JIST Journal of Information Science and Technology
Volume 12, NO 2 | JUL – DEC 2022 | 63-72
ISSN: 2651-1053 (Online)
ISSN: 1906-9553 (Print)

โพรโทคอลความมั่นคงปลอดภัยการพิสูจน์ทราบตัวจริงสำหรับเครือข่ายไร้สายบริเวณร่างกายกับบล็อกเชน

Security Protocol to Verify Authentication for Wireless Body Area Networks with Blockchain

แบ๊งค์ สันติวสุธา, วสุพล ไชยสง่าศิลป์, สัญชาติ ไพสิทธิ์, ชาลี ธรรมรัตน์ และ วทัญญู ยอดทอง*

Bank Santivasuta, Wasupol Chaisangasilp, Sanchat Phaisit, Chalee Thammarat and Watanyou Yodthong*

คณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีมหานคร

Faculty of Engineering and Technology, Mahanakorn University of Technology

Received: June 04, 2022; Revised: December 12, 2022; Accepted: December 13, 2022; Published: December 30, 2022

ABSTRACT – The advancement of wireless communication, Wireless Body Area Network (WBAN) has gained a lot of attention with the development of compact sensors Medical information is very sensitive. If any physiological information is tampered with or intercepted. It may affect the diagnosis or the patient's privacy. Security in WBAN is still important. Therefore, it is important to verify the authentication of each other's sending and receiving data between the sensor node and the server to protect patient information from malicious people, and for the privacy of patients. This research presents a protocol for secure authentication between sensor node and server nodes connected to the patient's body. We use the hash function and symmetric encryption to make the lightweight protocol. In addition, the security analysis and the integration of blockchain technology, it shows that the model in the research presented is consistent with the necessary safety features make the protocol efficient.

KEYWORDS: Authentication, Wireless Body Area Network, WBAN, Security Protocol

บทคัดย่อ -- ความก้าวหน้าของการสื่อสารไร้สาย Wireless Body Area Network (WBAN) ได้รับความสนใจอย่างมากจากการพัฒนาเซ็นเซอร์ขนาดย่อ ข้อความทางการแพทย์มีความละเอียดอ่อน ถ้ามีการดัดแปลงหรือดักฟังข้อความทางสรีรวิทยาใด ๆ อาจส่งผลต่อการวินิจฉัยหรือความเป็นส่วนตัวของผู้ป่วย การรักษาความปลอดภัยใน WBAN ยังคงเป็นเรื่องที่สำคัญ ดังนั้นจึงเป็นสิ่งสำคัญที่จะตรวจสอบการพิสูจน์ทราบตัวจริงของการส่งและรับข้อความซึ่งกันและกันระหว่างเซ็นเซอร์โหนดและเซิร์ฟเวอร์ เพื่อปกป้องข้อความของผู้ป่วยจากผู้ไม่หวังดีและเพื่อความเป็นส่วนตัวของผู้ป่วย งานวิจัยฉบับนี้ได้นำเสนอโพรโทคอลสำหรับการพิสูจน์ทราบตัวจริงที่ปลอดภัยระหว่างเซ็นเซอร์โหนดและเซิร์ฟเวอร์ โหนดที่เชื่อมต่อกับร่างกายของผู้ป่วย ฟังก์ชันแฮชและการเข้ารหัสลับแบบสมมาตรถูกนำมาใช้งาน ทำให้โพรโทคอลมีน้ำหนักเบา นอกจากนี้การวิเคราะห์ความปลอดภัยและการนำเทคโนโลยีบล็อกเชนมาใช้ร่วมกัน ทำให้เห็นว่ารูปแบบในงานวิจัยที่นำเสนอนั้นสอดคล้องกับคุณสมบัติความปลอดภัยที่จำเป็นและทำให้โพรโทคอลมีประสิทธิภาพ

คำสำคัญ: การพิสูจน์ทราบตัวจริง, Wireless Body Area Network, WBAN, โพรโทคอลความมั่นคงปลอดภัย

**Corresponding Author: chalee23@gmail.com*

1. บทนำ

ความก้าวหน้าทางเทคโนโลยีล่าสุดใน Wireless Body Area Network (WBAN) [1] ร่วมกับเทคโนโลยีสารสนเทศและการสื่อสาร Information and Communication Technology (ICT) WBAN เป็นเทคนิคที่ใช้สำหรับการตรวจสอบสุขภาพของผู้ป่วยจากระยะไกลและรวบรวมข้อความที่เกี่ยวข้องจากเซ็นเซอร์ ประกอบด้วยเครือข่ายไร้สายขนาดเล็กที่มีอุปกรณ์ขนาดเล็กหลายอย่าง เช่น ปุ่มเซ็นเซอร์และตัวกระตุ้น ปุ่มเซ็นเซอร์จะถูกวางไว้โดยตรงบนร่างกายหรือใต้ผิวหนังของบุคคลเพื่อคำนวณลักษณะของร่างกาย เช่น การตรวจคลื่นไฟฟ้าหัวใจ Electrocardiogram (ECG), การตรวจคลื่นสมองไฟฟ้า Electroencephalography (EEG), การเคลื่อนไหวของร่างกาย, อุณหภูมิ, ความดันโลหิต, ระดับน้ำตาลในเลือด, การตรวจโมเลกุลสารโดยใช้แสง, อัตราการเต้นของหัวใจ, ระดับอัตราการหายใจ และส่งข้อความที่เก็บรวบรวมข้อความหลังการประมวลผลไปยังฐานข้อความเพื่อที่จะวิเคราะห์และประมวลผลต่อไป ขั้นตอนการเข้ารหัสช่วยรักษาข้อความไม่ให้ถูกเปลี่ยนโดยผู้ไม่หวังดีได้ [2, 4] เทคโนโลยีนี้ช่วยให้การตรวจสุขภาพและการดูแลสุขภาพของผู้สูงอายุรวมถึงผู้พิการเพื่อให้พวกเขาอาศัยอยู่อย่างสบายและปลอดภัยในบ้านของพวกเขาเพื่อลดการรักษาในโรงพยาบาล และลดจำนวนการเข้ารับการรักษาจำนวนมากในโรงพยาบาล นอกจากนี้ยังช่วยควบคุมจำกัด และการเคลื่อนไหวสุขภาพต่อเนื่อง [3]

บทความวิจัยนี้มีองค์ประกอบในการนำเสนอดังนี้ บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 งานวิจัยที่นำเสนอ บทที่ 4 การวิเคราะห์ความปลอดภัย และบทที่ 5 บทสรุปและการอภิปราย

2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

Wireless Body Area Network [1] เป็นการพัฒนาการแนวคิดเครือข่ายพื้นที่ส่วนบุคคล และเครือข่ายไร้สายกับจุดที่อยู่ตามร่ายกายหรือบริเวณใกล้เคียง ความก้าวหน้าของการสื่อสารและเทคโนโลยีอิเล็กทรอนิกส์ทำให้เกิดการพัฒนาอุปกรณ์ขนาดกะทัดรัดและอัจฉริยะที่สามารถถูกวางไว้บนร่างกายของมนุษย์หรือฝังอยู่ภายในร่างกาย ในอนาคต WBAN จะมีการประมวลผลที่สูงและมีความซับซ้อนที่จะให้ฟังก์ชั่นของการคำนวณที่มีประสิทธิภาพเพื่อรองรับสำหรับการใช้งานที่สูงขึ้นเมื่อความต้องการมากขึ้นจึงได้นำไปสู่การวิจัยและการพัฒนาที่เพิ่มขึ้น

แนวคิดของเครือข่ายไร้สายบริเวณร่างกายเริ่มต้นเพื่อวัตถุประสงค์ทางการแพทย์ สำหรับการจัดเก็บและบันทึกข้อความสุขภาพของผู้ป่วยอย่างต่อเนื่องตลอดเวลา โดยเซนเซอร์ที่มีอยู่ตามจุดต่าง ๆ ของร่างกายมนุษย์สำหรับการวัดค่าพารามิเตอร์ที่ต้องการและส่งสัญญาณในร่างกาย เช่น ความดันโลหิต สัญญาณการเต้นของหัวใจ ระดับน้ำตาล และอุณหภูมิ เพื่อเก็บรวบรวมข้อความหรือสัญญาณคำสั่งไปยังเซนเซอร์ตามจุดต่าง ๆ ของร่างกาย เพื่อที่จะให้ดำเนินตามคำสั่งที่ต้องการ WBAN สามารถการตรวจสุขภาพได้ระยะยาวไม่จำกัดจำนวนครั้งในแต่ละวัน ระบบดังกล่าวสามารถนำไปใช้ในการพัฒนากระบวนการตรวจสอบสุขภาพได้ดีและราคาไม่แพง ซึ่งสามารถใช้เป็นส่วนหนึ่งของการวินิจฉัยโรคได้ ในอนาคตระบบจะสามารถตรวจผู้สูงอายุและผู้ป่วยเรื้อรังได้จากระยะไกล โดยที่ผู้ป่วยอาศัยอยู่บ้านของตนเอง ไม่ต้องมารับการตรวจที่โรงพยาบาล [2] แสดงได้ดังรูปที่ 1

รูปที่ 1. Wireless Body Area Network

บล็อกเชน (Blockchain) เป็นเทคโนโลยีที่จะมาเปลี่ยนวิธีการทำธุรกรรมทุกชนิด และเป็นแพลตฟอร์มในการทำธุรกรรมแบบ Peer-to-Peer ที่มีการบันทึกข้อความรายการธุรกรรมทั้งหมดแบบกระจายศูนย์ โดยทุกคนจะรับทราบร่วมกัน ว่าใครเป็นเจ้าของและมีสิทธิในข้อความตัวจริง เมื่อมีการเพิ่มข้อความ ก็จะอัปเดตตามไปด้วยทันที ซึ่ง Blockchain ได้ถูกการพัฒนาเป็นครั้งแรกในภาคการเงิน เพื่อใช้เป็นเทคโนโลยีแพลตฟอร์มของระบบ (Decentralized) เงินดิจิทัล (Cryptocurrency) ดังนั้น Block chain จึงเป็นระบบที่มีความมั่นคงปลอดภัยไม่จำเป็นต้องอาศัยตัวกลาง จึงทำให้เทคโนโลยี

Blockchain เป็นเทคโนโลยีที่สามารถเอาชนะการรักษาความมั่นคงแบบเก่าได้ด้วยธรรมชาติของเทคโนโลยีที่มีรูปแบบการเก็บข้อความแบบกระจาย และมีการตรวจสอบซึ่งกันและกัน [12]

เทคโนโลยีบล็อกเชน (Blockchain) เป็นจุดสนใจในช่วงไม่กี่ปีที่ผ่านมา ปัจจุบันเทคโนโลยีบล็อคเชนได้ถูกนำมาใช้กับแอพพลิเคชั่น Internet of Things (IoT) ต่าง ๆ เช่น การดูแลสุขภาพ, การผลิต, การขนส่ง ซึ่งรูปแบบการสื่อสารที่สมบูรณ์ของ WBAN ประกอบด้วย ผู้ป่วย ผู้ให้บริการเครือข่าย ผู้ให้บริการด้านสุขภาพ หน่วยแพทย์ฉุกเฉิน แพทย์ พยาบาล และอื่น ๆ ดังนั้นข้อความทางสรีรวิทยาจากการตรวจติดตามผู้ป่วยจึงต้องการการเข้าถึงจากหลายแหล่ง [10] การเผยแพร่ข้อความหรือการเข้าถึงข้อความในช่วงเวลาต่าง ๆ ของกระบวนการวินิจฉัย ถือได้ว่าเป็นบล็อกของการทำธุรกรรมในบริบทของเทคโนโลยีบล็อกเชน เทคโนโลยีบล็อกเชนถูกนำมาใช้ เพื่อรักษาความปลอดภัยข้อความโดยเกี่ยวข้องกับเชนของค่าแฮช เพื่อเลือกค่าที่เหมาะสมที่ใช้สำหรับการเข้ารหัสลับ ในทางกลับกัน ลายเซ็นดิจิทัลถูกใช้เพื่อเป็นตัวตรวจสอบ ซึ่งหมายความว่าช่วยให้มั่นใจได้ว่าข้อความสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบ [11]

2.2 งานวิจัยที่เกี่ยวข้อง

Monalisha Polai และคณะ [5] นำเสนอเครือข่ายที่ถูกนำมาใช้ทางด้านการบริการทางการแพทย์แก่ผู้ป่วยในสภาพแวดล้อมที่มีทรัพยากรจำกัดและสถานที่ห่างไกล การพิสูจน์ทราบตัวจริงแบบไม่ระบุชื่อและการยกเลิกการเชื่อมโยงของข้อความเป็นบริการที่จำเป็นสำหรับ WBAN ทั้งที่เป็นการโจมตีอย่างเป็นทางการและไม่เป็นทางการ ที่ได้รับการวิเคราะห์ตรวจสอบของงานที่นำเสนอและพบว่าป้องกันต่อการโจมตีแบบ Active และ Passive ได้

MyeongHyun Kim และคณะ [6] นำเสนอการพิสูจน์ทราบตัวจริงผู้ใช้และเซสชันคีย์ที่ไม่ระบุชื่อที่มีน้ำหนักเบา การติดตั้งอุปกรณ์สำหรับสวมใส่ ตามแบบแผนไม่สามารถป้องกันการแอบอ้างเป็นผู้ใช้ การเปิดเผยเซสชันคีย์และการโจมตีที่ถูกขโมยอุปกรณ์สวมใส่ได้ นอกจากนี้ยังเสนอพิสูจน์ทราบตัวจริงผู้ใช้ร่วมกันที่มีความปลอดภัย น้ำหนักเบาและรูปแบบการสร้างเซสชันคีย์โดยใช้อุปกรณ์สวมใส่เพื่อแก้ไขปัญหาข้อบกพร่องด้านความปลอดภัยที่เหมาะสมกับสภาพแวดล้อมที่จำกัดทรัพยากรได้

Kakali Chatterjee [7] นำเสนอWBAN เป็นที่นิยมอย่างมากสำหรับการใช้งานด้านการดูแลสุขภาพสมัยใหม่ เครือข่ายแบบไร้สายบริเวณร่างกายประกอบด้วยเซ็นเซอร์สวมใส่ขนาดเล็กซึ่งฝังอยู่ในร่างกายมนุษย์ เพื่อเก็บข้อความทางการแพทย์และส่งไปยังเซิร์ฟเวอร์ทางการแพทย์ผ่านตัวเชื่อมต่อเครือข่ายไปยังฐานข้อความ ดังนั้นจึงมีข้อจำกัดด้านความปลอดภัย ที่ต้องได้รับการป้องกันระหว่างการเชื่อต่อ จึงเสนอโพรโตคอลการพิสูจน์ทราบตัวจริงร่วมกันที่ความมั่นคงปลอดภัย ซึ่งอิงจากการเข้ารหัสลับคีย์สาธารณะเพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยทั้งหมด การพิสูจน์ทราบตัวจริงจะป้องกันการโจมตีที่มีช่องโหว่ที่สำคัญในเครือข่ายเซ็นเซอร์ร่างกายไร้สายที่มีการคำนวณและการสื่อสารต่ำได้

Kamal Parvez และคณะ [8] นำเสนอ WBAN เป็นระบบการดูแลสุขภาพที่ใช้ IoT มีความสำคัญในการช่วยปรับปรุงบริการทางการแพทย์ โดยการเปิดใช้งานการตรวจสุขภาพของผู้ป่วยจากระยะไกล เนื่องจาก WBAN จัดการข้อความด้านสุขภาพที่ละเอียดอ่อน ปัญหาด้านความปลอดภัยและความเป็นส่วนตัว มีความสำคัญสูงสุดที่ต้องได้รับการป้องกัน จึงเสนอโพรโตคอลและการพิสูจน์ทราบตัวจริงผู้ใช้ที่มีน้ำหนักเบา ข้อตกลงเซสชันคีย์ระหว่างเซ็นเซอร์โหนดและผู้เชี่ยวชาญทางการแพทย์ ซึ่งรูปแบบการสื่อสารทั้งสองแบบ ต้องได้รับความปลอดภัย จึงจำเป็นต้องมีการวิเคราะห์ความปลอดภัยเสมอ

Bander A. Alzahrani [9] เสนอโปรโตคอลที่ใช้ Telecare Medical Information System (TMIS) ที่มีประสิทธิภาพและมีความมั่นคงปลอดภัย โดยใช้การทำงานของเซสชันคีย์แบบสมมาตรน้ำหนักเบา โมเดลที่นำเสนอได้รับการพิสูจน์โดยการวิเคราะห์ความปลอดภัย ได้รับการตรวจสอบภายโดยใช้เครื่องมือ ProVerif แบบอัตโนมัติ ความมั่นคงปลอดภัยโดยเฉลี่ยมากกว่า 38%

Gajala Praveen และคณะ [10] นำเสนอ Blockchain รักษาความปลอดภัยข้อความด้านสุขภาพที่มีความสำคัญ จุดมุ่งหมายของการศึกษานี้คือ เพื่อศึกษาเกี่ยวกับแอพพลิเคชั่นด้านการดูแลสุขภาพด้วยบล็อคเชน ซึ่งกล่าวถึงการจัดการข้อความทางการแพทย์ รวมถึงการแบ่งปันข้อความทางการแพทย์ การแบ่งปันรูปภาพ และการจัดการบันทึก การตรวจสอบยาตามการจัดส่งในมุมของการรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว

บทความนี้วิเคราะห์และเปรียบเทียบเอกสารการวิจัยในด้านการแพทย์ และสรุปที่ใช้ในการดูแลสุขภาพด้วยข้อดีและข้อเสีย

Luun Xiao และคณะ [11] นำเสนอแบบจำลองในสถาปัตยกรรม Wireless Body Sensor Network ที่ใช้เทคโนโลยี Blockchain ซึ่งโพรโตคอลการพิสูจน์ทราบตัวจริงและโพรโตคอลไม่ปรากฏการลงชื่อระหว่างโหนดที่ได้รับการออกแบบในรูปแบบ WBAN ทำให้ระบบส่งข้อความ Blockchain ในเครือข่ายไร้สาย สภาพแวดล้อมที่ปลอดภัยและเชื่อถือได้ ผลการทดลองแสดงให้เห็นว่าวิธีการที่เสนอมีแนวโน้มที่ดีและแสดงระดับความปลอดภัยและความมั่นคงที่สูงกว่าวิธีอื่น ๆ

3. งานวิจัยที่นำเสนอ

งานวิจัยฉบับนี้ นำเสนอโพรโทคอลสำหรับการพิสูจน์ทราบตัวจริงและการส่งข้อความผ่านเครือข่าย ที่มีความมั่นคงปลอดภัย ซึ่งมีขั้นตอนการทำงาน 2 ขั้นตอน ขั้นตอนการลงทะเบียนและขั้นตอนการพิสูจน์ทราบตัวจริง สัญลักษณ์ที่ใช้ในงานวิจัยนี้แสดงไว้ในตารางที่ 1 โดยจะมีการส่งข้อมูลเพื่อพิสูจน์ทราบตัวจริงดังรูปที่ 2

รูปที่ 2. โครงสร้างเครือข่าย Wireless Body Area Network การพิสูจน์ทราบตัวจริง

รูปที่ 2 แสดงโครงสร้างเครือข่าย Wireless Body Area Network การพิสูจน์ทราบตัวจริง โดยทั่วไปเซ็นเซอร์โหนด (SN) ที่เชื่อมต่อกับร่างกายมนุษย์จะรวบรวมข้อความเกี่ยวกับพารามิเตอร์ต่าง ๆ ของร่างกาย และส่งข้อความไปยังที่เก็บข้อความบนคลาวด์เซิร์ฟเวอร์ (HN) ผ่านอุปกรณ์เชื่อมต่อ (GW) ที่อยู่ใกล้เคียง

ตารางที่ 1. แสดงสัญลักษณ์ที่ใช้ในงานวิจัย

สัญลักษณ์	รายละเอียด
HN	ผู้ให้บริการคลาวด์เซิร์ฟเวอร์/เซิร์ฟเวอร์
GW	อุปกรณ์ที่เชื่อมต่อกับเน็ตเวิร์ค
SN	เซ็นเซอร์โหนด
MK_{A-B}	มาสเตอร์คีย์ใช้ร่วมกันระหว่าง A กับ B
SI	ซิลิคอนไอดี
ID_A	ระบุตัวตนของ A
H(.)	ฟังก์ชันแฮช
SK_{A-B}	การเข้ารหัสลับแบบสมมาครเซสชันคีย์ใช้ร่วมกันระหว่าง A กับ B
R	ค่านอนซ์ (Nonce)
T	การประทับเวลา (Timestamp)
E{.}	ดำเนินการเข้ารหัสลับ

3.1 ขั้นตอนการลงทะเบียน

ขั้นตอนนี้ SN และ GW ทำหน้าที่ลงทะเบียนกับ HN โดยดำเนินการตามขั้นตอนต่อไปนี้

1. ขั้นตอนการลงทะเบียนสำหรับ SN โดยที่ SN ทำการส่ง SI_{SN} ไปยัง HN เพื่อทำการลงทะเบียน จากนั้น HN ทำการส่ง ID_{SN} และ MK_{SN-HN} กลับเพื่อยืนยันการลงทะเบียนสำเร็จ ดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัยเช่น Secure Socket Layer (SSL) หรือ Wireless Transport Layer Security (WTLS)

2. ขั้นตอนการลงทะเบียนสำหรับ GW โดยที่ GW ทำการส่ง SI_{GW} ไปยัง HN เพื่อทำการลงทะเบียน จากนั้น HN ทำการส่ง ID_{GW} และ MK_{GW-HN} กลับเพื่อยืนยันการลงทะเบียนสำเร็จ ดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัยเช่น SSL หรือ WTLS

3.2 ขั้นตอนการพิสูจน์ทราบตัวจริง

ขั้นตอนนี้ การพิสูจน์ทราบตัวจริงร่วมกันระหว่างเซ็นเซอร์โหนดและเซิร์ฟเวอร์ โดยที่เซ็นเซอร์โหนดจะส่งข้อความผ่านเกตเวย์ไปยังเซิร์ฟเวอร์ เกตเวย์และเซ็นเซอร์โหนดจะกำหนดเซสชันคีย์เฉพาะขึ้นเพื่อรับพารามิเตอร์ของร่างกายที่ละเอียดอ่อนจากผู้ป่วย ตามขั้นตอนต่อไปนี้

M1: SN⟶GW: ID_{SN}, T1, $H(ID_{SN}, SI_{SN}, T1, MK_{SN-HN})$

M2: GW⟶HN: ID_{SN}, ID_{GW}, T1, T2, $H(ID_{SN}, SI_{SN}, T1, MK_{SN-HN})$, $H(T2, H(ID_{SN}, SI_{SN}, T1, MK_{SN-HN}), MK_{GW-HN})$

M3: HN⟶GW : T3, $EMK_{GW-HN}\{ID_{SN}, ID_{GW}, T2, T3, R1\}$, $EMK_{SN-HN}\{ID_{SN}, ID_{GW}, T1, T3, R1\}$

M4: GW⟶SN: ID_{GW}, T3, T4, $H(ID_{SN}, ID_{GW}, T3, T4, SK)$, $EMK_{SN-HN}\{ID_{SN}, ID_{GW}, T1, T3, R1\}$

M5: SN⟶GW: T5, $H(ID_{SN}, ID_{GW}, T3, T4, T5, SK)$

$SK = H(ID_{SN}, ID_{GW}, T3, R1)$

M1: SN ดำเนินการประทับเวลา T1 แล้วส่งข้อความเพื่อพิสูจน์ทราบตัวจริงกับ HN โดยจะส่งข้อความผ่าน GW โดยส่ง ID_{SN}, T1, $H(ID_{SN}, SI_{SN}, T1, MK_{SN-HN})$ ไปยัง GW

M2: เมื่อ GW ได้รับข้อความจาก SN จะทำการประทับเวลา T2 และตรวจสอบ $T1'-T1 \leq \Delta T$ เพื่อยืนยันว่าได้รับข้อความภายในเวลาที่กำหนด ถ้าไม่ใช่จะยกเลิกการติดต่อสื่อสารทันที จากนั้น GW จะสร้าง $H(ID_{SN}, SI_{SN}, ID_{GW}, SI_{GW}, T2, MK_{GW-HN})$ แล้วส่ง ID_{SN}, ID_{GW}, T, T, $H(ID_{SN}, SI_{SN}, T1, MK_{SN-HN})$, $H(T2, H(ID_{SN}, SI_{SN}, T1, MK_{SN-HN}), MK_{GW-HN})$ ไปยัง HN เมื่อ T1' คือเวลาที่ GW ได้รับข้อความ

M3: เมื่อ HN ได้รับข้อความจะทำการจะทำการประทับเวลา T3 และตรวจสอบ $T2'-T2 \leq \Delta T$ เพื่อยืนยันว่าได้รับข้อความภายในเวลาที่กำหนด ถ้าไม่ใช่จะยกเลิกการติดต่อสื่อสารทันที จากนั้น HN จะทำการถอดข้อความที่ได้รับ ด้วยมาสเตอร์คีย์ใช้ที่ร่วมกัน และ HN จะเข้ารหัสลับข้อความที่ส่งกลับไปยัง GW และ SN เพื่อรับการพิสูจน์ทราบตัวจริง โดยจะส่ง T3, $EMK_{GW-HN}\{ID_{SN}, ID_{GW}, T2, T3, R1\}$, $EMK_{SN-HN}\{ID_{SN}, ID_{GW}, T1, T3, R1\}$ ไปยัง GW เมื่อ T2' คือเวลาที่ HN ได้รับข้อความ

M4: เมื่อ GW ได้รับข้อความจะทำการจะทำการประทับเวลา T4 และตรวจสอบ $T3'-T3 \leq \Delta T$ เพื่อยืนยันว่าได้รับข้อความภายในเวลาที่กำหนด ถ้าไม่ใช่จะยกเลิกการติดต่อสื่อสารทันที และทำการถอดรหัสลับข้อความด้วยมาสเตอร์คีย์ที่ใช้ร่วมกันระหว่า GW และ HN จากนั้นจะส่ง ID_{GW}, T, T4, $H(ID_{SN}, ID_{GW}, T3, T4, SK)$, $EMK_{SN-HN}\{ID_{SN}, ID_{GW}, T1, T3, R1\}$ ไปยัง SN เมื่อ T3' คือเวลาที่ GW ได้รับข้อความ

M5: เมื่อ SN ได้รับข้อความจะทำการประทับเวลา T5 และตรวจสอบ $T4'-T4 \leq \Delta T$ เพื่อยืนยันว่าได้รับข้อความภายในเวลาที่กำหนด ถ้าไม่ใช่จะยกเลิกการติดต่อสื่อสารทันที และทำการถอดรหัสลับข้อความด้วยมาสเตอร์คีย์ที่ใช้ร่วมกันระหว่าง SN และ HN จากนั้นจะส่ง T5, $H(ID_{SN}, ID_{GW}, T3, T4, T5, SK)$ ไปยัง GW จะได้ $SK = H(ID_{SN}, ID_{GW}, T3, R1)$ สำหรับการเข้ารหัสลับข้อความเพื่อติดต่อสื่อสารระหว่าง SN และ GW เป็นการสิ้นสุดการพิสูจน์ทราบตัวจริงระหว่าง SN และ HN เมื่อ T4' คือเวลาที่ SN ได้รับข้อความ

3.3 การนำเทคโนโลยีบล็อกเชนมาผสานการพิสูจน์ทราบตัวจริง

การนำเทคโนโลยีบล็อกเชน (Blockchain) มาผสมผสานการพิสูจน์ทราบตัวจริงที่ได้ออกแบบในงานวิจัยนี้ โดย HN เป็นคลาวด์ของ WBAN สามารถพิสูจน์การพิสูจน์ทราบตัวจริงร่วมกันกับ SN ได้อย่างมีประสิทธิภาพ หลังจากที่ HN ได้รับข้อความจาก SN แล้ว โหนดนั้นจะถูกเก็บข้อมูลในรูปแบบของบล็อคเชนส่วนตัว ข้อความแบ่งออกเป็นข้อความการลงทะเบียนโหนด และข้อความทางสรีรวิทยาของผู้ป่วย ข้อความการลงทะเบียนโหนดใช้สำหรับการตรวจสอบความถูกต้องร่วมกันและข้อตกลงหลักระหว่าง HN และ SN ซึ่งผู้ใช้สามารถเข้าถึงข้อความทางสรีรวิทยาของผู้ป่วย รวมถึงแพทย์ พยาบาล และผู้ป่วย สามารถเข้าถึงข้อความทางสรีรวิทยาของผู้ป่วยโดยการเข้าถึง HN

รูปที่ 3. การนำบล็อกเชนมาผสานกับงานวิจัยนี้

จากรูปที่ 3 เป็นการนำระบบบล็อกเชนมาใช้ร่วมกับโพโทคอลที่ได้ออกแบบในงานวิจัยนี้ โดย SN ซึ่งผู้ใช้สามารถเข้าถึงข้อความทางสรีรวิทยาของผู้ป่วย รวมถึงแพทย์ พยาบาล และผู้ป่วย สามารถเข้าถึงข้อความทางสรีรวิทยาของผู้ป่วย โดยส่งข้อความเพื่อพิสูจน์ทราบตัวจริงกับ HN ซึ่ง HN เป็นคลาวด์ของ WBAN สามารถพิสูจน์การพิสูจน์ทราบตัวจริงร่วมกันกับ SN ได้อย่างมีประสิทธิภาพ เนื่องจาก มีกระบวนการเก็บข้อความในรูปแบบของบล็อกเชนส่วนตัว โดยบล็อกเชนถูกกำหนดเป็นความลับเพื่อป้องกันไม่ให้ถูกเข้าถึงข้อความโดยที่ไม่ได้รับอนุญาตและกำหนดสิทธิการเข้าถึงหรือการตรวจสอบสิทธิการเข้าถึงเพื่อให้การรับรองความถูกต้องของข้อความ ความเป็นส่วนตัว และความปลอดภัย สำหรับการอนุญาตและรับรองข้อความ

4. การวิเคราะห์ความปลอดภัยและประสิทธิภาพ

ในส่วนนี้เป็นการวิเคราะห์ความปลอดภัยและประสิทธิภาพ ประกอบด้วย การวิเคราะห์ความปลอดภัยและการวิเคราะห์ความมั่นคงปลอดภัยโดยใช้ Scyther สามาอธิบายได้นี้

4.1 การวิเคราะห์ความปลอดภัย

4.1.1 การโจมตีแบบ Replay Attack

ผู้โจมตีจะใช้ข้อความที่ดักจับมาได้และกระทำการส่งข้อความกลับไปอีกครั้ง งานวิจัยที่นำเสนอมีการป้องกันการโจมตีประเภทนี้ ด้วยวิธีการสร้างค่าสุ่มและตรวจสอบเวลาในการรับข้อความ
ทั้งค่าสุ่มและเวลาจะไม่นำมาใช้ซ้ำ

4.1.2 การโจมตีแบบ Impersonation Attack

ผู้โจมตีที่จะปลอมแปลงเป็นอุปกรณ์ที่ถูกต้องที่มีการติดต่อสื่อสาร เพื่อต้องการรับข้อความที่เป็นความลับระหว่างอุปกรณ์ที่ถูกต้อง โพรโทคอลที่นำเสนอสามารถป้องกันได้ด้วยวิธีการพิสูจน์ทราบตัวจริง โดยการใช้ฟังก์ชันแฮชร่วมกับมาสเตอร์คีย์ ซึ่งมาสเตอร์คีย์แต่ละอุปกรณ์จะไม่ซ้ำกัน ส่วนเซสชันคีย์ที่นำมาใช้งานจะถูกสร้างใหม่เมื่อถึงเวลาที่กำหนด

4.1.3 การโจมตีแบบ Man-in-the-Middle Attack

ผู้โจมตีอยู่ตรงกลางในการติดต่อสื่อสารระหว่างอุปกรณ์ เพื่อทำการเก็บข้อความที่สื่อสารระหว่างอุปกรณ์ การโจมตีประเภทนี้ผู้โจมตีไม่สามารถกระทำได้สำเร็จ เนื่องจากงานวิจัยที่นำเสนอมีการรักษาความลับของข้อความในทุกข้อความของงานวิจัยที่นำเสนอ ผู้โจมตีไม่สามารถถอดข้อความและอ่านข้อความเข้าใจได้

4.1.4 การโจมตีแบบ (Forward/Backward Secrecy)

ผู้โจมตีทำการเดาเซสชันคีย์ที่ใช้เข้ารหัสลับข้อความ เพื่อใช้ในการถอดรหัสลับข้อความ ผู้โจมตีไม่สามารถทำการเดาเซสชันคีย์ได้ง่าย เนื่องจากการสร้างเซสชันคีย์ด้วยค่าแฮชของ $H(ID_{SN}, ID_{GW}, T3, R1)$ ซึ่งค่า R1 เป็นค่าสุ่ม เพิ่มความทนทานในการเดาเซสชันคีย์

4.1.5 การรักษาความลับ (Confidentiality)

ในทุกข้อความที่ติดต่อสื่อสารของงานวิจัยที่นำเสนอใช้การเข้ารหัสลับและฟังก์ชันแฮช ทำให้ผู้โจมตีไม่สามารถอ่านข้อความรู้เรื่อง

4.1.6 การพิสูจน์ทราบตัวจริงร่วมกัน (Mutual Authentication)

งานวิจัยที่นำเสนอสามารถพิสูจน์ทราบตัวจริงของผู้ส่งข้อความและผู้รับข้อความ โดยการใช้ฟังก์ชันแฮชร่วมกับมาสเตอร์คีย์และมาสเตอร์คีย์แต่ละมาสเตอร์คีย์จะไม่ซ้ำกัน

4.1.7 การคงสภาพของข้อความ (Integrity)

งานวิจัยที่นำเสนอได้นำฟังก์ชันแฮชมาใช้งาน ทำให้สามารถตรวจสอบความถูกต้องของข้อความได้ นอกจากนี้ฟังก์ชันแฮช

ยังนำมาใช้ร่วมกับเซสชันคีย์ เพื่อพิสูจน์ทราบตัวจริงของผู้ส่งข้อความอีกด้วย

4.1.8 การโจมตีแบบ Resilient to User Masquerading Attack ผู้โจมตีที่จะปลอมแปลงเป็นอุปกรณ์การติดต่อสื่อสาร เพื่อต้องการรับข้อความที่เป็นความลับระหว่างอุปกรณ์ จะไม่สามารถทำได้ เนื่องจากมีป้องกันการโจมตีที่พยายามแอบอ้างสิทธิ์สวมรอยเป็นผู้ใช้เข้ามายังภายในระบบ ซึ่งมีการป้องกันด้วยวิธีการพิสูจน์ทราบตัวจริง

4.2 การวิเคราะห์ประสิทธิภาพ

หัวข้อนี้เป็นการเปรียบเทียบจำนวนครั้งของการใช้วิทยาการการเข้ารหัสลับและพลังงานที่ใช้ โดยจะเปรียบกันระหว่างโพรโทคอลที่นำเสนอกับงานวิจัย [5, 7, 8, 9]

ตารางที่ 2. การเปรียบเทียบวิทยาการเข้ารหัสลับโพรโทคอลการพิสูจน์ทราบตัวจริง

Cryptographic Operation	[5]	[7]	[8]	[9]	โพรโทคอลที่นำเสนอ
Symmetric Encryption	-	4	4	4	2
Symmetric Decryption	-	4	4	4	2
Hash Function	18	8	6	16	5

จากตารางที่ 2 การดำเนินการเข้ารหัสลับ ใช้จำนวนการข้ารหัสลับแบบสมมาตรและฟังก์ชันแฮชน้อยกว่า [5, 7, 8, 9] ดังนั้นโพรโทคอลที่นำเสนอจึงเหมาะสมสำหรับการสื่อสารผ่านไร้สาย

ตารางที่ 3. การเปรียบเทียบการสูญเสียพลังงาน

	[5]	[7]	[8]	[9]	โพรโทคอลที่นำเสนอ
AES (μJ/byte)	-	9.68	4.84	4.84	2.42
SHA1 (μJ/byte)	13.68	6.08	4.56	12.16	6.84
Total	13.68	15.67	9.4	17	9.26

Symmetric Encryption (Advanced Encryption Standard (AES): 1.21 μJ), Hash Function (Secure Hash Algorithm 1 (SHA1): 0.76 μJ)

จากตารางที่ 3 แสดงการสูญเสียพลังงานในการพิสูจน์ทราบตัวจริง โพรโทคอลที่นำเสนอโดยส่วนใหญ่จะสูญเสียพลังงานให้แก่โพรโทคอลน้อยกว่าโพรโทคอล [5, 7, 8, 9] เพราะการออกแบบโพรโทคอลจะเน้นการใช้ฟังก์ชันแฮชและการเข้ารหัสลับและการเข้ารหัสลับแบบแบบสมมาตรเท่าที่จำเป็นแต่ยังคงมีความมั่นคงปลอดภัยที่เพียงพอ พลังงานที่ใช้ในวิทยาการการเข้ารหัสลับอ้างอิงจากงานวิจัย [13, 14] ซึ่งงานวิจัยจำนวนมาก [15, 16] ใช้ในการวัดพลังงานวิทยาการการเข้ารหัสลับ

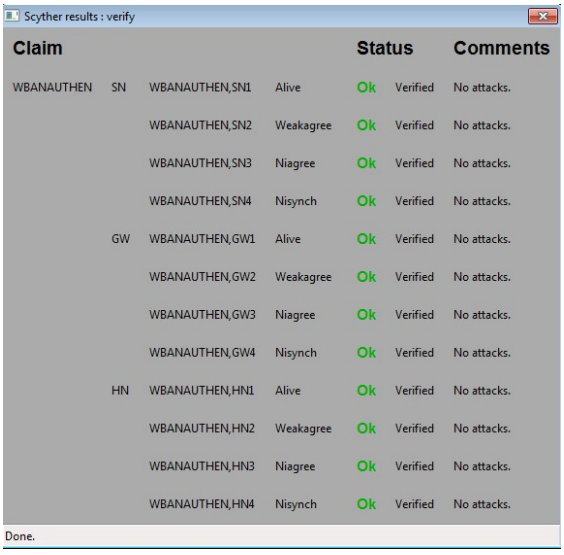
4.3 การวิเคราะห์ความมั่นคงปลอดภัยโดยใช้ Scyther

ในส่วนนี้เราจะใช้ Scyther [17] เพื่อใช้ในการตรวจสอบโพรโทคอลความมั่นคงปลอดภัยที่รู้จักกันดีและงานวิจัยจำนวนมาก [18, 19] ได้ใช้ในการตรวจสอบความถูกต้องของโพรโทคอลและการโจมตี

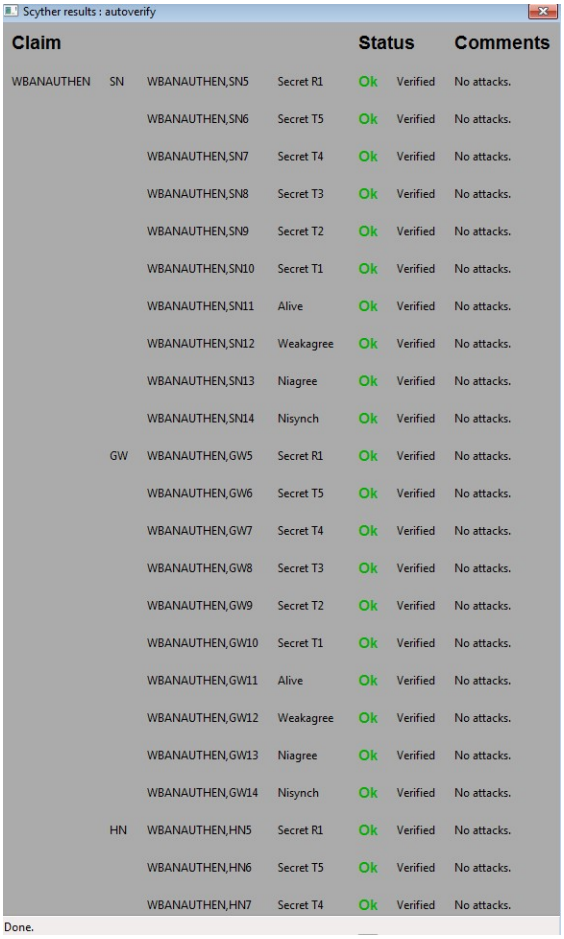
```
usertype String;
usertype TimeStamp;
usertype SessionKey;
hashfunction H;

const IDSN, SISN, IDGW, SIGW : String;
const MKSN-HN, MKGW-HN, MKSN-HN, SK :
SessionKey;
```

```
macro M1 = IDSN, T1,  H(IDSN, SISN , T1, MKSN-HN);
macro M2 = IDSN, IDGW, T1, T2, H(IDSN, SISN, T1,
MKSN-HN), H(T2, H(IDSN, SISN, T1, MKSN-HN),
MKGW-HN);
macro M3 = T3, {IDSN, IDGW, T2, T3, R1}MKGW-HN,
{IDSN, IDGW, T1, T3, R1}MKSN-HN;
macro M4 = IDGW, T3, T4, H(IDSN, IDGW, T3, T4, SK),
{IDSN, IDGW, T1, T3, R1}MKSN-HN;
macro M5 = T5, H(IDSN, IDGW, T3, T4, T5, SK);

protocol WBANAUTHEN(SN, GW, HN)
{
  role SN
  {
                fresh T1, T2, T3, T4, T5: TimeStamp;
                fresh R1: Nonce;

                send_1(SN, GW, M1);
                recv_4(GW, SN, M4);
                send_5(SN, GW, M5);

                claim_SN1(SN, Alive);
                claim_SN2(SN, Weakagree);
                claim_SN3(SN, Niagree);
                claim_SN4(SN, Nisynch);
        }
        role GW
        {
                fresh T1, T2, T3, T4, T5: TimeStamp;
                fresh R1 : Nonce;

                recv_1(SN, GW, M1);
                send_2(GW, HN, M2);
                recv_3(HN, GW, M3);
                send_4(GW, SN, M4);
                recv_5(SN, GW, M5);

                claim_GW1(GW, Alive);
                claim_GW2(GW, Weakagree);
                claim_GW3(GW, Niagree);
                claim_GW4(GW, Nisynch);
        }
        role HN
        {
                fresh T1, T2, T3, T4, T5: TimeStamp;
                fresh R1 : Nonce;

                recv_2(GW, HN, M2);
                send_3(HN, GW, M3);
                        claim_HN1(HN, Alive);
                claim_HN2(HN, Weakagree);
                claim_HN3(HN, Niagree);
                claim_HN4(HN, Nisynch);
        }
}
```

รูปที่ 4. โค้ดโปรแกรมของโพรโทคอลที่นำเสนอ



รูปที่ 5. ผลลัพธ์การตรวจสอบแบบ Verify Claim


Scyther results : autoverify

Claim				Status		Comments
WBANAUTHEN	SN	WBANAUTHEN,SN5	Secret R1	Ok	Verified	No attacks.
		WBANAUTHEN,SN6	Secret T5	Ok	Verified	No attacks.
		WBANAUTHEN,SN7	Secret T4	Ok	Verified	No attacks.
		WBANAUTHEN,SN8	Secret T3	Ok	Verified	No attacks.
		WBANAUTHEN,SN9	Secret T2	Ok	Verified	No attacks.
		WBANAUTHEN,SN10	Secret T1	Ok	Verified	No attacks.
		WBANAUTHEN,SN11	Alive	Ok	Verified	No attacks.
		WBANAUTHEN,SN12	Weakagree	Ok	Verified	No attacks.
		WBANAUTHEN,SN13	Niagree	Ok	Verified	No attacks.
		WBANAUTHEN,SN14	Nisynch	Ok	Verified	No attacks.
	GW	WBANAUTHEN,GW5	Secret R1	Ok	Verified	No attacks.
		WBANAUTHEN,GW6	Secret T5	Ok	Verified	No attacks.
		WBANAUTHEN,GW7	Secret T4	Ok	Verified	No attacks.
		WBANAUTHEN,GW8	Secret T3	Ok	Verified	No attacks.
		WBANAUTHEN,GW9	Secret T2	Ok	Verified	No attacks.
		WBANAUTHEN,GW10	Secret T1	Ok	Verified	No attacks.
		WBANAUTHEN,GW11	Alive	Ok	Verified	No attacks.
		WBANAUTHEN,GW12	Weakagree	Ok	Verified	No attacks.
		WBANAUTHEN,GW13	Niagree	Ok	Verified	No attacks.
		WBANAUTHEN,GW14	Nisynch	Ok	Verified	No attacks.
	HN	WBANAUTHEN,HN5	Secret R1	Ok	Verified	No attacks.
		WBANAUTHEN,HN6	Secret T5	Ok	Verified	No attacks.
		WBANAUTHEN,HN7	Secret T4	Ok	Verified	No attacks.

Done.

รูปที่ 6. ผลลัพธ์การตรวจสอบแบบ Autoverify Claim

รูปที่ 5 และรูปที่ 6 แสดงผลลัพธ์การตรวจสอบโพรโทคอลที่นำเสนอด้วย Scyther สถานะ “OK” ของ Alive, Weakagree, Niagree และ Nisynch แสดงให้เห็นว่าโพรโทคอลที่นำเสนอมีความถูกต้องและมีความมั่นคงปลอดภัยจากการโจมตีทั้ง Verify Claim และ Autoverify Claim

5. บทสรุปและการอภิปราย

งานวิจัยนี้นำเสนอโพรโทคอลสำหรับการพิสูจน์ทราบตัวจริงที่ปลอดภัยระหว่างเซ็นเซอร์โหนดและเซิร์ฟเวอร์ โหนดที่เชื่อมต่อกับร่างกายของผู้ป่วย เราใช้ฟังก์ชันแฮช เพื่อทำให้โพรโทคอลมีน้ำหนักเบา นอกจากนี้การวิเคราะห์ความปลอดภัยและการนำเทคโนโลยีบล็อกเชนมาใช้ร่วมกัน ทำให้เห็นว่ารูปแบบในงานวิจัยที่นำเสนอนั้นสอดคล้องกับคุณสมบัติความปลอดภัยที่จำเป็น เช่น การป้องกันการโจมตีแบบ Replay Attack, การป้องกันการโจมตีแบบ Impersonation Attack, การรักษาความลับ, การพิสูจน์ทราบตัวจริงร่วมกัน เป็นต้น นอกจากนี้งานวิจัยที่นำเสนอยังใช้พลังน้อยกว่าโพรโทคอลที่มีอยู่ ทำให้โพรโทคอลมีประสิทธิภาพเหมาะสำหรับการสื่อสารไร้สาน งานวิจัยในอนาคตผู้วิจัยจะดำเนินการต่อจะพัฒนาโปรแกรมต้นแบบโดยใช้โพรโทคอลที่นำเสนอร่วมกับเทคโนโลยีบล็อกเชน เพื่อให้สามารถใช้งานได้จริงและให้มีประสิทธิภาพเพิ่มขึ้น

เอกสารอ้างอิง

[1] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu, "A survey of routing protocols in WBAN for healthcare applications. Sensors", vol. 19, no. 7, pp. 1638, 2019.

[2] M. Ghamari, B. Janko, R.S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, “A survey on wireless body area networks for ehealthcare systems in residential environments”, Sensors, vol. 16, no.6, pp. 831, 2016.

[3] B. Narwal, and A.K. Mohapatra, “A survey on security and authentication in wireless body area networks”, Journal of Systems Architecture, vol. 113, pp. 101883, 2021.

[4] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications”, Egyptian Informatics Journal, vol. 18, no. 2, pp. 113-122, 2017.

[5] M. Polai, S. Mohanty, and S.S. Sahoo, “A lightweight mutual authentication protocol for wireless body area network”, In international conference on signal processing and integrated networks, pp. 760-765, 2019.

[6] M. Kim, J. Lee, S. Yu, K. Park, Y. Park, and Y. Park, “A secure authentication and key establishment scheme for wearable devices”, In International Conference on Computer Communication and Networks, pp. 1-2. 2019.

[7] K. Chatterjee, “An improved authentication protocol for wireless body sensor networks applied in healthcare

applications", Wireless Personal Communications, vol.111, no. 4, pp. 2605-2623, 2020.

[8] K. Parvez, F.T. Zohra, and M. Jahan, "A secure and lightweight user authentication mechanism for wireless body area network", In Proceedings of the International Conference on Networking, Systems and Security, pp. 139-143, 2019.

[9] B.A. Alzahrani, "Secure and efficient cloud-based IoT authenticated key agreement scheme for e-health wireless sensor networks", Arabian Journal for Science and Engineering, vol. 46, no. 4, pp. 3017-3032, 2021.

[10] G. Praveen, P.K. Singh, and P. Ranjan, "The impact of blockchain on the healthcare environment", Central University of South Bihar, Gaya, India, 7 Jun 2021.

[11] L. Xiao, D. Han, X. Meng, W. Liang, and K. Li, "A secure framework for data sharing in private blockchain-based WBANs", IEEE Access, vol. 8, pp. 153956-153968, 2020.

[12] Y. Ren, Y. Leng, F. Zhu, J. Wang, and H. Kim, "Data storage mechanism based on blockchain with privacy protection in wireless body area network", Sensors, vol. 19, no. 10, pp. 2395, 2019.

[13] N.R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," in IEEE Trans. Mobile computing, vol. 5, no. 2, pp. 128-143, 2006.

[14] A. Castiglione, F. Palmieri, U. Fiore, A. Castiglione, and A. De Santis, "Modeling energy-efficient secure communications in multi-mode wireless mobile devices," Journal of Computer and System Sciences, vol 81, no. 8, pp. 1464-1478, 2015.

[15] C. Thammarat, and C. Techapanupreeda, "Secure mutual authentication protocol based on wireless body area networks", Journal of Information Science and Technology, vol. 11, no. 2, pp. 29-37, 2021.

[16] C. Thammarat, and C. Techapanupreeda, "A secure authentication and key exchange protocol for M2M communication", Electrical Engineering Congress (iEECON), pp. 456-459, 2021.

[17] C.J.F. Cremers, "The scyther tool: verification, falsification, and analysis of security protocols," In: International Conference on Computer Aided Verification. Springer, pp. 414-418, 2008.

[18] C. Thammarat, and C. Techapanupreeda, "A secure mobile payment protocol for handling accountability with formal verification", International Conference on Information Networking (ICOIN), pp. 249-254), 2021.

[19] C. Thammarat, and C. Techapanupreeda, "Secure key establishment protocol for smart homes based on symmetric cryptography", International Conference on Information Networking (ICOIN), pp. 46-51, 2022.