JIST Journal of Information Science and Technology
Volume 12, NO 2 | JUL – DEC 2022 | 21-30
ISSN: 2651-1053 (Online)
ISSN: 1906-9553 (Print)

โพรโทคอลพิสูจน์ทราบตัวจริงและปลอดภัยที่น้ำหนักเบาสำหรับสมาร์ทโฮมด้วยเทคโนโลยีบล็อกเชน

Lightweight Authentication and Secure Communication Protocol for Smart Home with Blockchain Technology

ปิยวิทย์ คุ้มครอง, ภูมิจิต ภูมินาถ, ฟารีด หมานเหล็บ, ชาลี ธรรมรัตน์ และ วทัญญู ยอดทอง*

Piyawit Khumkrong, Bhoomjit Bhoominath, Fareed Marnleb, 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 – Nowadays, smart home technology has been developed and applied widely. Applications includes automatic light on-off and air conditioning control systems where users can send commands to a device gateway or an Internet of Things (IoT) device via smartphones as needed. During the last few years, many research papers have investigated security and authentication protocols. However, it is still lack of consideration for the power constraints of IoT devices. This research paper presents a security and authentication protocol which reduces the use of encryption and hash functions. Therefore, it consumes less power in the operation and, hence, complies with the power limitation of IoT and mobile devices. We also introduce examples of how to use the protocol with blockchain technology.

KEYWORDS: Smart Home, IoT, Lightweight Protocol, Authentication Protocol

บทคัดย่อ -- **ปัจจุบันมีได้มีการพัฒนาและนำเทคโนโลยีสมาร์ทโฮม(Smart Home) มาใช้งานกันอย่างแพร่หลาย เพื่ออำนวยความสะดวกในการดำเนินชีวิตประจำวัน เช่น ระบบเปิด-ปิดไฟอัตโนมัติ ระบบควบคุมเครื่องปรับอากาศ เป็นต้น ซึ่งผู้ใช้งานสามารถควบคุมอุปกรณ์เหล่านี้ผ่านสมาร์ทโฟน(Smart Phone) ให้สามารถส่งคำสั่งไปยังอุปกรณ์เกตเวย์ (Gateway Device) หรืออุปกรณ์ Internet of Things (IoT) ได้ตามต้องการ มีงานวิจัยจำนวนมากได้ได้นำเสนอความมั่นคงปลอดภัยของการใช้งานสมาร์ทโฮมและได้นำเสนอโพรโทคอลความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริง การรักษาความลับและการคงสภาพข้อความแต่อย่างไรก็ตามงานวิจัยที่นำเสนอจำนวนมากยังขาดการคำนึงถึงข้อจำกัดการใช้พลังงานของอุปกรณ์เหล่านั้น งานวิจัยนี้ได้นำเสนอความมั่นคงปลอดภัยและการพิสูจน์ทราบตัวจริงที่ลดการใช้การเข้ารหัสลับ(Encryption) และการใช้งานฟังก์ชั่นแฮช (Hash Function)แต่ยังคงความมั่นปลอดภัยอยู่และงานวิจัยนี้ได้นำเสนอยังใช้พลังงานน้อยเพื่อเหมาะสมกับข้อจำกัดด้านพลังงานของอุปกรณ์เกตเวย์และอุปกรณ์IoT สุดท้ายนี้งานวิจัยนี้ยังได้เสนอแนวทางการนำไปใช้งานร่วมกับเทคโนโลยีบล็อกเชน**

คำสำคัญ: สมาร์ทโฮม, IoT, โพรโทคอลน้ำหนักเบา, โพรโทคอลพิสูจน์ทราบตัวจริง

*Corresponding Author: *chalee23@gmail.com*

1. บทนำ

ปัจจุบัน Internet of Things (IoT) เทคโนโลยีถูกพัฒนาอย่างรวดเร็วจึงทำให้เกิดวิวัฒนาการในด้านการติดต่อสื่อสารระหว่างผู้ใช้งานและเครื่องใช้ไฟฟ้าภายในบ้านที่จะอำนวยความสะดวกให้กับผู้ใช้งานเป็นอย่างมาก เช่น การบอกสถานะการทำงานของเครื่องใช้ไฟฟ้า การสั่งงานเครื่องใช้ไฟฟ้าผ่านสมาร์ทโฟน เป็นต้น โดยอาศัยการเชื่อมต่อเครือข่ายไร้สายภายในบ้านเช่น ZigBee,Zwave [1] และ Wi-Fi ซึ่งเป็นเครือข่ายไร้สาย มีความเสี่ยงในด้านความมั่นคงปลอดภัยที่อาจถูกดักข้อความ ปลอมแปลงข้อความ หรือ สวมรอยเข้ามาในสมาร์ทโฮม งานวิจัยความมั่นคงปลอดภัยสมาร์ทโฮม(Smart Home) [2, 3, 4, 5] ได้นำเสนอวิธีการรักษาความมั่นคงปลอดภัยการพิสูจน์ทราบตัวจริงร่วมกัน (Mutual Authentication) การรักษาความลับ (Confidentiality) และการคงสภาพของข้อความ (Integrity) แต่อย่างไรก็ตามงานวิจัยจำนวนมาก ที่ได้นำเสนอยังขาดการคำนึงถึงข้อจำกัดด้านการใช้พลังงานของอุปกรณ์ IoT [2, 4, 5, 6, 7, 8, 9] และด้านของความความมั่นคงปลอดภัยยังขาดความสามารถในการป้องกันการโจมตีโดยการดักฟังข้อความ (Eavesdropping Attack) [2, 4, 5, 6, 7]

บทความวิจัยฉบับนี้นำเสนอความมั่นคงปลอดภัยการพิสูจน์ทราบตัวจริงอุปกรณ์สมาร์ทโฮม นอกจากนี้โพรโทคอลที่นำเสนอยังใช้พลังงานน้อยเมื่อเปรียบเทียบกับโพรโทคอลที่มีอยู่ เนื่องจากใช้เพียงการเข้ารหัสลับแบบสมมาตร (Symmetric Encryption) และฟังก์ชั่นแฮช (Hash Function) ขณะที่ยังคงมีคุณสมบัติความมั่นคงปลอดภัยที่จำเป็น เช่น การพิสูจน์ทราบตัวจริง การรักษาความลับ และการคงสภาพของข้อความ นอกจากนี้ยังมีใช้เทคนิคการกระจายคีย์ เพื่อป้องกันการใช้งานคีย์ซ้ำเพื่อป้องกันการโจมตีการส่งข้อความซ้ำ

บทความวิจัยฉบับนี้มีโครงสร้างดังนี้ บทที่ 2 กล่าวถึงพื้นฐานที่เกี่ยวข้อง บทที่ 3 นำเสนองานวิจัย บทที่ 4 วิเคราะห์ความมั่นคงปลอดภัพ บทที่ 5 การวิเคราะห์ประสิทธิภาพของโพรโทคอลที่นำเสนอ บทที่6 การตรวจสอบความมั่นคงงานวิจัยที่นำเสนอปลอดภัยด้วย Scyther Tool บทที่7 เสนอแนวความคิดการนำบล็อกเชนมาประยุกต์ใช้ในสมาร์ทโฮม และ บทที่ 8 สรุปผลการวิจัย

2. พื้นฐานที่เกี่ยวข้อง

Smart home เป็นการนำเทคโนโลยี IoT มาประยุกต์ใช้งานในการควบคุมอุปกรณ์ไฟฟ้าผ่านอินเตอร์เน็ต ด้วยเทคโนโลยีที่พัฒนาขึ้นอย่างก้าวกระโดดในปัจจุบันทำให้ต้นทุนของอุปกรณ์เหล่านี้มีราคาถูกลง ทำให้อุปกรณ์เหล่านี้ถูกใช้งานอย่างแพร่หลายเพื่อเพิ่มความสะดวกสบายให้แก่ผู้ใช้งานในการติดตาม ควบคุม บริหารจัดการและทำให้เครื่องใช้ไฟฟ้า [10] แต่ทั้งนี้ด้วยโครงสร้างการทำงานที่ต้องอาศัยเครือข่ายอินเทอร์เน็ต จึงต้องคำนึงถึงความมั่นคงปลอดภัยที่จะสามารถป้องกันภัยคุกคามจากผู้ที่ไม่หวังดี เข้ามาสอดแนม ขัดขวางหรือสร้างอันตรายแก่สมาร์ทโฮมได้ หรือแม้กระทั่งโดนควบคุมเพื่อใช้ในการโจมตี [11] จากการศึกษาจะเห็นได้ว่าสมาร์ทโฮมนั้นยังมีข้อจำกัดในหลายๆ ด้านโดยข้อจำกัดและก่อให้เกิดช่องโหว่ เนื่องจากอุปกรณ์เหล่านี้ถูกออกแบบมาเพื่อให้ใช้พลังงานน้อยและกำลังในการประมวลผลต่ำ [12, 13, 14]

บล็อกเชน (Blockchain) คือ เทคโนโลยีที่ถูกสร้างขึ้นมาเพื่อใช้กับระบบการเก็บข้อมูลแบบโครงสร้าง (Data Structure) ซึ่งไม่มีศูนย์กลางในการจัดเก็บ ข้อมูลจะถูกแชร์และจัดเก็บเป็นสำเนาไว้ในโหนด (Node) ของเครือข่ายบล็อกเชนที่ใช้โครงสร้างข้อมูลเดียวกันเสมือนห่วงโซ่ (Chain) [15] โดยทุกโหนดจะรับทราบร่วมกันว่าใครเป็นเจ้าของข้อมูล เมื่อมีเพิ่มข้อมูลใหม่จะสำเนาข้อมูลในโครงสร้างข้อมูลเดียวกันให้กับทุกโหนดในเครือข่ายบล็อกเชน บล็อกเชนเป็นนวัตกรรมที่ถูกสร้างขึ้นเพื่อพิสูจน์ธุรกรรมทั้งหมดที่เกิดขึ้นในระบบหรือเครือข่าย โดยการบันทึกบัญชีแบบกระจายอำนาจ ที่ผู้ใช้สามารถตรวจสอบความถูกต้องซึ่งกันและกันได้ อีกทั้งความสามารถที่ป้องกันการเปลี่ยนแปลงข้อมูล โดยการตรวจสอบย้อนหลังจากบล็อคก่อนหน้า เป็นที่มาของคำว่าบล็อกเชนและด้วยความสามารถนี้จึงสามารถนำเอามาประยุกต์ใช้กับระบบสมาร์ท

โฮมได้เป็นอย่างดี ทั้งในการรักษาความปลอดภัย ความถูกต้องของข้อความ และธุรกรรมที่เกิดขึ้นทั้งหมด และยังสามารถใช้เพื่อกำหนดสิทธิ์การเข้าถึง หรือเงื่อนไขอื่น ๆ โดยการใช้ชุดคำสั่งผ่านองค์ประกอบอย่าง Smart Contract ผ่านแพลตฟอร์ม Ethereum [16]

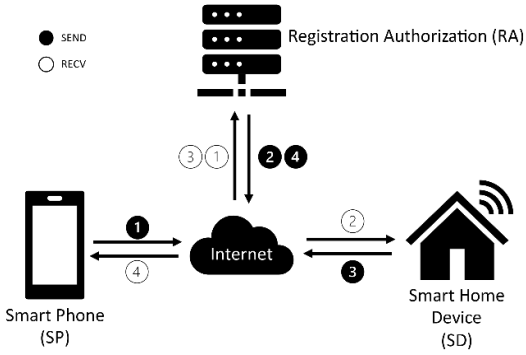
3. งานวิจัยที่นำเสนอ

หัวข้อนี้นำเสนอโพรโทคอลเพื่อแก้ไขปัญหาและข้อจำกัดของงานวิจัยที่มีอยู่ได้แก่คุณสมบัติความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริง ความคงสภาพของข้อความและการรักษาความลับของข้อความและทนทานต่อการโจมตีเช่น การดักฟังข้อความ (Eavesdropping Attack) การปลอมแปลง (Impersonation Attack) การโจมตีแบบคนกลาง (Man-in-the-Middle Attack) การปลอมตัว (Masquerade Attack) การปลอมข้อความ (Message-Forgery Attack) และการโจมตีแบบทำซ้ำ (Replay Attack) งานวิจัยนี้ได้กำหนดสัญลักษณ์เพื่อใช้ในการอธิบายโพโตคอลและคำอธิบายของสัญลักษณ์ดังตารางที่ 1

ตารางที่ 1 เครื่องหมายและความหมายในบทความวิจัย

สัญลักษณ์	คำอธิบาย
RA	เซิฟเวอร์ที่ใช้ลงทะเบียน (Registration Authorization)
SP	สมาร์ทโฟน (Smart Phone)
SD	อุปกรณ์อัจฉริยะ (Smart Home Device)
ID_{SP}	เอกลักษณ์ของ SP
ID_{SD}	เอกลักษณ์ของ SD
SN_{SP}	หมายเลขประจำเครื่อง SP
SN_{SD}	หมายเลขประจำอุปกรณ์ SD
MK	มาสเตอร์คีย์
SK	เซสชั่นคีย์
H(•)	ฟังก์ชั่นแฮช
T	การประทับเวลา
N	นอนซ์ (Nonce) คือค่าสุ่ม
E{•}	เข้ารหัสลับแบบสมมาตร (Symmetric Encryption)
ΔT	ค่าดีเลย์สูงสุดของการส่งข้อความ

ในส่วนนี้จะเป็นการนำเสนอโพรโทคอลที่ประกอบไปด้วยขั้นตอนการลงทะเบียน (RegisterPhase) และการพิสูจน์ทราบตัวจริงและกระจายเซสชั่นคีย์ (Authentication and Key Agreement Phase) โดยจะมีการทำงานร่วมกันระหว่างSP, RA และSDรูปที่ 1แสดงขั้นตอนการทำงานของโปรโตคอลที่นำเสนอ



รูปที่ 1. โครงสร้างการเชื่อมต่อของสมาร์ทโฮม

3.1 การลงทะเบียน (Register Phase)

วัตถุประสงค์การลงทะเบียนเพื่อแชร์มาสเตอร์คีย์ระหว่าง RA และ SP แชร์มาสเตอร์คีย์MK_{RA-SP}ดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัยเช่น SSL (Secure Socket Layer) หรือ Wireless Transport Layer Security (WTLS) และระหว่าง RA

และ SD แชร์มาสเตอร์คีย์ MK_{RA-SD}ดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัยเช่น SSL หรือ WTLS

3.2 การพิสูจน์ทราบตัวจริงและการกระจายเซสชั่นคีย์ (Authentication and Key Agreement Phase)

Step 1: SP →RA: {ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, A}

Step 2: RA → SD: {ID_{SP}, ID_{SD}, SN_{SP}, T2, N2, C}

Step: 3 SD → RA: {SN_{SD},T3, N3, D}

Step 4: RA → SP: {SN_{SD}, T4, N4, F}

Step 5: SP → SD: {SK_{SP-SD}{Messagei, Ti}}

จากโพรโทคอลด้านบนเป็นการพิสูจน์ทราบตัวจริงและการและกระจายเซสชั่นคีย์สามารถอธิบายดังนี้

Step 1: SP →RA: {ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, A}

- SP ดำเนินการประทับเวลา T1
- SP ทำการสุ่มค่านอนซ์ตัวแปร N1
- SP คำนวณค่า A = H(ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, MK_{RA-SP})
- SP ส่งข้อความ {ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, A} ไปยัง RA
- SP บันทึกค่า T1, N1 ไว้ในหน่วยความจำ

รูปที่ 1 ตามลำดับเส้นเชื่อมโยงจาก ❶ ส่งข้อความไป ①

Step 2: RA → SD: {ID_{SP}, ID_{SD}, SN_{SP}, T2, N2, C}

- RA ดำเนินการประทับเวลาปัจจุบัน T2 และทำการตรวจสอบ T2 – T1 <ΔT ว่าเป็นจริงหรือไม่หากเป็นจริง RA จะดำเนินการต่อไปหากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารทันที
- RA คำนวณค่า A* โดยการนำค่า ID_{SP}, ID_{SD}, SN_{SP}, T1, N1 ที่ได้รับจาก SP และมาสเตอร์คีย์ที่ใช้ร่วมกันระหว่าง RA และ SD(MK_{RA-SD}) ที่มีการแชร์ระหว่างกันตั้งแต่ขั้นตอนของการลงทะเบียนมาเข้าฟังก์ชั่นแฮชโดย A* = H(ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, MK_{RA-SP}) และดำเนินการตรวจสอบ A* = A เป็นจริงหรือไม่หากเป็นจริง RA จะดำเนินการต่อไปหากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารกับ SP ทันที
- RA ทำการสุ่มค่านอนซ์โดยใช้ตัวแปร N2
- RA ดำเนินการกำหนดค่าเซสชั่นคีย์ที่จะใช้ระหว่าง SP และ SD (SK_{SP-SD})
- RA คำนวณค่า B = H(ID_{SP}, ID_{SD}, SN_{SP}, T2, N2, SK_{SP-SD})
- RA นำค่า B และ SK_{SP-SD}มาเข้ารหัสลับด้วย MK_{RA-SD} โดย C = EMK_{RA-SD}{$SK_{SP-SD,}$ B}
- RA ส่งข้อความ {ID_{SP}, ID_{SD}, SN_{SP}, T2, N2, C} ไปยัง SD
- RA ดำเนินการบันทึกค่า ID_{SP}, ID_{SD}, SN_{SP}, T1, N1,SK_{SP-SD} และ C ในหน่วยความจำ

รูปที่ 1 ตามลำดับเส้นเชื่อมโยงจาก ❷ ส่งข้อความไป ②

Step: 3 SD → RA:{SN_{SD},T3, N3, D}

- SD เมื่อได้รับข้อความจาก RA ดำเนินการประทับเวลาปัจจุบัน T3 และทำการตรวจสอบ T3 – T2 <ΔT ว่าเป็นจริงหรือไม่หากเป็นจริงSD จะดำเนินการต่อไป แต่หากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารกับ RA ทันที
- SD ดำเนินการถอดรหัสลับข้อความ C ด้วย MK_{RA-SD}ซึ่งจะทำให้ SD ทราบค่า SK_{SP-SD} และ B
- SD คำนวนค่า B* โดยนำค่า ID_{SP}, ID_{SD}, SN_{SP}, T2, N2 และ SK_{SP-SD} ที่ได้จากการถอดรหัสลับมาเข้าฟังก์ชั่นแฮชแบบทางเดียว โดย B* = H(ID_{SP}, ID_{SD}, SN_{SP}, T2, N2, SK_{SP-SD}) และดำเนินการตรวจสอบ B* = B ว่าเป็นจริงหรือไม่หากเป็นจริงSD จะดำเนินการต่อไปหากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารกับ RA ทันที
- SD ทำการสุ่มค่านอนซ์ตัวแปร N3
- SD คำนวณค่า D = H(SN_{SD}, T3, N3, C, MK_{RA-SD})
- SD ส่งข้อความ {SN_{SD},T3, N3, D} ไปยัง RA

ในรูปที่ 1 ตามลำดับเส้นเชื่อมโยงจาก ❸ ส่งข้อความไป ③

Step 4: RA → SP:{SN_{SD}, T4, N4, F}

- RA ดำเนินการประทับเวลาปัจจุบัน T4 และทำการตรวจสอบ T4 – T3 <ΔT ว่าเป็นจริงหรือไม่หากเป็นจริง

RA จะดำเนินการต่อไปหากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารทันที

- RA คำนวณค่า D* โดยการนำค่า SN_{SD}, T3, N3,MK_{RA-SD} ซึ่งเป็นมาสเตอร์คีย์ที่มีการแชร์ระหว่างกันตั้งแต่ขั้นตอนของการลงทะเบียน และค่า C ในหน่วยความจำมาเข้าฟังก์ชั่นแฮชทางเดียวโดย D* = H(SN_{SD}, T3, N3, C, MK_{RA-SD}) และดำเนินการตรวจสอบ D* = D เป็นจริงหรือไม่หากเป็นจริง RA จะดำเนินการต่อไปแต่หากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารกับ SD ทันที
  RA ทำการสุ่มค่านอนซ์ใช้ตัวแปร N4

- RA คำนวนค่า E โดยการนำค่าที่อยู่ในหน่วยความจำได้แก่ ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, ค่าของตัวแปรที่ได้รับจาก SD ได้แก่ SN_{SD} รวมถึงค่าเวลาปัจจุบัน T4, ค่านอนซ์ที่ดำเนินการสุ่มขึ้น N4 และค่ามาสเตอร์คีย์ MK_{RA-SP} ซึ่งแชร์กันตั้งแต่ขั้นตอนของการลงทะเบียน มาเข้าฟังก์ชั่นแฮชโดย E = H(ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, SN_{SD}, T4, N4, MK_{RA-SP})
- RA นำค่า E และSK_{SP-SD}ที่เก็บไว้ในหน่วยความจำมาเข้ารหัสลับด้วยมาสเตอร์คีย์ที่แชร์กันระหว่าง RA และ SP (MK_{RA-SP}) โดย F = EMK_{RA-SP}{$SK_{SP-SD,}$ E}
- RA ส่งข้อความ {SN_{SD}, T4, N4, F} ไปยัง SP

Step 5: SP → SD: {SK_{SP-SD}{Messagei, Ti}}

- SP ดำเนินการประทับเวลาปัจจุบัน Tiและทำการตรวจสอบ Ti – T4 <ΔT ว่าเป็นจริงหรือไม่หากเป็นจริง SP จะดำเนินการต่อไปหากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารทันที
- SP ดำเนินการถอดรหัสลับข้อความ F ด้วย MK_{RA-SP}จะทำให้ SP ทราบค่า SK_{SP-SD} และ E
- SP คำนวนค่า E* โดยการนำค่า ID_{SP}, ID_{SD}, SN_{SP}, T1, N1 ในหน่วยความจำ ค่า SN_{SD}, T4, N4 ที่ได้รับจาก RA และมาสเตอร์คีย์ MK_{RA-SP} ที่มีการแชร์ร่วมกันตั้งแต่ขั้นการลงทะเบียนมาเข้าฟังก์ชั่นแฮช โดย E* = H(ID_{SP}, ID_{SD}, SN_{SP}, T1, N1, SN_{SD}, T4, N4, MK_{RA-SP}) และดำเนินการตรวจสอบ E* = E เป็นจริงหรือไม่หากเป็นจริง SP จะดำเนินการต่อไปหากไม่เป็นจริงจะดำเนินการยุติการติดต่อสื่อสารทันที
- SP กำหนด Messageiในการติดต่อสื่อสารกับ SD
- SP นำ Messageiและ Tiมาเข้ารหัสลับด้วยเซสชั่นคีย์ SK_{SP-SD}
- SP ส่งข้อความ {SK_{SP-SD}{Messagei, Ti}} ไปยัง SD

รูปที่ 1 ตามลำดับเส้นเชื่อมโยงจาก ❹ ส่งข้อความไป ④ ทั้ง SP และ SD ใช้เซสชั่นคีย์ SK_{SP-SD}ในการติดต่อสื่อสาร เซสชั่นคีย์ SK_{SP-SD} จะถูกสร้างใหม่เมื่อหมดอายุ

4. การวิเคราะห์ความมั่นคงปลอดภัยของโพรโทคอลนำเสนอ

4.1 การโจมตีโดยการดักฟังข้อความ (Eavesdropping Attack)

ผู้โจมตีหรือผู้ไม่ประสงค์ดีดักฟังข้อความที่ติดต่อสื่อสาร โพรโทคอลที่นำเสนอสามารถป้องกันการดักฟังข้อความที่ติดต่อสื่อสารได้ เนื่องจากในแต่ละข้อความที่ติดต่อสื่อสารมีการเข้ารหัสลับทุกครั้งในการติดต่อสื่อสาร เมื่อผู้โจมตีการดักจับข้อความก็จะไม่สามารถถอดข้อความและอ่านข้อความเข้าใจได้ การเข้ารหัสลับโพรโทคอลที่นำเสนอทำให้ยืนยันได้ว่าข้อความที่ส่งหากันมีความมั่นคงปลอดภัย

4.2 การโจมตีโดยการปลอมแปลง (Impersonation Attack)

ผู้โจมตีหรือผู้ไม่ประสงค์ดีปลอมแปลงเป็นอุปกรณ์ที่มีการติดต่อสื่อสารที่ถูกต้อง เพื่อต้องการรับข้อความที่เป็นความลับระหว่างอุปกรณ์ที่มีการติดต่อสื่อสารกัน โพรโทคอลที่นำเสนอสามารถป้องกันการปลอมแปลงเป็นอุปกรณ์ที่มีการติดต่อสื่อสาร ไม่สามารถปลอมแปลงเป็นอุปกรณ์ที่มีการติดต่อสื่อสารที่ถูกต้อง เนื่องจากมีการใช้มาสเตอร์คีย์ที่มีการเข้ารหัสลับและมีการพิสูจน์ทราบตัวจริงระหว่างอุปกรณ์ หากจะปลอมแปลงเป็นอุปกรณ์ฝั่งใดฝั่งหนึ่งจำเป็นจะต้องมีมาสเตอร์คีย์ที่ตรงกันเพื่อถอดข้อความที่ติดต่อสื่อสาร

4.3 การโจมตีแบบคนกลาง (Man-in-the-Middle Attack)

โจมตีหรือผู้ไม่ประสงค์ดีอยู่ตรงกลางในการติดต่อสื่อสารระหว่างอุปกรณ์ เพื่อทำการเก็บรวบรวมข้อมูลการติดต่อสื่อสาร

ระหว่างอุปกรณ์ การโจมตีประเภทนี้โจมตีหรือผู้ไม่ประสงค์ดีไม่สามารถถอดข้อความและอ่านข้อความเข้าใจได้ เนื่องจากในแต่ละข้อความที่ติดต่อสื่อสารระหว่างอุปกรณ์มีการเข้ารหัสลับทุกครั้ง

4.4 การโจมตีโดยการปลอมตัว (Masquerade Attack)
ผู้โจมตีหรือผู้ไม่ประสงค์ดีปลอมตัวเป็นอุปกรณ์ที่มีการติดต่อสื่อสารที่ถูกต้อง เพื่อรับข้อความและส่งข้อความที่เป็นความลับจากอุปกรณ์ที่มีการติดต่อสื่อสารที่ถูกต้อง โพรโทคอลที่นำเสนอสามารถป้องกันการปลอมตัวประเภทนี้ได้ โดยการใช้การพิสูจน์ทราบตัวจริงทั้งอุปกรณ์ส่งข้อความและอุปกรณ์รับรับข้อความสามารถตรวจสอบได้ทั้งสองฝั่ง

4.5 การโจมตีโดยการปลอมข้อความ (Message-Forgery Attack)
การโจมตีประเภทนี้ผู้โจมตีหรือผู้ไม่ประสงค์ดีกระทำการปลอมข้อความที่ติดต่อสื่อสารกันระหว่างอุปกรณ์ที่ถูกต้อง โพรโทคอลที่นำเสนอมีการใช้มาสเตอร์คีย์ที่ตรงกันทั้งสองฝั่งและการใช้ค่านอนซ์นอกจากนี้ยังใช้ฟังชั่นแฮชเพื่อใช้ตรวจสอบทราบตัวจริงของข้อความ ทำให้การโจมตีประเภทนี้ไม่ประสบความสำเร็จ

4.6 การพิสูจน์ทราบตัวจริงร่วมกัน) Mutual Authentication)
โพรโทคอลที่นำเสนอใช้มาสเตอร์คีย์ เซสชั่นคีย์และแฮชฟังก์ชั่นทำให้สามารถพิสูจน์ทราบตัวจริงร่วมกันของแต่ละฝ่าย พิสูจน์ได้ว่าใครเป็นผู้รับข้อความและใครเป็นคนส่งข้อความจะไม่สามารถปลอมแปลงและแก้ไขการพิสูจน์ทราบตัวจริงร่วมกันได้โดยสมบูรณ์

4.7 การต้านทานการโจมตีแบบทำซ้ำ (Replay Attack)
เนื่องจากในแต่ละขั้นตอนของการส่งข้อความจะมีการเก็บบันทึกการประทับเวลา (Time Stamp) และค่านอนซ์ไว้ซึ่งไม่ซ้ำกันในแต่ละครั้ง จึงเป็นไปไม่ได้ที่จะใช้ข้อความที่ดักจับได้ส่งเข้ามาใหม่อีกครั้งเพราะโพรโทคอลที่นำเสนอสามารถตรวจสอบได้

4.8 การรักษาความลับของข้อความ (Message Confidentiality)
มีการเข้ารหัสลับด้วยมาสเตอร์คีย์และเซสชั่นคีย์ ทำให้ข้อความที่ติดต่อสื่อสารมีมีคุณสมบัติการรักษาความลับ เนื่องจากการถอดรหัสลับได้นั้นอีกฝั่งหนึ่งจำเป็นจะต้องมีคีย์ที่ตรงกันจึงจะสามารถถอดรหัสลับนี้ได้

4.9 ความคงสภาพของข้อความ (Message Integrity)
มีการใช้ฟังก์ชั่นแฮช ทำให้สามารถตรวจสอบได้ว่าข้อความที่ส่งหากันยังคงสภาพเดิม ถูกต้อง และไม่ถูกแก้ไขหรือเปลี่ยนแปลงระหว่างทางจากบุคคลอื่นไม่ได้รับอนุญาต

5. การวิเคราะห์ประสิทธิภาพของโพรโทคอล

โพรโทคอลที่นำเสนอมีการดำเนินการออกแบบโดยคำนึงถึงประสิทธิภาพของการใช้พลังงานและมีคุณสมบัติความมั่นคงปลอดภัยทนทานต่อการถูกโจมตี โดยมีการใช้การเข้ารหัสลับ การใช้ฟังก์ชั่นแฮช และจำนวนข้อความที่เหมาะสม

ตารางที่ 2. แสดงจำนวนการใช้วิทยาการการเข้ารหัสลับ

	[2]	[4]	[5]	[6]	[7]	Protocol
SymmetricEncryption	-	4	4	4	8	4
Asymmetric Encryption	4	-	-	-	-	-
Hash Function	17	12	22	16	26	5
Message	2	4	4	4	4	4

ตารางที่ 3. การใช้พลังงานวิทยาการการเข้ารหัสลับ

	[2]	[4]	[5]	[6]	[7]	Our
AES	-	4.84	4.84	4.84	-	4.84
RSA	2,186	-	-	-	-	-
SHA1	12.92	9.12	16.72	12.16	19.76	3.8
Total	2,198	13.96	21.56	17	29.44	13.96

SymmetricEncryption (Advanced Encryption Standard (AES): 1.21 μJ), AsymmetricEncryption (Rivest–Shamir–Adleman (RSA): 546.5 μJ), Hash Function (Secure Hash Algorithm 1 (SHA1): 0.76 μJ)

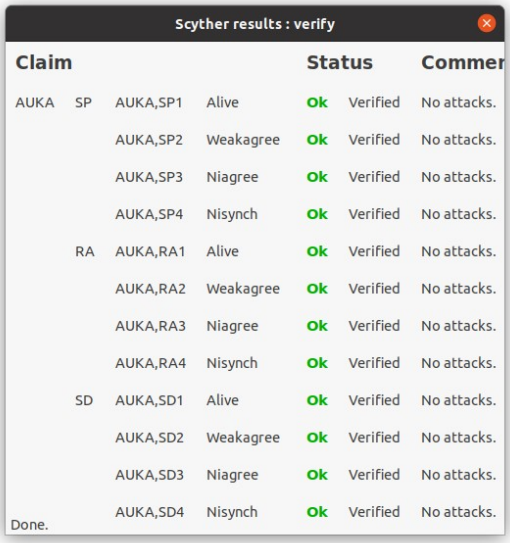
จากตาราง 2 และ 3 จะแสดงให้เห็นถึงจำนวนครั้งในการใช้วิทยาการการเข้ารหัสลับและการใช้พลังงานในวิทยาการเข้ารหัสลับเปรียบเทียบงานวิจัยที่มีอยู่กับงานวิจัยที่นำเสนอ โพรโทคอลที่นำเสนอใช้พลังงานน้อยกว่าโพรโทคอล [2, 5, 6, 7] ขณะที่โพรโทคอล [4] ใช้พลังงานเท่ากับโพรโทคอลที่นำเสนอ จึงทำให้การพิสูจน์ทราบตัวจริงระหว่างกัน มีประสิทธิภาพและใช้พลังงานน้อย พลังงานในวิทยาการเข้ารหัสลับอ้างอิงจาก [20, 21]

6. การตรวจสอบความมั่นคงปลอดภัยด้วย Scyther Tool

โพรโทคอลที่นำเสนอใช้ Scyther Tool [17] เป็นเครื่องมือที่ใช้ตรวจสอบความถูกต้องและความมั่นคงปลอดภัยของโพรโทคอลที่ออกแบบ โค้ดแสดงดังรูปที่ 2และรูปที่ 3เป็นเอาท์พุทจากการรันโค้ด สถานะ OK หัวข้อดังนี้ Alive, Weakagree, Niagree และ Nisynchแสดงว่าโพรโทคอลที่นำเสนอถูกต้องและความมั่นคงปลอดภัยทนทานต่อการโจมตี

```
usertype String;
usertypeTimeStamp;
usertypeSessionKey;
hashfunction H;
const IDSP,IDRA,IDSD,SNSP,SNSD: String;
const MKRA-SP,MKRA-SD,SKSP-SD: SessionKey;
macro M1 = IDSP,IDSD,SNSP,T1,N1,H(IDSP,IDSD,SNSP,T1,N1,MKRA-SP);
macro M2 = IDSP,IDSD,SNSP,T2,N,{SKSP-SD,H(IDSP,IDSD,SNSP,T2,N2,SKSP-SD)}MKRA-SD;
macro M3 = SNSD,T3,N3,H(SNSD,T3,N3),{SKSP-SD,H(IDSP,IDSD,SNSP,T2,N2,SKSP-SD)}MKRA-SD;
macro M4 = SNSD,T4,N4,H(SNSD,T4,N4),{SKSP-SD,H(IDSP,IDSD,SNSP,T1,N1,SNSD,T4,N4,MKRA-SP)}MKRA-SP;
protocol AUKA(SP,RA,SD) {
    role SP {
        fresh T1,T4: TimeStamp;
        fresh N1,N4: Nonce;
        send_1(SP,RA,M1);
        recv_4(RA,SP,M4);
        claim_SP1(SP,Alive);
        claim_SP2(SP,Weakagree);
        claim_SP3(SP,Niagree);
        claim_SP4(SP,Nisynch);
    }
    role RA {
        fresh T1,T2,T3,T4: TimeStamp;
        fresh N1,N2,N3,N4: Nonce;
        recv_1(SP,RA,M1);
        send_2(RA,SD,M2);
        recv_3(SD,RA,M3);
        send_4(RA,SP,M4);
        claim_RA1(RA,Alive);
        claim_RA2(RA,Weakagree);
        claim_RA3(RA,Niagree);
        claim_RA4(RA,Nisynch);
    }
    role SD {
        fresh T2,T3: TimeStamp;
        fresh N2,N3: Nonce;
        recv_2(RA,SD,M2);
        send_3(SD,RA,M3);
        claim_SD1(SD,Alive);
        claim_SD2(SD,Weakagree);
        claim_SD3(SD,Niagree);
        claim_SD4(SD,Nisynch);
    }
}
```

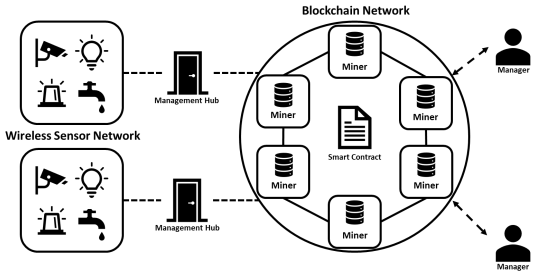
รูปที่ 2. ซอร์สโค้ด Scyther Tool



รูปที่ 3. แสดงผลการทดสอบ Scyther Tool

7. แนวความคิดการนำบล็อกเชนมาประยุกต์ใช้ในสมาร์ทโฮม

ในงานวิจัยนี้ได้มีการศึกษาเพิ่มเติมเกี่ยวกับการนำเทคโนโลยีบล็อกเชนส่วนตัว (Private Blockchain) มาใช้ร่วมกับสมาร์ทโฮม [18] โดยบล็อกเชนเข้ามาช่วยในส่วนของการกระจายการบริหารจัดการและการจัดเก็บข้อมูลซึ่งข้อมูลที่จัดเก็บจะเป็นความลับเปิดเผยเฉพาะคนที่ได้รับอนุญาตเท่านั้น รวมไปถึงการรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว โดยมีโครงสร้างตามรูปที่ 4 สามารถอธิบายได้ดังนี้



รูปที่ 4. แสดงการนำบล็อกเชนมาใช้งานในระบบสมาร์ทโฮม

7.1 Wireless Sensor Network

เป็นอุปกรณ์ที่ทำหน้าที่ค่อยรับส่งข้อมูลให้กับ IoT หรือสมาร์ทโฮม เช่น การวัดอุณหภูมิห้อง ณ ปัจจุบันและส่งข้อมูลอุณหภูมิไปจัดเก็บ เพื่อแสดงผลในภายหลัง หรือการรับคำสั่งจากผู้ใช้งานให้ทำงานตามคำสั่งเช่นเปิด-ปิดไฟแสงสว่าง หรือเพิ่มลดอุณหภูมิของเครื่องปรับอากาศ

7.2 Management Hub

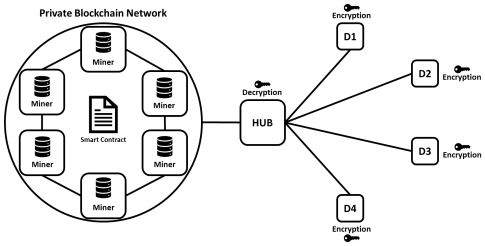
เป็นอุปกรณ์หรือระบบที่ทำหน้าที่เป็นตัวกลางเชื่อมต่อระบบระหว่างอุปกรณ์IoT เปรียบเสมือนเกตเวย์ ที่จะทำหน้าที่รักษาความปลอดภัยของข้อมูลโดยการเข้ารหัสลับและถอดรหัสลับในการสื่อสารระหว่างกัน อีกทั้งยังมีหน้าที่ในการสื่อกับระบบบล็อกเชนเพื่อตรวจสอบสิทธิ์การเข้าถึง หรือบันทึกข้อมูลในระบบบล็อกเชน

7.3 Blockchain Network

เครือข่ายบล็อกเชนจะถูกกำหนดเป็นความลับเพื่อป้องกันไม่ให้ถูกเข้าถึงข้อมูลโดยที่ไม่ได้รับอนุญาตได้ และประกอบไปด้วย Miner ที่ทำหน้าที่ในการบำรุงรักษาระบบบล็อกเชนให้สามารถดำเนินการต่อไปได้ โดยมี Smart Contract ที่จะเป็นชุดคำสั่ง [19] ที่จะเป็นตัวกำหนดควบคุมความสามารถของเครือบล็อกเชนเช่น การกำหนดสิทธิการเข้าถึงหรือการตรวจสอบสิทธิการเข้าถึง

7.4 Manager

ผู้บริหารจัดการระบบหรือผู้ใช้งานที่จะเป็นผู้เรียกใช้ข้อมูล ส่งคำสั่งไปยังอุปกรณ์ หรือการบริหารจัดการระบบทั้งระบบบล็อกเชนและอุปกรณ์ IoT ในระบบสมาร์ทโฮม



รูปที่ 5. แสดงการนำบล็อกเชนมาใช้งานวิจัยที่นำเสนอ

จากรูปที่ 5 การนำบล็อกเชนมาใช่ร่วมกับโพรโทคอลที่ได้ออกแบบในบทความวิจัยนี้โดยการนิยามให้ระบบบล็อกเชนเสมือนกับเป็น Registration Authorization (RA) ที่ทำหน้าที่ในการเป็นตัวกลางให้กับสมาร์ทโฮม เพื่อจัดเก็บบันทึกข้อมูลกิจกรรมต่างๆ กระจายเซสชั่นคีย์ในการรักษาความลับระหว่างการรับส่งข้อมูล

8. สรุปผลการวิจัยและการอภิปราย

งานวิจัยนี้ได้นำเสนอโพรโทคอลสำหรับพิสูจน์ทราบตัวจริง ซึ่งได้นำการกระจายเซสชันคีย์และการใช้แฮชฟังก์ชันมาใช้งานทำให้โพรโทคอลมีน้ำหนักเบาเหมาะสมกับอุปกรณ์สื่อสารไร้สายในปัจจุบันเพราะมีการคำนวณน้อย นอกจากนี้ยังมีคุณสมบัติความมันคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริง การรักษาความลับของข้อความและการคงสภาพของข้อความ นอกจากนี้โพรโทคอลที่นำเสนอยังใช้พลังงานน้อยเมื่อเปรียบเทียบกับโพรโทคอลที่มีอยู่ สุดท้ายความถูกต้องของโพรโทคอลถูกตรวจสอบด้วย Scyther Toolทำให้มั่นใจได้ว่าโพรโทคอลที่นำเสนอมีความมั่นคงปลอดภัย

งานวิจัยในอนาคตผู้วิจัยจะพัฒนาโปรแกรมต้นแบบโดยใช้โพรโทคอลที่นำเสนอร่วมกับเทคโนโลยีบล็อกเชน เพื่อให้สามารถใช้งานได้จริงและพัฒนาให้มีประสิทธิภาพเพิ่มขึ้น

เอกสารอ้างอิง

[1] XX.C. Gomez, and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” IEEE Communications Magazine, vol. 48, no. 6, pp. 92–101, 2010.

[2] M. Alshahrani, and I. Traore, “Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain,” Journal of Information Security and Applications, vol. 45, pp. 156–175, 2019.

[3] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P.H. Ha, “Anonymous Secure Framework in Connected Smart Home Environments,” in IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 968-979, 2017.

[4] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, “Remotely Access My Smart Home in Private: An Anti-Tracking Authentication and Key Agreement Scheme,” in IEEE Access, vol. 7, pp. 41835-41851, 2019.

[5] M. Wazid, A.K. Das, V. Odelu, N. Kumar, and W. Susilo, “Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment,” in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 391- 406, 2020.

[6] M. Shuai, N. Yu, H. Wang, and L. Xiong, “Anonymous authentication scheme for smart home environment with provable security,” Computers & Security, vol. 86, pp. 132-46, 2019.

[7] S. Naoui, M. E. Elhdhili, and L.A. Saidane, “Lightweight and Secure Password Based Smart Home Authentication Protocol: LSP-SHAP,” Journal of Network and Systems Management, 2019

[8] S. Bhardwaj, T. Ozcelebi, J. Lukkien, and C. Uysal, “Resource and service management architecture of a low capacity network for smart spaces,” Consumer Electronics, IEEE Transactions on, vol. 58, no. 2, pp. 389–396, 2012.

[9] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, “Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments,” in IEEE Sensors Journal, vol. 16, no. 1, pp. 254-264, 2016.

[10] S.S.I. Samuel, “A review of connectivity challenges in IoT-smart home,” 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, pp. 1-4, 2016.

[11] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” in Computer, vol. 50, no. 7, pp. 80-84, 2017.

[12] M. Yu, J. Zhuge, M. Cao, Z. Shi, and L. Jiang, “A Survey of Security Vulnerability Analysis, Discovery,

Detection, and Mitigation on IoT Devices." Future Internet, 12, 27, 2020.

[13] A. Balte, A. Kashid, and B. Patil, "Security issues in Internet of things (IoT): A survey," Int. J. Adv. Res. Comput. Sci. Softw. Eng. vol. 5, pp. 450–455, 2015.

[14] F.A. Alaba, M. Othman, I.A.T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.

[15] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf, 2008.

[16] G. Wood, "Ethereum: A secure decentralisedgeneralised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[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] A. Mukherjee, M. Balachandra, C. Pujari, S. Tiwari, A. Nayar, and S.R. Payyavulaf. "Unified smart home resource access along with authentication using Blockchain technology," 1st International Conference on Advances in Information, Computing and Trends in Data Engineering (AICDE - 2020), pp. 29-34, 2020.

[19] K. Christidis, and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[20] 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.

[21] 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.

[22] 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.

[23] C. Thammarat, "Efficient and secure NFC authentication for mobile payment ensuring fair exchange protocol", Symmetry, vol. 12, no. 10, pp. 1649, 2020.

[24] C. Thammarat, and W. Kurutach, "A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification", International Journal of Communication Systems, vol. 32, no. 12, pp. e3991, 2019.