PERANCANGAN SISTEM ABSENSI SISWA DENGAN IMPLEMENTASI QR-CODE DAN KRIPTOGRAFI AES-128 BERBASIS ANDROID

Decky Azmi Pratama[1], Deni Arifianto[2], Lutfi Ali Muharom[3]
[1)]Program Studi Informatika
Email: [1]deckyazmi@gmail.com

ABSTRAK

Terdapat berbagai permasalahan pada saat melakukan kegiatan absensi manual. baik dari segi keamanan dimana data dapat dengan mudah dimanipulasi, dan dari segi efisiensi yang membutuhkan waktu dalam pengerjaanya, dan tidak dapat di cek secara *realtime* oleh walimurid. Sehingga dibutuhkan sistem absensi siswa secara *online* dengan memperhatikan aspek keamanan, dan efisiensi sistem sehingga proses absensi dapat di lakukan dengan mudah dan juga aman dalam menjaga keaslian data. dengan memperhatikan berbagai aspek tersebut, Desain sistem yang dibuat adalah scan absensi *Qr Code* berbasis *android* dikarenakan kemudahan dan efisiensinya untuk diterapkan disekolah, dan Enkripsi data mengunakan kriptografi *AES-128* untuk menjaga keamanan sistem. Hasil pengujian yang dilakukan untuk mengukur tingkat *acceptability* sistem dengan menggunakan *System Ussabillity Scale (SUS)* dalam penelitian ini dengan yaitu *grade* C dari murid, B dari guru, dan B dari wali murid. Dan hasil uji keamanan sistem dengan melakukan *Dictionary Attack* menggunakan aplikasi thc-hydra gagal menembus keamanan sistem.

Kata kunci: *android, qr code, enkripsi aes-128, scanning, absensi.*

ABSTRACT

There are various problems when conducting manual attendance both in terms of security where data can be easily manipulated, and in terms of efficiency which take times to do it, and cannot be checked in realtime by the student's guardian. So that an online student attendance system is needed with attention to both security and system efficiency aspect so that the attendance process can be done easily and safely in maintaining the authenticity of the data. By paying attention to those aspects, the system design made is an Android-based Qr Code attendance scan due to its ease and efficiency to be implemented in schools, and data encryption using AES-128 cryptography to maintain system security. The result of the test that was conducted using System Usability Scale (SUS) to measure the acceptability of the system are grade C from the student, B from the teacher, and B from the student's guardian. And the result of the system security test by performing dictionary attack using the thc-hydra failed to penetrate system security.

Keywords: *android, qr code, aes-128 encryption, scanning, attendance*

1. PENDAHULUAN

Kemajuan suatu bangsa dapat dilihat dari berbagi aspek, salah satu aspek yang ada yaitu pendidikan. Jika kualitas pendidikan di suatu bangsa baik maka akan diiringi dengan perkembangan Sumber Daya Manusia (SDM) sehingga dapat memajukan suatu bangsa. Dalam pendidikan para siswa tidak hanya dilatih untuk menguasai materi pada buku/literatur, siswa juga dilatih disiplin dan tanggung jawab dengan kewajibanya salah satunya yaitu hadir ke sekolah untuk mengikuti pelajaran. sehingga absensi kehadiran merupakan salah satu faktor penting dalam pendidikan. Kehadiran/absensi siswa secara manual dengan memanggil nama siswa satu persatu dan guru mencatat kehadiran siswa pada lembar absensi cukup membutuhkan waktu dalam proses pengerjaanya, hal ini dapat di mudahkan dengan menggunaan teknologi informasi. Hingga saat ini teknologi yang sering di implementasikan dalam proses absensi sangatlah beragam, seperti absensi berbasis BIO (sidik jari, wajah, retina), dan absensi *QR Code*.

QR (Quick Response) Code atau merupakan evolusi dari *barcode* (kode batang) yang merupakan kode berbentuk garis mempresentasikan suatu karakter yang dapat

dibaca oleh *scanner*. *QR (Quick Response) Code* merupakan suatu kode matriks yang ditemukan oleh Denso 1994 dan disetujui sebagai standar nasional ISO pada tahun 2000 (Soon, 2008). *QR Code* merupakan gambar matriks dua dimensi yang merepresentasikan suatu data, terutama data berbentuk teks (Pasca Nugraha & Munir, 2011). Bukan hanya karena kecepatan dan kemudahan *QR Code* dalam menyampaikan informasi yang menjadi daya tarik tersendiri, melainkan juga karena *QR Code* dapat dibuat secara gratis. Sehingga banyak perusahaan dan instansi memilih menggunakan *QR Code* dalam kesehariannya. (Bashir, dkk., 2013)

Pesatnya perkembangan teknologi informasi semakin terasa dengan dikembangkanya *Smartphone*/ponsel pintar. *Smartphone* merupakan evolusi dari generasi sebelumnya yaitu ponsel atau telepon genggam. Berdasarkan sistem operasinya terdapat berbagai macam *Smartphone* yaitu Symbian, Blackberry OS, Android, dll. Smartphone android memiliki berbagai fitur layaknya komputer yang salah satu fiturnya yaitu dilengkapi dengan kamera untuk menangkap objek dan menyimpanya dalam bentuk gambar. dengan fitur ini smartphone dapat dijadikan sebagai altenatif scanner untuk membaca *QR Code*.

Terdapat berbagai tantangan dalam mengimplementasikan teknologi informasi pada kehidupan sehari hari yang harus dipertimbangkan, salah satunya dari segi keamanan yaitu teknologi yang dibuat untuk melakukan proses absensi dapat mencegah manipulasi data yang sering terjadi pada absensi manual. Sehingga, dalam penerapan tekologi informasi sangat diperlukan adanya kontrol keamanan data untuk mencegah dari hal yang tidak di inginkan. Salah satu upaya untuk mencegah hal tersebut yaitu menggunakan kriptorafi, kriptografi merupakan seni dan ilmu pengetahuan untuk menjaga data agar tetap aman saat di kirimkan (Hidayatullah, 2016).

Pesatnya perkembangan teknologi, kesadaran akan keamanan data juga meningkat, sehingga algoritma kriptografi pun juga terus berkembang. Dimulai dari kriptografi sederhana yang dikenal dengan kriptografi klasik, hingga menjadi kriptografi yang lebih kompleks. Salah satunya adalah kriptografi *Advanced Encryption Standard* (AES) menurut Aisha (2017) AES merupakan algoritma kriptografi simetris (kunci sama untuk melakukan ekripsi dan dekripsi). Dalam survey algoritma kriptografi (Abood, dkk., 2018) AES masih menjadi kriptografi yang dinilai lebih baik tingkat kemananya dibandingkan dengan algoritma kriptografi lain.

Penelitian ini bertujuan untuk merancang dan mengimplementasikan kriptografi AES-128 pada aplikasi absensi *QR Code* berbasis android. karena peneliti beranggapan bahwa *QR Code* sangat efektif dalam proses absensi disekolah, dengan siswa yang rata-rata telah memiliki *smartphone* sehingga tidak perlu antri satu persatu untuk melakukan scaning absensi *QR Code* seperti presensi manual dan presensi sidik jari, sehingga waktu untuk proses absensi dapat dilakukan lebih cepat. Dikembangkanya aplikasi ini peneliti berharap dapat memudahkan baik guru dan murid dalam melakukan kegiatan absensi yang cepat dan aman, juga dapat mempermudah wali murid dalam monitoring kegiatan absensi anak.

2. METODE

R&D (*Research and Development*). Penelitian dan pengembangan ini salah satunya bertujuan untuk menghasilkan sebuah produk yang efektif. Produk yang dihasilkan tidak selalu berbentuk perangkat keras , tetapi juga bisa dalam bentuk Perangkat Lunak. (Muhammad, dkk., 2020). Berikut merupakan tahapan yang digunakan penulis dalam penelitian ini antara lain:

A. PENGUMPULAN DATA

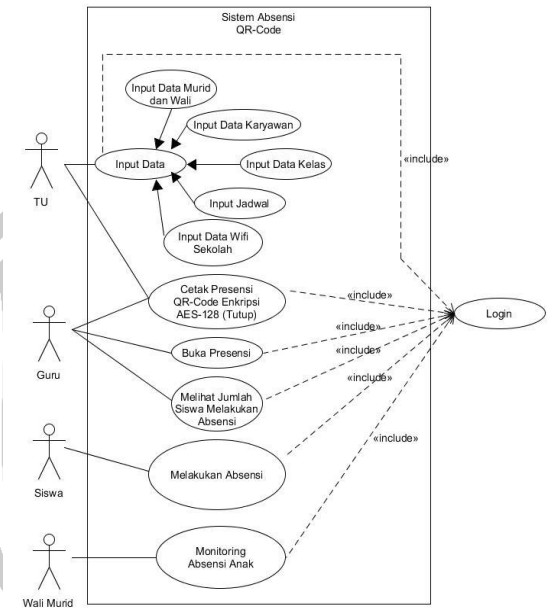
Tahap ini dilakukan dengan cara mencari data primer dan data sekunder yang dibutuhkan dalam meng- implementasikan algoritma *AES-128* dan *QR Code* pada aplikasi yang akan dikembangkan. Data primer diperoleh langsung dari objek penelitian yang akan digunakan dalam pembuatan aplikasi absesnsi menggunakan *QR Code*. Data-data primer terdiri dari Data *Stakeholder,* fasilitas dan alur absensi yang ada di lokasi penelitian yang akan di terapkan pada aplikasi absensi *QR Code*.

Menurut (Hidayatullah, 2017) “Data sekunder diperoleh dengan cara studi literatur pada penelitian-penelitian terdahulu di

berbagai jurnal, skripsi, dan *e-book*. Studi literatur dibutuhkan untuk menunjang pemahaman dan pengetahuan penulis tentang materi, dan metode yang diperlukan dalam proses pengerjaan tugas akhir."

B. DESAIN / RANCANGAN

Perancangan sistem yang digunakan menggunakan konsep berbasis objek dengan pemodelan *Unified Modelling Language* (UML). Pemodelan UML yang digunakan pada penelitian ini yaitu *Usecase* Diagram untuk menjelaskan interaksi *user* dengan aplikasi. *Use case* diagram dapat dilihat pada gambar 2 berikut.



Gambar 1. Use Case Diagram.

Dari diagram tersebut diketahui untuk user dengan role TU memiliki hak admin untuk melakukan input data guru, murid, wali murid, jawal, kelas sedangkan user role guru memiliki akses untuk mencetak absensi dalam bentuk QR Code yang dapat di scan langsung oleh murid untuk elakukan absensi sehingga wali murid dapat memonitor absensi anak secara real time.

Sehingga model rancangan awal aplikasi di modelkan seperti pada gambar berikut.

Gambar 2. Desain awal aplikasi.

C. IMPLEMENTASI

Tahap implementasi ini dilakukan dengan melakukan transformasi desain sistem yang telah dibuat ke dalam sebuah bahasa pemrograman berorientasi objek sehingga dapat dihasilkan suatu aplikasi absensi siswa berbasis android dengan implementasi Algoritma AES-128 dan QR Code berbasis android untuk menjaga keamanan proses absensi.

D. PENGUJIAN

Tahap pengujian dilakukan apabila aplikasi yang dibuat telah selesai dan siap untuk digunakan. Pengujian yang dilakukan berguna untuk mengetahui sejauh mana pengimplementasian algoritma *AES-128* dan *QR Code* pada aplikasi absensi siswa. Terdapat dua pengujian yang dilakukan peneliti, yang pertama dengan menggunakan kuisioner SUS yang merupakan salah satu alat pengujian usability paling populer untuk mengetahui tingkat *acceptability* aplikasi. SUS terdiri dari 10 pertanyaan dan telah di terjemahkan ke dalam Bahasa Indonesia (Shafrina & Santoso, 2017). dan yang kedua melakukan Dicionary Attack pada server untuk menguji keamanan sistem karena menurut Alexan, et., 2019 "metode kriptografi modern terbukti rentan terhadap *brute force* dan *side channel attacks*".

3. HASIL DAN PEMBAHASAN

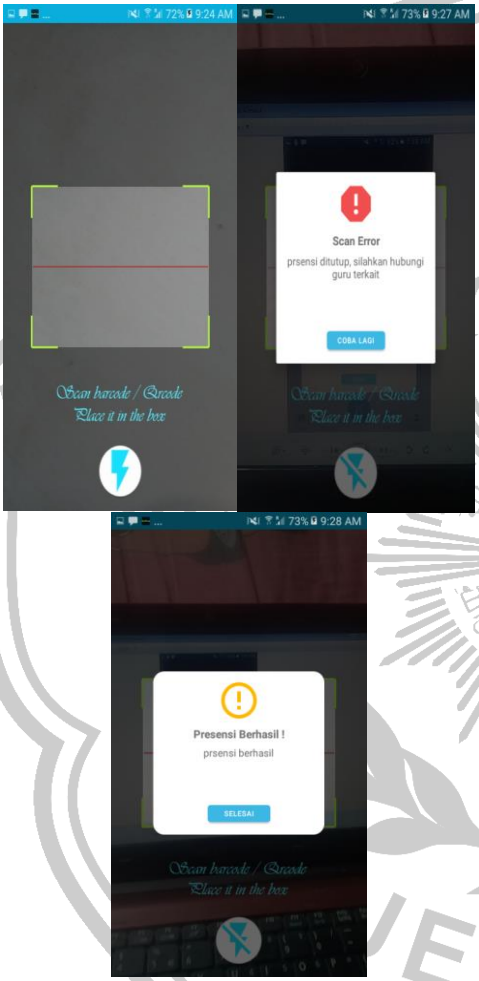
3.1 Implementasi Sistem

Pada tahap ini dilakukan pengkodean ke dalam bahasa pemrograman dari rancangan yang telah dibuat sebelumnya. Tahap Implementasi ini akan menghasilkan beberapa interface atau tampilan sistem yang sesuai dengan hak akses dimiliki user. Berikut ini beberapa tampilan utama sistem absensi.

3.1.1 Tampilan scanner

Tampilan *Activity Scanner* merupakan *activity* untuk melakukan proses scanning QR-Code yang dibuat oleh sistem. Saat user melakukan proses absensi, pertama sistem akan melakukan pengecekan dengan mendekripsi QR-Code, jika proses dekripsi berhasil maka akan dilanjutkan dengan pengecekan apakah absensi WIFI dinyalakan. jika menyala, sistem akan melakukan pengecekan apakah SSID dan BSSID wifi yang

tersambung merupakan wifi yang telah terdaftar, jika seseuai akan melanjutkan ke proses input absensi. namun jika absensi WIFI tidak menyala maka sistem akan melewati pengecekan WIFI dan melakukan proses input absensi. proses input absensi dilakukan dengan mendekripsi ID User dan pengecekan apakah absensi sedang di buka oleh guru, jika semua tahap dilalui dengan benar maka aplikasi akan menampilkan dialog presensi berhasil namun aplikasi akan menampilkan dialog gagal jika absensi tidak berhasil.



Gambar 3. Tampilan Scan Absensi

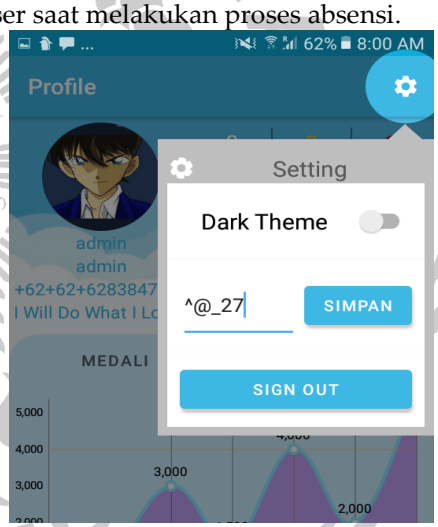
3.1.2 Tampilan Kuisioner

Kuisioner SUS yang akan di jadikan sebagai salah satu uji dari penelitian di sisipkan di dalam aplikasi, ketika admin mengaktifkan setting kuisioner di database maka aplikasi akan memunculkan dialog kusioner saat user membuka aplikasi, Dialog tersebut tidak dapat di *dismiss* sampai user menginputkan respon dari kuisioner tersebut.

Gambar 4. Tampilan Kuisioner

3.1.2 Tampilan Setting Key

Tampilan Setting Key terdapat di menu setting yang berada pada toolbar di fragment profil, setting key berfungsi untuk menginputkan dynamic key 5 digit yang akan digunakan untuk proses enkripsi dan dekripsi Id user saat melakukan proses absensi.

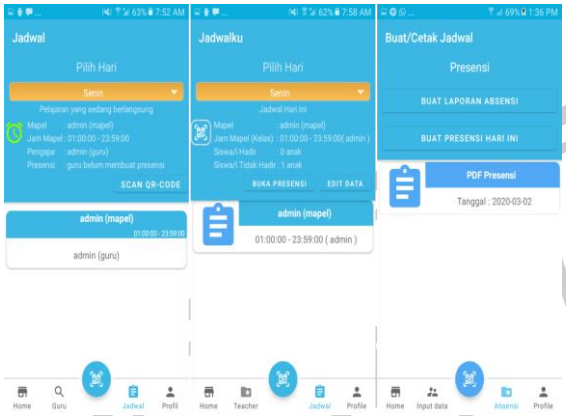


Gambar5. Tampilan Setting Key

3.1.3 Tampilan Jadwal

Tampilan jadwal merupakan tampilan list jadwal user. Pada fragment ini ditampilkan jadwal pelajaran yang dimiliki oleh masing-masing user, dan terdapat tampilan pelajaran yang sedang berlangsung yang berisi data kehadiran, sehingga siswa dan wali dapat cek presensi secara *real-time*. Pada user level guru terdapat tiga button, yaitu button untuk membuka/menutup absensi, button cetak qr berfungsi untuk menampilkan QR-Code terenkripsi yang dapat di scan oleh siswa untuk melakukan absensi, dan button edit absensi yang akan mengarahkan user ke menu edit

untuk melakukan edit absensi input absensi siswa yang izin/sakit/alpa dan juga edit jika terdapat kesalahan pada absensi. pada user level TU terdapat button untuk mengisialisasi absensi pada hari yang sedang berlangsung, sehingga guru dan murid dapat melakukan proses absensi.



Gambar 6. Tampilan Jadwal

3.2 Pengujian Sistem

3.2.1 Pengujian Usability Dengan Kuisioner SUS

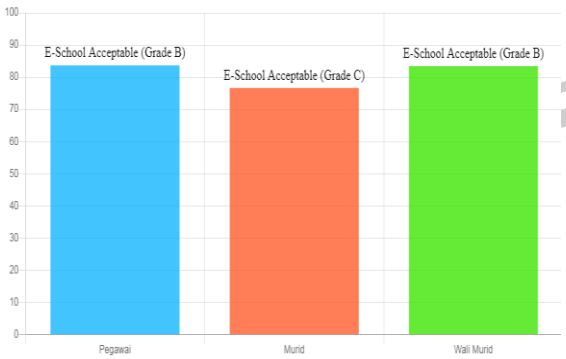
Pengujian usability dilakukan dengan memberikan kuisioner SUS kepada guru, murid dan walimurid. Kemudian dihitung menggunakan aturan perhitungan SUS yaitu:

$$\bar{x} = \frac{\sum x}{n}$$

Dimana: $\bar{x}$ = skor rata-rata
$\sum x$ = jumlah skor SUS
n = jumlah responden

Dari jumlah responden murid di dapatkan jumlah skor 76,6, responden guru didapatkan skor 83,67, dan responden walimurid mendapatkan skor 83,43. Sehingga dapat di ilustrasikan nilai rata-rata yang di peroleh adalah sebagai berikut.

Rata-Rata System Usability Scale (SUS)
Aplikasi M-School



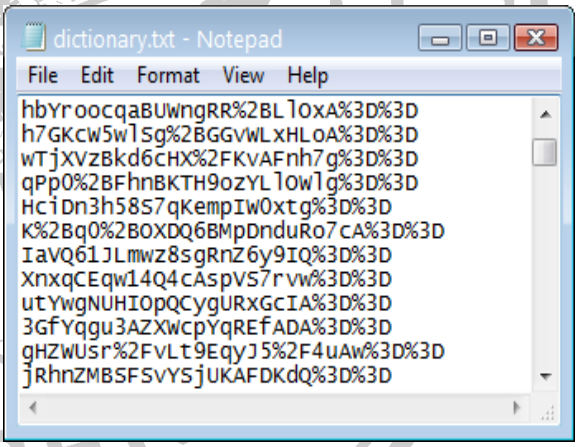
Gambar 6. Rata-rata SUS

Dari gambar tersebut didapatkan *acceptable range* aplikasi dari penghitungan jawaban kuisioner dari masing-masing level user. untuk pegawai atau karyawan aplikasi mendapatkan grade B bernilai acceptable, dari murid aplikasi mendapatkan grade C bernilai acceptable, dari user wali aplikasi mendapatkan grade B dengan scale bernilai acceptable.

3.1.2 Pengujian keamanan Dengan Dictionary Attack

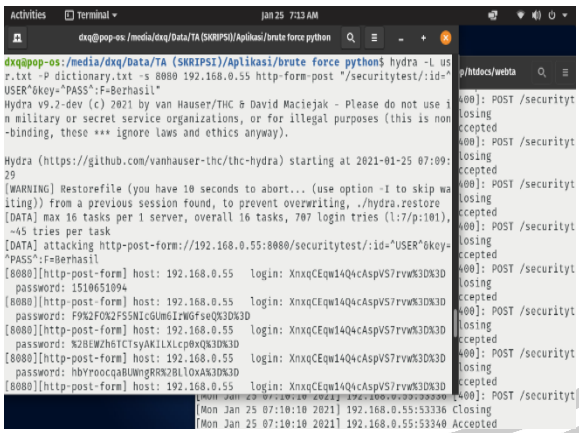
Dictionary Attack merupakan serangan yang dilakukan dengan cara menguji daftar kata kemungkinan (Dictionary) secara satu persatu (Pragusna, 2017). Terdapat banyak tools populer yang dapat digunakan untuk melakukan *penetration testing* dictionary attack seperti Medusa, Ncrack, THC-Hydra (Son, dkk., 2019). Adapun tool yang dilakukan dalam pengujian ini menggunakan THC-Hydra.

Langkah pertama untuk melakukan uji keamanan yaitu mengumpulkan daftar kata kemungkinan (*Dictionary*) yang akan dikumpulkan pada satu file berformat txt. adapun kata yang dikumpulkan dan aka diuji dalam penelitian ini sebanyak 101 kata.



Gambar 7. List Dictionary

Setelah kata *diconary* terkumpul, langkah selanjunya yaitu menjalankan aplikasi hydra untuk melakukan penetration testing dengan menggunakan data *dictionary* yang telah dikumpulkan pada langkah sebelumnya dan didapatkan hasil beikut.



Gambar 8. Running THC-Hydra

Dari running yang telah dilakukan, hasil uji keamanan didapatkan tabel *test scenario* sebagai berikut

Test Scenario ID	Test Dictionary Attack	Test Case ID	1
Test Case Description	Melakukan Dictionary Attack ke server untuk menguji keamanan	Test Priority	High (Test yang segera dilakukan)
Pre-Requisite (Prasyarat sebelum melakukan uji)	Menonaktifkan apikey dan pembatasan Invalid API request, THC-Hydra, File Dictionary yang berisi kumpulan NIS yang terenkripsi.	Post-Requisite (Setelah melakukan uji)	N/A (Not Aplicable / tidak ada / kosong)
Test Execution Steps: Menyiapkan seluruh Mengumpulkan data enkripsi dari situs enkripsi online dalam satu file, jalankan program dictionary attack melalui CMD/ Terminal			

No	Action	Inputs	Expected Output	Actual Output	Test Result	Test Comment
1	Request Post	ID dan key enkripsi dari sistem	Response code : 202	Response code : 202	*Pass*	Attack Gagal
2	Request Post	ID dan key enkripsi generate diluar system	Response code : 400	Response code : 400	*Pass*	Attack Gagal

Sehingga Dari hasil tersebut diperoleh kesimpulan dengan gagalnya serangan *dictionary attack* yang dilakukan, membuktikan bahwakri ptografi AES yang digunakan sistem dapat dikatakan baik dalam menjaga dan mengamankan keaslian data.

4. KESIMPULAN

Berdasarkan hasil pengujian yang di dapatkan pada proses uji sebelumnya mengenai Perancangan Sistem Absensi Siswa Dengan Implementasi Qr-Code Dan Kriptografi AES-128 Berbasis Android, dapat diambil kesimpulan bahwa:

1. Dari hasil pengujian menggunakan kuisioner SUS dapat disimpulkan bahwa implementasi QR-Code pada sistem Absensi siswa berbasis android, dapat diterima oleh guru dengan grade B, murid dengan grade C, dan wali murid dengan grade B dalam melakukan proses absensi.
2. Gagalnya Dictionary Attack yang telah dilakukan untuk menguji kemanan pada server, membuktikan bahwa sistem absensi siswa berbasis android dengan implementasi AES-128, dapat mengamankan dan menjaga keaslian data absensi.

5. SARAN

Penelitian ini masih jauh dari kata sempurna, sehingga penulis menyarankan bagi penelitian selanjutnya agar dapat mengembangkan lebih lanjut sistem ini dengan :

1. Menggunakan metode kriptografi yang lain seperti AES-192, AES-256, agar dapat melakukan perbandingan antar metode yang satu dengan yang lain.

DAFTAR PUSTAKA

Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms.

Adha, R (2019). Evaluasi Usability Sistem Ujian Online Penerimaan Mahasiswa Baru Institut Teknologi dan Bisnis Bank Rakyat Indonesia.

Alexan, W., Hamza, A., & Medhat, H. (2019). An AES Double–Layer Based Message Security Scheme An AES Double–Layer Based Message Security Scheme.

Bashir, I., Rama, J., Madavaiah, J. (2012). Potential Business Applications of Quick Response (QR) Codes.

Hidayatullah, H. (2017). Implementasi Algoritma AES-128 dan QR Code Untuk Validasi Tiket Pada Perusahaan Travel PT.Bumindo Jaya Cemerlang. Skripsi. Universitas Jember.

Hidayatullah, A. & Isnaudin, E (2016). Pengenalan Kriptografi Dan Pemakaianya Sehari-Hari.

Muhammad, H., Murtinugraha, E., Musalamah, S (2020). Pengembangan Media Pembelajaran E-Learning Berbasis Moodle Pada Mata Kuliah Metodologi Penelitian.

Nuur, S., & Rahman, F. (2013). Analisis dan Perancangan Program Apliksai Music Player dengan Menggunakan Metode Kriptografi 3DES. 2013: Universitas Bina Nusantara.

Pasca Nugraha, M., & Munir, R. (2011). Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image. Konferensi Nasional Informatika.

Sharfina, Z., & Santoso, H. B. (2017). An Indonesian adaptation of the System Usability Scale (SUS). 2016 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2016, 145–148.