สัญญาเลขที่ R2560B080

รายงานวิจัยฉบับสมบูรณ์

โครงการวิจัยเรื่อง โปรโตคอลที่มีความปลอดภัยสำหรับการใช้ข้อมูลลายนิ้วมือในการพิสูจน์ตัวบุคคล

คณะผู้วิจัย

ดร.อนงค์พร ไศลวรากุล

สังกัดภาควิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร

สนับสนุนโดย

งบประมาณแผ่นดิน มหาวิทยาลัยนเรศวร

ปีงบประมาณ 2560

โครงการวิจัยเรื่อง โปรโตคอลที่มีความปลอดภัยสำหรับการใช้ข้อมูลลายนิ้วมือ

ในการพิสูจน์ตัวบุคคล

สารบัญ

บทสรุปผู้บริหาร

โครงการวิจัยนี้มุ่งเน้นเพื่อทำการวิเคราะห์ลักษณะของโหวทางด้านความปลอดภัยของการใช้ข้อมูลชีวภาพเพื่อการพิสูจน์ตัวบุคคลเพื่อให้ข้อมูลชีวภาพของผู้ใช้มีความปลอดภัยไม่ถูกขโมย หรือถูกดักจับเพื่อนำไปใช้งานโดยไม่เต็มใจ โดยที่ในงานวิจัยนี้จะทำการวิเคราะห์ความเป็นไปได้ของปัญหาด้านความปลอดภัยของการนำเอาข้อมูลชีวภาพมาใช้งาน และสร้างการจู่โจมที่เป็นไปได้ในระหว่างการนำเอาข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคล ซึ่งอาจเกิดได้ตั้งแต่การจัดเก็บข้อมูลชีวภาพสู่ระบบ หรือแม้กระทั่งขั้นตอนการเปรียบเทียบข้อมูลชีวภาพของผู้ใช้ในขณะที่แสดงตัวกับระบบเทียบกับข้อมูลชีวภาพที่จัดเก็บไว้ ซึ่งคณะผู้วิจัยจะทำการออกแบบโปรโตคอลในการใช้งานข้อมูลชีวภาพในการพิสูจน์ตัวบุคคล แล้วให้การจู่โจมแบบต่างๆ ทำงาน โดยการจำลองจากโปรแกรมจำลองการจู่โจม ซึ่งจะทำการวิเคราะห์ผู้จู่โจมในรูปแบบของ Dolev-Yao Style attacker โดยที่เมื่อทำการทดสอบการทำงานของโปรโตคอลต่อการจู่โจมต่างๆ แล้ว จะได้โครงสร้างโปรโตคอลที่มีความปลอดภัยในนำข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคล ทั้งนี้โครงการวิจัยนี้มีวัตถุประสงค์คือ

1. เพื่อพัฒนาโปรโตคอลที่ปลอดภัยในการนำข้อมูลลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคล
2. เพื่อให้ข้อมูลลายนิ้วมือของผู้ใช้มีความปลอดภัย
3. เพื่อพัฒนาโปรโตคอลนำร่องในการใช้งานข้อมูลลายนิ้วมือเพื่อพิสูจน์ตัวบุคคลอย่างปลอดภัย

ทั้งนี้งานวิจัยนี้มุ่งหวังประโยชน์ที่ได้รับคือ

1. ได้โปรโตรคอลที่มีความปลอดภัยในการนำข้อมูลลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคล
2. ได้องค์ความรู้ในการเผยแพร่การนำเอาข้อมูลลายนิ้วมือมาใช้อย่างปลอดภัย

โดยที่กระบวนการในการดำเนินการวิจัยโดยสังเขปมีดังนี้

1. ทบทวรรณวรรณกรรม
2. วิเคราะห์ของโหวของการนำเอาข้อมูลชีวภาพมาใช้
3. วิเคราะห์แนวทางในการนำเสนอ และการใช้ข้อมูลชีวภาพอย่างปลอดภัย
4. สร้างโปรโตคอลที่มีความปลอดภัย
5. จำลองผู้จู่โจม (attacker) ที่มีต่อโปรโตคอล

หลังจากกำหนดรายละเอียดคุณสมบัติด้านความปลอดภัย และทำการสร้างโครงสร้างของโปรโตคอลเรียบร้อยแล้ว ได้ทำการวิเคราะห์ความปลอดภัยของโปรโตคอล พบว่าโปรโตคอลสามารถเก็บข้อมูลชีวภาพของผู้ใช้ไว้เป็นความลับสร้าง และ ผู้จู่โจมไม่สามารถนำผลลัพธ์ของการจับคู่มาใช้เสมือนเป็นข้อมูลของตนได้

บทคัดย่อ

งานวิจัยฉบับนี้นำเสนอรายละเอียดและโครงสร้างของการทำการพิสูจน์ตัวบุคคลโดยการใช้ลายนิ้วมือในสถานการณ์ที่ไม่มีการควบคุม ซึ่งรายละเอียดของคุณสมบัติด้านความปลอดภัยของโปรโตคอลจะรับประกันได้ว่าข้อมูลลายนิ้วมือของผู้ใช้มาจากบุคคลจริง และความต้องการในการพิสูจน์ตัวบุคคลของผู้ใช้ไม่ถูกเปลี่ยนแปลง

โครงสร้างที่สอดคล้องกับรายละเอียดด้านความปลอดภัยของโปรโตคอลจะถูกนำเสนอในงานวิจัยฉบับนี้ ดังนั้นเครื่องอ่านลายนิ้วมือที่ถูกใช้ในโปรโตคอลที่มีความสามารถในการตรวจจับความมีชีวิตของข้อมูลลายนิ้วมือจะถูกนำมาใช้ นอกเหนือจากนี้การเข้ารหัส และ ค่า nonce จะถูกใช้ในโครงสร้างโปรโตคอลนี้ด้วย

เพื่อให้การรับรองว่าคุณสมบัติด้านความปลอดภัยที่โปรโตคลอรับรองจะให้บริการแก่ผู้ใช้ถูกต้อง จึงความจำเป็นข้อมูลในการวิเคราะห์คุณสมบัติด้านความปลอดภัยโดยการสร้างโมเดล ProVeif ขึ้นมาและทำการวิเคราะห์ โปรโตคอลที่ได้นำเสนอในงานวิจัยฉบับนี้รับรองได้ว่าข้อมูลชีวภาพของผู้ใช้มีความปลอดภัย และความต้องการในการพิสูจน์ตัวบุคคลของผู้ใช้ได้ยังคงถูกต้องไม่มีการเปลี่ยนแปลง

Abstract

This research proposes authentication specifications and a framework for the fingerprint authentication in the circumstance that the presentation of the user's biometric information is not supervised. The specifications of the security properties are to certify that the liveness of the user's fingerprint information is confirmed and that the intention of the user's authentication is not manipulative or illegal. The framework for compliance with the specification of the fingerprint authentication protocol is proposed. Liveness detection by the fingerprint reader is considered to be essential in these situations. Cryptography and the fresh random number, nonce, are included in the framework. Analysis of the authentication framework shows that the proposed security properties are confirmed, the user's biometric data is secured and the user's intention of authentication is preserved.

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหาที่ทำการวิจัย

เมื่อกล่าวถึงการรักษาความปลอดภัยในการเข้าใช้ระบบ ไม่ว่าจะเป็นการเข้าใช้บริการ หรือการเข้าใช้คอมพิวเตอร์ หรือเข้าใช้ระบบนั้น การรักษาความปลอดภัยแบบพื้นฐานที่ได้รับความนิยม เนื่องจากง่าย และสะดวกในการประยุกต์คือการนำรหัสผ่านเข้ามาใช้ในการพิสูจน์ตัวบุคคล ซึ่งอยู่บนพื้นฐานสมมุติฐานว่าถ้าผู้ใช้นั้นสามารถระบุตัวตน (user name) และรหัสผ่าน (password) ได้ถูกต้องถือได้ว่าเป็นบุคคลตามที่ได้กล่าวอ้างจริง

แต่ในความเป็นจริงแล้วในการพิสูจน์ตัวบุคคลนั้นสามารถทำได้หลายอย่าง เช่นการใช้สิ่งที่ผู้ใช้รู้ ยกตัวอย่างเช่น รหัสผ่าน หรือสิ่งที่ผู้ใช้มี เช่นบัตร (ในกรณีของบัตรเอทีเอ็ม) หรือสิ่งที่เป็นใช้เป็น เช่นข้อมูลชีวภาพ

เมื่อพูดถึงข้อมูลชีวภาพนั้นนอกจากจะหมายถึงข้อมูลชีวภาพของบุคคล เช่น ลายนิ้วมือ ม่านตา แล้วยังสามารถแปลความรวมได้ถึงพฤติกรรมของผู้ใช้ เช่นการเดิน การพิมพ์บนคีย์บอร์ดได้อีกด้วย ซึ่งเหล่านี้ถือเป็นข้อมูลเฉพาะบุคคล

ดังนั้นการนำข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคลนั้นจะสามารถทำให้เชื่อมั่นได้ว่าผู้ที่กล่าวอ้างเป็นตัวจริง ซึ่งในปัจจุบันการนำเอาข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคลมีบทบาทมากขึ้น เช่นในขั้นตอนการตรวจสอบตัวบุคคลเข้าออกเมือง (immigration border) ซึ่งมีการระบบการอ่านลายนิ้วมือเข้ามาช่วยเพื่อเพิ่มความสะดวก และถูกต้องในการตรวจสอบตัวบุคคล หรือแม้กระทั่งการนำมาใช้ในการเข้าใช้โทรศัพท์ซึ่งมีโทรศัพท์บางยี่ห้อที่นำเอาเทคโนโลยีเข้ามาใช้เพื่อให้ผู้ใช้สามารถเข้าใช้โทรศัพท์ได้เมื่อเป็นเจ้าของเท่านั้น

อย่างไรก็ตามถึงแม้ว่าจะเริ่มมีการนำเทคโนโลยีข้อมูลชีวภาพเข้ามาใช้ในการพิสูจน์ตัวบุคคลเพิ่มมากขึ้น อันเนื่องจากความสามารถในการระบุได้ว่าเป็นบุคคลที่กล่าวอ้างจริง แต่ว่าข้อมูลชีวภาพนั้นยังมีข้อความระมัดระวังในการนำมาใช้ยกตัวอย่างเช่น ข้อมูลชีวภาพเป็นข้อมูลที่ไม่สามารถสร้างขึ้นมาใหม่เพื่อทดแทนได้ถ้าถูกขโมย ซึ่งถ้าเปรียบเทียบกับการใช้รหัสผ่าน ถ้ารหัสผ่านนั้นถูกขโมย หรือยกให้ด้วยความสมัครใจ รหัสผ่านนั้นสามารถเปลี่ยนแปลงหรือยกเลิกได้ในภายหลังทำให้รหัสผ่านนั้นไม่สามารถใช้ได้อีกต่อไป แต่ในกรณีของข้อมูลชีวภาพนั้นถ้าข้อมูลที่นำไปใช้ในระบบถูกขโมยไป จะไม่สามารถสร้างขึ้นมาใหม่ได้อีก ยกตัวอย่างเช่น ไม่สามารถสร้างนิ้วมือใหม่ได้ถ้าลายนิ้วมือนั้นถูกขโมยไป

ทั้งนี้การใช้ข้อมูลชีวภาพเพื่อพิสูจน์ตัวบุคคลนั้นทำได้ดีในระบบปิด หรือระบบที่มีผู้ควบคุมดูแล อันเนื่องจากสามารถตรวจสอบระหว่างการพิสูจน์ตัวบุคคลได้ว่าบุคคลนั้นได้แสดงข้อมูลชีวภาพของตนเองจริงไม่ได้นำข้อมูลชีวภาพที่ถูกขโมยมาแสดงต่อระบบเพื่อกล่าวอ้างว่าเป็นบุคคลนั้นๆ ทั้งนี้เนื่องจากมีหลายงานวิจัยที่ได้นำเสนอการสร้างลายนิ้วมือปลอม หรือนิ้วมือยาง [1] เพื่อนำไปใช้ในการเข้าใช้ระบบ และสามารถเข้าใช้ระบบได้สำเร็จ

แนวโน้มการนำเอาข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคลมีเพิ่มมากขึ้น ไม่ว่าจะเป็นสำหรับอุปกรณ์ส่วนบุคคล เช่นการเข้าใช้โทรศัพท์มือถือบางยี่ห้อที่มีการนำเอาการพิสูจน์ตัวบุคคลโดยการใช้ลายนิ้วมือ หรือไปถึงระดับองค์กร เช่น การตรวจสอบการเวลาการเข้าทำงานโดยการแสกนลายนิ้วมือแทนที่จะเป็นการใช้การตอกบัตรแบบเก่า หรือไปจนถึงองค์กรขนาดใหญ่เช่นการตรวจสอบตัวบุคคลที่จุดตรวจคนเข้าเมือง ซึ่งจะเห็นได้ว่าการนำเอาข้อมูลชีวภาพามาใช้ในการตัวสอบตัวบุคคลได้ขยายไปอย่างรวดเร็วเนื่องจากสามารถพิสูจน์ตัวบุคคลได้อย่างแท้จริง โดยไม่สามารถกล่าวอ้างแทนกันได้

แต่อย่างไรก็ตาม ความคำนึงถึงการรักษาความปลอดภัยในการนำเอาข้อมูลชีวภาพมาใช้นั้นยังอยู่ในระดับที่ควรต้องมีการระมัดระวังอันเนื่องจากไม่สามารถสร้างทดแทนใหม่ได้ตามเหตุผลที่ได้กล่าวไปข้างต้น และมีความเป็นเป็นได้เป็นอย่างสูงในการขโมยหรือดักจับข้อมูลชีวภาพ ในที่นี้จะเน้นไปที่ลายนิ้วมือของผู้ใช้จะถูกขโมยไปได้โดยง่าย เช่นการที่ผู้ใช้ไปใช้งานคอมพิวเตอร์สาธารณะ เช่นอินเตอร์เน็ตคาเฟ่ หรือคอมพิวเตอร์ในสนามบิน หรือแม้แต่การจับแก้วน้ำหรือสัมผัสพื้นผิว หรือแม้กระทั่งในบางหน่วยงาน หรือองค์กร ที่มีการนำเอาระบบการตรวจสอบเวลาเข้าทำงานโดยการใช้ลายนิ้วมือ ก็สามารถดักจับลายนิ้วมือเพื่อนำไปสร้างนิ้วมือยางเพื่อนำไปใช้ต่อไปได้

โครงการวิจัยนี้ตจึงเล็งเห็นว่าในการนำข้อมูลชีวภาพซึ่งมีความไวต่อความปลอดภัยนั้น ระบบ หรือผู้ควรมีโปรโตคอลที่มีมาตรฐานในการนำเอาข้อมูลชีวภาพมาใช้เพื่อเกิดความปลอดภัยต่อข้อมูลของผู้ใช้ แต่ต่อระบบเอง คณะผู้วิจัยจึงนำเสนอโปรโตคอลที่มีความปลอดภัยในการนำเอาข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคล

จากในปัจจุบันเห็นได้ว่ามีการนำลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคลเริ่มแพร่หลายมากขึ้นโดยที่ผู้ใช้อาจไม่ได้ระมัดระวังถึงภัยใกล้ตัว อันเนื่องมาจากการใช้โทรศัพท์ที่ได้รับความนิยมในปัจจุบัน และมีแนวโน้มในการนำเอาข้อมูลชีวภาพมาใช้

1.2 วัตถุประสงค์ของโครงการวิจัย

1. เพื่อพัฒนาโปรโตคอลที่ปลอดภัยในการนำข้อมูลลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคล
2. เพื่อให้ข้อมูลลายนิ้วมือของผู้ใช้มีความปลอดภัย
3. เพื่อพัฒนาโปรโตคอลนำร่องในการใช้งานข้อมูลลายนิ้วมือเพื่อพิสูจน์ตัวบุคคลอย่างปลอดภัย

1.3 ขอบเขตของโครงการวิจัย

โครงการวิจัยนี้จะทำการวิเคราะห์ เพื่อทำการสร้างโปรโตคอลที่มีความปลอดภัยสำหรับการพิสูจน์ตัวบุคคลเพื่อเข้าใช้ระบบโดยจำลองการทำงานของการเข้าใช้ระบบจากลายนิ้วมือ

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้โปรโตรคอลที่มีความปลอดภัยในการนำข้อมูลลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคล
2. ได้องค์ความรู้ในการเผยแพร่การนำเอาข้อมูลลายนิ้วมือมาใช้อย่างปลอดภัย

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 TPM (Trusted Platform Module)

TPM [17] คืออุปกรณ์ฮาร์ดแวร์อย่างหนึ่งซึ่งสามารถทำการจัดเก็บสถานะของแพตฟอร์มที่กำลังทำงานอยู่ได้ ดังนั้นอุปกรณ์ TPM จะถือว่าเป็นอุปกรณ์หนึ่งที่จะช่วยในการรักษาความปลอดภัยของระบบ โดยที่ในแต่ละ TPM จะมีชุดของคีย์สาธารณะและคีย์ส่วนตัว (public / private key pair) ติดมาจากโรงงานผลิต ในการทำงานของ TPM เพื่อทำการตรวจสอบระดับความปลอดภัยของเครื่อง หรือ แพลตฟอร์มที่ผู้ใช้ทำงาน TPM จะเริ่มทำงานตั้งแต่เมื่อเครื่องเริ่มบูตการทำงาน และทำการจัดเก็บ และตรวจสอบสถานะไว้ ซึ่งถ้าสถานะใดมีการเปลี่ยนแปลง (เช่นโปรแกรมบางโปรแกรมที่ทำงานถูกเปลี่ยนแปลงค่า จากเมื่อครั้งก่อนที่เคยทำงาน ซึ่งอาจเกิดจากโปรแกรมนั้นติด Trojan เพื่อแอบเก็บข้อมูลของผู้ใช้) TPM จะทำการเก็บสถานะนั้นไว้ และผู้ใช้จะสามารถตรวจสอบการสถานะได้ว่ามีการเปลี่ยนแปลง และผู้ใช้จะสามารถตัดสินใจได้ว่าจะใช้งานแพลตฟอร์มนั้นๆหรือไม่ และเนื่องจากว่า TPM มีชุดคีย์สาธารณะและคีย์ส่วนตัวที่ใช้ในการเข้ารหัสข้อมูลสถานะที่ทำการตรวจสอบ ดังนั้นจึงสามารถมั่นใจได้ว่าโปรแกรมที่มีอันตรายจะไม่สามารถทำการแก้ไขค่าได้

2.1.2 Dolev-Yao Style Attacker

Dolev-Yao Style attacker [25] ถือว่าเป็นลักษณะการจู่โจมต่อระบบ ที่มีประสิทธิภาพ เนื่องจากลักษณะการจู่โจมจะอยู่บนสมมุติฐานว่าผู้จู่โจมจะสามารถฟัง ตรวจจับ แทรกแซง และสร้างข้อความขึ้นมาให้ได้เพื่อให้สามารถค้นหาความลับของข้อมูลที่กำลังจัดส่งหรือทำงานอยู่ ทั้งนี้รวมถึงสมมุติฐานว่าถ้าผู้จู่โจมมีคีย์ที่ใช้ในการเข้ารหัสหรือถอดรหัสได้ ผู้จู่โจมจะสามารถทำการเข้ารหัสข้อมูลที่ตรวจจับได้เพื่อหลอกผู้รับสาร รวมถึงสามารถถอดรหัสข้อมูลเมื่อต้องการข้อมูลที่ถูกเข้ารหัสอยู่ อีกทั้งลักษณะการจู่โจมแบบ Dolev-Yao Style ยังสามารถแอบอ้างเป็นผู้ใช้ที่แท้จริงเพื่อหลอกผู้ที่กำลังติดต่อเพื่อให้ได้มาซึ่งข้อมูลที่ต้องการ ดังนั้นในการตรวจสอบความปลอดภัยของระบบว่าสามารถเก็บข้อมูลได้เป็นความลับ หรือไม่มีการรั่วไหลของข้อมูลนั้น จำเป็นต้องมีการสร้างการจู่โจมในลักษณะนี้เพื่อทดสอบ

โครงการวิจัยนี้มุ่งเน้นเพื่อทำการวิเคราะห์ลักษณะช่องโหว่ทางด้านความปลอดภัยของการใช้ข้อมูลชีวภาพเพื่อการพิสูจน์ตัวบุคคลเพื่อให้ข้อมูลชีวภาพของผู้ใช้มีความปลอดภัยไม่ถูกขโมย หรือถูกดักจับเพื่อนำไปใช้งานโดยไม่เต็มใจ โดยที่ในงานวิจัยนี้จะทำการวิเคราะห์ความเป็นไปได้ของปัญหาด้านความปลอดภัยของการนำเอาข้อมูลชีวภาพมาใช้งาน และสร้างการจู่โจมที่เป็นไปได้ในระหว่างการนำเอาข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคล ซึ่งอาจเกิดได้ตั้งแต่การจัดเก็บข้อมูลชีวภาพสู่ระบบ หรือแม้กระทั่งขั้นตอนการเปรียบเทียบข้อมูลชีวภาพของผู้ใช้ในขณะที่แสดงต่อระบบเทียบกับข้อมูลชีวภาพที่จัดเก็บไว้ ซึ่งคณะผู้วิจัยจะ

ทำการออกแบบโปรโตคอลในการใช้งานข้อมูลชีวภาพในการพิสูจน์ตัวบุคคล แล้วให้การจู่โจมแบบต่างๆ ทำงาน โดยการจำลองจากโปรแกรมจำลองการจู่โจม ซึ่งจะทำการวิเคราะห์ผู้จู่โจมในรูปแบบของ Dolev-Yao Style attacker โดยที่เมื่อทำการทดสอบการทำงานของโปรโตคอลต่อการจู่โจมต่างๆ แล้ว จะได้โครงสร้างโปรโตคอลที่มีความปลอดภัยในนำข้อมูลชีวภาพมาใช้ในการพิสูจน์ตัวบุคคล

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 ขั้นตอนการทำงานของระบบไบโอเมติกซ์

จากการศึกษางานวิจัยขององค์กร National Science & Technology Council's [2] และงานวิจัยของ Gerrit Bleumer [3] สามารถสรุปการทำงานของระบบไบโอเมตริกซ์โดยรวมแล้วไม่ว่าจะเป็นคุณลักษณะประเภทไหน ก็จะมีส่วนการทำงานที่สำคัญดังนี้

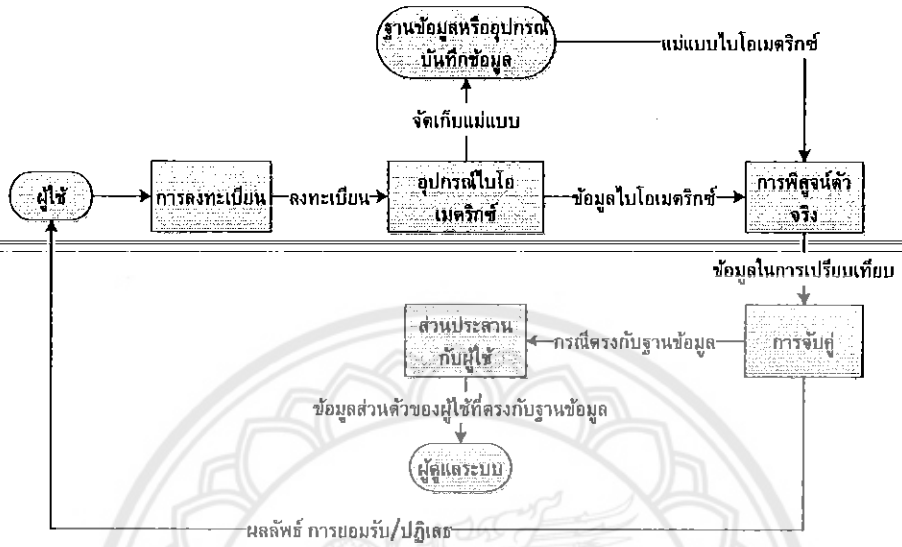
1. การลงทะเบียน (Enrollment) เป็นขั้นตอนแรกของระบบ โดยให้ระบบทำการบันทึกและรู้จำคุณลักษณะทางไบโอเมตริกซ์ของผู้ใช้ที่ถูกต้องลงในระบบฐานข้อมูลหรือที่เรียกว่า การบันทึกแม่แบบ โดยคุณลักษณะที่ถูกบันทึกนั้น อาจถูกเก็บไว้ในฐานข้อมูลส่วนกลางหรืออาจบันทึกไว้ในบัตรสมาร์ทการ์ดเพื่อให้ผู้ใช้เป็นผู้ถือครองเองก็ได้
2. การพิสูจน์ตัวจริง (Authentication) เป็นขั้นตอนในการในการระบุยืนยันตัวบุคคลโดยเริ่มจากการที่ผู้ใช้นำเสนอคุณลักษณะทางไบโอเมตริกซ์ของผู้ใช้กับอุปกรณ์ไบโอเมตริกซ์เพื่อทำการสกัดคุณลักษณะที่ได้เป็นข้อมูลสำหรับนำไปใช้ในการเปรียบเทียบกับคุณลักษณะเดิมที่ได้ทำการลงทะเบียนไว้ก่อนหน้านี้
3. การจับคู่ (Match) เมื่อระบบได้รับข้อมูลทางไบโอเมตริกซ์จากผู้ใช้จากขั้นตอนการพิสูจน์ตัวจริงแล้ว ก็จะเข้าสู่ขั้นตอนการจับคู่โดยนำข้อมูลที่ได้นั้นมาวิเคราะห์ผลว่ามีค่าความถูกต้องเพียงพอหรือไม่ ตัวตนของผู้ใช้ก็จะได้รับการยืนยันและสามารถทำธุรกรรมต่าง ๆ ที่กำหนดไว้ได้ แต่หากผลลัพธ์ออกมาไม่ตรงกับฐานข้อมูล ระบบก็จะทำการปฏิเสธผู้ใช้ทันที

2.2.2 อุปกรณ์และส่วนสนับสนุนของระบบไบโอเมตริกซ์

การที่ระบบไบโอเมตริกซ์จะสามารถทำงานได้อย่างมีประสิทธิภาพจำเป็นต้องมีอุปกรณ์และส่วนสนับสนุนที่สำคัญในระบบดังนี้

1. อุปกรณ์อ่านไบโอเมตริกซ์(Biometric Reader) คืออุปกรณ์สำหรับการอ่านคุณลักษณะทางไบโอเมตริกซ์ เช่น เครื่องสแกนลายนิ้วมือ ใช้สำหรับในขั้นตอน การลงทะเบียน และ การพิสูจน์ตัวจริง
2. ส่วนต่อประสานกับผู้ใช้(User Interface) ส่วนนี้มักแสดงอยู่ในส่วนของผู้ดูแลระบบ เมื่อผู้ใช้ทำการเสนอคุณลักษณะใด ๆ ต่อ อุปกรณ์ไบโอเมตริกซ์แล้ว ระบบก็จะทำการแสดงรายละเอียดข้อมูลของผู้ใช้ขึ้นทางจอภาพ เช่น รูปใบหน้า ชื่อ รหัสประชาชน เป็นต้น ซึ่งในส่วนนี้อาจมีหรือไม่มีก็ได้

3. ฐานข้อมูลหรืออุปกรณ์บันทึกข้อมูล(Storage) เป็นส่วนสำคัญสำหรับใช้ในการจัดเก็บแม่แบบที่ผ่านการลงทะเบียนไว้ เพื่อใช้ในการเปรียบเทียบในการเข้าสู่ระบบ ซึ่งอาจเป็นฐานข้อมูลคอมพิวเตอร์ บัตรสมาร์ทการ์ด หรืออุปกรณ์อื่น ๆ ก็ได้



ภาพที่ 1 แสดงการทำงานของระบบไบโอเมตริกซ์

2.2.3 ความเสี่ยงด้านความปลอดภัยของไบโอเมตริกซ์แต่ละประเภท

เนื่องจากระบบไบโอเมตริกซ์ถูกแบ่งคุณลักษณะที่ใช้ในการตรวจสอบออกเป็นหลายประเภท โดยแต่ละประเภทที่มีการนิยมใช้กันทั่วไปต่างก็มีข้อเสียหรือข้อบกพร่องดังนี้

1. ลายนิ้วมือ

ในบางครั้งอายุและการประกอบอาชีพก็มีผลในการทำให้อุปกรณ์ไบโอเมตริกซ์ตรวจสอบได้ยาก เช่น นิ้วมือแตก หรือหยาบมากจากการทำงาน อีกทั้งเรื่องของลายนิ้วมือแฝง ที่เมื่อเวลาเราสัมผัสกับสิ่งต่าง ๆ มักจะเกิดสารเคมีตกค้างที่ผลิตโดยต่อมเหงื่อจากนิ้วมือ ซึ่งในทางทฤษฎีแล้วมีความเป็นไปได้ที่จะนำเอาลายนิ้วมือแฝงนี้ใช้ในการสร้างลายนิ้วมือเทียม ในงานวิจัยของ Antti Sténและคณะ [4] และ งานวิจัยของ Tsutomu Matsumoto และคณะ [7]ได้นำเสนอถึงการนำลายนิ้วมือแฝงมาใช้ในการสร้างลายนิ้วมือเทียมโดยใช้วิธีทั่วไปและอุปกรณ์ที่หาได้โดยง่าย ส่วนแม่พิมพ์ในการสร้างใช้วิธีการประยุกต์จากวิธีการสร้างแผงวงจรโดยพิมพ์ลายนิ้วมือแฝงที่ได้บนแผ่นใสโดยลงสารเคลือบไว้และวางซ้อนบนบอร์ดหรือแผ่นทองแดง เมื่อถูกแสง UV ส่วนพื้นผิวที่เป็นสีเข้มหรือส่วนลายที่นูนของลายนิ้วมือจะถูกปกป้องด้วยสารที่เคลือบไว้ ทิ้งไว้สักพักให้ล้างออกด้วยน้ำด่างก็จะได้แม่พิมพ์มา จากนั้นเทเจลาตินลงไปบาง ๆ รอให้เจลาตินแข็งตัวก็จะได้ลายนิ้วมือเทียม เมื่อได้ลายนิ้วมือเทียมมาแล้วเราจะนำมาใช้โดยวางลายนิ้วมือเทียมไว้บนนิ้วมือของเราแล้วใช้สแกนเข้าสู่ระบบ

ผลทดลองจากงานวิจัยพบว่าประสบความสำเร็จในการตรวจสอบ

2. ม่านตาและกระจกตา

ในขั้นตอนการตรวจสอบม่านตา มักจะมีปัจจัยรบกวนจากการถูกบดบังจากขนตา เปลือกตา หรือสิ่งสะท้อนจากกระจกตาทำให้ระบบไม่สามารถตรวจสอบได้ หรืออาจมีการใช้คอนแท็คเลนส์เพื่อปลอมแปลงม่านตาซึ่งถึงแม้จะทำได้ยากแต่ก็มีความเป็นไปได้[11] และการจะนำระบบมาใช้จำเป็นต้องมีการฝึกอบรมก่อนการนำมาใช้ เนื่องจากผู้ดูแลจำเป็นต้องมีความรู้ความเข้าใจในการประเมินคุณภาพแม่แบบในขั้นตอนการลงทะเบียน และผู้ใช้ก็ต้องมีความรู้ความเข้าใจเกี่ยวกับระบบ ไม่ว่าจะเป็นระยะในการตรวจสอบ เวลาในการตรวจสอบ เป็นต้น ซึ่งมีขั้นตอนละเอียดอ่อนกว่ามากเมื่อเทียบกับรูปแบบลายนิ้วมือที่เพียงแค่เอานิ้วแตะอุปกรณ์

3. โครงหน้า

ใบหน้าคนเรามีการเปลี่ยนแปลงตามเวลา และยังถูกบดบังได้ง่ายโดยผม หมวก แว่นตาหรืออื่น ๆ ซึ่งระบบนี้จะมีความไวต่อแสงมาก ในที่ ๆ แสงมากหรือน้อยเกินไปอาจทำให้ผลลัพธ์ที่ได้ไม่ถูกต้องหรือการใช้อุปกรณ์ไบโอเมตริกซ์ที่ได้ภาพคุณภาพต่ำ เช่นใช้กล้องที่มีความละเอียดต่ำก็อาจทำให้ได้ผลลัพธ์ที่ไม่ถูกต้อง

4. โครง/รูปทรงมือ

มีความต้องการของระบบสูงและการตรวจสอบรูปทรงมือจะมีเสถียรภาพสูงในวัยผู้ใหญ่ขึ้นไปหรือคือระยะที่เติบโตเต็มที่แล้วเท่านั้นเพราะในวัยเด็กหรือวัยเจริญเติบโตรูปทรงสามารถมีการเปลี่ยนแปลงได้ตามการเจริญเติบโตของร่างกาย [2]

5. เสียง

ข้อเสียหลักคือเสียงเป็นสิ่งที่ยากแก่การควบคุมและเหมาะสำหรับการใช้เฉพาะบุคคลไม่เหมาะแก่การใช้กับฐานข้อมูลที่มีขนาดใหญ่ เนื่องจากอาจเกิดความซ้ำซ้อนกันได้

2.2.4 ช่องทางและความเป็นไปได้ในการโจมตีระบบไบโอเมตริกซ์

ในที่นี้จะกล่าวถึงในส่วนของระบบสแกนลายนิ้วมือเป็นหลักเนื่องจากเป็นที่นิยมอย่างแพร่หลาย

1. **การดักจับข้อมูลแล้วนำมาใช้เข้าสู่ระบบ (Capture/replay attacks)**

ลักษณะการทำงาน เป็นวิธีการโจมตี ในรูปแบบการดักจับข้อมูลการเข้าสู่ระบบแล้วเก็บบันทึกไว้ และนำมาแสดงเพื่อใช้เข้าสู่ระบบในภายหลังถึงแม้ข้อมูลจะมีการเข้ารหัสไว้ก็ตาม เนื่องจากวิธีนี้ไม่มีความจำเป็นต้องอ่านข้อมูลภายใน อาจเกิดขึ้นในระบบที่เป็นลักษณะระบบเครือข่าย[5] โดยผู้ไม่ประสงค์ดีจะทำการแอบบันทึกการสื่อสารโต้ตอบระหว่างผู้ใช้กับระบบ แล้วนำข้อมูลที่ได้นำมาแสดงกับระบบเพื่อเข้าสู่ระบบใน

ฐานะผู้ใช้คนนั้นแทน ซึ่งสามารถแก้ไขได้โดยการใช้เทคนิค time stamp กำกับเวลาการใช้งานทุกครั้งที่เข้าสู่ระบบ หรือการใช้การกำกับลายเซ็นต์ดิจิตอลเพื่อป้องกันการนำข้อมูลมาใช้ซ้ำได้

2. **การใช้ลายนิ้วมือแฝงบนอุปกรณ์สแกนลายนิ้วมือโดยใช้เทคนิคการพ่นลมหายใจ**

ลักษณะการทำงานคือวิธีการใช้คราบน้ำมันหรือสารคล้ายเหงื่อที่ผลิตออกมาจากบริเวณนิ้วมือ จนเกิดเป็นคราบลายนิ้วมือ ที่ติดอยู่บนแป้นของอุปกรณ์สแกนลายนิ้วมือ โดยปกติแล้วเมื่อเราสัมผัสอุปกรณ์ไปครั้งหนึ่งแล้วจะเหลือคราบเป็นลายนิ้วมือติดอยู่ ซึ่งอาจไม่ค่อยชัดเจน แต่สามารถทำให้มันชัดเจนขึ้นได้ด้วยการหายใจบนคราบนั้น หรือการพ่นลมใส่ โดยพื้นฐานแล้วน้ำมันจะปฏิเสธน้ำโดยสิ้นเชิงทำให้มันสามารถป้องกันน้ำและความชื้นบริเวณจุดนั้นได้ และน้ำและอื่น ๆ เป็นสื่อนำกระแสไฟฟ้าได้ดีและมีปริมาตรความจุเดียวกันกับผิว ซึ่งเมื่อเราเป่าลมหรือหายใจลงไป ความชื้นก็จะเพิ่มสูงขึ้นบริเวณที่เป็นสันนูนของลายนิ้วมือและทำให้เกิดลายนิ้วมือขึ้นมา ถึงแม้จะมีความผกผันอยู่บ้างแต่จากความสัมพันธ์ของคุณลักษณะที่ตรงกันก็สามารถที่จะบอกได้ว่าเป็นเจ้าของลายนิ้วมือจริง[3] ในบางครั้งก็ไม่สามารถอธิบายได้จากการที่มันไม่สามารถทำงานได้อย่างที่มันควรจะเป็นในการใช้วิธีการหายใจนี้ บางทีก็มีการแจ้งเตือนว่านิ้วมือชื้นหรือเปียกเกินไปหรือลายนิ้วมือไม่ถูกต้อง แต่ก็มีโอกาสประสบความสำเร็จ

3. **การใช้ลายนิ้วมือปลอม**

ลักษณะการทำงานการจะสร้างลายนิ้วมือปลอมจำเป็นจะต้องมีแม่แบบลายนิ้วมือ หรือลายนิ้วมือของเป้าหมายที่ต้องการนำมาสร้างเป็นลายนิ้วมือปลอม ซึ่งการจะได้แม่แบบในการสร้างลายนิ้วมือปลอมนั้นมีอยู่ 2 วิธี คือ การสร้างแม่แบบลายนิ้วมือจากลายนิ้วมือจริง และการสร้างแม่แบบลายนิ้วมือโดยใช้ลายนิ้วมือแฝง ซึ่งก็คือ คราบลายนิ้วมือ ที่ติดอยู่กับสิ่งของต่าง ๆ ที่เราสัมผัส

ความเป็นจริง การจะสร้างลายนิ้วมือปลอมคงไม่ได้รับการร่วมมือจากเป้าหมายเราจึงต้องอาศัยการสร้างแม่พิมพ์จากลายนิ้วมือแฝงซึ่งปกติก็จะเกิดจากการที่เราสัมผัสสิ่งต่าง ๆ ก็จะเหลือลายนิ้วมือแฝงไว้ซึ่งสามารถทำให้มองเห็นได้ เช่น การโรยผงละเอียดบริเวณคราบลายนิ้วมือก็จะทำให้เห็นลายนิ้วมือเด่นชัดขึ้น ทำให้สามารถเก็บคราบลายนิ้วมือมาได้ หลังจากนั้นก็นำลายนิ้วมือแฝงที่ได้ไปสร้างแม่พิมพ์และสามารถสร้างลายนิ้วมือเทียมได้จากอุปกรณ์ที่หาได้ทั่ว ๆ ไป เช่น เจลลาติน[4][7] วิธีนี้จะเห็นได้ว่าสามารถใช้อุปกรณ์ราคาถูกที่มีอยู่ทั่วไปได้และอัตราความสำเร็จในการลักลอบก็จะสูงขึ้นหากใช้วัสดุที่มีคุณภาพสูงขึ้น

2.2.5 การป้องกันการจู่โจม

1. Liveness detection

Liveness detection หมายถึง ระบบตรวจสอบว่าข้อมูลทางไบโอเมตริกซ์ที่ได้รับมานั้นเป็นของจริงกล่าวคือมาจากมนุษย์ที่มีชีวิตจริง โดยใช้คุณสมบัติต่าง ๆ ที่เป็นคุณสมบัติเฉพาะของมนุษย์มาใช้ในการตรวจสอบ เช่น อุณหภูมิ ชีพจร ความดันเลือดเป็นต้น จุดประสงค์เพื่อป้องกันและตรวจสอบการใช้ข้อมูลไบโอ

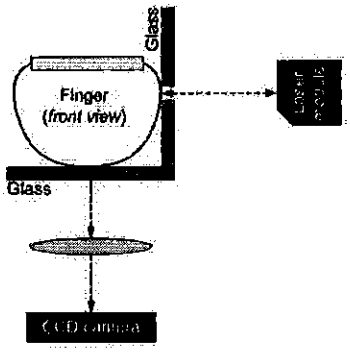
เมตริกซ์ปลอม ตัวอย่างรูปแบบหรือคุณสมบัติที่นำมาใช้ในการตรวจสอบไบโอเมตริกซ์ปลอมของระบบ Liveness detection ในระบบสแกนลายนิ้วมือมีดังนี้

2. **การวัดความอิ่มตัวของออกซิเจนในเลือดและคุณสมบัติการซึมซับแสง**

เป็นวิธีการตรวจสอบ liveness ในงานวิจัยของ Venkata Reddy และคณะ[9] วิธีนี้จะใช้วิธีการตรวจวัดความอิ่มตัวของออกซิเจนของฮีโมโกลบิน และการวัดค่าอัตราการดูดซึมแสงของผิว โดยนำทั้งหมดนี้มาใช้เป็นการตรวจสอบ liveness การดูดซึมแสงจะแตกต่างกันตามออกซิเจนในเลือด เนื่องจากฮีโมโกลบินกับฮีโมโกลบินที่มีความอิ่มตัวของออกซิเจนมีสเปกตรัมแสงที่แตกต่างกันอย่างมีนัยสำคัญในช่วง 500 นาโนเมตร ถึง 1000 นาโนเมตร เมื่อออกซิเจนรวมเข้ากับฮีโมโกลบินในเซลล์เม็ดเลือดแดงจะทำให้ออกซิเจนเกือบทั้งหมดอิ่มตัว ในการทดลองนี้จำเป็นต้องมีการติดตั้งตัวฉายแสงที่เป็นหลอด LED สองตัวเพื่อฉายแสงในมุมที่ต่างกันเพื่อใช้ในการวัดความยาวคลื่น และจะมีส่วนของ photo detector ในการจับภาพสัญญาณแรงดันไฟฟ้าที่ส่งกลับมา โดยทำการกรองออกมาให้เป็นภาพคลื่นสัญญาณและมีกระบวนการในการกรองสัญญาณและลบสิ่งรบกวนที่ไม่ต้องการออกไป จากนั้นนำมาวิเคราะห์เพื่อหาค่าความอิ่มตัวของออกซิเจนในเลือด จากการทดลองจากกลุ่มตัวอย่างที่ได้มาในกรณีนิ้วมือจริงนั้นจะปรากฏอัตราการเต้นของชีพจรซึ่งสังเกตได้จากภาพคลื่นสัญญาณที่จะมีการเปลี่ยนแปลงของคลื่นสัญญาณในทันที แต่ในกรณีของลายนิ้วมือเทียมนั้นสัญญาณการเต้นของชีพจรจะหายไปและลักษณะคลื่นสัญญาณจะไม่มีการเปลี่ยนแปลงหรือมีการเปลี่ยนแปลงตำแหน่งเพียงเล็กน้อย โดยตัดสินได้จากเกณฑ์กำหนดที่โดยเฉลี่ยแล้วลายนิ้วมือจริงจะต้องมีค่าความอิ่มตัวออกซิเจนในเลือดมากกว่า 30%

3. **การวิเคราะห์การเคลื่อนไหวของพื้นผิวสัมผัสบริเวณปลายนิ้ว จากการไหลเวียนของเลือด**

วิธีการนี้เป็นวิธีการตรวจสอบ liveness รูปแบบใหม่ในงานวิจัยของ Martin Drahanský และคณะ [8] โดยทำการวิเคราะห์การเคลื่อนไหวของพื้นผิวสัมผัสที่ปลายนิ้วเนื่องจากการไหลเวียนของเลือดและการเต้นของหัวใจโดยการทำงานนั้นจะถูกแบ่งเป็นสองส่วนคือส่วนของ กล้อง กับ เลเซอร์ ซึ่งเลเซอร์ใช้สำหรับวิเคราะห์การเคลื่อนไหวของผิวในระดับไมโครเมตรลงไป



ภาพที่ 2 แสดงแบบจำลองการทำงานของระบบ

ที่มา Martin Drahansky และคณะ [8]

แนวคิดหลักคือจะมีช่องขนาดเล็กประมาณ 6 มิลลิเมตรจะถูกสร้างขึ้นบริเวณตรงกลางของแผ่นกระจกดังแสดงในภาพที่ 2 ในขั้นตอนแรกระบบจะทำการสแกนให้ได้มาซึ่งลายนิ้วมือและลายนิ้วมือจะถูกจัดเก็บ โดยการฉายลายนิ้วมือบนกล้อง CCD ต่อไปกระจกจะทำการส่งผ่านส่วนหนึ่งของนิ้วมือที่วางอยู่บนช่องกระจกนั้นสะท้อนภาพไปทางขวาและฉายบน CCD camera โดย macro lens และส่วนสุดท้ายของระบบคือการใช้ภาพวิดีโอที่ได้ในการวิเคราะห์การตรวจสอบ liveness สิ่งสำคัญในกรณีนี้คือการวิเคราะห์ภาพวิดีโอ ในเฟรมแรกของวิดีโอทุกครั้งจะใช้ในการประมวลผลหาจุดพิเศษบนลายนิ้วมือเพื่อหาความแตกต่างของลายนิ้วมือเพื่อนำไปใช้ในการวิเคราะห์

4. ความต้านทานไฟฟ้าของผิว

เป็นอีกคุณสมบัติหนึ่งในอุปกรณ์สแกนลายนิ้วมือปัจจุบัน ซึ่งมีการทดสอบแล้วว่าความต้านทานไฟฟ้าของผิวมนุษย์ค่าที่ได้จะอยู่ระหว่าง 20 kΩ ถึง 3MΩการวัดความต้านทานไฟฟ้า สำหรับลายนิ้วมือเทียมที่สร้างจากวัสดุที่ไม่ได้มีคุณสมบัติเหมือนผิวจริงจะมีค่าความต้านทานไฟฟ้าสูงกว่ามาก แต่ก็มีซิลิโคนและเจลาตินหลายชนิดที่ถูกนำมาใช้สร้างลายนิ้วมือปลอมซึ่งเมื่อตรวจสอบแล้วได้ค่าความต้านทานไฟฟ้าในระดับเดียวกับผิวของมนุษย์จริง[8]

5. อุณหภูมิ

การวัดอุณหภูมิทำการวัดอุณหภูมิพบว่าอุณหภูมิจะอยู่ในช่วง 30.1°C ถึง 36.2°C [7] โดยทั่วไปอุปกรณ์สแกนลายนิ้วมือในปัจจุบันจะมีความสามารถในการตรวจสอบอุณหภูมิอยู่แล้ว ซึ่งผู้ที่ต้องการปลอมแปลงจะใช้ลายนิ้วมือเทียมที่มีลักษณะบางมากติดไว้บนนิ้วมือ โดยจะทำให้ค่าอุณหภูมิที่ได้อยู่ในช่วงที่ถูกต้องทำให้ไม่สามารถตรวจจับได้

6. ความดันเลือด

การวัดความดันเลือดโดยสำหรับผู้ที่มีสุขภาพดีทั่วไปจะมีค่าความดันช่วงหัวใจคลายตัวไม่ต่ำกว่า 80 มม. ปรอท และค่าความดันช่วงหัวใจบีบตัวจะต้องไม่ต่ำกว่า 120 มม. ปรอท สำหรับคนที่เป็นความดันโลหิตสูงจะค่าความดันในช่วงหัวใจคลายตัวที่ 140 มม. ปรอท และมีค่าความดันช่วงหัวใจบีบตัวที่ 300 มม. ปรอท ซึ่งหากค่าความดันเลือดที่วัดได้ไม่อยู่ในช่วงดังกล่าวก็จะสามารถระบุได้ว่าเป็นตัวอย่างปลอม[8] แต่การใช้ลายนิ้วมือเทียมที่มีลักษณะบางก็ยังคงให้ค่าความดันอยู่ในช่วงที่ยอมรับได้อยู่ดี

7. การประยุกต์การป้องกันแบบหลายทาง

คือการเพิ่มความปลอดภัยของระบบโดยการเพิ่มวิธีการป้องกันการเข้าถึงข้อมูลมากกว่าสองทางขึ้นไปนอกจากการใช้ข้อมูลไบโอเมตริกซ์เพียงอย่างเดียว โดยอาจใช้อุปกรณ์ต่าง ๆ ดังนี้

2.2.6 การพิสูจน์โดยใช้รหัสผ่าน (Password authentication)

รหัสผ่านเป็นรูปแบบที่มีการใช้มากที่สุดในปัจจุบัน [10] มีความต้องการพื้นฐานทั้งในเรื่องของระบบและค่าใช้จ่ายน้อย แต่ก็ถือว่าเป็นระบบที่มีความปลอดภัยมากหากตั้งรหัสผ่านให้ยากขึ้น ซึ่งส่วนใหญ่แล้วผู้ใช้มักตั้งรหัสผ่านที่เกี่ยวข้องกับตนเองเพื่อให้จดจำได้ง่าย แต่ก็ทำให้เดาได้ง่ายด้วย อย่างไรก็ตามก็สามารถกำหนดนโยบายการตั้งรหัสผ่านที่ดีได้โดยผู้ดูแลระบบโดยกำหนดลักษณะรหัสผ่านและความยาวให้มีความปลอดภัยเพียงพอ และแม้รหัสผ่านจะมีความยากเพียงพอแต่ก็อาจเสี่ยงต่อการถูกดักจับ เช่นโปรแกรมดักจับคีย์บอร์ด หรือไวรัสได้

1. ชิปรักษาความปลอดภัย (TPM embedded security chip authentication)

เป็นชิปรักษาความปลอดภัยที่ถูกฝังไว้ในเครื่องคอมพิวเตอร์ ซึ่งสามารถปกป้องข้อมูลที่อยู่ภายในด้วยฟังก์ชันการเข้ารหัส TPM ไม่ได้เป็นอุปกรณ์ตรวจสอบบุคคลโดยตรง แต่มีไว้สำหรับการเช็คหรือตรวจสอบความปลอดภัยในสภาพก่อนการเข้าสู่ระบบ[10] ว่ามีความปลอดภัยหรือไม่

2. บัตรสมาร์ทการ์ด (Smart card authentication)

สมาร์ทการ์ดเป็นการรวมเอาสองปัจจัยเข้าด้วยกันคือผู้ใช้จำเป็นต้องมีสมาร์ทการ์ดและรู้ PIN หรือรหัสผ่านจึงจะสามารถใช้งานได้ทำให้เป็นการยกระดับความปลอดภัยของข้อมูลให้สูงขึ้น นอกจากนี้สมาร์ทการ์ดยังให้ความปลอดภัยในเรื่องของการทำบัตรสูญหายซึ่งจะไม่มีผลในเรื่องของความปลอดภัย และเพิ่มความสะดวกในเรื่องของการพกพา ทำให้ผู้ใช้ไม่จำเป็นต้องยึดติดกับอุปกรณ์หรือระบบใดระบบหนึ่ง ผู้ใช้สามารถนำไปใช้ในสถานที่อื่น ๆ ได้

3. ยูเอสบีโทเค็น (USB token authentication)

เหมือนกับสมาร์ทการ์ดคือมีการผนวกรวมสองปัจจัยเข้าด้วยกันคือผู้ใช้ต้องมีอุปกรณ์ USB token ใน

การเชื่อมต่อกับอุปกรณ์ผ่านพอร์ต USB และต้องรู้ PIN ในการปลดล็อคเพื่อทำการตรวจสอบผู้ใช้ การเข้าใช้งานที่ไม่ถูกต้องสามารถตรวจจับได้ทำให้สามารถดำเนินการป้องกันได้ และเช่นเดียวกับสมาร์ทการ์ดคือผู้ใช้สามารถพกพาได้ไม่จำเป็นต้องผูกติดกับไคลเอนต์ใดเพียงอย่างเดียว ซึ่ง USB token ส่วนใหญ่จะมีชิปหรือระบบการเข้ารหัสปกป้องข้อมูลเพื่อเพิ่มความปลอดภัย

4. การพิสูจน์โดยใช้อุปกรณ์ไบโอเมตริกซ์ (Biometric fingerprint authentication)

อุปกรณ์ไบโอเมตริกซ์ใช้คุณลักษณะทางกายภาพเพื่อตรวจสอบตัวบุคคล อุปกรณ์ไบโอเมตริกซ์ที่ใช้กันโดยทั่วไปคือเครื่องสแกนลายนิ้วมือ เพราะง่ายแก่การตรวจสอบและมีความปลอดภัยสูงกว่าระบบรหัสผ่านเพียงอย่างเดียว แต่ระบบก็ยังมีข้อผิดพลาดได้คือการยอมรับที่ผิดพลาดและการปฏิเสธที่ผิดพลาด หรืออาจมีการลักลอบใช้คุณลักษณะปลอมทำให้เกิดความเสี่ยงด้านความปลอดภัยและระบบยังอ่อนแอต่อปัจจัยรบกวนอื่น ๆ เช่น มีความชื้นสูงเกินไป นิ้วแห้ง เป็นต้น[5] ดังนั้นเพื่อให้ได้ผลลัพธ์ที่ดีที่สุดจึงควรใช้งานร่วมกับเทคโนโลยีตรวจสอบอื่น ๆ โดยการนำไปใช้บริษัทจะต้องคำนึงถึงขนาดหรือจำนวนบัญชีผู้ใช้ สถานที่และความยืดหยุ่นในการใช้งาน

5. การพิสูจน์โดยใช้โทเค็นเสมือน (Virtual token authentication)

คือการสร้างโทเค็นเสมือน การทำงานจะคล้ายกับ สมาร์ทการ์ด และ USB token โดยผู้ใช้สามารถสร้างโทเค็นบนระบบและเก็บหรือบันทึกไว้ในอุปกรณ์ต่าง ๆ เช่น SD cards ,Diskettes ,Hard drive เป็นต้น [10] จากนั้นเมื่อต้องการเข้าสู่ระบบผู้ใช้จะต้องมีอุปกรณ์ที่มีการบันทึกโทเค็นไว้ใช้ในการเข้าสู่ระบบทุกครั้ง

บทที่ 3
ผลการวิจัย

3.1 โปรโตคอล

3.1.1 รายละเอียดของโปรโตคอล

ในการสร้างหรือกำหนดรายละเอียดของโปรโตคอลที่ใช้ข้อมูลทางชีวภาพในการพิสูจน์ตัวบุคคลนั้น คุณสมบัติทางด้านความปลอดภัยของโปรโตคอลควรจะต้องเข้าใจง่าย ชัดเจน และกระจ่าง ทั้งนี้เพื่อให้การรักษาความปลอดภัยของโปรโตคอลเป็นไปด้วยความถูกต้อง นอกเหนือจากนี้ตัวแปรต่างๆที่ใช้ในการปฏิบัติการในกระบวนการต่างๆของการพิสูจน์ทราบตัวบุคคลความต้องมีการระบุให้ชัดเจน เพื่อรับประกันว่าโปรโตคอลที่สร้างขึ้นนั้นมีความปลอดภัย หรือมีคุณสมบัติด้านความปลอดภัยตามที่ผู้ใช้ต้องการ ความคลุมเคลือของการดำเนินการต่างๆในกระบวนการพิสูจน์ทราบตัวบุคคลมีผลทำให้การรักษาความปลอดภัยในโปรโตคอลอาจเกิดช่องโหว่ได้ ทั้งนี้การสร้างโปรโตคอลที่เกี่ยวข้องกับข้อมูลทางด้านชีวภาพของตัวบุคคลควรเก็บความเป็นส่วนตัวของบุคคลนั้น และทำให้ข้อมูลชีวภาพของบุคคลนั้นๆยังคงเป็นความลับอยู่ แต่โปรโตคอลยังต้องยังสามารถระบุตัวตนของบุคคลที่ต้องการพิสูจน์ทราบต่อระบบได้

จากความต้องการที่ได้กล่าวมาข้างต้น อุปกรณ์ที่ใช้ในการอ่านข้อมูลชีวภาพของบุคคลจะต้องมีคุณสมบัติที่สามารถรับประกันได้ว่าข้อมูลชีวภาพ หรือการอ่านข้อมูลชีวภาพนั้นจะต้องมาจากบุคคลจริง มิใช่ทำการอ้อมหรือผ่านอุปกรณ์ในทางใดทางหนึ่ง ทั้งนี้การอ้อมหรือผ่านอุปกรณ์ในที่นี้อาจจะเกิดขึ้นในกระบวนการที่ผู้ใช้ หรือบุคคลที่ต้องการพิสูจน์ทราบตัวตนกับระบบทำการวางลายนิ้วมือตัวเอง หรือ เกิดในกระบวนการทำการจับคู่ลายนิ้วมือที่แสดงกับระบบ เข้ากับลายนิ้วมือที่ทำการลงทะเบียนไว้ หรือ อาจเกิดขึ้นในขั้นตอนที่ทำการส่งผลลัพธ์ของการจับคู่ส่งกลับไปที่ระบบ

ในขั้นตอนกระบวนการแสดงข้อมูลลายนิ้วมือต่อระบบนั้น มีความเป็นไปได้ที่จะมีช่องโหว่ในการใช้ลายนิ้วมือปลอม หรือการใช้ลายนิ้วมือยางที่ถูกสร้างขึ้นจากเจ้าของจริง [11, 12] ดังนั้นเพื่อป้องกันปัญหาที่เกิดขึ้นจากขั้นตอนนี้อุปกรณ์ในการอ่านลายนิ้วมือควรมีความสามารถในการตรวจจับความแตกต่างระหว่างลายนิ้วมือเทียม กับลายนิ้วมือจริง

สำหรับระหว่างขั้นตอนในการจับคู่ข้อมูลลายนิ้วมือที่ถูกจัดเก็บไว้ในระบบกับข้อมูลลายนิ้วมือจริงจากผู้ใช้ในขณะที่ต้องการพิสูจน์ตัวบุคคล มีความเป็นไปได้ที่จะเกิด ข้อมูลลายนิ้วมือของจริงของผู้ใช้ที่ถูกขโมยมาอาจถูกนำมาใช้เพื่อแทนที่ลายนิ้วมือของผู้จู่โจมเพื่อให้สามารถเข้าระบบได้ และถ้าระบบไม่สามารถตรวจจับความผิดปกติ หรือช่องโหว่ที่เกิดขึ้นนี้ ผู้จู่โจมจะสามารถเก็บ และนำกลับมาใช้ได้อีกเรื่อยๆ

ดังนั้นจากช่องโหว่ทางด้านความปลอดภัยทั้งหมดที่กล่าวมาข้างต้นนั้น รายละเอียดด้านคุณสมบัติในการรักษาความปลอดภัยควรจะต้องถูกพิจารณาอย่างละเอียดถี่ถ้วน และควรต้องสามารถป้องกันความเป็นไปได้ทั้งหมดในการพยายามเข้าถึงระบบอย่างไม่ถูกต้อง

สำหรับการพิสูจน์ตัวบุคคลโดยการใช้ลายนิ้วมือในลักษณะที่ไม่มีการควบคุมนั้น เครื่องอ่านลายนิ้วมือถือเป็นส่วนสำคัญ และเป็นสิ่งที่อาจเกิดการจู่โจมได้ง่าย ทั้งนี้เนื่องจากผู้จู่โจมอาจดักจับข้อมูลโดยที่ผู้ดูแลระบบไม่อาจทราบได้ หรือแม้กระทั่งเครื่องอ่านลายนิ้วมือที่ถูกผู้จู่โจมปรับปรุงแก้ไขเพื่อให้สามารถดักจับลายนิ้วมือของผู้ใช้คนใดคนหนึ่งที่ผู้จู่โจมต้องการ และนำไปใช้เป็นของตนเอง ดังนั้นเพื่อป้องกัน และทำให้เกิดความปลอดภัย เครื่องอ่านลายนิ้วมือจึงควรถูกยืนยันความถูกต้องว่าไม่ได้ถูกปลอมปนด้วยซอฟต์แวร์ที่ไม่ประสงค์ดี เช่นการใส่ โทรจัน หรือ ซอฟต์แวร์อื่นๆที่จะทำการเปลี่ยนแปลงการทำงานที่ถูกต้องไป ก่อนที่เครื่องอ่านลายนิ้วมือจะทำการอ่านข้อมูลชีวภาพจริง

นอกเหนือจากนี้ในสถานการณ์การพิสูจน์ตัวบุคคลแบบไม่มีการควบคุมนี้ ผู้จู่โจมระบบอาจครอบครองข้อมูลชีวภาพของผู้ใช้จริงและนำไปใช้ และแสดงต่อเครื่องอ่านลายนิ้วมือโดยที่ผู้ดูแลระบบอาจไม่ทราบได้ ซึ่งข้อมูลนี้อาจถูกดักจับโดยการลอกลายนิ้วมือจากแก้ว หรือสิ่งที่เจ้าของลายนิ้วมือสัมผัส และนำลายนิ้วมือที่ลอกได้นั้นไปทำการสร้างลายนิ้วมือเทียม หรือลายนิ้วมือยาง และนำลายนิ้วมือเทียมไปวางบนเครื่องอ่านลายนิ้วมือในกระบวนการพิสูจน์ตัวบุคคลซึ่งเป็นผลได้ผู้จู่โจมระบบสามารถเข้าระบบได้ในฐานะเจ้าของตัวจริง ดังนั้นเพื่อเพิ่มความปลอดภัยในการทำงาน และป้องกันการจู่โจมในลักษณะนี้ เครื่องอ่านลายนิ้วมือควรมีความสามารถในการตรวจจับความร้อน หรืออุณหภูมิร่างกายมนุษย์ หรือตรวจจับชีพจร ซึ่งจะทำให้ทราบได้ว่าลายนิ้วมือที่ถูกแสดงที่เครื่องอ่านนั้นมาจากมนุษย์จริงหรือไม่ และความสามารถในลักษณะนี้ของเครื่องอ่านลายนิ้วมือจะสามารถตรวจพบได้ทันทีว่าลายนิ้วมือที่แสดงนั้นเป็นลายนิ้วมือเทียม และจะไม่อนุญาตให้เข้าระบบ ดังนั้นจากที่ได้กล่าวถึงความเป็นไปได้ในการจู่โจม เครื่องอ่านลายนิ้วมือที่จะถูกนำมาใช้ในโปรโตคอลจะต้องสามารถแสดงค่าค่าหนึ่งที่แสดงได้ว่าข้อมูลนั้นมาจากมนุษย์จริงๆหรือไม่ และเป็นการรับรองได้ว่าถึงแม้ลายนิ้วมือของผู้ใช้ที่แท้จริงจะถูกดักจับได้ในกระบวนการใดกระบวนหนึ่งของการพิสูจน์ตัวบุคคล แต่จะไม่สามารถถูกนำมาใช้เพื่อจับคู่กับข้อมูลลายนิ้วมือที่ถูกจับเก็บในระบบ และทำให้ผู้จู่โจมเข้าสู่ระบบได้

ถ้าในกรณีของโปรโตคอลด้านความปลอดภัยที่มีช่องโหว่ ผู้จู่โจมอาจจะอาศัยช่องโหว่นั้นในการพยายามแทนที่ข้อมูลลายนิ้วมือของตนเองด้วยลายนิ้วมือของเจ้าของที่แท้จริง ในขณะที่กำลังจะถูกส่งผ่านเครือข่ายเพื่อไปที่เซิฟเวอร์เพื่อทำการจับคู่ โดยที่ผู้จู่โจมอาจทำการดักจับระหว่างทางที่ทำการส่งข้อมูลระหว่างอุปกรณ์อ่านลายนิ้วมือ ไปที่เครื่องเซิฟเวอร์ที่ใช้ทำหน้าที่ในการจับคู่ลายนิ้วมือ และทำการเปลี่ยนข้อมูลลายนิ้วมือของผู้จู่โจม ด้วยข้อมูลลายนิ้วมือของผู้ใช้ตัวจริงที่ดักจับได้ไว้ก่อนแล้ว ดังนั้นเพื่อให้กระบวนการนี้มีความปลอดภัยและป้องกันความเป็นไปได้ของการจู่โจมดังที่ได้กล่าวมา ดังนั้น โปรโตคอลจึงควรมีกระบวนการในการใช้ nonce และ การเข้ารหัสเพื่อเพิ่มความปลอดภัยในโปรโตคอล

กรณีของโปรโตคอลที่มีจุดอ่อน อาจมีการจู่โจมได้ในช่วงเวลาที่มีการดักจับผลการจับคู่ที่ถูกต้อง และนำผลลัพธ์ในการจับคู่นั้นมาใช้ซ้ำอีกครั้งเพื่อแสดงว่าเป็นผู้ใช้ที่แท้จริง ซึ่งการทำ replay attack ของข้อความที่ส่งในเน็ตเวิร์คนั้น สามารถป้องกันได้โดยการใช้ nonce และตัวตนของผู้ใช้ คู่กับผลลัพธ์ของการจับคู่เพื่อดังนั้นเมื่อทำการตรวจสอบข้อความที่ได้รับมา ระบบจะสามารถทำการตรวจสอบได้ว่าเป็นข้อความใหม่ ไม่ใช่มาจากข้อความเก่าแล้วนำมา replay

3.1.2 โครงสร้างโปรโตคอลที่มีความปลอดภัยในการนำข้อมูลลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคล

ในการรักษาคุณสมบัติด้านความปลอดภัยของโปรโตคอล ทุกๆองค์ประกอบที่เกี่ยวข้องในโปรโตคอลจะต้องมีคุณสมบัติด้านความปลอดภัยที่ต้องการ ทั้งนี้รวมถึงอุปกรณ์ในการอ่านลายนิ้วมือ เครื่องเซิฟเวอร์ที่ใช้ในการจับคู่ และช่องทางด้านการสื่อสาร จากที่ได้กล่าวข้างต้น ในสถานการณ์ที่ไม่ได้ควบคุม อุปกรณ์ในการอ่านลายนิ้วมือที่อยู่ อาจถูกปลอมแปลงโดยผู้จู่โจมโดยอาจทำการใส่ซอฟต์แวร์ที่ดักจับข้อมูลชีวภาพของผู้ใช้และนำไปใช้ต่อ ดังนั้นอุปกรณ์ในการอ่านนิ้วมือนั้นควรถูกตรวจสอบว่ามีความปลอดภัยก่อนที่ผู้ใช้จะแสดงข้อมูลชีวภาพของตนต่ออุปกรณ์นั้นๆ

ทีพีเอ็ม (TPM) อาจถูกนำมาใช้ในการรับรองอุปกรณ์ต่างๆที่เกี่ยวข้องในระบบ ว่าไม่มีการปลอมแปลงหรือมีการดัดแปลงเพื่อดักจับข้อมูลของผู้ใช้ ดังนั้นสำหรับโปรโตคอลที่งานวิจัยนี้ TPM จะถูกใช้เพื่อในการรับรองว่าอุปกรณ์ต่อพ่วงต่างๆไม่มีการดัดแปลงหรือถูกเปลี่ยนแปลงโดยที่ TPM จะทำหน้าที่ในการจัดการตรวจสอบค่าความถูกต้องของเครื่อง และอุปกรณ์ต่างๆ รวมถึงอุปกรณ์อ่านลายนิ้วมือถ้ามีการนำลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคล ซึ่งกระบวนการตรวจสอบนี้ทำให้ทราบได้ว่าโครงสร้าง หรือองค์ประกอบทั้งหลายของระบบมีการเปลี่ยนแปลงค่าไปจากเดิมหรือไม่ ถ้ามีการเปลี่ยนแปลงไปทำให้ทราบได้ว่ามีความเป็นไปได้ที่มีการปลอมแปลงค่าไปโดยผู้จู่โจมระบบ แต่ทั้งนี้ค่าความเปลี่ยนแปลงนี้สามารถแสดงให้กับผู้ใช้ได้ทราบ และให้ผู้ใช้ตัดสินใจได้เองว่าจะเชื่อถือระบบที่ใช้อยู่หรือไม่ ดังนั้นในการออกแบบโปรโตคอลในงานวิจัยนี้ได้นำ TPM มาใช้ร่วมด้วยเพื่อป้องกันการที่ข้อมูลชีวภาพของผู้ใช้ถูกดักจับ หรือถูกขโมยไปใช้ภายหลัง

สำหรับช่องทางการสื่อสารนั้นถือว่าเป็นอีกทางหนึ่งที่จะถูกแทรกแซงได้โดยผู้จู่โจมได้ ซึ่งผู้จู่โจมที่มีประสิทธิภาพเช่น Dolev-Yao Style สามารถทำงานกับข้อความได้หลายแบบ ดังนั้นเพื่อให้โปรโตคอลที่ออกแบบมีความปลอดภัย ข้อความที่ถูกส่งผ่านช่องทางสื่อสารต่างๆควรถูกเข้ารหัส และมีการรวมตัวตนของผู้รับเข้าไปในข้อความด้วย เพื่อให้ข้อความมีความปลอดภัย จะมั่นใจได้ว่าข้อความนั้นต้องการส่งถึงใคร

I. USER -> FINGERPRINT READER
FP, REQUEST
II. FINGERPRINT READER -> MATCHING SERVER
{{LD}skBR, {FP}skTPM, ID, n1, TPM, request}pkMS
III. MATCHING SERVER -> SERVICE
{{result}skMS, ID, request, n2}pkService

ภาพที่ 3 การส่งข้อความในโปรโตคอลที่มีความปลอดภัย

จากภาพที่ 3 แสดงลำดับการส่งข้อความในโปรโตคอลในงานวิจัยนี้ รูปแบบของโปรโตคอลคือเมื่อผู้ใช้ร้องขอบริการจากเครื่องเซิฟเวอร์ จะได้รับการร้องขอกลับให้ทำการพิสูจน์ตัวบุคคลโดยการใช้ลายนิ้วมือ ซึ่งผู้ใช้จะแสดงลายนิ้วมือบนเครื่องอ่าน ถ้าผู้ใช้เชื่อถือเครื่องอ่านลายนิ้วมือที่ถูกตรวจสอบโดย TPM ผู้ใช้จึงวางลายนิ้วมือเพื่อให้เครื่องอ่านทำการอ่านลายนิ้วมือ และเนื่องจากในโปรโตคอลที่ได้ออกแบบไว้นี้ มีสมมุติฐานในด้านอุปกรณ์ในการอ่านมีความสามารถในการตรวจจับความมีชีวิตของข้อมูลชีวภาพที่แสดงต่ออุปกรณ์อ่าน

ลายนิ้วมือดังนั้นโปรโตคอลจึงรับรองได้ว่าลายนิ้วมือที่แสดงต่อระบบเป็นลายนิ้วมือจริงที่ผู้ใช้ได้แสดงต่อระบบจริง และเซิฟเวอร์ที่ทำหน้าที่ในการจับคู่จะสามารถตรวจสอบคุณสมบัตินี้ก่อนที่ทำกระบวนการจับคู่ และเมื่อเซิฟเวอร์ได้รับข้อมูลที่ถูกตรวจสอบความถูกต้องแล้ว เซิฟเวอร์จะทำการตรวจสอบค่า LD จากเครื่องอ่านลายนิ้วมือ ซึ่งจะตรวจสอบความถูกต้องของแหล่งที่มาจาก signature ของเครื่องอ่านลายนิ้วมือ และแหล่งที่มาของข้อมูลลายนิ้วมือจะถูกตรวจสอบเพื่อให้มั่นใจว่าข้อมูลนั้นถูกส่งมาจาก TPM จริง เมื่อตรวจสอบเรียบร้อยแล้วข้อมูลลายนิ้วมือที่แสดงจะถูกจับคู่กับข้อมูลลายนิ้วมือที่ถูกเก็บไว้ การตรวจสอบความใหม่ของข้อมูลสามารถตรวจสอบได้ค่า nonce n1 ซึ่งค่านี้จะต้องไม่ซ้ำกับค่าที่เคยถูกใช้มาก่อน ในการป้องกัน replay attack เมื่อมีการส่งผลลัพธ์การจับคู่จากเครื่องเซิฟเวอร์ จะมีการสร้าง nonce n2 ขึ้นมา และส่งไปพร้อมกับข้อความ นอกเหนือจากนี้ตัวตนของผู้ใช้ และความต้องการในการพิสูจน์ตัวบุคคลจะถูกส่งไปพร้อมกันข้อความเพื่อรับรองจุดประสงค์ในการพิสูจน์ตัวบุคคลของผู้ใช้ และข้อความทั้งหมดจะถูกเข้ารหัสโดยการใช้ public key เพื่อป้องกันให้ข้อความเป็นความลับ

3.2 การประเมินโปรโตคอล

การประเมินคุณสมบัติด้านความปลอดภัยมีความสำคัญมาก เนื่องจากผลลัพธ์จากการประเมินสามารถพิสูจน์คุณสมบัติที่โปรโตคอลให้การรับรองกับผู้ใช้ว่าสามารถให้บริการทางด้านความปลอดภัยตามรายละเอียดที่แสดงไว้

ในการประเมินคุณสมบัติด้านความถูกต้องและคุณสมบัติด้านความปลอดภัยของโปรโตคอลที่งานวิจัยนี้ได้นำเสนอ คณะผู้วิจัยใช้ ProVerif เพื่อใช้เป็นเครื่องมือในการประเมิน ซึ่ง ProVerif เป็นเครื่องมือแบบอัตโนมัติในการพิสูจน์โปรโตคอลเพื่อทำการวิเคราะห์คุณสมบัติด้านความปลอดภัยของโปรโตคอล เมื่อทำการวิเคราะห์ด้วยเครื่องมือนี้ ProVerif จะใช้การจู่โจมแบบ Dolve-Yao เพื่อตรวจสอบข้อบกพร่องหรือความเป็นไปได้ที่เกิดช่องโหว่ทางด้านความปลอดภัย

การจู่โจมแบบ Dolve-Yao ถูกตั้งชื่อตามผู้ที่นำเสนอความคิดนี้ซึ่งเสนอว่าผู้จู่โจมที่ต้องการจู่โจมโปรโตคอลด้านความปลอดภัยจะมีความสามารถในการจัดการเปลี่ยนแปลงข้อความที่ถูกส่งผ่านเน็ตเวร์ค ซึ่งผู้จู่โจมมีความมีความสามารถในการฟัง ดักจับ และ replay ข้อความ ซึ่งการที่เครื่องมือ ProVerif ใช้การจู่โจมในลักษณะนี้ในการวิเคราะห์จะสามารถพิสูจน์และรับรองการวัดคุณสมบัติด้านความปลอดภัยที่ดีขึ้น โดยการวิเคราะห์โดยการใช้ ProVerif คุณสมบัติด้านความปลอดภัย และโปรโตคอลจะถูกจำลองให้อยู่ในรูป Applied Pi Calculus

ในการจำลองรูปแบบของโปรโตคอลใน ProVerif จะถูกจำลองในรูปแบบเดียวกันกับการที่ข้อความถูกส่งต่อในโปรโตคอลที่ได้ออกแบบไว้ ซึ่งโมเดล ProVerif จะถูกจำลองให้ข้อความถูกส่งในช่องทางที่เป็นสาธารณะเพื่อให้ตรวจสอบว่าผู้จู่โจมสามารถเข้าถึงข้อมูลที่ถูกส่งหรือไม่

ทุกๆองค์ประกอบจะถูกจำลองใน ProVerif ในรูปแบบของ process ซึ่งแต่ละ process ทำหน้าที่ในการสร้าง และรับข้อความที่ถูกส่งมา ซึ่ง process ทำหน้าที่ในการพิสูจน์ความถูกต้องของข้อความที่ได้รับว่ามาจากแหล่งกำเนิดที่ถูกต้องหรือไม่ และตรวจสอบว่าข้อความที่ได้รับมาไม่ได้ถูกแทรกแซงโดยผู้จู่โจม ข้อความ

เหล่านั้นจะถูกจากการถอดรหัส ค่า once และตรวจสอบ signature

3.2.1 แบบจำลอง ProVerif

แบบจำลอง ProVerif ของโปรโตคอลที่ได้ออกแบบขึ้นนั้นประกอบไปด้วย 4 process ที่เป็นไปตามโครงสร้างโปรโตคอลที่ได้ออกแบบไว้คือ 1. client 2. fingerprintReader 3. matchingServer 4. service ซึ่งในแต่ละ process หมายถึงการทำงานของ ผู้ใช้ เครื่องอ่านลายนิ้วมือ เครื่องเซิฟเวอร์ และการร้องขอบริการ ตามลำดับ

โดยที่ user process ทำหน้าที่ในการสร้างข้อมูลลายนิ้วมือจองผู้ใช้ และการร้องขอการทำงานจากผู้ใช้ และส่งข้อมูลทั้งสองนี้ไปทางช่องทางสาธารณะที่ชื่อ Ch โดยที่ค่าคีย์ส่วนตัวของเครื่องอ่านลายนิ้วมือจะได้รับอย่างปลอดภัยผ่านทางช่องทางส่วนตัวที่ชื่อ privCh ซึ่งเปรียบเสมือนทำหน้าที่เป็นผู้กระจายคีย์ต่างๆ ให้กับองค์ประกอบที่เกี่ยวข้องกับโปรโตคอล นอกเหนือจากนี้ privCh ยังเป็นช่องทางที่เป็นช่องทางในการรับข้อมูลชีวภาพของผู้ใช้

ในการจำลองการทำงานของเครื่องอ่านลายนิ้วมือ ที่ทำหน้าที่ในการอ่านลายนิ้วมือของผู้ใช้ LD จะถูกสร้างขึ้น และตัวตนของผู้ใช้จะถูกตรวจสอบจากค่า IDk นอกเหนือจากนี้ค่า nonce n1 ถูกสร้างและส่งไปพร้อมกับข้อความเพื่อแสดงถึงความใหม่ของข้อความนั้นๆ หลังจากนั้นข้อความทั้งหมดจะถูกเข้ารหัสโดยคีย์สาธารณะของ matching server และถูกส่งผ่านช่องทางสาธารณะ

จากแนวความคิดของโปรโตคอล เครื่อง matching server ทำหน้าที่ในการพิสูจน์ความถูกต้องของข้อมูลชีวภาพที่ถูกจัดเก็บไว้ กับ ข้อมูลชีวภาพที่ผู้ใช้แสดงมาที่ระบบ และส่งผลลัพธ์ในการจับคู่กลับไป ดังนั้นการจำลองโมเดล ProVerif เครื่อง matching server process จะได้รับคีย์ส่วนตัวอย่างปลอดภัยจากผู้แจกจ่ายคีย์ และเครื่อง matching server จะรอข้อความที่ประกอบไปด้วยข้อมูลลายนิ้วมือที่ถูกอ่านจากเครื่องอ่านลายนิ้วมือ เมื่อได้รับข้อความแล้ว ข้อความนั้นจะถูกถอดรหัสจะตรวจสอบต่อไป

ผลลัพธ์ของการจับคู่จะถูกสร้างขึ้น และเข้ารหัสโดยคีย์ส่วนตัวของ matching server และถูกส่งไปทางช่องทางสาธารณะ และเมื่อ service process ได้รับข้อความจะทำการถอดรหัส เพื่อตรวจสอบผลลัพธ์ และอนุญาตให้ทำงานหรือปฏิเสธการทำงานจากผลลัพธ์การจับคู่นั้น

โมเดลของ main process ทำหน้าที่ในการสร้างคีย์ และส่งคีย์ที่สร้างขึ้นไปทางช่องทางส่วนตัว รวมถึงทำหน้าที่ในการสั่งให้ process อื่นๆทำงานไปพร้อมๆกัน โดยที่เครื่องมือ ProVerif นี้จะทำการสร้างผู้จู่โจมแบบ Dolev-Yao เพื่อทำการตรวจสอบว่าผู้จู่โจมสามารถเข้าถึงความลับที่ต้องการปกปิดหรือไม่ โดยที่โมเดล ProVerif ของโปรโตคอลของงานวิจัยนี้แสดงดังภาพที่ 4

```
let user =
new FP
new request
out(Ch,(FP,request))

let fingerprintReader =
in(privChFR,skFR)
in(Ch,m1)
new LD
new ID
new TPM
new n1
out(Ch,enc((sign((LD),skFR),
   sign((FP),skTPM),ID,n1,TPM,request),pkMS))

let matchingServer =
in(privChMS,skMS)
in(Ch,m2)
 let(m3,m4,IDx,nx1,=TPM,request)=dec(m2,skMS) in
out(Ch,enc((sign(result,skMS),IDx,request,n2),
   pkService))

let service =
in(privChS,skService)
in(Ch,m5)
 let(resultReceived,ID,request,nx2) =
    dec(m5,skService) in

process
new skFR
new skMS
new skService
let pkFR = pk(skFR) in
let pkMS = pk(skMS) in
let pkService = pk(skService) in
out(Ch,pkFR)
out(Ch,pkMS)
out(Ch,pkService)
!(user) || !(fingerprintReader) || !(service)
 || !(matchingServer)
```

ภาพที่ 4 โมเดล ProVerif

3.2.2 การวิเคราะห์โมเดล

ในการวิเคราะห์คุณสมบัติด้านความปลอดภัยของโปรโตคอลที่ได้นำเสนอนั้นถือว่ามีความสำคัญสมบัติด้านความปลอดภัยที่โปรโตคอลตกลงให้บริการนั้นควรต้องถูกรับรองว่าสามารถทำได้อย่างที่ตั้งใจถูกต้องจริง โดยที่โปรโตคอลที่นำเสนอในงานวิจัยนี้ถูกวิเคราะห์โดยใช้ ProVerif ซึ่งจะทำการวิเคราะห์การจู่โจมแบบ Dolve-Yao และการนิยามการจู่โจมใน ProVerif จะถูกจัดการโดยการใช้คำสั่ง query attacker เป็นส่วนในการตรวจสอบ จากโปรโตคอลที่ได้ออกแบบไว้ ส่วนของการวิเคราะห์จะทำหน้าที่ในการตีความคุณสมบัติด้านการเป็นความลับ และคุณสมบัติ replay attack

ในการพิสูจน์คุณสมบัติการเป็นความลับของข้อมูลชีวภาพจะถูกวิเคราะห์โดยการใช้ คำสั่ง

query attacker : FP

ซึ่งในที่นี้ FP หมายถึงข้อมูลลายนิ้วมือของผู้ใช้ที่ถูกแสดงในกระบวนการพิสูจน์ตัวบุคคล ผลลัพธ์ของการวิเคราะห์จากคำสั่งดังกล่าวแสดงให้เห็นว่า ผู้จู่โจมไม่สามารถเข้าถึงข้อมูลลายนิ้วมือของผู้ใช้ได้ ซึ่งสามารถตีความได้ว่าข้อมูลลายนิ้วมือของผู้ใช้นั้นถูกเก็บเป็นความลับอยู่ภายในโปรโตคอล

สำหรับการวิเคราะห์ในเรื่องที่ผู้จู่โจมมีความสามารถในการแสดงข้อมูลชีวภาพของตนเอง และทำการผลลัพธ์การจับคู่ที่ถูกต้องเข้าสู่ระบบเพื่อให้ระบบอนุญาตในเข้าถึงได้ในฐานะเจ้าของตัวจริงได้หรือไม่ โดยใช้คำสั่ง

query attacker : result

ซึ่งคำสั่งดังกล่างสามารถพิสูจน์ได้ว่าผู้จู่โจมมีความสามารถในการเข้าถึงผลลัพธ์ของการจับคู่ และนำกลับมาใช้เสมือนเป็นผลลัพธ์ของการจับคู่ของตัวเองได้หรือไม่ ซึ่งผลลัพธ์การวิเคราะห์จากคำสั่งดังกล่าวนี้แสดงให้เห็นว่าไม่สามารถทำ replay attack ได้ ซึ่งแสดงให้เห็นว่าโปรโตคอลที่งานวิจัยนี้นำเสนอมีความปลอดภัย

บทที่ 4
บทสรุป

งานวิจัยนี้เสนอโปรโตคอลที่มีความปลอดภัยในการนำข้อมูลลายนิ้วมือมาใช้ในการพิสูจน์ตัวบุคคลในสถานการณ์ที่ไม่ควบคุม โดยที่วัตถุประสงค์ของโปรโตคอลมีความต้องการในการรักษาความลับของข้อมูลชีวภาพของผู้ใช้ในที่นี้เน้นในด้านลายนิ้วมือ นอกเหนือจากนี้ยังมีความต้องการในการรับรองว่าวัตถุประสงค์ของผู้ใช้ในการพิสูจน์ตัวบุคคลยังคงอยู่อย่างถูกต้อง ในการนี้โปรโตคอลที่นำเสนอจึงนำ TPM มาใช้ในการป้องกันระบบจากการปลอมแปลงจากผู้จู่โจม ความสามารถในการตรวจสอบของเครื่องอ่านลายนิ้วมือในด้านการตรวจสอบว่าข้อมูลนั้นมากจากผู้ใช้ที่เป็นบุคคลจริงนั้นจะสามารถทำให้ทราบได้ว่าข้อมูลลายนิ้วมือที่แสดงต่อโปรโตตอลนั้นมาจากบุคคลจริงๆ ซึ่งองค์ประกอบเหล่านี้ทำให้สามารถจัดการกับความเสี่ยงทั้งหลายที่อาจจะเกิดขึ้น เพื่อให้ข้อมูลที่ถูกจัดส่งข้อมูลผ่านทางช่องทางสาธารณะนั้นมีความปลอดภัย ข้อความจะถูกเข้ารหัสโดยการใช้คีย์สาธารณะ นอกเหนือจากนี้โปรโตคอลยังรับรองว่าผลลัพธ์การจับคู่ไม่สามารถถูกทำ replay attack และไม่สามารถนำมาใช้ใหม่ได้ในฐานะของเจ้าของตัวจริง

เอกสารอ้างอิง

[1] Matsumoto.T. , et al. : Impact of Artificial "Gummy" Fingers on Fingerprint Systems. Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV (2002).

[2] National Science & Technology Council's. Biometrics Frequently Asked Questions. 2006.

[3] Gerrit Bleumer. Biometric Authentication and Multilateral Security. AT&T Labs-Research, Shannon Laboratory, Florham Park, NJ. 1999.

[4] Antti Stén, Antti Kaseva, Teemupekka Virtanen. Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner. 4th Australian Information Warfare and IT Security Conference 2003. Helsinki University of Technology; 2003.

[5] Soweon Yoon, Jianjiang Feng, and Anil K. Jain. Altered Fingerprints: Analysis and Detection. 2012.

[6] the UK Government Biometrics Working Group (BWG). Biometric Security Concerns. 2003.

[7] Tsutomu Matsumoto,Hiroyuki Matsumoto, Koji Yamada,Satoshi Hoshino. Impact of Artificial Gummy Fingers on Fingerprint Systems. SPIE 2002.

[8] Martin Drahanský, Ralf Nötzel, Wolfgang Funk. Liveness Detection based on Fine Movements. IEEE;2006.

[9] P. Venkata Reddy , AJay Kumar, S. M. K. Rahman, Tanvir Singh Mundra. A new method for Fingerprint Antispoofing using Pulse Oximetry. 2007 Sep27-29.

[10] HP. Authentication technologies and sutiablity to task. 2005.

[11] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A and Minkyu Choi. Biometric Authentication: A Review. Hannam University. 2009.

[12] Chip and Pin Co. : The Chip and Pin Guide. Available at URL http://www.chipandpin.co.uk/reflib/Consumer_digiguide_Post_14_Feb_FINAL.PDF (2012).

[13] Bond, M.: Chip and Pin (EMV) Point-of-Sale Terminal Interceptor. Available at URL http://www.cl.cam.ac.uk/~mkb23/interceptor/ (2007).

[14] Chen, L., Pearson, S., Vamvakas, A.: Trusted Biometric System. Available at URL

http://www.hpl.hp.com/techreports/2002/HPL-2002-185.pdf (2002).

[15] Pearson. S.: How Can You Trust the Computer in Front of You?. Available at URL http://www.hpl.hp.com/techreports/2002/HPL-2002-222.pdf (2002).

[16] Pearson, S.: Trusted Computing Platforms, the Next Security Solution. Available at URL http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf (2002).

[17] Trusted Computing Group.: TPM Specification version 1.2 Parts 1-3. Available at URL http://www.trustedcomputinggroup.org/ resources/ (2009).

[18] Hutchinson, S.: Barclays launches anti-fraud card readers. Available at URL http://www.metro.co.uk/money/46080-barclays-launches-anti-fraud-card-readers (2012).

[19] Out-Laws.com.: Phishing attack evades bank's two-factor authentication. Available at URL http://www.theregister.co.uk/2007/04/19/ phishing_evades_two-factor_authentication/ (2012).

[20] Liveness Detection in Biometric Systems, International biometric group white paper, available at http://www.ibgweb.com/reports/public/reports/ liveness.html (2012).

[21] B. Tan, S. Schuckers, Liveness detection using an intensity based approach in fingerprint scanner, Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21 (2005).

[22] Salaiwarakul, A., Ryan, M.: Verification of Integrity and Secrecy Properties of a Biometric Authentication Protocol. Fourth Information Security Practice and Experience Conference (2008).

[23] Salaiwarakul, A., Ryan, M.: Analysis of a Biometric Authentication Protocol for Signature Creation Application. Third International Workshop on Security (2008).

[24] Polon, T., Sander, S.: Attestation-Based Remote Biometric Authentication. Biometric Symposium: Special Session on Research at the Biometric Consortium Conference (2006).

[25] Dolev, D. and Yao, A.C.: On the Security of Public Key Protocols. In Proceedings of 22nd IEEE Symposium on Foundations of Computer Science (1981).