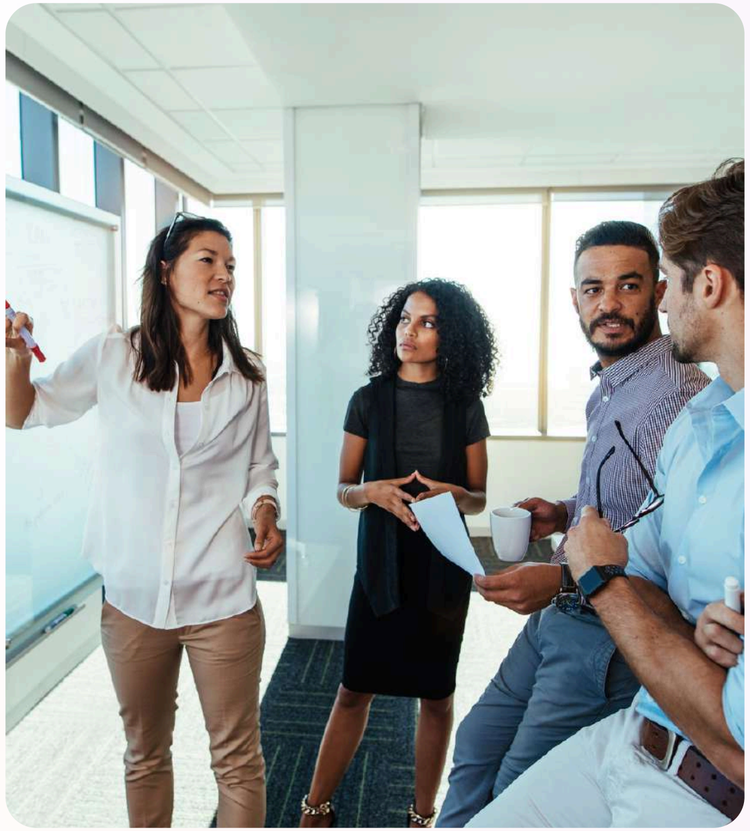
Universitas Pertamina

Cryptography and Cybersecurity Course

Smart Attendance System With RFID (IoT)

Presented By Group 7

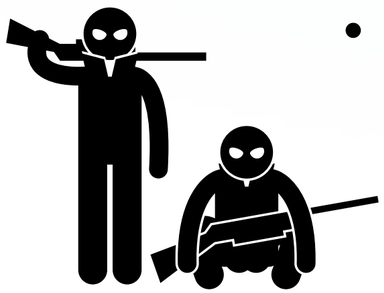


Anggota Kelompok

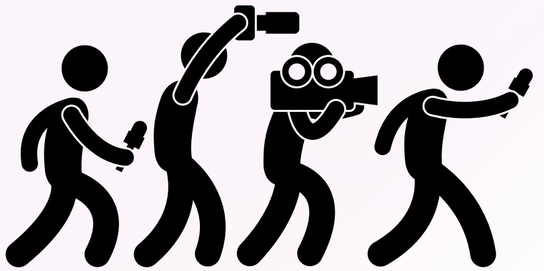
105222007 Bambang Istijab
105222008 Ni Putu Merta Bhuana
105222022 Jihan Fadila
105222023 Senopati Baruna Pasha

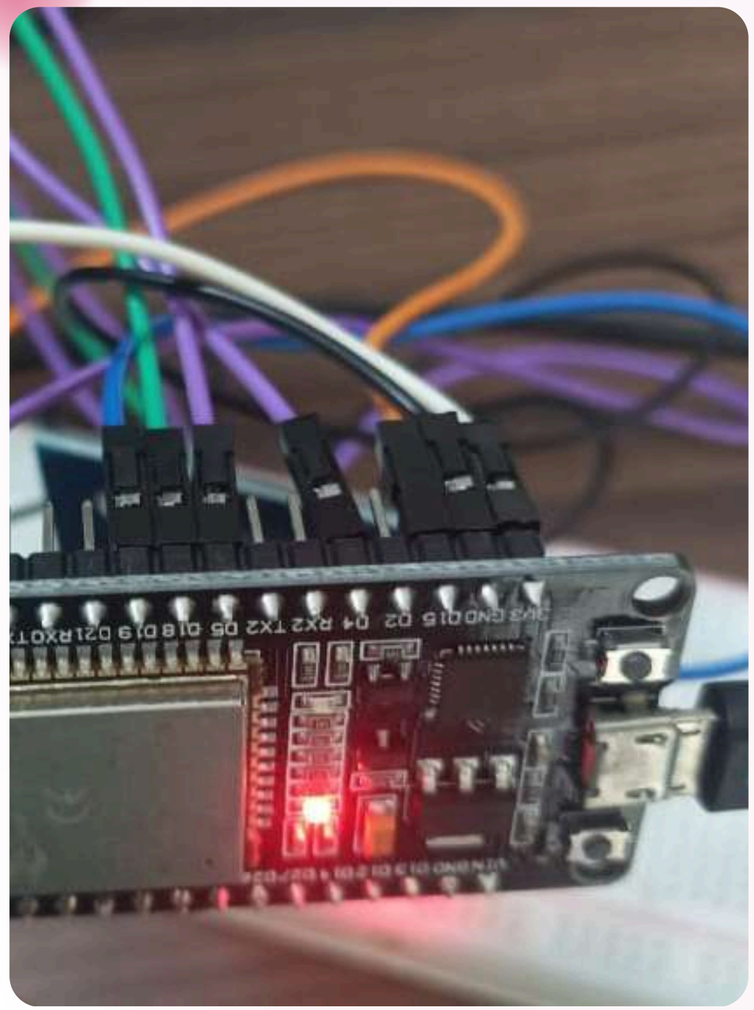
Latar Belakang

Keamanan informasi mengenai waktu absen sangat penting bagi individu yang membutuhkan perlindungan terhadap data pribadi, seperti petinggi pemerintah atau individu yang terlibat dalam dunia bisnis dan politik.



- Contoh Kasus:
  - Seorang ketua DPR yang membutuhkan kerahasiaan mengenai waktu tap terakhir untuk menghindari media yang akan mengejar informasi tersebut.
  - Mafia yang perlu menyembunyikan keberadaannya agar tidak diketahui musuh dan menghindari ancaman pembunuhan.
- Dengan waktu absen yang terenskripsi, informasi mengenai keberadaan seseorang tidak akan terdeteksi secara real-time, yang meningkatkan tingkat privasi dan keamanan.





Penggunaan IoT dengan RFID

- Setiap pengguna dilengkapi dengan ID Card yang memiliki ID unik, yang digunakan untuk melakukan tap pada RFID reader.

Proses Absensi:

- Pengguna melakukan tap dengan kartu ID mereka pada RFID reader untuk mencatat waktu kehadiran mereka.
- Data waktu dan ID pengguna kemudian dikirimkan ke server untuk diproses dan disimpan.
- Informasi waktu akan dienkripsi menggunakan algoritma kriptografi untuk melindungi data dari potensi kebocoran.

Alur Program IoT yang Terenkripsi

Membaca RFID

Menggunakan RFID Reader untuk mendeteksi ID unik dari ID Card

Enkripsi

Data waktu akan dienkripsi menggunakan algoritma DES (Data Encryption Standard) untuk mencegah akses tidak sah.

Proses Pengiriman & Penyimpanan Data

Data waktu kehadiran yang telah terenkripsi akan dikirimkan database.

Dekripsi

Melakukan dekripsi dari data waktu yang sudah terenkripsi, dan ditampilkan pada web

Algoritma DES

Apa itu Algoritma DES?

Algoritma kriptografi simetris klasik yang digunakan untuk mengamankan data dengan cara mengenkripsi dan mendekripsi menggunakan kunci yang sama. DES bekerja dengan membagi data menjadi blok 64-bit dan menjalankan proses enkripsi melalui 16 ronde yang melibatkan operasi bit-level seperti permutasi, substitusi melalui S-Box, ekspansi, dan XOR dengan subkey.

Alasan mengapa menggunakan DES

Dapat diimplementasikan secara manual tanpa membutuhkan library eksternal memiliki proses yang lebih ringan dibanding algoritma modern seperti AES, dan lebih cepat serta praktis dibanding RSA yang memerlukan perhitungan eksponensial besar. DES juga cocok untuk sistem berbasis lokal seperti localhost PHPMyAdmin, khususnya untuk mengamankan data seperti timestamp kehadiran yang bersifat sensitif

Perbandingan DES

dengan algoritma lainnya

Algoritma DES	Algoritma AES	Algoritma RSA
Lebih mudah diimplementasikan secara manual	AES memiliki struktur kompleks (banyak tahapan rumit)	RSA membutuhkan operasi matematika besar (modulo & eksponen)
Lebih ringan dan cepat untuk data kecil	AES cenderung lebih berat secara komputasi	RSA sangat lambat untuk enkripsi data kecil
Tidak membutuhkan library khusus	sulit dilakukan manual tanpa pustaka matematika	sulit dilakukan manual tanpa pustaka matematika

Demo

Kesimpulan

Sistem IoT dengan RFID ini, yang dilengkapi dengan enkripsi DES, memastikan bahwa informasi waktu kehadiran tidak dapat diakses oleh pihak yang tidak berwenang.

Sistem ini dapat diadaptasi untuk berbagai sektor, baik itu pemerintahan, bisnis, maupun untuk keperluan pribadi, guna menjaga kerahasiaan dan keamanan data.

Universitas Pertamina

THANK YOU