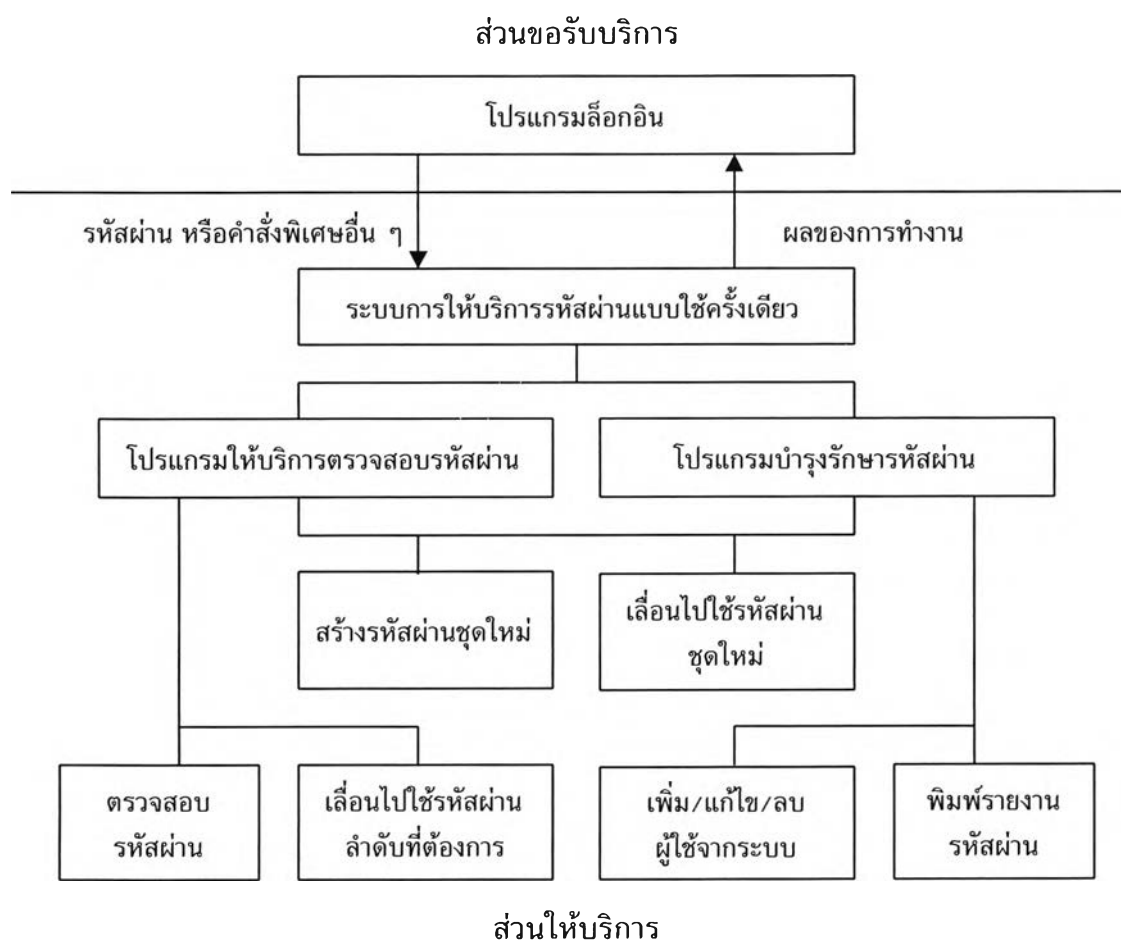


บทที่ 4

การพัฒนาโปรแกรม

เพื่อป้องกันผลร้ายอันอาจเกิดจากการลักลอบเข้าใช้บริการระบบจากผู้ไม่มีสิทธิในการเข้าใช้ที่ทราบรหัสผ่านของผู้อื่น ระบบที่พัฒนาขึ้นโดยคุณพิชญจะทำการการเปลี่ยนรหัสผ่านของผู้ใช้ทุกครั้งที่ใช้ระบบสำเร็จ ดังนั้นจะมีเพียงผู้ใช้ที่มีสิทธิและระบบเท่านั้นที่ทราบรหัสผ่านใหม่ รหัสผ่านเหล่านี้ถูกเก็บไว้เป็นฐานข้อมูลของโปรแกรมบนเครื่องคอมพิวเตอร์ระดับพีซีภายใต้ระบบปฏิบัติการดอสซึ่งทำหน้าที่ให้บริการในการตรวจสอบรหัสผ่าน บำรุงรักษาระบบรหัสผ่าน และพิมพ์รหัสผ่านส่งให้แก่ผู้ใช้ ส่วนโปรแกรมล็อกอินภายใต้ระบบปฏิบัติการยูนิกซ์ยังคงวิธีการใช้เช่นเดิม ลักษณะการติดต่อระหว่างโปรแกรมเป็นแบบผู้ใช้และผู้ให้บริการโดยใช้โพรโตคอลยูพีดี



รูปที่ 4.1 ระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียวของคุณพิชญ

สำหรับงานวิจัยนี้ จะเลือกเพียงบางส่วนของการพัฒนาโปรแกรมมาอธิบายในรายละเอียด เพื่อเป็นตัวอย่างแสดงให้เห็นในส่วนที่ได้รับการปรับปรุง ทั้งนี้ ในส่วนให้บริการรหัสผ่านจะถูกพัฒนา

ชั้นบนระบบปฏิบัติการยูนิกซ์ของลินุกซ์ (Linux) ซึ่งเป็นระบบปฏิบัติการที่กำลังได้รับความนิยมเพิ่มขึ้นในขณะนี้แทนระบบปฏิบัติการดอส เนื่องจากเหตุผลดังต่อไปนี้

ปัญหาจากระบบปฏิบัติการดอส

- 1) ระบบปฏิบัติการดอสกำลังล้าสมัยในขณะนี้
- 2) ซอฟต์แวร์มาตรฐานที่สนับสนุนระบบปฏิบัติการดอสเริ่มหาได้ยาก
- 3) ดอสไม่สนับสนุนการทำงานแบบหลายโปรเซสพร้อมกัน ทำให้ต้องพัฒนาโปรแกรมเรสซิเดนต์หรือโปรแกรมประเภทฝังตัวในหน่วยความจำ ซึ่งส่วนใหญ่นิยมใช้ภาษาแอสเซมบลี (Assembly) ในการเขียนโปรแกรมและลักษณะของภาษาจะยึดติดกับเครื่อง ถ้ามีการเปลี่ยนเครื่องอาจทำให้ระบบมีปัญหาได้

เหตุผลที่เลือกใช้ระบบปฏิบัติการลินุกซ์

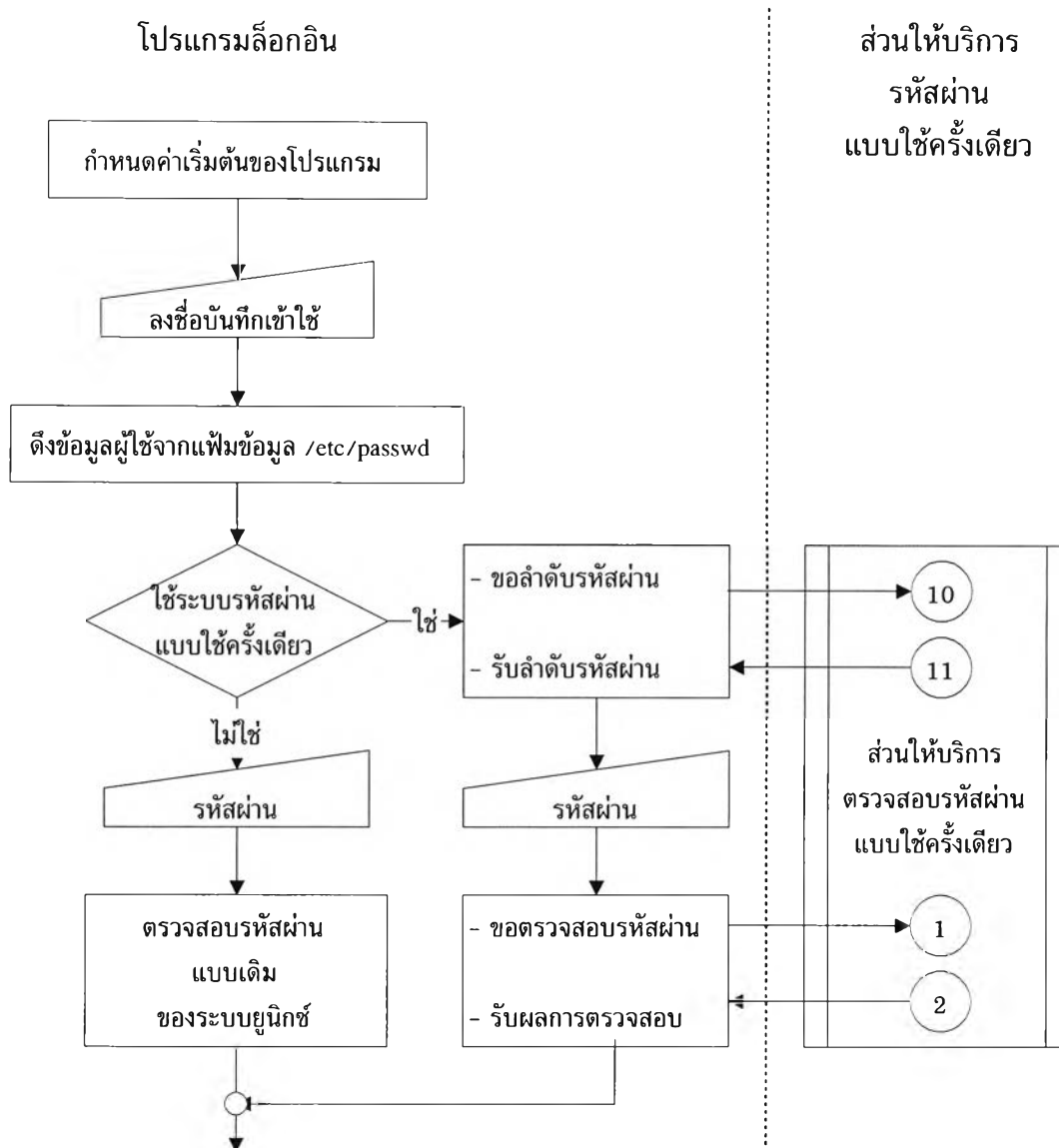
- 1) กำลังได้รับความนิยมเพิ่มขึ้นเรื่อย ๆ
- 2) เป็นระบบปฏิบัติการที่สนับสนุนการทำงานแบบหลายโปรเซสพร้อมกัน
- 3) มีซอฟต์แวร์มาตรฐานที่ไม่ต้องเสียค่าลิขสิทธิ์สนับสนุนมาก
- 4) อุปกรณ์ทางด้านคอมพิวเตอร์ราคาถูกลงทำให้คอมพิวเตอร์ส่วนใหญ่ในปัจจุบันมีทรัพยากรเพียงพอสำหรับรองรับความต้องการของระบบปฏิบัติการลินุกซ์ได้

การพัฒนาโปรแกรมต้นแบบสามารถแบ่งออกเป็น 2 ส่วนหลัก คือ

1. การพัฒนาส่วนขอใช้บริการรหัสผ่าน
2. การพัฒนาส่วนให้บริการรหัสผ่าน

การพัฒนาส่วนขอใช้บริการรหัสผ่าน

ส่วนขอใช้บริการรหัสผ่านหรือโปรแกรมล็อกอิน เพื่อให้โปรแกรมยังคงสามารถทำงานในลักษณะเดิมและสนับสนุนการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว การพัฒนาโปรแกรมจะปรับปรุงในส่วนของขั้นตอนและรูปแบบของกลุ่มข้อมูลที่ใช้ในการสื่อสารสำหรับชื่อลงบันทึกเข้าใช้ที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียวเท่านั้น



รูปที่ 4.2 ขั้นตอนการทำงานบางส่วนของโปรแกรมล็อกอินที่ได้รับการปรับปรุง

จากรูปแสดงขั้นตอนการทำงานบางส่วนของโปรแกรมล็อกอินที่ได้รับการพัฒนาจากระบบของคุณพิษณรูปที่ 2.2 เพื่อให้แสดงหมายเลขลำดับของรหัสผ่านปัจจุบันให้ผู้ใช้ทราบ

สามารถอธิบายขั้นตอนการทำงานของโปรแกรมล็อกอินสำหรับชื่อลงบันทึกเข้าที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว ได้ดังนี้

- 1) กำหนดค่าเริ่มต้นและแสดงข้อความ “login : ” เพื่อให้ผู้ใช้พิมพ์ชื่อลงบันทึกเข้าใช้

ตัวอย่าง

login : _____

2) ตรวจสอบประเภทของชื่อลงบันทึกเข้าจากแฟ้ม “/etc/passwd” โดยสังเกตข้อความในเขตที่สอง ถ้าเท่ากับ “*OTP*” แสดงว่าเป็นชื่อลงบันทึกเข้าที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว

ตัวอย่าง

root:qWBEatueNQ4f2:0:0:root:/root:/bin/bash

bin:*:1:1:bin:/bin:

std1: ytoGfSEUG03TM :12:100:Student:/home/std1:/bin/bash

jkrit:*OTP*:123:100: Jugkrit Nuntapinit:/home/jkrit:/bin/bash

3) กรณีที่เป็นชื่อลงบันทึกเข้าที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว โปรแกรมล็อกอินจะส่งรุ่นควบคุม เวลาที่โปรแกรมสร้างกลุ่มข้อมูล ชื่อเซิร์ฟเวอร์ ชื่อลงบันทึกเข้า อัลกอริทึมที่ใช้ในการสร้างหรือตรวจสอบรหัสผ่าน ชนิดการเข้ารหัส และประเภทของคำร้องขอทราบหมายเลขลำดับของรหัสผ่านปัจจุบัน ตามรูปแบบของกลุ่มข้อมูล

ตัวอย่าง

2 Byte 10 Byte 1 byte 17 Byte 1 Byte 4 Byte 1 Byte 1 Byte							
100	923756364	17	OtpC1.chula.ac.th	4	jkrit	0	0
1 Byte 1 Byte 0 Byte							
10	0						

4) รับข้อมูลที่ส่งกลับจากส่วนบริการตรวจสอบรหัสผ่าน ทั้งนี้ ข้อมูลในฟิลด์ของเวลาที่สร้างรหัสจะเปลี่ยนเป็นของส่วนให้บริการตรวจสอบรหัสผ่าน การตอบกลับจะถูกเปลี่ยนเป็นการส่งหมายเลขลำดับของรหัสผ่านปัจจุบัน และหมายเลขลำดับของรหัสผ่านปัจจุบันจะถูกจัดส่งมาให้ในฟิลด์ข้อมูลที่เกี่ยวข้อง

ตัวอย่าง

2 Byte 10 Byte 1 byte 17 Byte 1 Byte 4 Byte 1 Byte 1 Byte							
100	923756370	17	OtpC1.chula.ac.th	4	jkrit	0	0
1 Byte 1 Byte 2 Byte							
11	2	77					

5) หลังจากได้รับหมายเลขลำดับของรหัสผ่านปัจจุบันแล้ว โปรแกรมล็อกอินจะแสดงหมายเลขดังกล่าวให้ผู้ผู้ใช้เห็นเพื่อให้พิมพ์รหัสผ่านลำดับที่ตรงกับหมายเลขนั้น

ตัวอย่าง

login: jkit

otp 77

Password: _____

6) โปรแกรมล็อกอินจะส่งเวลาที่สร้างกลุ่มข้อมูลที่ถูกสร้างและส่งมาจากส่วนให้บริการตรวจสอบรหัสผ่านกลับไปเพื่อเป็นการยืนยันว่าเป็นโปรเซสที่ส่วนให้บริการตรวจสอบรหัสผ่านกำลังจ้องหมายเลขลำดับของรหัสผ่านปัจจุบันไว้ให้ พร้อมประเภทของคำร้องขอตรวจสอบรหัสผ่านที่ถูกส่งมาในฟิลด์ของข้อมูลที่เกี่ยวข้อง

ตัวอย่าง

2 Byte	10 Byte	1 byte	17 Byte	1 Byte	4 Byte	1 Byte	1 Byte
100	923756370	17	OtpC1.chula.ac.th	4	jkit	0	0
1 Byte	1 Byte	6 Byte					
1	6	Afx3ty					

7) รับข้อมูลที่ส่งกลับจากส่วนบริการตรวจสอบรหัสผ่าน ซึ่งส่วนบริการรหัสผ่านจะส่งเวลาที่สร้างกลุ่มข้อมูลที่ถูกสร้างโดยโปรแกรมล็อกอินกลับมาให้เพื่อเป็นการยืนยันเช่นกัน นอกจากนั้นการตอบกลับจะถูกเปลี่ยนไปเป็นการรายงานผลการตรวจสอบรหัสผ่านพร้อมกับผลการตรวจสอบรหัสผ่านที่ถูกจัดส่งมาให้ในฟิลด์ข้อมูลที่เกี่ยวข้อง

ตัวอย่าง

2 Byte	10 Byte	1 byte	17 Byte	1 Byte	4 Byte	1 Byte	1 Byte
100	923756364	17	OtpC1.chula.ac.th	4	jkit	0	0
1 Byte	1 Byte	2 Byte					
2	2	Ok					

8) โปรแกรมล็อกอินจะนำผลที่ได้รับมาพิสูจน์ตัวจริงขอผู้ใช้ เพื่ออนุญาตให้เข้าใช้ระบบต่อไป

สำหรับคำสั่งพิเศษอื่น ๆ เช่น การเลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป ขั้นตอนการทำงานของโปรแกรมล็อกอินยังคงคล้ายกัน แตกต่างกันเพียงวัตถุประสงค์ที่ใช้ในการรับส่งเท่านั้น

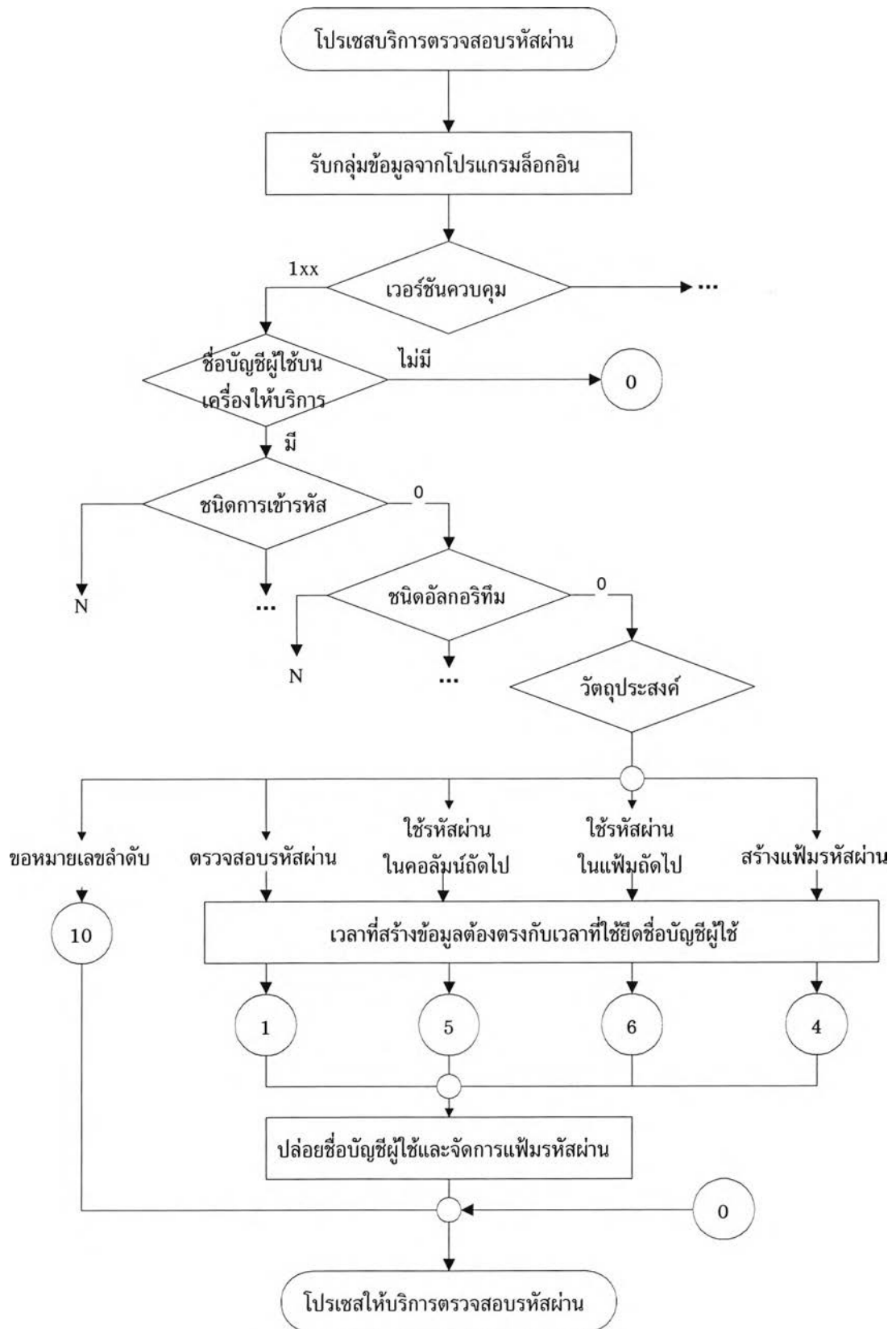
การพัฒนาส่วนให้บริการรหัสผ่าน

การพัฒนาส่วนให้บริการรหัสผ่านถูกแบ่งได้เป็น 2 ส่วน ดังนี้

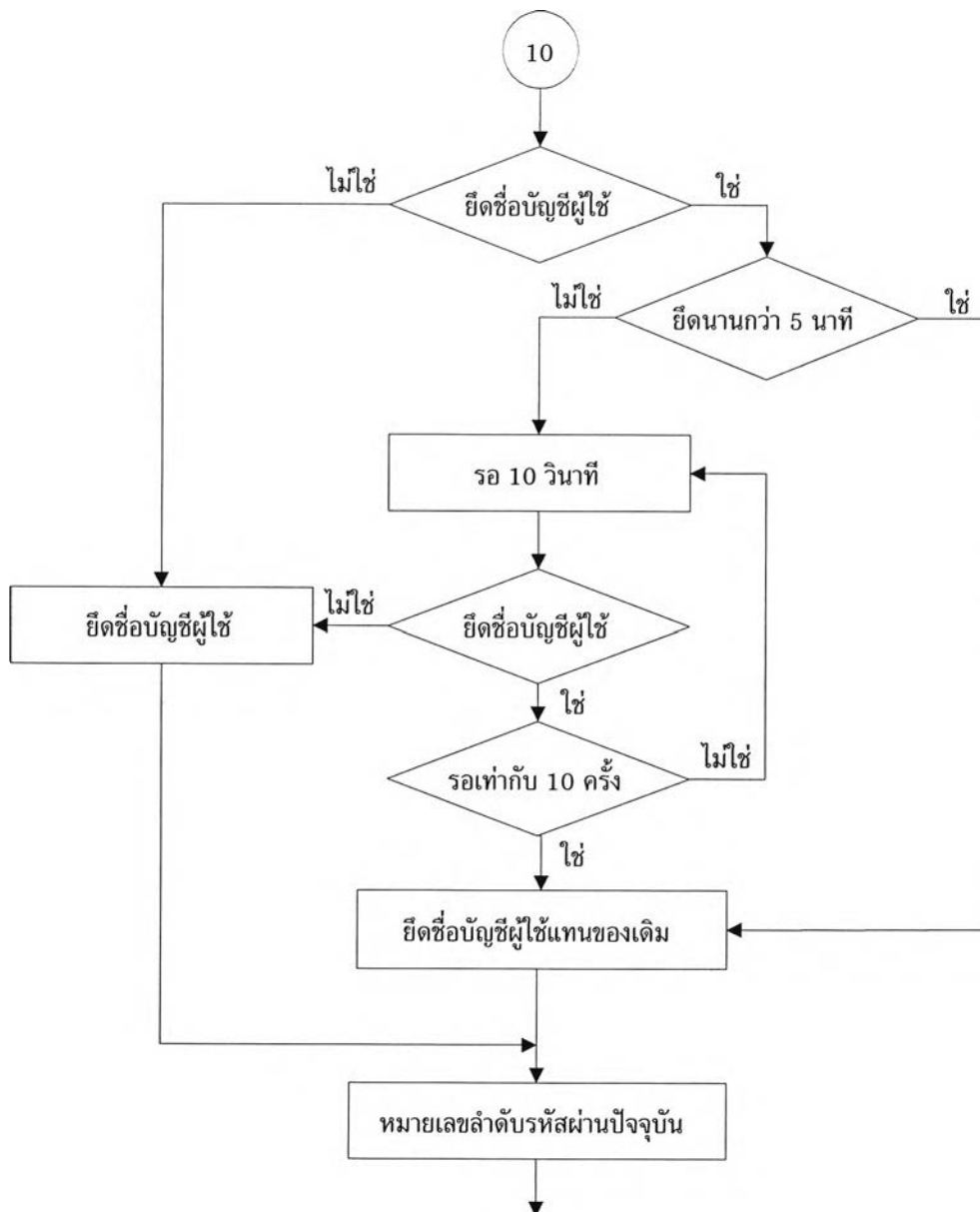
- 1) การพัฒนาส่วนให้บริการตรวจสอบรหัสผ่าน
- 2) การพัฒนาส่วนบำรุงรักษารหัสผ่าน

1. การพัฒนาส่วนให้บริการตรวจสอบรหัสผ่าน

ขั้นตอนการทำงานในส่วนให้บริการตรวจสอบรหัสผ่าน ได้ปรับปรุงจากระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ ในบทที่ 3 ให้มีความซับซ้อนมากขึ้น ทั้งนี้เนื่องมาจากการปรับปรุงรูปแบบของกลุ่มข้อมูลให้สามารถรองรับพัฒนาการที่หลากหลายของรหัสผ่านในอนาคต เช่น เพิ่มการตรวจสอบรุ่นควบคุม เพิ่มทางเลือกในการเข้ารหัสข้อมูล และทางเลือกในการสร้างและตรวจสอบรหัสผ่าน เป็นต้น ทำให้สามารถเลือกใช้วิธีการที่เหมาะสม ปลอดภัยกับระบบได้ สามารถแสดงขั้นตอนการทำงานที่แตกต่างไปจากเดิมได้ ดังรูปที่ 4.3 และรูปที่ 4.4 ตามลำดับ



รูปที่ 4.3 ขั้นตอนการทำงานของส่วนให้บริการตรวจสอบรหัสผ่านที่ได้รับการปรับปรุง



รูปที่ 4.4 แสดงรายละเอียดขั้นตอนการขอหมายเลขลำดับรหัสผ่านปัจจุบัน

สามารถอธิบายขั้นตอนการทำงานของส่วนให้บริการตรวจสอบรหัสผ่านที่ได้รับการปรับปรุงได้ดังนี้

1.1 การขอหมายเลขลำดับของรหัสผ่านปัจจุบัน

ขั้นตอนการขอหมายเลขลำดับรหัสผ่านปัจจุบันสามารถอธิบายได้ดังนี้

1) รับกลุ่มข้อมูลที่ส่งมาจากโปรแกรมล็อกอิน

2) ตรวจสอบรุ่นจากข้อมูลที่รับมาเพื่อส่งผ่านการทำงานต่อไปยังส่วนที่สามารถจัดการกับรุ่นนั้นได้

3) นำชื่อลงบันทึกเข้าและชื่อเซิร์ฟเวอร์รวมกันเป็นเงื่อนไขสำหรับค้นหาชื่อบัญชีผู้ใช้บนเครื่องให้บริการ เพื่อใช้แทนชื่อลงบันทึกเข้าใช้และชื่อเซิร์ฟเวอร์ที่รับมาในการดำเนินขั้นตอนต่อไป

4) ตรวจสอบชนิดการเข้ารหัสของข้อมูลที่รับมา

5) ตรวจสอบชนิดอัลกอริทึมที่ใช้เพื่อการตรวจสอบและบำรุงรักษาผ่าน

6) ตรวจสอบประเภทของคำร้องขอของโปรแกรมล็อกอินจากข้อมูลที่รับมา (สำหรับส่วนนี้ สมมุติว่าประเภทของคำร้องขอหมายเลขลำดับของรหัสผ่านปัจจุบัน)

7) ตรวจสอบการยึดชื่อบัญชีผู้ใช้ มีขั้นตอนดังนี้

7.1) ไม่มีโปรเซสอื่นล็อกอยู่ ส่วนให้บริการจะใช้เวลาของระบบร่วมกับเวลาที่ถูส่งมายึดชื่อบัญชีผู้ใช้นั้น

7.2) มีโปรเซสอื่นล็อกอยู่ ส่วนให้บริการจะใช้เวลาของระบบเปรียบเทียบกับเวลาของระบบที่ใช้ล็อกโปรเซสก่อนหน้าเพื่อดูว่าเกินเวลาที่กำหนดไว้หรือไม่

7.2.1) เกิน ส่วนให้บริการจะยกเลิกโปรเซสเดิมและยึดชื่อบัญชีผู้ใช้ด้วยโปรเซสใหม่แทน

7.2.2) ไม่เกิน ส่วนให้บริการจะรอชั่วระยะเวลาหนึ่งแล้วจึงตรวจสอบใหม่อีกครั้ง โดยจะทำซ้ำเช่นนี้จนกว่าโปรเซสเดิมปลดล็อกถึงจะยึดชื่อบัญชีผู้ใช้นั้นหรือทำซ้ำจนกระทั่งถึงจำนวนครั้งที่กำหนดจึงยกเลิกโปรเซสเดิมและยึดชื่อบัญชีผู้ใช้ด้วยโปรเซสใหม่แทน

8) ดึงข้อมูลหมายเลขลำดับของรหัสผ่านปัจจุบันและส่งข้อมูลไปให้โปรแกรมล็อกอินที่ขอมา

9) จบขั้นตอนของการขอหมายเลขลำดับของรหัสผ่านปัจจุบันในส่วนบริการ

1.2 การตรวจสอบรหัสผ่านปัจจุบัน

สำหรับขั้นตอนการตรวจสอบรหัสผ่านจะเหมือนกันกับของคุณพิษณุ แตกต่างกันเพียงขั้นตอนก่อนการตรวจสอบและหลังการตรวจสอบรหัส ดังนี้

1) ขั้นตอนที่ 1-6 จะทำซ้ำกับการขอหมายเลขลำดับรหัสผ่านปัจจุบัน เพียงแต่ประเภทของคำร้องขอเปลี่ยนเป็นการขอตรวจสอบรหัสผ่านแทน

2) ส่วนให้บริการจะอนุญาตให้โปรเซสที่ถูกส่งมาจากโปรแกรมล็อกอินที่เวลาที่ส่งมาตรงกับเวลาที่ใช้ยึดชื่อบัญชีผู้ใช้ในขณะนั้นเท่านั้นที่สามารถทำขั้นตอนต่อไปได้

3) ตรวจสอบรหัสผ่าน ถ้ารหัสผ่านถูกต้องส่วนบริการจะเปลี่ยนหมายเลขลำดับของรหัสผ่านเป็นหมายเลขถัดไป

- 4) ปลออย (unlock) ชื่อบัญชีผู้ใช้ และส่งผลการตรวจสอบรหัสผ่านพร้อมกับเวลาที่กลุ่มข้อมูลถูกสร้างจากโปรแกรมล็อกอินเพื่อเป็นการยืนยัน
- 5) จบขั้นตอนของการขอตรวจสอบรหัสผ่านในส่วนบริการ

สำหรับการให้บริการอื่น ๆ เช่น การเลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป วิธีการที่ใช้จัดการยังเหมือนกันกับของคุณพิชญ ส่วนขั้นตอนการทำงานจะไม่แตกต่างไปจากการขอตรวจสอบรหัสผ่านที่กล่าวมา

2. การพัฒนาส่วนบำรุงรักษารหัสผ่าน

การพัฒนาในส่วนของการบำรุงรักษารหัสผ่านเนื้อหาโดยหลักไม่แตกต่างไปจากเดิมของคุณพิชญในบทที่ 5 มากนัก จะมีเพิ่มเพียงส่วนของการกำหนดชื่อลงบันทึกเข้าใช้และชื่อเซิร์ฟเวอร์ให้กับชื่อบัญชีผู้ใช้เท่านั้น

ชื่อลงบันทึกเข้า	ชื่อเซิร์ฟเวอร์	ชื่อบัญชีผู้ใช้
------------------	-----------------	-----------------

ตาราง 4.1 แสดงรูปแบบของแฟ้มข้อมูลการกำหนดบัญชีผู้ใช้ระบบ

ตัวอย่าง

jkit	OtpC1.chula.ac.th	jugkrit
jkit	OtpC2.chula.ac.th	jugkrit
jkit	OtpC3.chula.ac.th	jkit
root	OtpC1.chula.ac.th	jugkrit

จากที่กล่าวมาในบทนี้แสดงให้เห็นขั้นตอนการทำงานของโปรแกรมล็อกอินสำหรับชื่อลงบันทึกเข้าใช้ที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว ลักษณะข้อมูลที่ใช้สื่อสารระหว่างส่วนขอใช้และส่วนให้บริการ ขั้นตอนการขอหมายเลขลำดับของรหัสผ่าน ขั้นตอนการตรวจสอบรหัสผ่าน และแฟ้มข้อมูลหลักที่ใช้กำหนดบัญชีผู้ใช้ สำหรับบทต่อไปจะเป็นการทดสอบระบบรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับการปรับปรุง