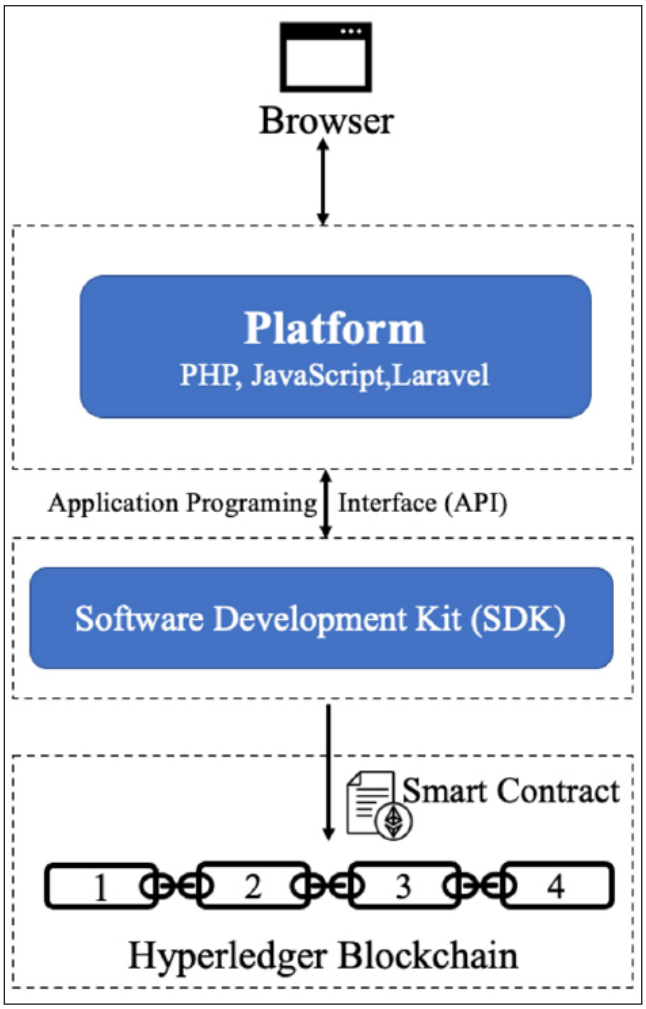
3.2.2 การออกแบบสมาร์ตคอนแทร็กต์ การออกแบบสมาร์ตคอนแทร็กต์ให้ทำงานร่วมกับแพลตฟอร์มได้อย่างมีประสิทธิภาพ ดังภาพที่ 6

จากภาพที่ 6 แสดงการเชื่อมต่อระหว่างสมาร์ตคอนแทร็กต์และแพลตฟอร์ม

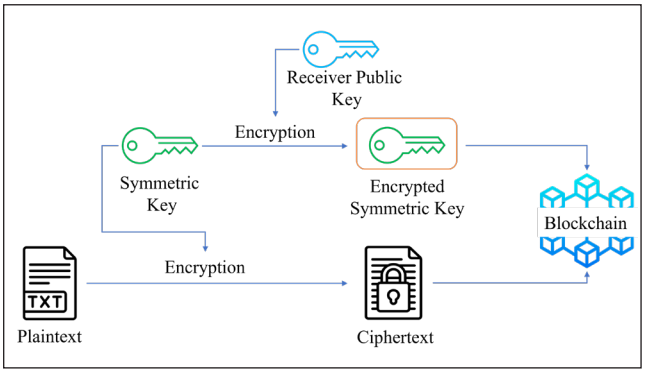
3.2.3 การออกวิทยาการเข้ารหัสลับในรูปแบบผสม (Hybrid Encryption)

การเข้ารหัสแบบผสม เป็นการผสมผสานข้อดีของการเข้ารหัสแบบกุญแจสมมาตร (Symmetric Key) และการเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric Key) เพื่อเพิ่มความเร็วและความปลอดภัยมากยิ่งขึ้น ดังภาพที่ 7 และภาพที่ 8

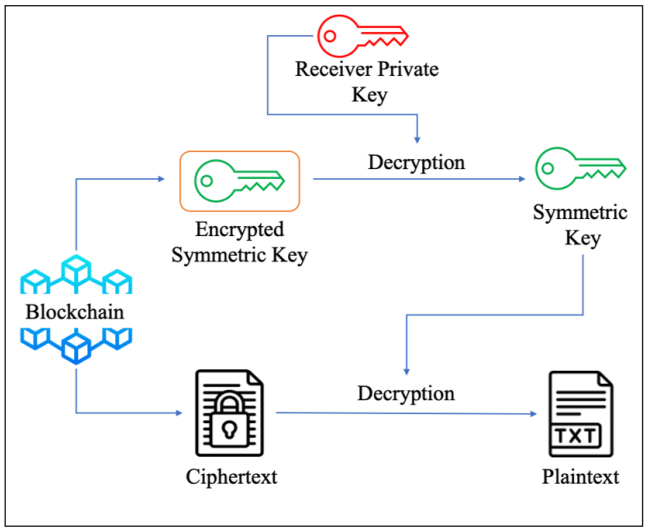
จากภาพที่ 7 และภาพที่ 8 แสดงการเข้ารหัสในรูปแบบผสม เป็นกระบวนการที่ผสมระหว่างการเข้ารหัสแบบสมมาตร (Symmetric) และอสมมาตร (Asymmetric) เพื่อเพิ่มประสิทธิภาพและความปลอดภัยในการรับส่งข้อมูล โดยที่กระบวนการเข้ารหัสแบบกุญแจสมมาตร จะถูกสร้างขึ้นเพื่อเข้ารหัสข้อมูลและคีย์หรือกุญแจนี้จะถูกเข้ารหัสอีกครั้งด้วยกุญแจสาธารณะ (Public Key) ของผู้รับก่อนที่จะส่งเข้าภายในเครือข่ายบล็อกเชนไปยังผู้รับ ฝั่งของผู้รับ ต่อมากุญแจสมมาตรจะต้องถอดรหัสด้วยกุญแจส่วนตัว (Private Key) และจากนั้นจึงใช้กุญแจสมมาตรนี้เพื่อถอดรหัสข้อมูลที่ถูกส่งมา ความแตกต่างของการเข้ารหัสแบบนี้คือการผสมผสานข้อดีของการเข้ารหัส



ภาพที่ 6 แสดงการเชื่อมต่อสมาร์ตคอนแทร็กต์และแพลตฟอร์ม



ภาพที่ 7 แสดงการเข้ารหัสข้อมูลในรูปแบบผสม



ภาพที่ 8 แสดงการถอดรหัสข้อมูลในรูปแบบผสม

แบบสมมาตรที่มีประสิทธิภาพสูงในการเข้ารหัสข้อมูลขนาดใหญ่ และการเข้ารหัสแบบอสมมาตรจะเป็นวิธีที่ปลอดภัยในการแลกเปลี่ยนคีย์

3.3 การพัฒนาระบบ (Development/coding)

ส่วนที่ 1 การพัฒนาสมาร์ตคอนแทร็กต์ ด้วยภาษา JavaScript ประกอบด้วย ฟังก์ชันกำหนดสิทธิ์ผู้ใช้งาน ฟังก์ชันการส่งข้อมูลผ่านเครือข่ายบล็อกเชน และฟังก์ชันการรับข้อมูลผ่านเครือข่ายบล็อกเชน

ส่วนที่ 2 การพัฒนาแพลตฟอร์มระบบจัดเก็บ และแลกเปลี่ยนข้อมูลสำหรับระบบบัญชาการและควบคุมของกองทัพอากาศ โดยใช้เทคโนโลยีบล็อกเชน การนำเสนอเนื้อหาและกิจกรรมผ่านแพลตฟอร์มในรูปแบบสื่อมัลติมีเดีย เช่น ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว ที่พัฒนาด้วยภาษา PHP, HTML5, Laravel Framework และ JavaScript

3.4 การทดสอบและบูรณาการระบบ (Testing/System integration)

การทดสอบและบูรณาการระบบเป็นขั้นตอนสำคัญในการประเมินความถูกต้อง ความเร็ว และความปลอดภัยของระบบแพลตฟอร์มที่เชื่อมต่อกับฐานข้อมูล และสัญญาผ่านเครือข่ายบล็อกเชน การทดสอบประกอบด้วยการทดสอบฟังก์ชันการทำงาน เช่น การส่งและรับข้อมูล การเข้ารหัสและถอดรหัสข้อมูล เพื่อให้แน่ใจว่าระบบทำงานตามที่ออกแบบไว้ รวมถึงการทดสอบข้อยกเว้นเพื่อตรวจสอบการตอบสนองเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด และการทดสอบประสิทธิภาพโดยวัดความเร็วในการประมวลผลข้อมูลขนาดต่าง ๆ

ความถูกต้องของข้อมูลที่ส่งและรับ และความปลอดภัยในการเข้าถึงข้อมูล การทดสอบที่ครอบคลุมทุกด้านช่วยให้มั่นใจว่าแพลตฟอร์มมีความพร้อมใช้งานและสามารถรองรับการทำงานในสภาพแวดล้อมจริงได้อย่างมีประสิทธิภาพ

4. ผลการดำเนินงาน

4.1 ผลการออกแบบสถาปัตยกรรมและพัฒนาระบบ

4.1.1 ผลการออกแบบสถาปัตยกรรมของสมาร์ตดิจิทัลแพลตฟอร์มโดยใช้เทคโนโลยีบล็อกเชนเป็นต้นแบบในการสร้างระบบบัญชาการและควบคุมสำหรับกองบิน 7 จ. สุราษฎร์ธานี โดยมีเป้าหมายให้ระบบที่สร้างขึ้นมีความถูกต้อง โปร่งใส พร้อมใช้งาน รักษาความลับข้อมูล และกระจายอำนาจอย่างเป็นธรรม โดยยังคงไว้ซึ่งมาตรฐานสากลในการทำงานของระบบ ผู้วิจัยได้ใช้เทคโนโลยีการเข้ารหัสแบบสผสมเป็นการเข้ารหัสแบบสมมาตร และแบบอสมมาตรเข้าด้วยกันในการเข้ารหัสข้อมูลก่อนที่จะส่งไปยังบล็อกเชนและเพื่อเพิ่มความมั่นคงปลอดภัยและความเชื่อถือในการส่งข้อมูลมากยิ่งขึ้น ดังภาพที่ 9

จากภาพที่ 9 พบว่าสมาร์ตดิจิทัลแพลตฟอร์มได้ใช้เทคโนโลยีบล็อกเชนเพื่อรองรับระบบบัญชาการและควบคุมของกองทัพอากาศ ซึ่งเป็นการบูรณาการเทคโนโลยีบล็อกเชนให้ใช้ในบริบททางทหารโดยที่ระบบถูกออกแบบมาเพื่อแลกเปลี่ยนข้อมูลกระหว่างหน่วยงานซึ่งเป็นแนวคิดใหม่ในการนำบล็อกเชนมาใช้ในการเข้ารหัสข้อมูล โดยใช้สมาร์ตคอนแทร็กต์ในการจัดการสิทธิ์การเข้าถึงข้อมูล ช่วยเพิ่มความปลอดภัย ความโปร่งใส และประสิทธิภาพในการจัดเก็บ และแลกเปลี่ยนข้อมูลให้ดียิ่งขึ้น ได้อย่างถูกต้อง ปลอดภัย และน่าเชื่อถือ จากภาพที่ 9 ผู้วิจัยแบ่งองค์ประกอบต่าง ๆ เป็น 6 ส่วน ดังต่อไปนี้

1) ข้อความที่จะส่งไปยังผู้รับ ในการส่งข้อความจะต้องระบุชื่อผู้รับเท่านั้นจึงจะส่งข้อความได้ เนื่องจากสมาร์ตดิจิทัลแพลตฟอร์มจะต้องใช้ชื่อผู้รับเพื่อกำหนดเป็นกุญแจสาธารณะ

2) การเข้ารหัสข้อความจะใช้การเข้ารหัสในรูปแบบผสม

3) ส่วนต่อประสานโปรแกรมประยุกต์ (Application Program Interface: API) หรือเอพีไอเป็นส่วนของการเขียนฟังก์ชันโดยใช้ NodeJS เพื่อให้เชื่อมต่อกับสมาร์ตคอนแทร็กต์ได้

4) บล็อกเชนจะรับข้อมูลจากสัญญาสมาร์ต และกระจายไปเก็บยังทุกโหนดในเครือข่าย

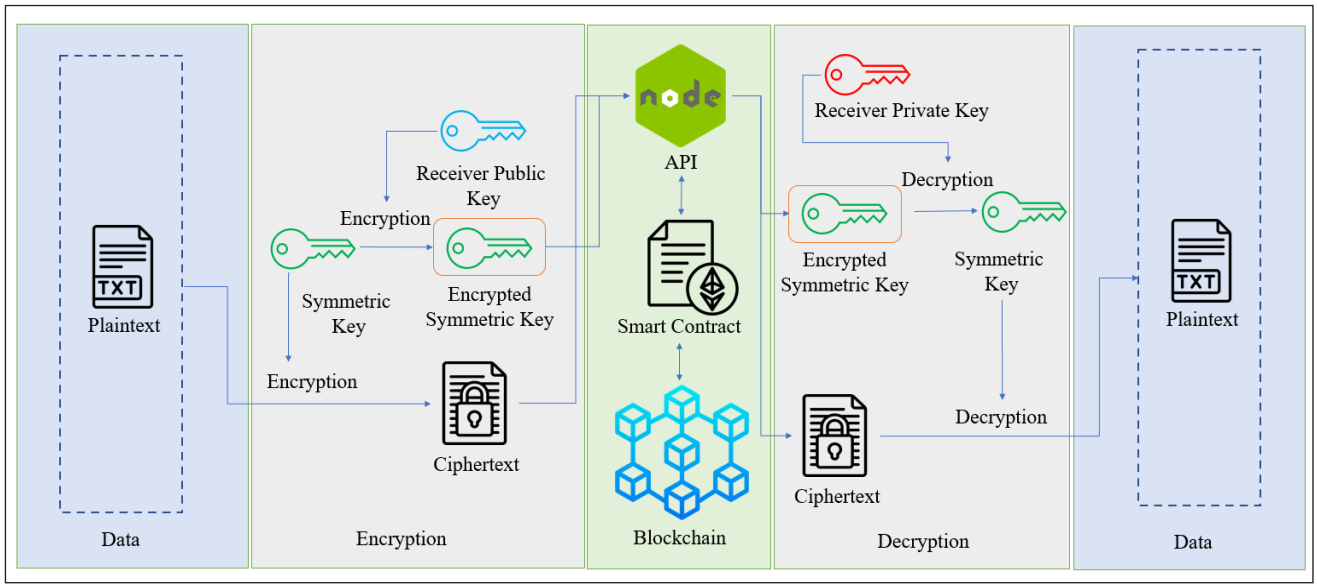
5) การถอดรหัสข้อความจะใช้การถอดรหัสในรูปแบบผสม

6) ผลลัพธ์หลังการถอดรหัสจะแสดงเป็นข้อข้อความที่เข้าใจได้

4.1.2 การพัฒนาสมาร์ตคอนแทร็กต์ดังภาพที่ 10

```
'use strict';

const { Contract } = require('fabric-contract-api');
const shim = require('fabric-shim');
const version = '1.0';

class rtaf extends Contract {

    async instantiate(ctx) {
        console.log('HelloWorld - Instantiate');
    }

    async sayHello(ctx) {
        return 'Hello, World Private Blockchain V.' + version;
    }
```

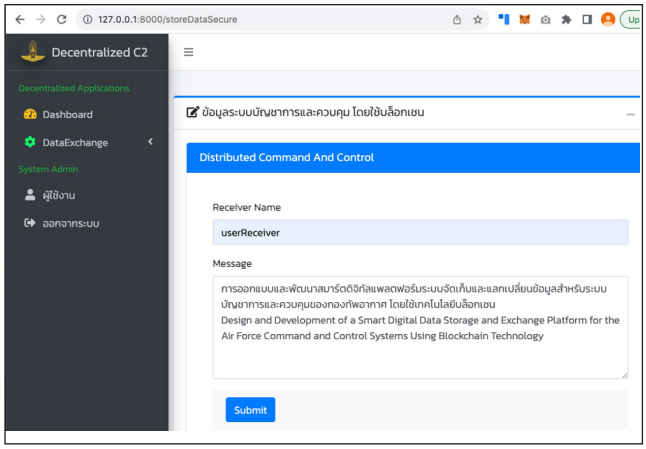
ภาพที่ 10 ตัวอย่างคำสั่งสร้างสมาร์ตคอนแทร็กต์



ภาพที่ 9 สถาปัตยกรรมของสมาร์ตดิจิทัลแพลตฟอร์ม

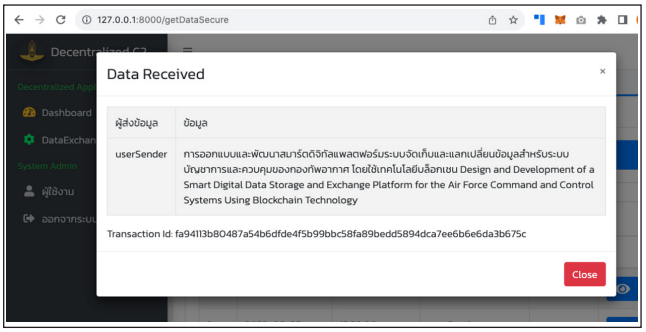
จากภาพที่ 10 แสดงตัวอย่างคำสั่งสร้างสมาร์ตคอนแทร็กต์ด้วยภาษา JavaScript

4.1.3 ผลการพัฒนาแพลตฟอร์มระบบจัดเก็บและแลกเปลี่ยนข้อมูลสำหรับระบบบัญชาการ และควบคุมของกองทัพอากาศ โดยใช้บล็อกเชน ดังภาพที่ 11 และ ภาพที่ 12



***ภาพที่ 11** ส่วนของการส่งข้อมูล*

จากภาพที่ 11 แสดงตัวอย่างการส่งข้อมูลระหว่างผู้ใช้ผ่านเครือข่ายบล็อกเชน การทำงานประกอบด้วยการระบุชื่อผู้รับ การเข้ารหัสข้อมูลก่อนส่ง และการตรวจสอบสิทธิ์การเข้าถึงของผู้รับ โดยการส่งข้อมูลจะต้องระบุชื่อผู้รับ และข้อความที่จะสื่อสาร ชื่อผู้รับจะต้องได้รับอนุญาตให้เข้าใช้งานเครือข่ายบล็อกเชนแล้วเท่านั้น ลักษณะการทำงานเริ่มต้นด้วยผู้ส่งข้อมูลระบุชื่อผู้รับที่ต้องการส่งข้อมูล ระบบทำการเข้ารหัสข้อมูลก่อนส่งเพื่อความปลอดภัย และตรวจสอบสิทธิ์การเข้าถึงของผู้รับ หากผู้รับได้รับอนุญาต ข้อมูลที่เข้ารหัสแล้วจะถูกส่งผ่านเครือข่ายบล็อกเชน และผู้รับที่ได้รับอนุญาตสามารถถอดรหัสข้อมูลเพื่ออ่านข้อความที่ถูกส่งมาได้



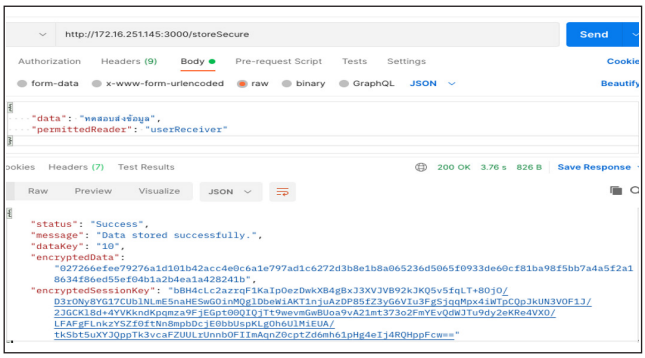
***ภาพที่ 12** ส่วนของการรับข้อมูล*

จากภาพที่ 12 แสดงตัวอย่างการรับข้อความซึ่งข้อความที่ได้รับจะแสดงเฉพาะข้อความที่ของตนเองเท่านั้น ไม่อาจเข้าถึงข้อความของผู้อื่นได้

4.2 ผลการทดสอบสมาร์ตคอนแทร็กต์

การทดสอบสมาร์ตคอนแทร็กต์ เป็นทดสอบฟังก์ชัน (Functional Tests) และ ทดสอบเกี่ยวกับประสิทธิภาพ ความเร็ว ความปลอดภัย (Non-Functional Tests) ดังนั้น วิธีการทดสอบสำหรับสัญญาสมาร์ตนี้ได้แบ่งออกเป็นขั้นตอนดังนี้

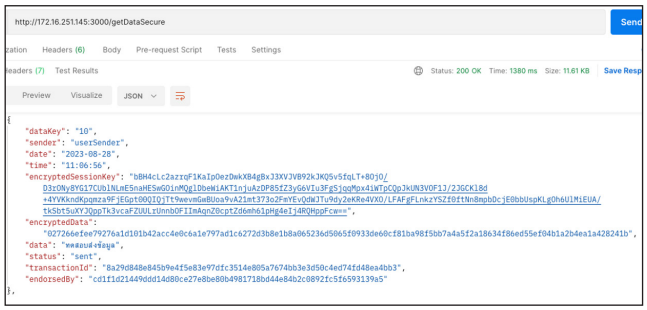
4.2.1 การทดสอบฟังก์ชันสำหรับส่งข้อมูล เครื่องมือที่ใช้ในการทดสอบฟังก์ชันสำหรับส่งข้อมูลจะใช้โปรแกรม Postman เป็นเครื่องมือที่ใช้สำหรับการทดสอบและพัฒนาเอพีไอ ดังภาพที่ 13



***ภาพที่ 13** แสดงการทดสอบฟังก์ชันส่งข้อมูลผ่านเครือข่ายบล็อกเชน*

จากภาพที่ 13 พบว่าระบบบัญชาการและควบคุมของกองทัพอากาศโดยใช้เทคโนโลยีบล็อกเชนสามารถส่งข้อมูลเข้าสู่เครือข่ายบล็อกเชนได้ และข้อมูลที่บันทึกเข้าสู่ Ledger ได้รับการเข้ารหัสและไม่อาจอ่านค่าได้

4.2.2 ฟังก์ชันสำหรับรับข้อมูล เครื่องมือที่ใช้ในการทดสอบฟังก์ชันสำหรับรับข้อมูลจะใช้โปรแกรม Postman เป็นเครื่องมือที่ใช้สำหรับการทดสอบและพัฒนาเอพีไอ ดังภาพที่ 14



***ภาพที่ 14** แสดงการทดสอบฟังก์ชันรับข้อมูล*

จากภาพที่ 14 พบว่าระบบบัญชาการและควบคุมของกองทัพอากาศโดยใช้เทคโนโลยีบล็อกเชนสามารถรับข้อมูลจากเครือข่ายบล็อกเชนได้ ซึ่งจะแสดงเฉพาะข้อมูลของตนเองเท่านั้น และข้อมูลดังกล่าวถูกเข้ารหัสไว้จะต้องใช้กุญแจส่วนตัวของตนเองในการถอดรหัสเพื่อให้ข้อความอ่านได้

4.2.3 การทดสอบข้อยกเว้น (Exception Testing) เพื่อทดสอบการตอบสนองของระบบเมื่อเกิดเหตุการณ์ที่ไม่คาดคิดหรือความผิดพลาดในการใช้งาน การทดสอบนี้จะช่วยให้เรามั่นใจว่าระบบจะไม่ล่มหรือแสดงผลผิดพลาด ทั้งนี้จะใช้เครื่องมือที่ชื่อว่า Unit Testing เพื่อจำลองเหตุการณ์ต่าง ๆ ที่จะทำให้เกิดข้อยกเว้น เช่น การส่งค่าพารามิเตอร์ที่ไม่ถูกต้อง การส่งข้อมูลโดยไม่มีสิทธิ์ที่เหมาะสม หรือการป้อนข้อมูลที่ไม่ตรงตามรูปแบบที่ต้องการ ซึ่งจะช่วยยืนยันความแข็งแกร่งและมีความเสถียรในสถานการณ์ต่าง ๆ ที่อาจเกิดขึ้น จากผลการทดสอบจำลองสถานการณ์ต่าง ๆ สรุปได้ดังนี้

ฟังก์ชันสำหรับส่งข้อมูล

1) การเก็บข้อมูลที่เข้ารหัสระบบสามารถบันทึกข้อมูลที่เข้ารหัสได้เมื่อมีการใช้งานโดยผู้ใช้งานที่มีสิทธิ์เป็นผู้ส่ง

2) การจัดการกับผู้ใช้ที่ไม่มีสิทธิ์เป็นผู้ส่งระบบจะแสดงข้อผิดพลาดเมื่อมีการเข้าถึงโดยไม่มีสิทธิ์

3) การจัดการตัวอักษรพิเศษระบบป้องกันปัญหา Injection ได้ดี และบันทึกข้อมูลที่มีตัวอักษรพิเศษได้

4) การจัดการข้อมูลที่ไม่ชัดเจน ระบบแสดงข้อผิดพลาดเมื่อข้อมูลเป็น Undefined, Null หรือ Empty

5) ขนาดข้อมูล ระบบจะแสดงข้อผิดพลาดเมื่อข้อมูลที่เข้ารหัสมีขนาดเกินขีดจำกัดที่กำหนด

ฟังก์ชันสำหรับรับข้อมูล

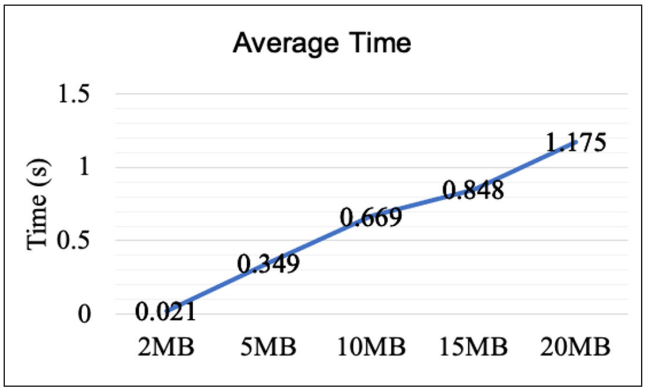
1) การเข้าถึงข้อมูล ระบบจะแสดงข้อผิดพลาดเมื่อผู้ใช้ที่ไม่มีสิทธิ์ที่สามารถรับข้อมูลได้และพยายามเข้าถึงข้อมูล

2) รูปแบบข้อมูล ข้อมูลที่ส่งมาจากระบบมีรูปแบบที่สมบูรณ์และถูกต้อง

3) การจัดการตัวอักษรพิเศษ ระบบจะแสดงข้อมูลที่มีตัวอักษรพิเศษได้โดยไม่มีปัญหาใด ๆ

4.2.4 การทดสอบเกี่ยวกับประสิทธิภาพ (Performance Testing)

การทดสอบประสิทธิภาพสำหรับสมาร์ตคอนแทร็กต์จะเป็นการทดสอบความสามารถในการรับการเรียกใช้งานในระดับสูง ความเร็วของการตอบสนอง และความทนทานต่อการโหลดที่เพิ่มขึ้นเรื่อย ๆ จากผลการทดสอบส่งข้อมูลที่มีขนาด 2MB, 5MB, 10MB, 15MB และ 20MB จำนวน 100 ธุรกรรมในแต่ละขนาดข้อมูล เพื่อหาค่าเฉลี่ยเวลาในแต่ละช่วงเวลา การเลือกขนาดข้อมูลเหล่านี้มีเหตุผลเพื่อให้สามารถประเมินประสิทธิภาพของระบบในสภาวะการใช้งานจริงที่มีการส่งข้อมูลขนาดต่าง ๆ ซึ่งจะช่วยให้เข้าใจถึงความสามารถของระบบในการจัดการกับข้อมูลที่มีขนาดใหญ่และมีความหลากหลาย และเพื่อให้แน่ใจว่าระบบสามารถตอบสนองได้อย่างรวดเร็วและมีประสิทธิภาพในการจัดการข้อมูลที่มีขนาดแตกต่างกัน ดังภาพที่ 15



***ภาพที่ 15** แสดงเวลาเฉลี่ยในการส่งข้อมูล*

จากภาพที่ 15 พบว่าการทดสอบการส่งข้อมูลขนาดต่าง ๆ ผ่านฟังก์ชันส่งข้อมูล แสดงให้เห็นว่าเมื่อข้อมูลมีขนาดเพิ่มขึ้น ประสิทธิภาพในการประมวลผลจะลดลงเนื่องจากเวลาที่ใช้ในการประมวลผลมีการเพิ่มขึ้นเป็นเชิงเส้นตามขนาดข้อมูลที่เพิ่มขึ้นมา ตัวเลขเฉลี่ยที่ได้จากการทดสอบแสดงให้เห็นว่าข้อมูลขนาดใหญ่ที่สุด 20 MB ใช้เวลาในการประมวลผลเฉลี่ย 1.175 วินาที ซึ่งสูงกว่าข้อมูลขนาด 2 MB ที่ใช้เวลาในการประมวลผลเฉลี่ย 0.021 วินาที นั่นหมายความว่า ในการใช้งานจริงควรระมัดระวังเรื่องขนาดข้อมูลที่ต้องการส่ง และคำนึงถึงเวลาประมวลผลที่อาจส่งผลกระทบต่อประสิทธิภาพของระบบ

5. สรุป

ผู้วิจัยได้นำเสนอแนวทางในการออกแบบ และพัฒนาสมาร์ตดิจิทัลแพลตฟอร์มของระบบจัดเก็บและแลกเปลี่ยนข้อมูลสำหรับระบบบัญชาการและควบคุมของกองทัพอากาศโดยใช้เทคโนโลยีบล็อกเชน ซึ่งระบบบัญชาการและควบคุมแบบใหม่ที่สร้างขึ้นนี้จะเป็นระบบที่มุ่งเน้นวิธีการและสถาปัตยกรรมของสมาร์ตดิจิทัลแพลต ฟอร์มสำหรับจัดการ

และควบคุมดำเนินงานของข้อมูลที่มีจำนวนมาก และเปลี่ยนแปลงอย่างรวดเร็ว ผู้วิจัยได้สร้างสถาปัตยกรรมของแพลตฟอร์มที่มีเทคโนโลยีบล็อกเชนเป็นฐานของการทำงาน ทั้งนี้เพื่อเพิ่มศักยภาพในการปกป้องข้อมูล และเสริมสร้างความปลอดภัยในการแลกเปลี่ยนข้อมูล อีกทั้งยังได้ทำการทดสอบประสิทธิภาพของสมาร์ตคอนแทร็กต์อันเป็นส่วนหนึ่งของระบบบัญชาการและควบคุมแบบใหม่อีกด้วย ผลที่ได้จากการวิจัยนี้ทำให้กองทัพอากาศสามารถพึ่งพาตนเองได้ในด้านเทคโนโลยีป้องกันประเทศ โดยมีแพลตฟอร์มเป็นของตนเองสำหรับบัญชาการและควบคุมให้การทำงานเป็นไปได้อย่างเข้มแข็งมีประสิทธิภาพสูง และเชื่อถือได้

6. เอกสารอ้างอิง

[1] C. Montha et al. *Blockchain for Government Services.* Digital Government Development Agency (Public Organization) (DGA), Vol. 2, 2021.

[2] V. Mishra, S. S. Yau, and C. Yenugunti. "Recovering Decentralized Critical Archival Data From Tampering in Smart City Environment Using Blockchain." *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI),* 2019.

[3] U. Khalil, M. Uddin, O. A. Malik, and S. Hussain. "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions." *IEEE Access,* Vol. 10, pp. 76805 - 76823, 2022.

[4] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi. "An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain." *Wireless Communications and Mobile Computing,* Vol. 2022, pp. 1 - 25, 2022.

[5] D. Chirtoaca, J. Ellul, and G. Azzopardi. "An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain." *Proceedings of IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS),* pp. 100 - 105, 2020.

[6] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. ur Rehman, and C. A. Kerrache. "The case of HyperLedger Fabric as a blockchain solution for healthcare applications." *Blockchain: Research and Applications,* Vol. 2, No. 1, March, 2021.

[7] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique. "Blockchain Application in Healthcare Systems: A Review." *Systems,* Vol. 11, No. 1, 2023.

[8] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System.* Available Online at: https://bitcoin.org/bitcoin.pdf, accessed on 7 May 2023.

[9] L. Gigli, I. Zyrianoff, F. Montori, C. Aguzzi, L. Roffia, and M. Di Felice. "A Decentralized Oracle Architecture for a Blockchain-Based IoT Global Market." *IEEE Communications Magazine,* Vol. 61, No. 8, pp. 86 - 92, 2023.

[10] M. H. Jeong and S. K. Kim. "Video Streaming Based on Blockchain State Channel with IoT Camera." *Journal of Web Engineering,* Vol. 21, No. 3, pp. 661 - 676, 2022.

[11] C. Thoppae, P. Praneetpolgrang, and N. Jirawichitchai. "Development of an Architectural Framework for Electronic Transaction Document Exchange between Government Agencies with Efficiency and Security Using Blockchain Technology." *Journal of Information Technology,* Vol. 17, No. 1, pp. 66 - 75, 2021.

[12] H. Sukhwani, N. Wang, K. S. Trivedi, and A. Rindos. "Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)." *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA),* Cambridge, MA, USA, pp. 1 - 8, 2018.

[13] A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur. "BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for

Healthcare System Using Blockchain Smart Contracts." *IEEE Access,* Vol. 10, pp. 78887 - 78898, 2022.

[14] J. Zhang, R. Tian, Y. Cao, X. Yuan, Z. Yu, X. Yan, X. Zhang. "A Hybrid Model for Central Bank Digital Currency Based on Blockchain." *IEEE Access,* Vol. 9, pp. 53589 - 53601, 2021.

[15] M. Hajiabbasi, E. Akhtarkavan, and B. Majidi. "Cyber-Physical Customer Management for Internet of Robotic Things-Enabled Banking." *IEEE Access,* Vol. 11, pp. 34062 - 34079, 2023.

[16] B. K. Mohanta, S. S. Panda and D. Jena. "An Overview of Smart Contract and Use Cases in Blockchain Technology." *Proceedings of the 9th International Conference on Computing, Communication and Networking Technologies,* Bengaluru, India, pp. 1 - 4, 2018.

[17] L. Zhang, B. Li, and X. Zhao. "Reconfigurable Hardware Implementation of AES-RSA Hybrid Encryption and Decryption." *Proceedings of the IEEE 5th International Conference on Signal and Image Processing (ICSIP),* Nanjing, China, pp. 970 - 974, 2020.

[18] P. Kulkarni, R. Khanai, and G. Bindagi. "A Hybrid Encryption Scheme for Securing Images in the Cloud." *Proceedings of the International Conference on Inventive Computation Technologies (ICICT),* Coimbatore, India, pp. 795 - 800, 2020.

[19] B. Su, H. Zhao, T. Qi, X. Liu, and R. Yu. "Research on Architecture of Intelligent Command and Control System." *2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS),* Jishou, China, pp. 362 - 364, 2019.

[20] A. Panwar, V. Bhatnagar, M. Khari, A. W. Salehi, and G. Gupta. "A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake." *Computational Intelligence and Neuroscience,* Vol. 2022, No. 1, pp. 1 - 19, 2022.

[21] U. Nadiya, M. I. Rizqyawan, and O. Mahnedra. "Blockchain-based Secure Data Storage for Door Lock System." *Proceedings of the 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE),* Yogyakarta, Indonesia, pp. 140 - 144, 2019.

[22] V. Buatongjun and P. Praneetpolgrang. *The Implementing Prototype in Trusted Digital Cooperative Service Systems in Thailand Using Blockchain Application.* A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Technology, Sripatum University, 2018.

[23] Q. Zhuohao, M. Firdaus, S. Noh and K. -H. Rhee. "A Blockchain-Based Auditable Semi-Asynchronous Federated Learning for Heterogeneous Clients." *IEEE Access,* Vol. 11, pp. 133394 - 133412, 2023.

[24] S. Barbaria, M. C. Mont, E. Ghadafi, H. M. Machraoui and H. B. Rahmouni. "Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks." *IEEE Access,* Vol.10, pp. 106334 - 106349, 2022.

[25] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, and M. Singh. "eHealthChain a blockchain-based personal health information management system." *Annals of Telecommunications,* Vol. 77, pp. 33 - 45, 2022.

[26] S. Lee, Y. Kim, and S. Cho. "Searchable Blockchain-Based Healthcare Information Exchange System to Enhance Privacy Preserving and Data Usability." *Sensors,* Vol. 24, No. 5, 2024.

[27] M. Wazid, A. K. Das, S. Shetty, and M. Jo. "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things." *IEEE Access,* Vol. 8, pp. 88700 - 88716, 2020.

[28] M. Chen, H. Jiang, H. Zhao, H. Zuo, and Q. Zhang. "Design and Optimization of Blockchain-Based Distributed Data-Sharing System for Urban Rail Transit." *Security and Communication Networks,* Vol. 2023, No. 1, pp. 1 - 11, 2023.

[29] T. Pengkian, P. Praneetpolgrang, and P. Sirinam. "Design and Development of a Data Storage and Exchange Systems for the Air Force Command and Control Systems Using Blockchain Technology."

Proceedings of the 19th National Conference on Computing and Information Technology, Thailand, pp. 103 - 109, 2023.

[30] F. Ashari, T. Catonsukmoro, W. M. Bad, Sfenranto, and G. Wang. "Smart Contract and Blockchain for Crowdfunding Platform." *International Journal of Advanced Trends in Computer Science and Engineering,* Vol. 9, No. 3, pp. 3036 - 3041, May - June, 2020.