การทบทวนการเข้ารหัสเพื่อระบุตัวตนด้วยอาร์เอฟไอดีสำหรับอินเทอร์เน็ตในทุกสิ่ง

A Review Cryptography RFID Identification Schemes for Internet of Things

สันติพงค์ แสงฮวด, พยุง มีสัตย์, สุนันทา สดสี
ภาควิชาเทคโนโลยีสารเทศ คณะเทคโนโลยีสารเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

Santipong Sanghoud, Phayung Meesad, Sunantha Sodsee
Major of Information Technology, Faculty of Information Technology, King Mongkut's University of Technology North Bangkok

Abstract

At present, the advancement of information and communications technology has developed technology applied to objects around them by a technology called Internet of Things (IoT). Currently, bringing IoT applications in the various fields, whether it is House, Logistics, and Health. As a result, the convenience of daily life. But there is still a risk to the security of the data. So this article is to review recent literature about the introduction of RFID in the management of security for the IoT. From a review of the literature of the past has found three algorithms that can be applied to IoT, including Zhao's scheme Zhang, Qi's scheme and Farash's scheme of Farash's scheme is suitable to be applied to most. Because Comparison of Computational Cost is minimal.

Keywords: *Identification, Radio frequency identification, Internet of Things, Encryption*

บทคัดย่อ

ในปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารได้มีการพัฒนาไปสู่การนำเอาเทคโนโลยีมาประยุกต์ใช้กับสิ่งของรอบตัวโดยที่เรียกเทคโนโลยีที่เรียกว่า Internet of Things (IoT) ในปัจจุบันนั้นได้มีการนำเอา IoT ไปประยุกต์ใช้กับด้านต่าง ๆ ไม่ว่าจะเป็น ด้านที่อยู่อาศัย ด้านโลจิสติกส์ ด้านสุขภาพ เป็นต้น จึงทำให้เกิดความสะดวกสบายในชีวิตประจำวัน แต่ก็ยังคงมีความเสี่ยงในการรักษาความปลอดภัยของข้อมูลได้ ดังนั้นบทความฉบับนี้ได้ทำการทบทวนวรรณกรรมที่ผ่านมาเกี่ยวกับการนำเอา RFID มาจัดการในส่วนของการรักษาความปลอดภัยให้กับ IoT จากการทบทวนวรรณกรรมที่ผ่านมาพบว่ามี 3 อัลกอริทึมที่สามารถนำเอามาประยุกต์ใช้กับ IoT ได้ ได้แก่ Zhao's scheme Zhang, Qi's scheme และ Farash's scheme ส่วน Farash's scheme มีความเหมาะสมที่จะนำไปประยุกต์ใช้มากที่สุด เพราะ Comparison of Computational Cost น้อยที่สุด

คำสำคัญ : *การระบุตัวตน, อาร์เอฟไอดี, อินเทอร์เน็ตในทุกสิ่ง, การเข้ารหัส*

1. บทนำ

Internet of Things (IoT) หรือ อินเทอร์เน็ตในทุกสิ่ง หมายถึง การที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น การสั่งเปิด-ปิด อุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรใน โรงงานอุตสาหกรรม อาคารบ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต โดย IoT จะเปลี่ยนวัตถุสิ่งของอิเล็กทรอนิกส์ทั้งหมดในชีวิตประจำวันของเราให้กลายเป็นส่วนหนึ่งของการเชื่อมต่อ Internet (Suwimon Vongsingthong, et al., (2014)) โดยการนำเทคโนโลยี IoT มาใช้ และได้มีการพัฒนาไปสู่ Smart City, Home Automation, Smart Grid, Traffic Management เป็นต้น ส่วนในด้านสุขภาพได้นำมาใช้ในการดูแลผู้ป่วย ผู้สูงอายุ เพื่อให้แพทย์ที่ดูแลอาการของผู้ป่วยเหล่านั้นสามารถติดตามอาการของผู้ป่วยได้อย่างใกล้ชิด (Amir Mohammad Rahmani. (2015); Partha P. Ray. (2014)) เป็นต้น หากวันนั้นมาถึงอย่างเต็มรูปแบบ จะเป็นทั้งประโยชน์อย่างมหาศาล และความเสี่ยงไปพร้อม ๆ กัน เพราะหากระบบรักษาความปลอดภัยของอุปกรณ์และเครือข่ายอินเทอร์เน็ตไม่ดีพอจะทำให้ผู้ไม่ประสงค์ดีเข้ามากระทำการที่ไม่พึงประสงค์ต่ออุปกรณ์ข้อมูลสารสนเทศหรือความเป็นส่วนตัวของบุคคลได้ ดังนั้นการพัฒนาไปสู่ IoT จึงมีความจำเป็นต้องพัฒนามาตรการและเทคนิคในการรักษาความปลอดภัยไอทีควบคู่กันไปด้วย

ในขนาดเดียวกันความปลอดภัยของ IoT ในปัจจุบันที่ต้องเผชิญกับความท้าทายที่มากขึ้นโดยมี

เหตุผลดังต่อไปนี้ 1) IoT ทำการขยายเครือข่ายอินเทอร์เน็ตไปยังเครือข่ายอื่น ๆ เช่น เครือข่ายมือถือ เครือข่ายการเซนเซอร์และเครือข่ายอื่น ๆ 2) สิ่งของทุกอย่างจะได้รับการเชื่อมต่อกับอินเทอร์เน็ต และ 3) สิ่งของเหล่านี้จะสามารถสื่อสารกับสิ่งอื่น ๆ ดังนั้นการรักษาความปลอดภัยและปัญหาความเป็นส่วนตัวที่จะเกิดขึ้น เราควรให้ความสำคัญกับปัญหาการวิจัยสำหรับการรักษาความลับ ความถูกต้องและความสมบูรณ์ของข้อมูลใน IoT ซึ่งในปัจจุบัน IoT นั้นได้รับความสนใจอย่างมากในการทำวิจัย ไม่ว่าจะเป็นในด้านการพัฒนาด้าน Application ด้าน Security เป็นต้นด้าน Security IoT ยังคงมีความเสี่ยงอยู่ซึ่งเป็นความท้าทายที่จะต้องรักษาความปลอดภัยจากผู้ไม่ประสงค์ดีทั้งหลายที่คอยดักจับหรือขโมยข้อมูลที่มีความสำคัญไปอยู่ตลอดเวลา โดยในบทความที่ได้ทำการทบทวนมาในเบื้องต้นนี้ได้มีการนำเสนอรูปแบบของการรักษาความปลอดภัยโดยการนำ Radio frequency identification (RFID) มาออกแบบการรักษาความปลอดภัยในมีประสิทธิภาพมากยิ่งขึ้นและได้มีการทบทวนงานวิจัยที่เกี่ยวกับ IoT ที่ผ่านมาว่าได้มีการพัฒนาไปในทางด้านไหนบ้าง

ในบทความนี้มีการอธิบายรายละเอียดในส่วนต่าง ๆ ดังต่อไปนี้ ส่วนที่ 2 จะกล่าวถึงการพัฒนา IoT ที่ผ่านมา ส่วนที่ 3 จะกล่าวถึงโครงสร้างระบบและความต้องการของการรักษาความปลอดภัยสำหรับ RFID ส่วนที่ 4 จะกล่าวถึงความช่องโหว่ที่มีผลต่อการรักษาความปลอดภัยสำหรับ IoT ส่วนที่ 5 เป็นการเอานำอัลกอริทึมการเข้ารหัสมาประยุกต์ใช้งาน ส่วนที่ 6 สรุปบทความที่ได้ทบทวนมา

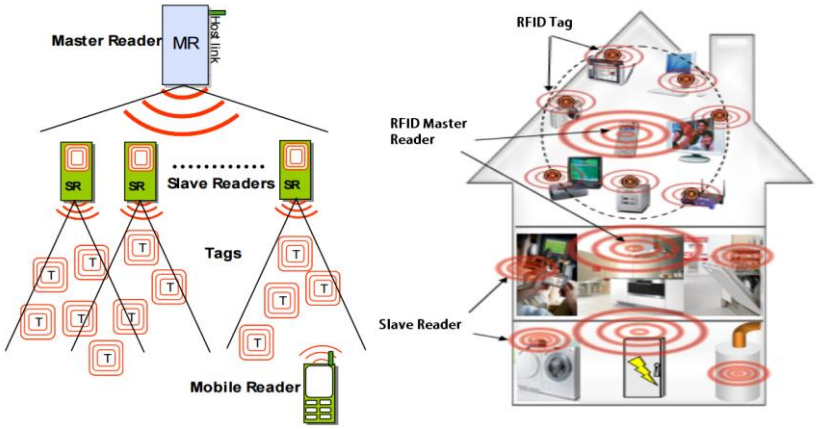
2. การพัฒนา IoT ที่ผ่านมา

ตลอดระยะเวลาที่ผ่านมาเทคโนโลยีเริ่มเข้ามามีบทบาทกับการใช้ชีวิตประจำวันมากขึ้นเรื่อย ๆ ไม่ว่าจะเป็นด้านที่อยู่อาศัย ด้านโลจิสติกส์ ด้านสุขภาพ ด้านการเกษตร เป็นต้น จึงเกิดการพัฒนา IoT กับสิ่งรอบข้างเพื่อให้ตอบสนองความสะดวกสบายของมนุษย์

2.1 ด้านที่อยู่อาศัย

ในปัจจุบันเริ่มมีการนำเอาเทคโนโลยี IoT เข้ามาใช้กับที่อยู่อาศัยเพื่ออำนวยความสะดวกสบายให้แก่ผู้พักอาศัยไม่ว่าจะเป็นการควบคุมอุปกรณ์ต่าง ๆ ภายในบ้าน หรือ เซนเซอร์ต่าง ๆ เช่น เซนเซอร์วัดอุณหภูมิ เซนเซอร์วัดแสง ที่ค่อยวัดอุณหภูมิและความสว่างภายในบ้าน (Moataz Soliman, et al., (2013)) โดยการจัดการผ่านทางเว็บไซต์ โดยใช้ Hypertext Transport Protocol (HTTP) และ Extensible Markup Language (XML) ในการส่งข้อมูล (Shushan Hu, et al., (2013)) และมีการนำเอาเทคโนโลยีการสื่อสารระบบ 3G เทคโนโลยี Zigbee เข้ามาประยุกต์ใช้ทำให้เกิดความสะดวกรวดเร็วในการติดต่อกับอุปกรณ์ภายในบ้าน นอกจากนี้ได้มีการจำลองสถานการณ์ในการติดต่อกันของ IoT ระหว่างบ้านหลาย ๆ หลังโดยนำเอาเทคโนโลยี WiFi และ LTE เข้ามาใช้ประยุกต์ใช้ (Yang Song, et al., (2012)) และยังมีการนำเอาเทคโนโลยี IoT มาใช้ร่วมกับเทคโนโลยี RFID (Mohsen Darianian, et al., (2008)) ดังแสดงในภาพที่ 1, NFC (Near Field Communication) และ UHF (Ultra High Frequency) มาใช้ร่วมกับการบริหารพลังงานไฟฟ้า

บริหารการจัดการน้ำ เพื่อช่วยให้ประหยัดค่าใช้จ่ายภายในบ้าน (Alberto M. C. Souza, et al., (2013)) ซึ่งจะเห็นได้ว่าในการพัฒนาด้านที่อยู่อาศัยนั้นจะเน้นไปทางความสะดวกสบายเป็นส่วนใหญ่ และยังไม่ค่อยสนใจด้านความปลอดภัยมากนัก

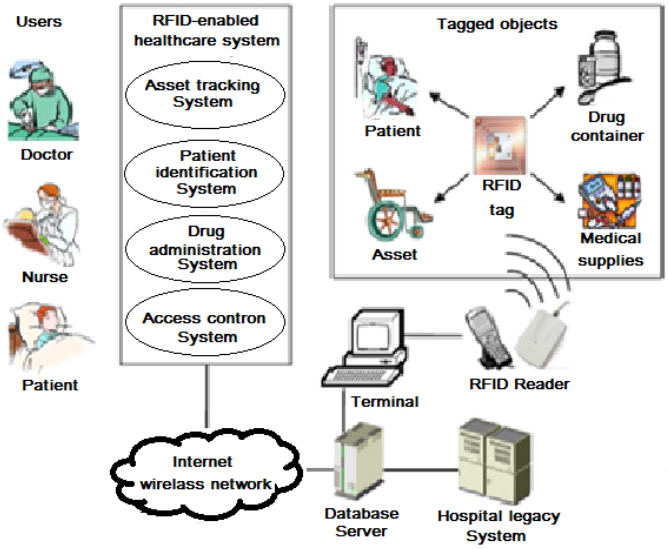


ภาพที่ 1 การนำเอา RFID มาประยุกต์ใช้กับ Internet of Things สำหรับสมาร์ทโฮม (Mohsen Darianian, et al., (2008))

2.2 ด้านสุขภาพ

ในด้านสุขภาพนี้ได้มีแนวคิดที่จะนำเอาเทคโนโลยีด้านการสื่อสารเข้ามาเชื่อมต่อกับอุปกรณ์ทางการแพทย์ โดยอุปกรณ์ทางการแพทย์จะติดเซนเซอร์และเทคโนโลยีการสื่อสารสำหรับการดูแลสุขภาพเพื่อที่จะใช้ติดตามผู้ป่วย ผู้พิการ และ ผู้สูงอายุ (Ning Yang, et al., (2012)) หากผู้ป่วยมีอาการผิดปกติอุปกรณ์ก็จะแจ้งเตือนแพทย์ผู้ที่ทำการดูแลผู้ป่วยทันที (Iuliana Chiuchisan, et al., (2014)) และข้อมูลที่ส่งมาจะถูกเก็บไว้ที่คลาวด์

ปัจจุบันได้มีการเอานำ Radio frequency identification (RFID) มาใช้กับ IoT ร่วมกับด้านสุขภาพทำให้ข้อมูลที่ได้รับจากผู้ป่วยมีความสามารถในการจัดเก็บข้อมูลที่สำคัญในการสื่อสารไร้สายกับวัตถุอื่น ๆ และยังสามารถระบุ และติดตามวัตถุได้อย่างอัตโนมัติ โดยในปัจจุบันได้มีการนำเอาเทคโนโลยี RFID มาใช้ร่วมกับ IoT ในทางการแพทย์เพื่อการติดตามผู้ป่วย การติดตามการรักษา (Debiao He, et al., (2015)) ดังแสดงในภาพที่ 2



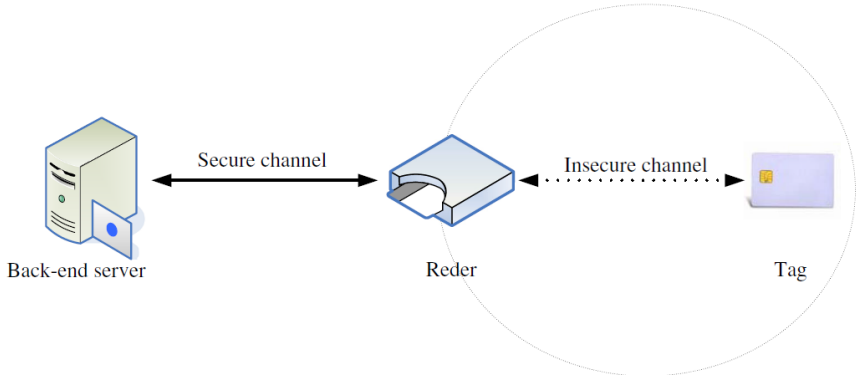
ภาพที่ 2 โครงสร้างของ RFID สำหรับระบบดูแลสุขภาพ (Debiao He, et al., (2015))

ในการพัฒนาความปลอดภัยให้กับ RFID จำเป็นต้องศึกษาหลักการทำงานหรือโครงสร้างของ RFID เพื่อทำการออกแบบโปรโตคอลที่จะใช้ในการรักษาความปลอดภัยที่จะนำมาใช้กับ IoT

3. โครงสร้างระบบและความต้องการของการรักษาความปลอดภัยสำหรับ RFID

3.1 โครงสร้างระบบ

โครงสร้างของระบบ RFID จะประกอบไปด้วย RFID tag, RFID reader และ Server ในโครงสร้างนี้จะแบ่งหน้าที่ที่แตกต่างกันไปและในแต่ละส่วนต้องการรักษาข้อมูลให้เป็นความลับระหว่างช่องทางการสื่อสาร ดังแสดงในภาพที่ 3



ภาพที่ 3 รูปแบบการตรวจสอบ RFID (Ning Yang, et al., (2012))

3.2 ความต้องการของการรักษาความปลอดภัยสำหรับ RFID (Security Requirements for RFID) (Debiao He, et al., (2015))

3.2.1 การตรวจสอบซึ่งกันและกัน (Mutual authentication) เป็นการตรวจสอบช่องทางการสื่อสารระหว่าง RFID reader และ Server เพื่อเช็คว่าอุปกรณ์ที่ติดต่อกันอยู่นั้นเป็นตัวจริงหรือไม่

3.2.2 การรักษาความลับ (Confidentiality) เป็นการรักษาข้อมูลให้เป็นความลับเพื่อไม่ให้ถูกเปิดเผย และกำหนดสิทธิการเข้าถึงข้อมูล เช่น การเก็บข้อมูลความลับไว้ใน RFID tag ซึ่งเป็นการรักษาความลับในการนำไปใช้งาน

3.2.3 การไม่เปิดเผยตัวตน (Anonymity) เป็นการปกปิดการตรวจสอบ RFID เพื่อไม่ให้ผู้ไม่ประสงค์ดีทำการตรวจสอบหรือดักจับข้อมูลได้ง่าย ๆ หรือไม่ก็ใช้เวลานานในการตรวจสอบ

3.2.4 ความพร้อมในการทำงาน (Availability) เป็นการรักษาความพร้อมในการใช้งานของข้อมูลของ RFID เพื่อไม่ให้เป็นการเปิดเผยตัวตนของ RFID tag และ server โดยจะทำการปรับปรุงข้อมูลให้เป็นความลับ

3.2.5 การรักษาความปลอดภัยในอนาคต (Forward security) เป็นการรักษาข้อมูลโดยข้อมูลที่ถูกเข้ารหัสโดยการสร้าง key pair สำหรับเข้า/ถอดรหัสใหม่ทุกครั้งที่มีการเชื่อมต่อโดยไม่อิงกับ private key เดิมและเมื่อการเชื่อมต่อนั้นสิ้นสุดลง key ก็จะไม่สามารถใช้งานได้ ทำให้แม้ว่า private key จะหลุดมาในอนาคต ก็ไม่สามารถนำมาใช้ถอดรหัสข้อมูลที่ถูกดักและเก็บเอาไว้ได้

3.2.6 การปรับขยาย (Scalability) เป็นการปรับขยายหรือลดโครงสร้างเพื่อความยืดหยุ่นตามการใช้งานที่สามารถเข้าถึงแพลตฟอร์มที่หลากหลายในการตรวจสอบ RFID tag และ Sever

3.2.7 ความต้านทานต่อการโจมตี (Attack resistance) เป็นการรับรองว่าสามารถป้องกันการโจมตีรูปแบบต่าง ๆ ได้ เพื่อเพิ่มความปลอดภัยให้กับระบบ RFID

โดยการพัฒนาของเทคโนโลยี IoT ที่ผ่านมานั้นยังคงมีช่องโหว่ที่อาจก่อให้เกิดอันตรายต่อข้อมูลและอุปกรณ์ต่างๆที่เกี่ยวข้องกับ IoT ได้

4. ช่องโหว่ที่มีผลต่อการรักษาความปลอดภัยสำหรับ IoT (OWASP**, (2014))**

ในปัจจุบันอุปกรณ์ที่ใช้ในชีวิตประจำวันสามารถเชื่อมต่ออินเตอร์เน็ตเพื่อรับส่งข้อมูลหากันได้ ไม่ว่าจะเป็นโทรศัพท์มือถือ รถยนต์ ตู้เย็น ทีวี และอื่นๆ จึงเกิดเป็นคอนเซ็ปต์ของ IoT ขึ้น และอุปกรณ์พวกนี้ยังมีปัจจัยที่ทำให้เกิดช่องโหว่อยู่ซึ่งสามารถสรุปออกมาได้ดังต่อไปนี้

เว็บอินเทอร์เฟสที่นำมาใช้งานกับ IoT ยังไม่ค่อยมีความปลอดภัยเพียงพอเนื่องจากการพิสูจน์ตัวตนและการกำหนดสิทธิ์ที่ยังไม่ได้ทำการเข้ารหัสข้อมูลให้ซับซ้อนมากขึ้นจึงทำให้ผู้ไม่ประสงค์ดีสามารถเดารหัสผ่านและใช้กลไกของ Password Recovery หรือระบบ Access Control ในการเจาะเข้าสู่ระบบ ส่งผลให้ข้อมูลอาจถูกขโมย และนอกจากนี้ยังมีความเสี่ยงทางด้านบริการด้านเครือข่ายที่จะถูกหาช่องโหว่ที่สามารถโจมตีอุปกรณ์ต่างๆของ IoT ได้อีกด้วย จากที่กล่าวมาในข้างต้นนี้ยังส่งผลกระทบไปในด้านอื่น ๆ อีกด้วย ไม่ว่าจะเป็น ด้านความเป็นส่วนบุคคล คลาวด์อินเตอร์เฟสที่

ไม่ปลอดภัย โมบายล์อินเตอร์เฟสที่ไม่ปลอดภัย ซึ่งที่กล่าวมานี้ถ้าไม่มีการรักษาความปลอดภัยที่ดีจะทำให้ผู้ไม่ประสงค์ดีทำการโจมตีเพื่อที่จะขโมยข้อมูลได้ นอกจากนี้ยังต้องให้ความสำคัญกับอุปกรณ์ด้วย ไม่ว่าจะเป็นทางด้าน การตั้งค่าความปลอดภัยให้กับอุปกรณ์โดยมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลและการควบคุมอุปกรณ์ การอัพเดตซอฟต์แวร์และเฟิร์มแวร์ ที่จะได้การอัพเดตให้กับอุปกรณ์ควรมีการป้องกันเพื่อไม่ให้ผู้ไม่ประสงค์ดีสามารถตรวจสอบเพื่อโจมตีได้ และต้องเพิ่มความปลอดภัยให้กับพวกอุปกรณ์เสริมต่าง ๆ ไม่ว่าจะเป็น USB, SD Card หรืออุปกรณ์เก็บข้อมูลประเภทอื่น ๆ ซึ่งอาจถูกใช้เป็นช่องทางในการเข้าถึงข้อมูลที่ถูกเก็บไว้ในอุปกรณ์ได้

โดยทั้งหมดที่กล่าวมานี้เป็นช่องโหว่ทางด้านความปลอดภัยของ IoT ที่จะมีความท้าทายขึ้นไปเรื่อย ๆ ไม่ว่าจะเป็นโครงสร้างของเครือข่ายที่เกี่ยวข้องกับ IoT ยังคงเป็นสิ่งที่ท้าทายในการรักษาความปลอดภัย นอกจากนี้ได้มีการนำเอาอัลกอริทึมการเข้ารหัสเข้ามามีส่วนในการรักษาความปลอดภัยให้กับข้อมูลสำหรับ IoT อีกด้วย

5. อัลกอริทึมการเข้ารหัส

รูปแบบการเข้ารหัสขณะนี้เป็นที่รู้จักกันดีและมีความน่าเชื่อถืออย่างมากในวิธีการเข้ารหัสลับที่นำไปใช้กับโปรโตคอลรักษาความปลอดภัยบนอินเทอร์เน็ตเพื่อช่วยในการยืนยันตัวตนไม่ว่าจะเป็นอัลกอริทึม Advanced encryption standard (AES) อัลกอริทึม Rivest Shamir adelman (RSA) อัลกอริทึม Elliptic Curve Cryptography (ECC) แต่ในการนำเอาอัลกอริทึมมาใช้กับอาร์เอฟไอดีร่วมกับ IoT ผู้วิจัยจะนิยมนำเอา อัลกอริทึม ECC เข้ามาประยุกต์ใช้เพราะมีคุณสมบัติที่เหมาะสมมากว่าอัลกอริทึมรูปแบบอื่นๆ

5.1 Elliptic Curve Cryptography (ECC)

ECC (ภูกิจ บุรีภักดี และคณะ (2012)) เป็นอัลกอริทึมที่ใช้ในการเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography) ได้รับการนำเสนอโดย Neal Koblitz และ Victor S. Miller ในปี 1985โดยอัลกอริทึมการเข้ารหัส ECC นี้ได้รับการพัฒนาจากสมการของเส้นโค้งของวงรี $y^2 = x^3 + ax + b$

ECC มีข้อดีที่เหนือกว่า RSA คือจะใช้ Key ที่สั้นกว่า (ECC 164 bit = RSA 1024 bit) แต่สามารถให้ความปลอดภัยเท่ากับ RSAถ้าใช้ Key มีความยาวเท่ากัน ECC จะมีความปลอดภัยสูงกว่านั่นคือหากต้องการโจมตีแบบ Brute-Force จะใช้เวลามากกว่า RSA เนื่องจาก ECC ใช้ Key ที่มีขนาดเล็กกว่า RSA มากและมีความสามารถในการคำนวณที่รวดเร็วใช้พลังงานต่ำและใช้หน่วยความจำน้อยดังนั้น ECC จึงเหมาะสำหรับการใช้งานในอุปกรณ์เคลื่อนที่ขนาดเล็ก เช่น โทรศัพท์มือถือ คอมพิวเตอร์ และ PDA เป็นต้น สำหรับการเอานำการเข้ารหัสแบบ ECC มาประยุกต์ใช้นั้นได้มีการนำเอาไปพัฒนาเป็นโปรโตคอลที่ใช้กับ RFID (Zhenguo Zhao, (2015)) โดยเป็นการพัฒนาออกมาเป็นต้นแบบและสามารถนำเอาไปประยุกต์ใช้กับระบบต่าง ๆ ที่มีการนำ RFID

เข้ามาใช้งานได้

นอกจากนี้ได้มีการนำเอาการเข้ารหัสแบบ ECC มาออกแบบประยุกต์ใช้กับการรักษาความปลอดภัยให้กับ RFID และได้มีการประเมินเปรียบเทียบผลในแง่ของความต้องการความปลอดภัยของ RFID (Debiao He, et al., (2015)) ทั้งหมด เพื่อเปรียบเทียบประสิทธิภาพของแต่ละอัลกอริทึมที่สามารถนำมาประยุกต์ใช้งานกับอุปกรณ์ IoT ได้ โดยดูจากการเปรียบเทียบ Security Requirements 1-7 (SR 1-7) ดังแสดงในตารางที่ 1 และเปรียบเทียบ Computation costs ที่ได้สรุปไว้เพื่อนำเสนอว่ารูปแบบโปรโตคอลแบบไหนที่สามารถพิจารณาเพื่อหาความเหมาะสมสำหรับการนำไปใช้งานได้จริงกับการประยุกต์ใช้กับ RFID โดยพิจารณาจาก Comparison of Computational Cost ดังแสดงในตารางที่ 2

ตารางที่ 1 Comparison of Security Requirements (Debiao He, et al., (2015))

Scheme	SR1	SR2	SR3	SR4	SR5	SR6	SR7
Lee et al.'s scheme	No	Yes	Yes	Yes	No	Yes	No
Bringer et al.'s scheme	No	Yes	Yes	Yes	No	Yes	No
Lee et al.'s tag identity transfer scheme	No	Yes	Yes	Yes	No	Yes	No
Lee et al.'s tag password transfer scheme	No	Yes	Yes	Yes	No	Yes	No
Lee et al.'s server transfer scheme	No	Yes	Yes	No	No	Yes	No
Sandhya et al.'s scheme	Yes	Yes	Yes	Yes	No	Yes	No
Martinez et al.'s scheme	Yes	Yes	Yes	Yes	No	Yes	Yes
Zhang et al.'s Improved EC-RAC scheme	Yes	Yes	Yes	Yes	Yes	Yes	No
Zhang et al.'s Improved Schnorr scheme	No	Yes	Yes	Yes	Yes	Yes	No
Godor and Imre's scheme	No	Yes	Yes	Yes	Yes	Yes	Yes
Chen et al.'s scheme	No	Yes	Yes	Yes	Yes	Yes	No
Bringer et al.'s scheme	No	Yes	Yes	Yes	Yes	Yes	No
Liu et al.'s scheme	Yes	Yes	No	Yes	Yes	Yes	No
Wang et al.'s scheme	No	Yes	Yes	Yes	Yes	No	No
Liao et al.'s scheme	No	Yes	Yes	Yes	Yes	Yes	No
Chou's scheme	No	Yes	Yes	Yes	Yes	Yes	No
Zhao's scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zhang and Qi's scheme	Y es	Yes	Yes	Yes	Yes	Yes	Yes
Farash's scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes

จากตารางที่ 1 แสดงการวิเคราะห์ความต้องการของการรักษาความปลอดภัยสำหรับ RFID แสดงให้เห็นว่าจากการนำเสนอรูปแบบโปรโตคอลที่ผ่านมาพบว่ารูปแบบโปรโตคอลส่วนใหญ่ที่นำมาใช้กับการตรวจสอบ RFID โดยใช้การเข้ารหัสแบบ ECC นั้น ไม่สามารถตอบสนองทุกความต้องการของการรักษาความปลอดภัย โดยเฉพาะอย่างยิ่งการตรวจสอบซึ่งกันและกัน (SR1 Mutual authentication) รองลงมาก็จะเป็นการต้านทานการโจมตี (SR7 Attack resistance) ซึ่งในส่วนนี้มีความสำคัญมากในการที่จะรักษาความลับของข้อมูล โดยดูจากการเปรียบเทียบรูปแบบโปรโตคอลที่ได้นำเสนอไว้ก่อนหน้านี้ ยกเว้นรูปแบบโปรโตคอลของ Zhao, Zhang และ Farash ที่สามารถตอบสนองความต้องการของการรักษาความปลอดภัยสำหรับ RFID ได้ทั้ง 7 ความต้องการ

ตารางที่ 2 Comparison of Computational Cost (Debiao He, et al., (2015))

scheme	Server side computational cost	Tag side computational cost	Total computational cost
Farash's scheme	1Tmul+ 2Tinv + 2Tecm + 2Th = 2408Tmul	3Tmul+ 2Tecm + 2Th = 2404Tmul	4Tmul+ 2Tinv + 4Tecm + 4Th = 4812Tmul
Zhang and Qi's scheme	1Teca + 2Tecm + 2Th = 2406Tmul	1Teca + 2Tecm + 2Th = 2406Tmul	2Teca + 4Tecm + 4Th = 4816Tmul
Zhao's scheme	2Tmul + 3Teca + 5Tecm = 6017Tmul	2Tmul + 3Teca + 5Tecm = 6017Tmul	4Tmul + 6Teca + 10Tecm = 12034Tmul

จากตารางที่ 2 แสดงการพิจารณา COMPUTATIONAL COST โดยนำค่าที่ได้จาก Tmu Tinv Tecm และ Th มาคำนวนหาค่าเวลาการทำงานของอัลกอริทึม เพื่อพิจารณาหาความเหมาะสมสำหรับการนำไปใช้งานได้จริงโดยเรียงลำดับจากน้อยไปยังมากตามลำดับ โดยพิจารณาจากรูปแบบโปรโตคอลที่มีคุณสมบัติของความต้องการของการรักษาความปลอดภัยสำหรับ RFID ที่ครบทั้ง 7 เพื่อพิจารณาในการนำไปประยุกต์ใช้กับ RFID และ IoT ต่อไป

โดยปกติแล้วขั้นตอนวิธีการเข้ารหัสแบบสมมาตรจะใช้ในการเข้ารหัสข้อมูลสำหรับการรักษาความลับ ซึ่งเป็นมาตรฐานการเข้ารหัสแบบ AES อัลกอริทึมสมมาตรและมักจะใช้ในรูปแบบของลายเซ็นดิจิตอล ส่วนอัลกอริทึมที่มักจะใช้บ่อยคือ RSA ดังนั้นขั้นตอนวิธีการเข้ารหัสที่ได้กล่าวมานี้ความเร็วในการประมวลผล และหน่วยความจำมีส่วนในการเข้ารหัส ส่วน ECC ก็มีคุณสมบัติที่เหมือนกับ RSA แต่ที่เหนือกว่า RSA คือสามารถนำมาประยุกต์ใช้กับอุปกรณ์พกพาได้ดังนั้นวิธีการการเข้ารหัสที่ได้กล่าวมานี้ที่จะนำไปประยุกต์ใช้กับ IoT ยังไม่มีความชัดเจนมากนัก และจะต้องมีการ

ทำวิจัยต่อไปเพื่อให้แน่ใจว่ามีวิธีการที่ทำให้ประสบความสำเร็จในการใช้ข้อจำกัดของหน่วยความจำและประมวลผลความเร็วต่ำใน IoT นอกจากนี้ยังต้องศึกษาโครงสร้างระบบและความต้องการของการรักษาความปลอดภัยสำหรับ RFID ว่ามีผลต่อการพัฒนาร่วมกับ IoT หรือไม่

6. สรุป

การตรวจสอบ RFID เป็นหนึ่งที่ใช้ในการรักษาความปลอดภัยที่สำคัญสำหรับ IoT โดยการนำ RFID มาใช้กับการระบุตัวตนเพื่อเพิ่มความปลอดภัยให้กับ IoT มากยิ่งขึ้น จากการทบทวนวรรณกรรมที่ผ่านมาได้พบว่ามีการพัฒนา IoT จำนวนมากแต่ก็ยังขาดการวิจัยในด้านรักษาความปลอดภัยอย่างจริงจัง แต่ก็ยังมีแนวคิดที่จะพัฒนาการรักษาความปลอดภัยให้กับ IoT และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับ IoT โดยได้มีการนำอัลกอริทึมในการเข้ารหัสรักษาความลับแบบต่าง ๆ มาทดสอบเพื่อหาความเหมาะสมที่จะนำมาในประยุกต์ใช้กับการรักษาความปลอดภัยให้กับ RFID ที่จะนำมาใช้กับ IoT โดยจากการทบทวนวรรณกรรมที่ผ่านมาพบว่ามีการนำเอาอัลกอริทึมการเข้ารหัสแบบ ECC มาประยุกต์ใช้กับ RFID ค่อนข้างมาก และยังพบว่ามี 3 อัลกอริทึมที่สามารถนำเอามาประยุกต์ใช้กับ IoT ได้ ได้แก่ Zhao's scheme Zhang and Qi's scheme และ Farash's scheme ส่วน Farash's scheme มีความเหมาะสมที่จะนำไปประยุกต์ใช้มากที่สุด เพราะ Comparison of Computational Cost น้อยที่สุด

เอกสารอ้างอิง

ภูกิจ บุรีภักดี และ ปราโมทย์ กั่วเจริญ. (2012). **การเพิ่มความปลอดภัยและประสิทธิภาพในการรับส่งข้อความ SMS Security and Efficiency in SMS Messaging.** ค้นเมื่อ 15 มิถุนายน 2559, จาก http://as.nida.ac.th/~pramote/publications/security_and_efficiency_in_sms_messaging-nccit2012.pdf

Amir Mohammad Rahmani. (2015). **Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems.** Annual IEEE Consumer Communications and Networking Conference.

Alberto M. C. Souza and Jose R. A. Amazonas. (2013). **A Novel Smart Home Application Using an Internet of Things Middleware**. Smart Objects, Systems and Technologies (Smart Sys Tech), Proceedings of European Conference.

Debiao He and Sherali Zeadally. (2015). **An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography.** IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, FEBRUARY.

Iuliana Chiuchisan, Hariton-Nicolae Costin and Oana Geman. (2014). **Adopting the Internet of Things technologies in health care systems**. Electrical and Power Engineering (EPE).

Mohsen Darianian, and Martin Peter Michael. (2008). **Smart Home Mobile RFID based Internet of Things Systems and Services.** International Conference on Advanced Computer Theory and Engineering.

Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou and Chung Horng Lung. (2013). **Smart Home: Integrating Internet of Things with Web Services and Cloud Computing**. Cloud Computing Technology and Science (Cloud Com), IEEE 5th International Conference. pp 317-320.

Ning Yang, Xingli Zhao and Z. Hong. (2012). **A non-contact health monitoring model based on the Internet of things**," Natural Computation (ICNC), Eighth International Conference, pp 502 -510.

OWASP. (2014). **10 อันดับภัยคุกคามบน Internet of Things ประจำปี 2014**. ค้นเมื่อ 15 มิถุนายน 2016, จาก https://www.techtalkthai.com/top-10-owasp-internet-of-things-2014/

Partha P. Ray. (2014) **Home Health Hub Internet of Things (H3IoT): An Architectural Framework for Monitoring Health of Elderly People.** International Conference on Science, Engineering and Management Research

Suwimon Vongsingthong and Sucha Smanchat (2014). **Internet of Things: A review of Applications and Technologies.**

Shushan Hu, Cunchen Tang, Riji Yu, Feng Liu and Xiaojun Wang. (2013). **Connected intelligent home based on the Internet of Things**. Information and Communications Technologies, Beijing, China.

Yang Song, Bingjun Han, Xin Zhang, and Dacheng Yang. (2012**). Modeling and simulation of smart home scenarios based on Internet of Things**. Network Infrastructure and Digital Content (IC-NIDC), IEEE International, pp 596 – 600.

Zhenguo Zhao. (2015). **A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem**. Springer Science Business Media New York.