



NFC Method for Troubleshooting External Security Systems on Microcontroller Devices for Safe Door Designs

Nurhalis Jusman, Aldito Rama Dana and M.Hajar Prasetyo

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

July 25, 2020

Metode NFC untuk Pemecahan Masalah Sistem Keamanan Eksternal pada Perangkat Microcontroller untuk Desain Pintu Brankas

1st Nurhalis Jusman

Program Studi Teknik Komputer
Universitas Amikom Yogyakarta
Sleman, Yogyakarta

nurhalis.jusman@students.amikom.ac.id

2nd Aldito Rama Dana

Program Studi Teknik Komputer
Universitas Amikom Yogyakarta
Sleman, Yogyakarta

aldito.1999@students.amikom.ac.id

3rd M.Hajar Prasetyo

Program studi Teknik Komputer
Universitas Amikom Yogyakarta
Sleman, Yogyakarta

mochammad.prasetyo@students.amikom.ac.id

Abstract—Di zaman sekarang, ketika semua perangkat menggunakan istilah “smart”, keamanan pada setiap perangkat perlu ditingkatkan. Dengan seiring kemajuan teknologi kejahatan di dunia cyber juga semakin meningkat. Dengan teknologi NFC (Near-Field Communication), pintu brankas dapat dibuka dengan lebih mudah dan mampu memberikan keamanan autentikasi yang lebih aman. Kunci pintu yang dikontrol NFC juga memiliki pemutus sirkuit yang diaktifkan di pintu brankas dan dinonaktifkan ketika tidak digunakan. Tidak seperti kunci pada umumnya yang masih menggunakan kunci analog, otentikasi NFC pengguna hanya memasukkan kode sandi dan memindai tag NFC untuk membuka pintu brankas. Untuk mencegah duplikasi ID tag NFC, sistem mengenkripsi ID tag dan kode sandi dengan menggunakan AES. Pada microcontroller ditautkan dengan website. website berguna sebagai kontrol untuk melihat login dari pengguna brankas.

Keywords—NFC, Brankas, IoT, Microcontroller, AES, Website

I. INTRODUCTION

Pada era globalisasi seperti saat ini perkembangan teknologi sangat pesat, teknologi yang terjadi pada alat yang tadinya manual kini menjadi serba otomatis dengan adanya mikrokontroler, hal ini dapat dilihat dari banyaknya peralatan elektronik dalam kehidupan sehari-hari yang serba otomatis, mulai dari pengaplikasian yang sederhana maupun yang lebih canggih. Peralatan elektronik yang berbasis mikrokontroler memang memiliki manfaat yang luar biasa apabila dikembangkan oleh para ahli dibidangnya, hal ini dapat dilihat dari maraknya penggunaan peralatan elektronik otomatis sebagai alat bantu dalam melaksanakan pekerjaan sehari-hari manusia[1].

Demikian juga halnya dengan keamanan zaman sekarang disekitar lingkungan kita, kebanyakan orang mengabaikan suatu keamanan pada suatu tempat penyimpanannya seperti lemari dan brankas. Sehingga tempat penyimpanannya tidak terjaga dengan baik, walaupun suatu brankas dikunci dengan kunci yang biasa digunakan tapi kemungkinan brankas tersebut bisa di buka dan bisa terjadinya pencurian.

Sistem keamanan sekarang sangat dibutuhkan. Salah satunya sistem keamanan pada pintu brankas yang rawan dan kemungkinan terjadinya pencurian sangat besar. Pada suatu brankas sekarang ini sangat diperlukan adanya sebuah keamanan, agar bisa mengantisipasi bahaya pencurian yang dapat terjadi secara tak terduga[2]. Pintu brankas ini tidak

semua orang bisa membuka karena pintu brankas ini mempunyai suatu alat yaitu dengan cara scanning card dan password. Keamanan pintu brankas masih sangat manual, dalam artian keamanan pintu brankas beredar di kalangan masyarakat saat ini masih menggunakan keamanan pintu brankas konvensional[3]. Dimana membuka pintu brankas dengan cara memutar dan memakai kode, yang di rasa hal tersebut tidak efisien

1.1 Identifikasi Masalah

Smart brankas merupakan sebuah alat teknologi 4.0 yang disesain secara optimal dalam penggunaan secara end-to-end akan tetapi memiliki sebuah kerentanan dalam kombinasi antara sistem microcontroller dengan database secara tidak langsung.

1.2 Rumusan Masalah

Bagaimana Pengoptimalan sebuah NFC (Near-Field Communication) yang digunakan untuk login pada brankas yang dikombinasikan dengan database untuk mengelola brankas secara menyeluruh.

1.3 Tujuan Penelitian

Menerapkan NFC untuk mengoptimalkan keamanan pada sebuah brankas dengan 2 kali autentifikasi dan ditambah dengan database pada era teknologi 4.0.

1.4 Manfaat Penelitian

Penelitian ini berdasarkan pada tolak ukur brankas dalam era teknologi 4.0 yang sangat penting untuk memudahkan dalam mengelola sebuah brankas tersebut sehingga mudah untuk di kendalikan secara remot atau tidak secara fisik.

II. LITERATUR REVIEW

Metode pengembangan yang terkait dalam pengembangan ini terutama dari aplikasi, yang di pakai memiliki kemiripan obyek dan juga framework yang digunakan adalah sebagai berikut. Database pada webserver, obyek pengembangan brankas, Framework pada web server, hasil pengembangan brankas terdapat layout web ketika di akses dengan perangkat PC, Laptop dan Smartphone[4]. Obyek pengembangan Sistem smart brankas, hasil pengembangan brankas manual menjadi smart brankas. Obyek pengembangan Aplikasi Media Sosial, menggunakan Framework Bootstrap, hasil pengembangan smart brankas untuk bank di indonesia yang bersifat responsive., hasil

pengembangan Implementasi Teknologi smart brankas pada Sistem Informasi brankas di Indonesia .

Perbedaan pengembangan ini dengan pengembangan sebelumnya terletak pada system brankas yang dikembangkan yaitu membuat sistem brankas yang menggunakan microcontroller sebagai mesin utama[5]. Untuk system keamanan akan di pantau melalui aplikasi dan website. Pengguna aplikasi ini adalah admin yang bertanggung jawab terhadap smart brankas tersebut.

Masalah otorisasi layanan telah banyak ditangani dalam literatur. Beberapa karya telah berfokus pada penerapan berbagai strategi kontrol akses. Discrete Access Control (DAC) membatasi akses ke objek berdasarkan identitas subjek dan / atau grup di dalamnya[6]. Manajemen bersifat opsional dalam arti bahwa objek dengan hak akses khusus dapat mentransfer izin ini ke topik lain. Kontrol akses berbasis peran (RBAC) didasarkan pada kebijakan yang membatasi akses sumber daya untuk objek yang ditugaskan peran tertentu[7]. Mekanisme otorisasi biasanya sangat tergantung pada langkah otentikasi yang harus diambil sebelumnya untuk mengidentifikasi pengguna untuk memverifikasi peran atau atribut mereka dan untuk mematuhi kebijakan akses[8]. Menerapkan mekanisme kontrol akses dalam skenario terbatas, seperti jaringan sensor nirkabel, bukanlah tugas yang mudah. Sistem kontrol akses yang kompleks dan kontekstual untuk skenario jaringan sensor medis yang mengidentifikasi masalah kritis kerahasiaan dan kerahasiaan[9]. Mekanisme yang diusulkan secara khusus memperhitungkan sifat campuran dari Internet yang diperluas, yang akan digunakan di tahun-tahun mendatang. Selain itu, struktur yang diusulkan bertujuan untuk mengurangi upaya penyedia layanan untuk memastikan keamanan layanan mereka dengan menyediakan sistem lisensi yang andal, standar, dan kompatibel[10].

Smart Brankas menjadi landasan pacu teknologi dalam sebuah penyimpanan uang, dalam hal uang dan teknologi merupakan sebuah terobosan solusi yang sangat efektif dan efisien ,berbagai acuan dalam menciptakan akses yang aman dalam perpaduan uang dan teknologi sangatlah sebuah masalah yang rumit namun smart brankas menjadi solusi utama di dalam peran perpaduan teknologi dan uang.

III. METODOLOGI PENELITIAN

Smart brankas merupakan sebuah brankas dengan system database dan juga memiliki keamanan dengan sytem online ,terdapat fitur sidik jari yang di gunakan sebagai masuk pada brankas di dalam brankas terdapat chip yang berwenang memilikinya untuk membuka keseluruhan brankasnya.

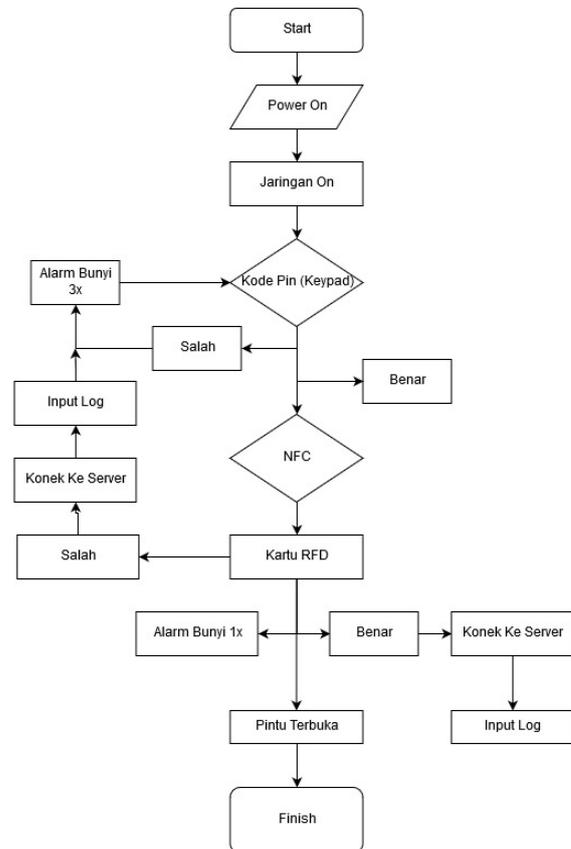
Smart Brankas mempunyai sebuah keamanan yang ketat yang berbentuk fisik maupun online ,terdapat sirine anti pencurian yang terdapat pada brankas ,setiap akses akan masuk kedalam database maka terekam secara jelas yang membuka sytem dari smart brankas .

Untuk memperoleh data dan fakta yang diperlukan penulis melakukan penelitian dengan cara mengumpulkan data-data dari buku, jurnal hasil penelitian, dan dokumen. Penelitian yang dilakukan dengan cara mempelajari literatur, diktat, jurnal-jurnal, serta bahan-bahan yang berhubungan dengan topik penulisan. Dengan cara membaca, mengutip, serta menyadur pendapat-pendapat para ahli yang ada hubungannya dengan objek penelitian.

Titik kelemahan	Metode fingerprnt	Metode keypad	Metode NFC
Pintu utama	sedang	mudah	sulit
Alarm	aktif	Tidak ada	aktif
database	Tidak ada	Tidak ada	ada
Log admin	Tidak ada	Tidak ada	ada

Gambar 1. Bagan perbandingan

Metode smart brankas sangat aman dan terkendali oleh system semua unit berkaitan pada kendali utama sehingga alur smart brankas sangat baik untuk di terapkan.



Gambar 2 : flowchart smart brankas

Sebuah input dari code yang di berikan oleh user atau admin akan mengakses dalam NFC terdapat peralihan jika code tersebut salah ,pada dasarnya code tersebut di baca oleh system jika terdapat dalam database yang akan di input maka smart brankas akan mengkalibrasi secara menyeluruh dan membuka sebuah pintu tersebut.

- Pada tahap ini penulis melakukan riset yang terkait dengan sistem keamanan brankas, kemudian mencari apa saja kemungkinan celah yang ada pada brankas tersebut. Pengamatan juga di lakukan meliputi lingkungan sekitar.
- Tahap ini dilakukan wawancara langsung pada karyawan tentang masalah apa saja yang terkait dengan sistem keamanan brankas seperti pencurian ataupun perampokan pada perusahaan.

- Pada tahap ini dilakukan analisa dengan mencari jurnal, buku, paper yang memuat informasi-informasi yang terkait dengan kebutuhan untuk penelitian ini agar lebih memahami tentang penggunaan dari teknologi NFC, website, database, algoritma AES dan semua komponen yang digunakan dalam penelitian ini.
- Menggunakan metode perancangan hardware seperti: Arduino uno r3 atau node mcu atau metode pengembangan software/sistem informasi seperti control management database, remote microcontroller, koneksi website, atau. Metode pengembangan brankas dengan metode input output log system, Metode implementasi security menggunakan Security Life Cycle dan sirine, atau menggunakan metode Security Policy Development Life Cycle, dan lain-lain.

IV. HASIL DAN PEMBAHASAN

4.1 Deskripsi atau Pembahasan

Bab ini membahas tentang hasil dari perancangan dan implementasi keamanan pintu brankas. Pintu brankas ini dilengkapi dengan fingerprint dengan system database. Pada sistem keamanan pintu brankas ini hashing algoritma AES akan diimplementasikan ke sistem dalam bahasa C dan tampilan interface server web menggunakan bahasa pemrograman PHP. Selain itu pintu brankas menyediakan pengoprasian sistem pengaturan kunci pintu. Untuk menghemat konsumsi daya untuk periode waktu yang lama, pintu ini didesain dengan menggunakan sensor dan MCU yang berdaya rendah untuk mengontrol waktu keadaan siaga atau tidur, konsumsi dari desain pintu ini hanya memakan daya 227,45mW yang sangat hemat jika dibandingkan dengan pintu lainnya. sistem keamanan pintu brankas ini dibuat dengan database MYSQL dimana terdapat fitur insert, delete, dan update yang bisa dikendalikan oleh pihak admin melalui backend yang berbasis web.

4.2 Implementasi Metode Penelitian

Pada tahap merupakan proses implementasi pada sisi penyatuan semua alan dan sistem meliputi, brankas, arduino, nodemcu, NFC, keypad, alarm, website, webserver, database dan perangkat lainnya. setelah melakukan tahapan tersebut selanjutnya ketahapan pengujian.

4.3 Pengujian dan Hasil

Tahap pengujian yang dilakukan pada brankas untuk untuk sistem keamanan brankas menggunakan NFC (Near Filed Communication). Pengujian dilakukan dengan dua metode, yaitu pengujian validasi dan pengujian usability. Pengujian validasi dilakukan untuk menguji apakah sistem brankas sudah memenuhi seluruh kebutuhan yang telah didefinisikan sebelumnya. Sedangkan pengujian usability merupakan pengujian yang bertujuan untuk mengetahui apakah sistem keamanan brankas menggunakan NCF dapat digunakan oleh pengguna atau komsumen dengan baik atau tidak.

4.3.1 Pengujian Validasi

Pengujian ini bertujuan untuk validasi terhadap setiap kebutuhan yang telah didefinisikan sebelumnya. hasil

dari pengujian ini akan dilampirkan dalam bentuk tabel yang berisi nomor kasus, nama kasus, case yang diujikan, tujuan dan prosedur pengujian. hasil dari pengujian dapat dikatakan valid apabila hasil dari yang terdapat pada tabel memiliki kesamaan dengan hasil yang diharapkan. pengujian yang dilakukan meliputi seluruh kebutuhan fungsional yang ada pada brankas. Pengujian pemanfaatan NFC dilakukan dengan melakukan akses terhadap sistem keamanan brankas dengan menggunakan kartu RFID yang sudah di daftarkan dan yang belum didaftarkan pada sistem. pengujian juga dilakukan pada website dan server yang digunakan sebagai tempat penyimpanan Log jika kartu RFID pada sistem dikenali atau tidak dikenali. dengan begitu user bisa memonitoring siapa dan kapan brankas tersebut dibuka.

4.3.2 Pengujian Usability

Pengujian usability dilakukan untuk mengetahui tingkatan kemudahan pengguna dalam menggunakan brankas tersebut. tujuan dari pengujian ini untuk mengukur tingkat kemudahan dan kepuasan user terhadap sistem brankas tersebut. tahapan yang dilakukan dalam pengujian usability menjelaskan sistem brankas telah dibuat dengan benar.

Dari 2 tahap pengujian tersebut, dapat ditarik hasilnya yaitu sistem keamanan brankas yang terhubung dengan website untuk menyimpan log saat ada yang membuka dan mencoba membuka brankas tersebut sudah dikatakan layak digunakan untuk kalangan perkantoran atau perbankan.

DAFTAR PUSTAKA

- [1] M. Atmega, E. Yuliza, and T. U. Kalsum, "Alat Keamanan Pintu Brankas Berbasis Sensor Sidik Jari Dan Password Digital Dengan Menggunakan," vol. 11, no. 1, pp. 1–10, 2015.
- [2] W. A. Hufstetler, M. J. H. Ramos, and S. P. Wang, "NFC Unlock: Secure Two-Factor Computer Authentication Using NFC," *Proc. - 14th IEEE Int. Conf. Mob. Ad Hoc Sens. Syst. MASS 2017*, pp. 507–510, 2017.
- [3] D. Kurnianto, E. S. Nugraha, and V. K. Ekaristi, "Penerapan Kartu Elektronik Berbasis Near Field Communication (NFC) Pada Sistem Keamanan Pintu Rumah Cerdas," *J. Infotel*, vol. 9, no. 1, p. 122, 2017.
- [4] M. Mena, A. Corral, L. Iribarne, and J. Criado, "A Progressive Web Application Based on Microservices Combining Geospatial Data and the Internet of Things," *IEEE Access*, vol. 7, pp. 104577–104590, 2019.
- [5] H. Horikoshi and H. Chujo, "Prevention Method of Electromagnetic Interference by Implementing NFC Radio Active Signal for Touchpad," *2018 IEEE 7th Glob. Conf. Consum. Electron. GCCE 2018*, pp. 691–693, 2018.
- [6] A. A. Malik, B. Hussain, S. Ozair, and H. Kazmi, "Access Control Model for Data Stored on Cloud Computing," vol. 20, no. 1, pp. 233–241, 2016.

- [7] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, no. c, pp. 12240–12251, 2018.
- [8] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An oauth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sens. J.*, vol. 15, no. 2, pp. 1224–1234, 2015.
- [9] E. Edwan, A. Shaheen, and A. Alloh, "Assets and Keys Management System Using NFC Technology," *Proc. - 2018 Int. Conf. Promis. Electron. Technol. ICPET 2018*, pp. 8–12, 2018.
- [10] C. H. Hung, Y. W. Bai, and J. H. Ren, "Design and implementation of a single button operation for a door lock control system based on a near field communication of a smartphone," *5th IEEE Int. Conf. Consum. Electron. - Berlin, ICCE-Berlin 2015*, pp. 260–261, 2016.