

Rancang Bangun Smart Handle Adaptif Berbasis Internet of Things (IoT) dengan Metode Mel-Frequency Cepstral Coefficients (MFCC) untuk Autentikasi Suara pada Sistem Keamanan Ruangan

Candra Imam Syahputra¹, Ajar Rohmanu², Ahmad Yakub³

¹ Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Panca Sakti Bekasi, Bekasi, Indonesia

² Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Panca Sakti Bekasi, Bekasi, Indonesia

³ Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Panca Sakti Bekasi, Bekasi, Indonesia

*Corresponding email:

candra.imam112@gmail.com ¹ ajarrohmanu@gmail.com ²

ahmadyakubkomarudin@gmail.com ³

ABSTRAK

Penelitian ini bertujuan merancang dan membangun Smart Handle Adaptif berbasis Internet of Things (IoT) dengan metode Mel-Frequency Cepstral Coefficients (MFCC) untuk autentikasi suara pada sistem keamanan ruang dokumen di PT Trima Laksana Jaya Pratama. Permasalahan utama berawal dari sistem keamanan ruang yang masih menggunakan kunci konvensional sehingga berisiko diduplikasi, hilang, atau disalahgunakan, serta belum tersedia mekanisme monitoring akses secara real-time. Penelitian menggunakan pendekatan kualitatif dengan metode pengembangan model (model development) melalui tahapan penelitian pendahuluan, analisis kebutuhan, perancangan model menggunakan Unified Modeling Language (UML), validasi dan telaah pakar (expert judgement), hingga pengujian produk. Perangkat keras yang digunakan terdiri atas mikrokontroler ESP32, sensor mikrofon, Relay, dan Solenoid Door Lock, sedangkan pemrosesan suara dan ekstraksi ciri MFCC dijalankan pada server melalui tahapan pre-emphasis, framing, windowing, Fast Fourier Transform (FFT), Mel Filter Bank, dan Discrete Cosine Transform (DCT). Sistem juga diintegrasikan dengan Telegram Bot sebagai media notifikasi dan monitoring aktivitas akses secara real-time. Hasil pengujian menunjukkan bahwa seluruh komponen sistem berfungsi sesuai rancangan, pengguna terdaftar berhasil dikenali dan memperoleh akses, sedangkan pengguna tidak terdaftar berhasil ditolak dengan kondisi pintu tetap terkunci. Rekapitulasi tiga kasus uji fungsional menghasilkan Pass Rate sebesar 100%. Temuan ini menunjukkan kelayakan teknis awal model, sekaligus menegaskan bahwa integrasi MFCC dan IoT dapat mendukung sistem keamanan akses ruangan yang lebih adaptif dan informatif. Penerapan pada skala operasional tetap memerlukan pengujian lanjutan pada jumlah kasus yang lebih besar dan kondisi lingkungan yang lebih beragam.

Kata Kunci: Internet of Things (IoT); Mel-Frequency Cepstral Coefficients (MFCC); autentikasi suara; Smart Handle; ESP32

ABSTRACT

This study aims to design and build an Adaptive Smart Handle based on the Internet of Things (IoT) using the Mel-Frequency Cepstral Coefficients (MFCC) method for voice authentication in the document room security system at PT Trima Laksana Jaya Pratama. The main issue stems from the room security system that still relies on conventional keys, which are prone to duplication, loss, or misuse, and from the absence of a real-time access monitoring mechanism. The research applies a qualitative approach through a model development method, covering preliminary research, needs analysis, model design using the Unified Modeling Language (UML), validation and expert judgement, and product testing. The hardware consists of an ESP32 microcontroller, a microphone sensor, a Relay, and a Solenoid Door Lock, while voice processing and MFCC feature extraction are carried out on a server through pre-emphasis, framing, windowing, Fast Fourier Transform (FFT), Mel Filter Bank, and Discrete Cosine Transform (DCT) stages. The system is also integrated with a Telegram Bot as a real-time notification and monitoring medium. The test results show that all system components function according to the design, registered users are successfully recognized and granted access, while unregistered users are rejected with the door remaining locked. The recapitulation of three functional test cases produced a 100% Pass Rate. These findings indicate the initial technical feasibility of the model and confirm that integrating MFCC and IoT can support a more adaptive and informative room access security system. Operational-scale deployment still requires further testing with a larger number of cases and more varied environmental conditions.

Keywords: Internet of Things (IoT); Mel-Frequency Cepstral Coefficients (MFCC); voice authentication; Smart Handle; ESP32

PENDAHULUAN

Transformasi teknologi digital mendorong berbagai inovasi pada bidang sistem keamanan. Sistem keamanan konvensional berupa kunci mekanik masih memiliki kelemahan karena mudah diduplikasi, hilang, atau disalahgunakan oleh pihak yang tidak berwenang, sehingga dibutuhkan sistem keamanan yang lebih adaptif dan memberikan tingkat perlindungan lebih tinggi.

Salah satu pendekatan yang banyak diterapkan adalah autentikasi biometrik, seperti sidik jari, wajah, dan suara. Autentikasi suara menarik untuk dikembangkan karena bersifat unik, sulit ditiru secara persis, dan memungkinkan interaksi tanpa kontak fisik. Metode Mel-Frequency Cepstral Coefficients (MFCC) merupakan teknik ekstraksi ciri yang umum digunakan pada pengolahan sinyal suara karena mampu merepresentasikan karakteristik suara manusia secara efektif dengan meniru mekanisme pendengaran manusia (Davis & Mermelstein, 1980; Rabiner & Juang, 1993). O'Shaughnessy (2000) menambahkan bahwa pendekatan ini memproses frekuensi rendah secara lebih detail dibandingkan frekuensi tinggi, sehingga representasi yang dihasilkan lebih sesuai dengan persepsi auditori manusia.

Selain metode MFCC, integrasi Internet of Things (IoT) pada sistem keamanan ruang memberikan keunggulan karena memungkinkan perangkat keamanan terhubung dengan jaringan sehingga proses monitoring, pencatatan akses, dan pengendalian dapat dilakukan secara otomatis dan real-time. Administrator dapat memantau aktivitas akses dari jarak jauh serta memperoleh notifikasi apabila terjadi upaya akses yang tidak sah, sehingga efektivitas pengawasan keamanan pada lingkungan perusahaan dapat meningkat.

PT Trima Laksana Jaya Pratama merupakan perusahaan yang memiliki kebutuhan terhadap sistem keamanan ruang untuk melindungi aset dan dokumen penting. Hasil observasi awal menunjukkan bahwa sistem keamanan ruang yang digunakan masih bersifat konvensional sehingga belum memberikan tingkat keamanan yang optimal dan belum mendukung monitoring digital, sehingga berpotensi menimbulkan risiko penyalahgunaan akses.

Kesenjangan tersebut diperlakukan sebagai masalah pengembangan sistem, bukan sebagai bukti bahwa metode autentikasi biometrik yang digunakan tidak valid. Pada konteks yang lebih dekat dengan objek penelitian, Maulana et al. (2023) merancang sistem Smart Door Lock berbasis ESP32 dan Internet of Things (IoT) yang dikendalikan melalui smartphone Android, namun belum menerapkan autentikasi berbasis karakteristik suara. Penelitian ini berbeda karena menambahkan lapisan autentikasi biometrik suara menggunakan MFCC pada arsitektur Smart Handle berbasis IoT, sekaligus melengkapi sistem dengan notifikasi Telegram Bot sebagai media monitoring real-time bagi administrator.

Berdasarkan uraian tersebut, penelitian ini mengembangkan Smart Handle Adaptif berbasis IoT dengan metode MFCC untuk autentikasi suara pada sistem keamanan ruang dokumen. Tujuan penelitian dirumuskan untuk: (1) merancang dan membangun Smart Handle Adaptif berbasis IoT untuk keamanan ruang dokumen; (2) menerapkan metode MFCC pada proses ekstraksi ciri suara pengguna; (3) mengimplementasikan proses autentikasi suara untuk menentukan hak akses pengguna; (4) mengintegrasikan ESP32, mikrofon, Relay, dan Solenoid Door Lock sebagai perangkat pengendali akses pintu; serta (5) mengintegrasikan Telegram Bot sebagai media notifikasi dan monitoring aktivitas akses ruangan.

METODE

Desain dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode pengembangan model (model development), karena berfokus pada proses merancang, membangun, dan mengembangkan produk berupa Smart Handle Adaptif berbasis IoT untuk sistem keamanan ruang dokumen. Pengumpulan informasi dilakukan melalui observasi terhadap kondisi ruang dan sistem keamanan yang digunakan, serta wawancara dengan pihak yang berkaitan dengan pengelolaan ruang dokumen. Data tersebut menjadi dasar penentuan fungsi Smart Handle, proses autentikasi suara menggunakan MFCC, mekanisme pengendalian Solenoid Door Lock, serta kebutuhan monitoring melalui Telegram Bot.

Tempat, Waktu, dan Sasaran Penelitian

Penelitian dilaksanakan di PT Trima Laksana Jaya Pratama selama enam bulan, yaitu Februari sampai Juli 2026, mencakup identifikasi masalah, analisis kebutuhan, perancangan perangkat keras dan perangkat lunak, implementasi, pengujian, hingga penyusunan laporan. Sasaran penelitian meliputi pengguna yang memiliki hak akses ruang dokumen, administrator sebagai pemantau aktivitas akses, para pakar (ahli sistem informasi, IoT, dan pengolahan sinyal suara) sebagai validator rancangan, serta kelompok kecil (small group try-out) berjumlah tiga responden untuk uji coba awal sistem.

Kerangka Pengembangan Model

Pengembangan model dilakukan melalui tahapan yang sistematis, yaitu penelitian pendahuluan, analisis kebutuhan, perancangan model, validasi/evaluasi/revisi model, produk model yang telah direvisi, serta telaah pakar (expert judgement). Pada tahap penelitian pendahuluan diidentifikasi kesenjangan antara keadaan ideal, yaitu ruang dokumen yang memiliki sistem autentikasi aman dan monitoring real-time, dengan kenyataan bahwa sistem keamanan masih konvensional. Analisis kebutuhan dibagi menjadi kebutuhan pengguna dan kebutuhan sistem/teknis, meliputi spesifikasi ESP32, sensor suara, metode MFCC, Relay, Solenoid Door Lock, jaringan Wi-Fi, serta Telegram Bot. Rancangan model diterjemahkan melalui Unified Modeling Language (UML), meliputi Use Case Diagram, Activity Diagram, Class Diagram, dan Sequence Diagram, sebelum divalidasi oleh pakar sistem informasi, IoT, dan pengolahan sinyal suara serta diujicobakan pada kelompok kecil.

Arsitektur dan Komponen Sistem

Smart Handle Adaptif dibangun menggunakan mikrokontroler ESP32 sebagai pengendali utama dan penghubung jaringan IoT, sensor mikrofon untuk menangkap suara pengguna, Relay sebagai pengendali aktuator, serta Solenoid Door Lock sebagai mekanisme penguncian pintu. Laptop berfungsi sebagai server yang menjalankan proses ekstraksi fitur dan autentikasi suara menggunakan MFCC melalui bahasa pemrograman Python, sedangkan ESP32 diprogram menggunakan Arduino IDE berbahasa C++. Komunikasi antara ESP32 dan server berlangsung melalui jaringan Wi-Fi, sedangkan Telegram Bot API digunakan sebagai media notifikasi dan monitoring.

Proses ekstraksi ciri suara pada server dilakukan melalui tahapan pre-emphasis untuk menguatkan frekuensi tinggi, framing untuk membagi sinyal menjadi segmen berdurasi 20–25 ms dengan overlap 30–50%, windowing menggunakan Hamming window untuk mengurangi spectral leakage, Fast Fourier Transform (FFT) untuk mengubah sinyal ke domain frekuensi, pemetaan ke Mel Filter Bank, kompresi logaritmik, dan Discrete Cosine Transform (DCT) untuk menghasilkan koefisien MFCC yang ringkas dan tidak berkorelasi (Rabiner & Juang, 1993; Davis & Mermelstein, 1980).

Sistem memiliki dua kondisi utama pada proses akses. Apabila hasil ekstraksi ciri suara pengguna sesuai dengan data referensi yang telah terdaftar, ESP32 mengaktifkan Relay sehingga Solenoid Door Lock terbuka. Sebaliknya, apabila suara tidak dikenali, sistem menolak akses dan pintu tetap terkunci. Setiap aktivitas autentikasi, baik berhasil maupun ditolak, dikirimkan sebagai notifikasi kepada administrator melalui Telegram Bot berisi identitas pengguna, waktu akses, dan status autentikasi.

Teknik Pengujian dan Evaluasi

Evaluasi teknis dilakukan melalui pengujian fungsional terhadap komponen utama sistem, yaitu input suara, proses MFCC, autentikasi pengguna terdaftar, penolakan pengguna tidak terdaftar, pengendalian Relay dan Solenoid Door Lock, komunikasi IoT, serta notifikasi Telegram Bot. Pengujian dilakukan menggunakan tiga pengguna sebagai sampel untuk mengetahui keberhasilan sistem dalam mengenali suara terdaftar sekaligus menolak suara yang tidak terdaftar. Tingkat keberhasilan pengujian dihitung menggunakan rumus Pass Rate, yaitu jumlah kasus uji Valid dibagi jumlah keseluruhan kasus uji dikalikan 100%.

HASIL DAN PEMBAHASAN

Hasil Implementasi Komponen Sistem

Implementasi menunjukkan bahwa seluruh komponen Smart Handle Adaptif dapat berfungsi sesuai rancangan, mulai dari input suara, pengolahan dan ekstraksi MFCC, autentikasi, pengendalian Relay dan Solenoid Door Lock, komunikasi IoT, hingga pengiriman notifikasi Telegram, sebagaimana dirangkum pada Tabel 1.

Tabel 1. Hasil Implementasi Komponen Sistem

Komponen/Fungsi	Hasil Implementasi	Status
Input suara	Mikrofon menerima suara pengguna	Berfungsi
Pengolahan suara	Data suara diproses sistem	Berfungsi
Ekstraksi MFCC	Fitur suara diperoleh	Berfungsi

Komponen/Fungsi	Hasil Implementasi	Status
Autentikasi suara	Sistem menentukan hasil pencocokan	Berfungsi
Relay	Dikendalikan sesuai hasil autentikasi	Berfungsi
Solenoid Door Lock	Terbuka/terkunci sesuai keputusan	Berfungsi
Komunikasi IoT	Perangkat terhubung via jaringan	Berfungsi
Telegram Bot	Notifikasi aktivitas terkirim	Berfungsi

Sumber: Data diolah peneliti, 2026

Hasil Uji Coba Awal dan Pengujian Autentikasi

Uji coba awal melibatkan tiga pengguna yang memberikan perintah suara “Buka Pintu” dan “Tutup Pintu” secara bergantian. Seluruh percobaan menunjukkan hasil pengenalan berhasil dengan keputusan akses yang sesuai perintah. Pengujian autentikasi suara terhadap tiga pengguna terdaftar, masing-masing dua kali percobaan, menunjukkan seluruh suara dikenali dan diterima oleh sistem. Sebaliknya, pengujian terhadap pengguna yang tidak terdaftar menunjukkan bahwa seluruh percobaan berhasil ditolak oleh sistem dengan kondisi kunci tetap terkunci, sebagaimana dirangkum pada Tabel 2.

Tabel 2. Ringkasan Pengujian Fungsional Sistem

Fungsi yang Diuji	Skenario	Hasil
Autentikasi terdaftar	3 pengguna x 2 percobaan	Dikenali, akses diterima
Autentikasi tidak terdaftar	3 percobaan	Ditolak, kunci terkunci
Relay & Solenoid	Autentikasi berhasil/gagal	Sesuai hasil autentikasi
Komunikasi IoT (Wi-Fi)	Koneksi & kirim data	Berhasil terhubung
Notifikasi Telegram	Akses berhasil/ditolak	Notifikasi terkirim

Sumber: Data diolah peneliti, 2026

Rekapitulasi Hasil Pengujian

Rekapitulasi pengujian menunjukkan bahwa dari tiga kasus uji fungsional, seluruh kasus uji berstatus Valid atau sesuai dengan hasil yang diharapkan, sehingga diperoleh Pass Rate sebesar:

$$Pass Rate = (3 / 3) \times 100\% = 100\%$$

Tingkat keberhasilan sebesar 100% menunjukkan bahwa fungsi yang diuji pada Smart Handle Adaptif berbasis IoT dengan metode MFCC telah berjalan sesuai rancangan pada skenario pengujian yang dilakukan. Meskipun demikian, hasil tersebut diperoleh dari jumlah kasus uji yang masih terbatas sehingga belum menggambarkan kinerja sistem pada seluruh kondisi penggunaan.

Pembahasan

Hasil pengembangan menunjukkan bahwa integrasi antara autentikasi suara berbasis MFCC dan pengendalian perangkat pengunci melalui IoT memungkinkan Smart Handle tidak hanya melakukan pengenalan suara, tetapi juga menindaklanjuti hasil autentikasi tersebut menjadi tindakan nyata pada perangkat pengunci, sekaligus menyampaikan informasi aktivitas akses kepada administrator secara real-time melalui Telegram Bot. Kelebihan model ini terletak pada penggantian kunci fisik dengan autentikasi suara yang lebih sulit diduplikasi, serta ketersediaan jejak monitoring aktivitas akses yang sebelumnya tidak dimiliki oleh sistem konvensional.

Dibandingkan dengan Maulana et al. (2023) yang merancang Smart Door Lock berbasis ESP32 dan IoT dengan pengendalian melalui smartphone Android tanpa lapisan biometrik suara, penelitian ini memperluas mekanisme kontrol akses dengan menambahkan autentikasi suara menggunakan MFCC sebagai faktor verifikasi identitas, sehingga akses tidak lagi bergantung pada kepemilikan perangkat semata. Konsistensi hasil autentikasi turut didukung oleh tahapan ekstraksi ciri suara yang mengikuti kerangka MFCC baku (Rabiner & Juang, 1993; Davis & Mermelstein, 1980; O'Shaughnessy, 2000), sehingga karakteristik suara pengguna dapat direpresentasikan secara ringkas dan konsisten untuk proses pencocokan.

Di sisi lain, model ini masih menggunakan satu faktor autentikasi, yaitu suara pengguna, sehingga tingkat keamanan dapat ditingkatkan lebih lanjut melalui penambahan multi-factor authentication seperti sidik jari, pengenalan wajah, kartu RFID, atau PIN. Pengujian autentikasi suara juga baru dilakukan pada kondisi lingkungan dengan tingkat kebisingan terbatas, sehingga penerapan pada lingkungan yang lebih bising memerlukan teknik noise reduction, speech enhancement, atau kombinasi MFCC dengan algoritma klasifikasi seperti Support Vector Machine (SVM), Hidden Markov Model (HMM), Gaussian Mixture Model (GMM), atau Deep Neural Network (DNN) agar akurasi autentikasi tetap terjaga.

Keterbatasan Penelitian

Penelitian ini dibatasi oleh jumlah kasus uji yang masih terbatas, yaitu tiga pengguna dengan skenario pengujian pada satu lokasi penelitian, belum tersedianya penyimpanan riwayat autentikasi (access log) secara lengkap dalam jangka panjang, serta pengujian yang belum

mencakup variasi kondisi lingkungan dan tingkat kebisingan yang lebih luas. Oleh karena itu, kesimpulan penelitian terutama berkaitan dengan kelayakan teknis awal model dan belum dapat digunakan untuk menyatakan bahwa sistem akan selalu berhasil pada seluruh kondisi penggunaan operasional.

SIMPULAN

Penelitian ini berhasil merancang dan membangun Smart Handle Adaptif berbasis Internet of Things (IoT) menggunakan mikrokontroler ESP32, sensor mikrofon, Relay, dan Solenoid Door Lock, serta server sebagai pusat pengolahan data, yang mampu melakukan autentikasi suara secara real-time sehingga pengguna terdaftar dapat mengakses ruangan tanpa kunci konvensional, sedangkan pengguna yang tidak memiliki hak akses ditolak secara otomatis. Metode Mel-Frequency Cepstral Coefficients (MFCC) berhasil diimplementasikan sebagai metode ekstraksi ciri suara melalui tahapan pre-emphasis, framing, windowing, FFT, Mel Filter Bank, log energy, dan DCT, sehingga sistem mampu membedakan suara pengguna terdaftar dari suara pengguna lain. Integrasi sistem berbasis IoT turut berhasil diterapkan sehingga ESP32 dapat berkomunikasi dengan server melalui jaringan Wi-Fi dan mengirimkan notifikasi status autentikasi kepada administrator melalui Telegram secara real-time.

Hasil pengujian terhadap tiga kasus uji fungsional menunjukkan Pass Rate sebesar 100%, yang mendukung kelayakan teknis awal model sekaligus konsistensi implementasi fungsi yang telah dirancang. Secara praktis, sistem ini berpotensi menggantikan mekanisme kunci konvensional dengan sistem autentikasi biometrik suara yang lebih aman, adaptif, dan responsif untuk pengamanan akses ruang dokumen di lingkungan perusahaan. Penelitian lanjutan disarankan untuk menambahkan multi-factor authentication, basis data riwayat akses yang lebih lengkap, dashboard monitoring berbasis web, serta teknik noise reduction atau kombinasi MFCC dengan algoritma klasifikasi lanjutan agar akurasi autentikasi tetap tinggi pada lingkungan yang lebih bising dan pada jangka waktu penggunaan yang lebih panjang.

DAFTAR PUSTAKA

- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805.
- Davis, S. B., & Mermelstein, P. (1980). Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 28(4), 357–366.
- Maulana, I., Azriadi, E., & Musrido, J. (2023). Rancang bangun sistem Smart Door Lock menggunakan mikrokontroler ESP32 berbasis Internet of Things (IoT) dan smartphone Android. *Jurnal Teknik Industri Terintegrasi (JUTIN)*, 6(1), 195–208. <https://doi.org/10.31004/jutin.v6i1.15123>
- O'Shaughnessy, D. (2000). *Speech communications: Human and machine*. IEEE Press.

- Pressman, R. S., & Maxim, B. R. (2020). *Software engineering: A practitioner's approach* (9th ed.). McGraw-Hill Education.
- Rabiner, L. R., & Juang, B. H. (1993). *Fundamentals of speech recognition*. Prentice Hall.
- Reynolds, D. A., & Rose, R. C. (1995). Robust text-independent speaker identification using Gaussian mixture speaker models. *IEEE Transactions on Speech and Audio Processing*, 3(1), 72–83.