



SECURE CHAT

CP422011 INTRODUCTION TO COMPUTER NETWORKING
สาขา ความมั่นคงปลอดภัยไซเบอร์

EXAMPLE

อาจารย์ที่ปรึกษา ศ.ดร. จักรชัย ไสอินทร์

หลักการและเหตุผล

โครงการนี้จัดทำขึ้นเพื่อศึกษาและพัฒนา แอปพลิเคชันแชทแบบ Real-time ที่ใช้เทคโนโลยี การเข้ารหัสแบบต้นทางถึงปลายทาง (End-to-End Encryption) ร่วมกับเทคโนโลยีสื่อสารสมัยใหม่ เช่น WebSocket, WebRTC และ Socket.IO เพื่อให้ผู้ใช้สามารถ สนทนา แลกเปลี่ยนข้อมูล หรือโทรแบบวิดีโอได้อย่างปลอดภัย พร้อมนำเสนอแนวทางพัฒนาระบบที่มีความทันสมัย ตอบสนองใจ และ คำนึงถึงความเป็นส่วนตัวสูงสุด

วัตถุประสงค์

- พัฒนาแอปพลิเคชันแชทที่ปลอดภัยด้วย E2EE
- ออกแบบระบบ Real-time โดยใช้ WebSocket (Socket.IO)
- เพิ่มฟีเจอร์โซเชียล เช่น ฟีดข่าว โพสต์ และระบบเพื่อน
- พัฒนาแอปพลิเคชันแบบ Single Page Application (SPA)
- ศึกษาการใช้ WebRTC สำหรับเสียงและวิดีโอคอลแบบ Peer-to-Peer

ขอบเขตการศึกษา

- ลงทะเบียน/เข้าสู่ระบบอย่างปลอดภัย
- แชท 1-1 และแชทกลุ่มแบบเข้ารหัส
- การแจ้งเตือน Real-time และสถานะออนไลน์
- ฟีดโซเชียล (โพสต์ ฟีด กดไลค์ แสดงความคิดเห็น)
- ระบบเพื่อนและการโทรเสียง/วิดีโอแบบ P2P
- ใช้งานผ่านเว็บเบราว์เซอร์ (ไม่ต้องติดตั้งแอป)

วิธีการดำเนินงาน

โครงการนี้ใช้แนวคิด Client-Server โดยแบ่งการทำงานออกเป็น 3 ส่วนหลัก:

Client: พัฒนาโดยใช้ React.js และ Web Crypto API สำหรับเข้ารหัสข้อมูลก่อนส่ง

Server: ใช้ Node.js และ Socket.IO สำหรับสื่อสารแบบ Real-time

Database: ใช้ MariaDB จัดเก็บข้อมูลที่ถูกรับหรือส่งอย่างปลอดภัย

ขั้นตอนหลักประกอบด้วย

ออกแบบและพัฒนาระบบให้รองรับการสื่อสารแบบ Real-time

สร้างระบบเข้ารหัส End-to-End เพื่อปกป้องข้อมูลผู้ใช้

ทดสอบการทำงาน เช่น การแชท การโทร และการส่งข้อมูลแบบเข้ารหัส

ระบบที่ได้สามารถสื่อสารได้อย่างปลอดภัย ลื่นไหล และรักษาความปลอดภัย

เป็นส่วนต่อของผู้ใช้ได้อย่างมีประสิทธิภาพ

เครื่องมือซอฟต์แวร์

- Frontend: React.js, React Router, Tailwind CSS
- Backend & Database: MariaDB
- Communication: WebSocket, Socket.IO, WebRTC
- Security: Web Crypto API,
- End-to-End Encryption (E2EE)

ฟังก์ชัน

- การจัดการผู้ใช้: สมัครสมาชิก เข้าสู่ระบบ และแก้ไขโปรไฟล์ได้อย่างปลอดภัย พร้อมระบบสร้างกฎและเข้ารหัสอัตโนมัติสำหรับแต่ละผู้ใช้
- ระบบแชท: สนทนาแบบ 1-ต่อ-1 และแบบกลุ่ม ข้อความทั้งหมดถูกเข้ารหัสแบบ End-to-End เพื่อความเป็นส่วนตัวสูงสุด
- การสื่อสารแบบ Real-time: ใช้ WebSocket เชื่อมต่อโดยตรงระหว่างผู้ใช้ ให้ภาพและเสียงคมชัด ทันท่วงที
- ฟีดโซเชียล: สามารถโพสต์ ฟีดข่าว กดไลค์ แสดงความคิดเห็น ค้นหาและเพิ่มเพื่อนได้ เพื่อเสริมการสื่อสารในรูปแบบโซเชียล
- ความปลอดภัยของระบบ: ใช้ HTTPS และ SSL/TLS ป้องกันการดักฟัง พร้อมเข้ารหัสข้อมูลทุกครั้งก่อนส่งผ่านเครือข่าย
- Client ผู้ใช้เลือกไฟล์ → ปรวิพินด้วย URL.createObjectURL(file) → แปลงไฟล์เป็น Base64 แล้วส่งไปเซิร์ฟเวอร์ → ขอไฟล์กลับผ่าน secure endpoint → รับเป็น Blob → แสดงผล/ดาวน์โหลดไฟล์ด้วย URL.createObjectURL(blob).
- Server ตรวจสอบ/คิวคิว (ต้องเป็นเพื่อนหรือสมาชิกกลุ่มที่อนุญาต) → รับ Base64 → แปลงเป็น Buffer → เซพเป็นไฟล์บนดิสก์ (ตั้งชื่อใหม่) → ให้บริการ secure download: ตรวจสอบสิทธิ์อีกครั้ง แล้วส่งไฟล์พร้อม Header ที่ถูกต้อง.

สรุป

โครงการ "เว็บแอปพลิเคชันโซเชียลแชทแบบ Real-time" ที่มีการเข้ารหัสข้อมูลแบบต้นทางถึงปลายทาง พัฒนาได้สำเร็จและใช้งานได้จริงตามเป้าหมาย จุดเด่นของระบบคือ ความปลอดภัยของข้อมูล การสื่อสารแบบ Real-time และส่วนติดต่อผู้ใช้ที่ใช้งานง่าย การเข้ารหัสข้อมูลช่วยให้การสื่อสารมีความเป็นส่วนตัวและป้องกันการดักฟังจากบุคคลภายนอกได้อย่างมีประสิทธิภาพ ระบบนี้สามารถต่อยอดเป็นแพลตฟอร์มการสื่อสารที่ใช้ได้จริงในองค์กรหรือชุมชน และยังช่วยยกระดับความเข้าใจด้านความปลอดภัยทางไซเบอร์และเทคโนโลยีสื่อสารยุคใหม่ให้แก่ผู้พัฒนาอีกด้วย

GROUP 9 Section 4

นายคณกร พันธุ์ชา รหัสนักศึกษา 673380366-2
 นายจิรวัฒน์ วงษ์คำจันทร์ รหัสนักศึกษา 673380367-0
 นายสทพล พรหมศร รหัสนักศึกษา 673380383-2
 นายชัชฌาญพงศ์ จิตมาลย์ รหัสนักศึกษา 673380541-0
 นายนันทสิทธิ์ ศรีสลับ รหัสนักศึกษา 673380547-8
 นายเสกฐรูดิ บุญสุภาพร รหัสนักศึกษา 673380570-3



COLLEGE OF
COMPUTING
KHON KAEN UNIVERSITY

