RABIT : Jurnal Teknologi dan Sistem Informasi Univrab
Volume 9 No. 1 | Januari 2024 : Hal : 113-119

ISSN CETAK : 2477-206
ISSN ONLINE : 2502-891

PENGAMANAN SISTEM INFORMASI PENGGUNA PADA APLIKASI *GRANT ME* MENGGUNAKAN *ANDVANCED ENCRYPTION STANDARD*

[1)] Aulyah Zakilah Ifani, [2)] Akbar Abdurrahman Jafaruddin, [3)] Antika Diana Liku, [4)]Indriani

[1)]Sistem Teknologi Informasi, Institut Teknologi dan Bisnis Nobel Indonesia
[2,3,4)]Teknik Komputer, Fakultas Teknik, Universitas Negeri Makassar
[1)]Jl. Sultan Alauddin No. 212
[2,3,4)]Jl. Mallengkeri Raya, Parang Tambung Makassar – Sulawesi Selatan - Indonesia
E-mail : *aulyah@nobel.ac.id, akbarabdulrahman8@gmail.com, antikadianaliku06@gmail.com, indriani9ndri5@gmail.com*

ABSTRAK

Pendidikan memiliki peran penting dalam menjamin kelangsungan hidup berbangsa dan bernegara, serta meningkatkan kualitas sumber daya manusia untuk berpartisipasi dalam pembangunan bangsa. Teknologi yang berkembang saat ini, termasuk dalam bidang pendidikan, dapat memudahkan pelajar dalam mempelajari hal-hal baru dan mendapatkan informasi, termasuk mengenai program beasiswa. Namun, keamanan data penerima beasiswa perlu dipertimbangkan agar tidak mudah diakses oleh orang yang tidak berhak. Kriptografi dapat menjadi pendekatan yang tepat untuk mengamankan data tersebut. Penelitian ini bertujuan untuk mengamankan informasi pengguna aplikasi Grant Me yang menggunakan algoritma AES untuk mengenkripsi username dan password penerima beasiswa serta penyedia beasiswa. Metode yang digunakan yakni pengujian eksperimental terhadap sistem yang akan dibangun menggunakan algoritma AES. Hasil penelitian menunjukkan bahwa penerapan algoritma AES dengan nilai key 256 byte membuktikan bahwa informasi login pengguna tidak mudah untuk diketahui baik dari pemilik aplikasi maupun pihak ketiga. Dengan penerapan AES sebagai sistem keamanan, dapat disimpulkan bahwa aplikasi menjadi lebih aman dari gangguan peretas.

Kata Kunci: Algoritma *AES,* Aplikasi *Grant Me*, Keamanan Data, Kriptografi.

ABSTRACT

Education has an important role in ensuring the survival of the nation and state, as well as improving the quality of human resources to participate in national development. Today's developing technology, including in the field of education, can make it easier for students to learn new things and get information, including about scholarship programs. However, the security of scholarship recipient data needs to be considered so that it is not easily accessed by unauthorized people. Cryptography can be an appropriate approach to secure such data. This research aims to secure Grant Me application user information using the AES algorithm to encrypt the username and password of scholarship recipients and scholarship providers. The method used is experimental testing of the system to be built using the AES algorithm. The results showed that the application of the AES algorithm with a key value of 256 bytes proved that user login information was not easy to know from either the application owner or a third party. With the application of AES as a security system, it can be concluded that the application becomes more secure from hacker interference.

Keyword: *AES Algorithm, Cryptography, Data Security, Grant Me app .*

PENDAHULUAN

Pendidikan saat ini merupakan salah satu bidang yang sangat diperlukan karena berperan penting dalam menjamin kelangsungan hidup berbangsa dan bernegara. Kualitas suatu Pendidikan seseorang tidak hanya pada proses dalam menempuh Pendidikan tersebut melainkan dimana seseorang tersebut menempuh Pendidikan, kualitas pengajar yang baik, dan lingkungan yang mendukung [1]. Hal itu tak luput dari biaya yang bisa dibilang cukup mahal untuk menempuh Pendidikan di perguruan tinggi.

Program beasiswa adalah solusi bagi pelajar yang ingin melanjutkan pendidikan ke

DOI : https://doi.org/10.36341/rabit.v9i1.3666

perguruan tinggi. Tujuannya adalah meningkatkan akses dan kesempatan belajar, serta mengurangi jumlah pelajar yang putus sekolah atau kuliah karena alasan finansial [2] [3]. Dengan Hadirnya Teknologi membantu pendidikan dengan memfasilitasi akses informasi dan pemberian beasiswa. Aplikasi mobile menjadi salah satu alat yang sangat berguna dalam memudahkan pelajar mendapatkan informasi dan mendaftar beasiswa [4]. Seiring perkembangannya zaman, aplikasi mobile menjadi salah satu tren yang mulai banyak diterapkan dan digunakan pada berbagai bidang karena beberapa factor yakni mudah diakses, mudah digunakan, dan membantu banyak kebutuhan dan kepentingan manusia [12].

Penggunaan aplikasi mobile juga membantu mengurangi kecurangan dalam pemberian beasiswa. Namun aplikasi yang dibuat harus memiliki keamanan tingkat tinggi untuk mengamankan data pengguna [5]. Keamanan yang bagus dan cocok untuk digunakan dalam mengamankan hal tersebut yakni dengan menggunakan pendekatan kriptografi [6]. Kriptografi memungkinkan kita mengubah data asli menjadi chipper record dengan menggunakan kunci khusus sehingga data yang dimiliki menjadi aman karena tidak mudah untuk dibaca oleh orang lain [7].

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang terkenal dan dapat digunakan untuk melindungi data. Algoritma AES mengenkripsi dan mendekripsi data menggunakan kunci kriptografi dengan panjang 128, 192, atau 256 bit pada cipher blok 128 bit [8]. *Key* merupakan nilai yang akan digunakan untuk melakukan enkripsi dan dekripsi, proses enkripsi proses mengubah sebuah pesan asli menjadi pesan dalam Bahasa sandi atau acak, dan proses dekripsi proses mengubah kembali data yang telah dienkripsi menjadi bentuk aslinya yang mudah dibaca dan dimengerti [9].

Terdapat beberapa penelitian sebelumnya yang juga membahas terkait pengamanan aplikasi ataupun sistem informasi yakni penelitian terkait autentikasi yang menggunakan teknologi *blokchain* yang mengamankan *username* dan *password* yang memiliki tingkat kerentanan terhadap peretasan pada tingkat *medium* dan *low* sebesar 68 dan 256. Hasil tersebut menunjukkan bahwa teknologi yang diterapkan dapat digunakan untuk pengamanan informasi *login* pengguna [13]. Masih menggunakan teknologi blokchain, terdapat juga penelitian yang diterapkan untuk mengamankan informasi pengguna juga namun pada penelitian tersebut dilakukan perbandingan yakni sebelum menerapkan blokchain dan setelah menerapkan blokchain. Hasil dari penelitian tersebut menunjukkan bahwa dengan menggunakan blokchain, informasi login pengguna jadi lebih aman dan tidak mudah untuk diakses oleh pihak ketiga [14].

Pada penelitian sebelumnya juga terdapat penerapan *One Time Password* (OTP) dalam mengamankan informasi pengguna pada aplikasi *M-Commerce* yang menggunakan metode *Pseudo Random Number Generator* (PRNG). Hasil dari penelitian tersebut menunjukkan bahwa OTP yang dihasilkan setiap transaksi yakni hanya 0,332 detik sehingga dapat membantu mengamankan informasi pengguna dengan cepat dan tepat [15]. Terkait keamanan informasi, terdapat juga penelitian yang mengamankan informasi manajemen pengguna yakni mengamankan data pribadi pengguna. Metode yang digunakan pada penelitian tersebut yakni dilakukan observasi dan penerapan *Single Sign-on* pada sistem informasi yang dikembangkan. Hasil dari penelitian tersebut menunjukkan bahwa data pribadi pengguna tidak mudah untuk diakses oleh pihak ketiga

DOI : https://doi.org/10.36341/rabit.v9i1.3666 *Corresponding Author* : Aulyah Zakilah Ifani

[16].

Pada penelitian terkait menggunakan aplikasi berbasis desktop dalam sebagai *platform* pengamanan [10]. Penelitian tersebut mengamankan file atau dokumen yang disimpan oleh pengguna pada aplikasi tersebut. Pada penelitian kedua, tertulis bahwa peneliti mengamankan data pribadi menggunakan AES dengan nilai *key* 128 *byte* hasil enkripsi tersebut disimpan di kunci pintar yang dibuat sehingga tidak mudah ditebak oleh orang lain [11].

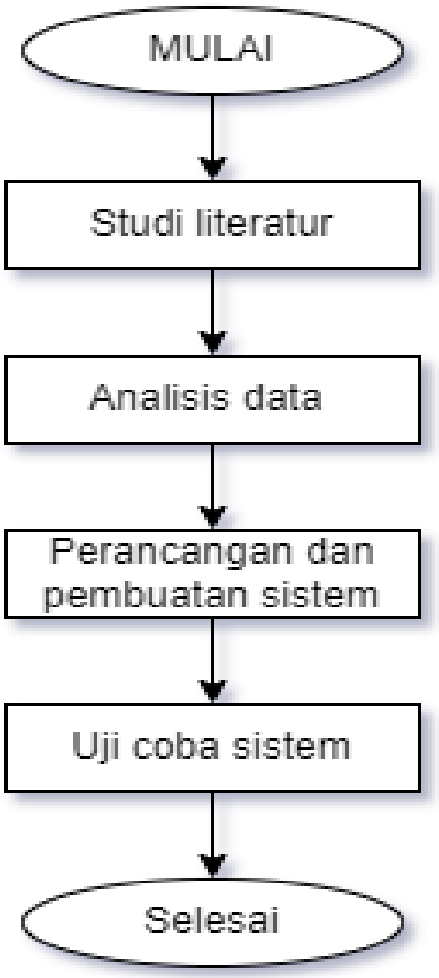
Berdasarkan penelitian-penelitian yang telah dijelaskan diatas. Peneliti bertujuan yakni menerapkan algoritma AES pada aplikasi yang dibuat yakni *Grant Me* aplikasi beasiswa berbasis mobile untuk mengamankan data *username* dan *password* pengguna yakni penerima dan penyedia. Data pengguna tersebut disimpan ke dalam *platform firebase* yang terkoneksi dengan aplikasi. Nilai key yang digunakan yakni sebesar 256 *byte*. Peneliti berharap dengan menggunakan algoritma AES dengan nilai *key* yang lebih besar dapat berdampak juga terhadap tingkat keamanan aplikasi yang akan dikembangkan.

METODE

Penelitian ini menggunakan metode eksperimental untuk menguji keamanan sistem informasi penerima beasiswa pada aplikasi Grant Me dengan menggunakan algoritma AES. Dalam hal ini, variabel independen adalah penggunaan algoritma AES, sementara variabel dependen adalah keamanan sistem informasi pengguna aplikasi Grant Me.

Diagram Alir Metode Penelitian

Untuk mempermudah dalam pengerjaan penelitian ini, maka penulis membuatkan kerangka kerja penelitian seperti pada gambar 1 berikut ini.



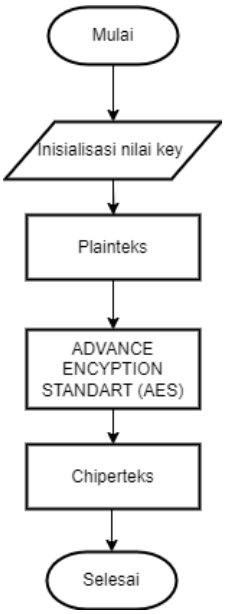
Gambar 1. Diagram Alir Metode Penelitian

Gambar 1 menunjukkan diagram alir metode penelitian. Tahapan pertama dilakukan studi literatur dengan membaca beberapa penelitian termasuk jurna, buku, dll. Tahapan kedua mulai menganalisis data. Tahapan ketiga dilakukan perancangan kemudian dilanjutkan dengan pembuatan sistem. Tahapan keempat sebagai tahapan terakhir yaitu tahapan dilakukan uji coba sistem.

Alur Kerja Sistem

Untuk mempermudah mudah proses pembuatan sistem, maka penulis membuatkan diagram alir untuk penerapan algoritma AES seperti gambar 2.

DOI : https://doi.org/10.36341/rabit.v9i1.3666 *Corresponding Author* : Aulyah Zakilah Ifani

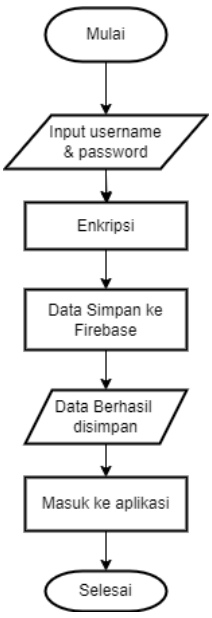


Gambar 2. Diagram Alir Sistem

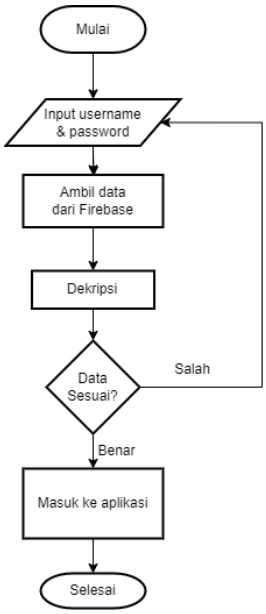
Gambar 2 menunjukkan diagram alir sistem dimana dilakukan inisialisasi nilai key, kemudian pengisian plainteks sebagai pesan aslinya diberikan keamanan berupa pemberian Algoritma Kriptografi yaitu AES. Setelah di berikan pengamanan, selanjutnya akan muncul kode unik yang disebut Chiperteks.

Alur Sistem Untuk Pengguna

Untuk mempermudah pengguna dalam mendaftarkan akun dan masuk ke aplikasi, maka penulis membuatkan diagram alir untuk registrasi dan masuk ke aplikasi seperti gambar 3 dan 4 berikut.



Gambar 3. Diagram Alir Registrasi



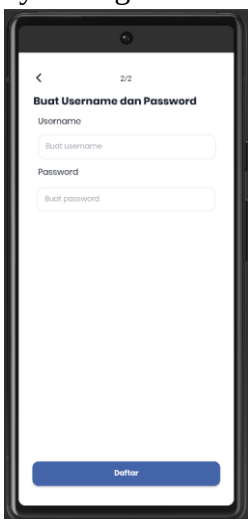
Gambar 4. Diagram Alir Masuk Aplikasi

Gambar 3 dan gambar 4 alur ketika pengguna akan melakukan registrasi (gambar 3) apabila belum memiliki akun. Setelah memiliki akun, pengguna akan di arahkan ke menu login.

HASIL

Desain Sistem

Sistem yang akan kami gunakan yakni sistem operasi android versi 12 keatas dan memiliki minimum SDK 30. Aplikasi ini akan mengamankan username dan password pengguna yakni penerima dan penyedia beasiswa. Desain sistem yang telah dibuat untuk tampilannya sebagai berikut.



Gambar 5. Tampilan Untuk Pengisian *username* dan *password*

DOI : https://doi.org/10.36341/rabit.v9i1.3666
Corresponding Author : Aulyah Zakilah Ifani

Rancangan Hasil

a. Proses enkripsi *username* dan *password* menggunakan key yang telah dibuat pada aplikasi yang akan dibangun menggunakan *library crypto* dan *security* pada Bahasa java.
   Berikut adalah rumus untuk enkripsi.
   C = K(P)
   Keterangan :
   C = Chipperteks (teks sandi acak)
   K = key (nilai kunci yang digunakan)
   P = Plainteks (teks berupa username dan password).

```
private static final String AES_KEY_256_BIT = KEY.substring(
```

Gambar 6. Potongan kode untuk nilai *key* yang dibuat

Nilai *key* tersebut dibuat secara otomatis lalu akan dimasukkan ke proses enkripsi seperti gambar berikut.

```
public static String encrypt(String value) {
    try {
        IvParameterSpec iv = new IvParameterSpec(INIT_VECTOR.getBytes());
        SecretKeySpec keySpec = new SecretKeySpec(AES_KEY_256_BIT.getBytes(),

        Cipher cipher = Cipher.getInstance( transformation: "AES/CBC/PKCS5PADDING");
        cipher.init(Cipher.ENCRYPT_MODE, keySpec, iv);

        byte[] encrypted = cipher.doFinal(value.getBytes());
        return Base64.encodeToString(encrypted, Base64.DEFAULT);
```

Gambar 7. Potongan Kode Program Enkripsi

Setelah nilai *key* dimasukkan, maka proses perubahan *plaintext* dirubah menjadi *chippertext* yang berdasarkan *byte* dari nilai *key*.

b. Proses Dekripsi *username* dan *password* key yang telah dibuat pada aplikasi yang akan dibangun menggunakan *library crypto* dan *security* pada Bahasa java.
   P = K(C)
   Keterangan :
   C = Chipperteks (teks sandi acak)
   K = key (nilai kunci yang digunakan)
   P = Plainteks (teks berupa *username* dan *password*).

   Nilai *key* yang digunakan seperti pada gambar 6. Lalu akan dimasukkan ke proses dekripsi seperti gambar berikut.

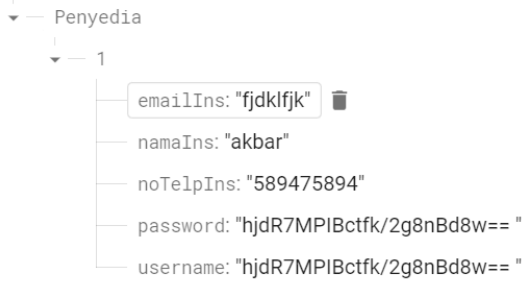
```
public static String decrypt(String encrypted) {
    try {
        IvParameterSpec iv = new IvParameterSpec(INIT_VECTOR.getBytes());
        SecretKeySpec keySpec = new SecretKeySpec(AES_KEY_256_BIT.getBytes(),

        Cipher cipher = Cipher.getInstance( transformation: "AES/CBC/PKCS5PADDING");
        cipher.init(Cipher.DECRYPT_MODE, keySpec, iv);

        byte[] original = cipher.doFinal(Base64.decode(encrypted, Base64.DEFAULT));
        return new String(original);
```

Gambar 8. Potongan Kode Program Dekripsi

Setelah nilai *key* dimasukkan, maka proses perubahan *chippertext* dirubah menjadi *plaintext* yang berdasarkan *byte* dari nilai *key*.

Hasil

Gambar 9. Enkripsi Pada Penerima



Gambar 10. Enkripsi Pada Penyedia

Hasil dari proses enkripsi *username* dan *password* yang disimpan berbentuk sandi acak yang memiliki jumlah yang sama. Setelah dilakukan enkripsi maka ketika pengguna ingin menggunakan atau masuk ke aplikasi dilakukan proses pengecekan *username* dan *password* yang akan didekripsi terlebih dahulu. Hasil yang didapatkan dengan nilai *key* 256 byte memiliki kelebihan tersendiri yakni username dan password yang tertampil berisi sandi acak yang lebih sulit untuk ditebak dibandingkan dengan nilai key 128 byte[11].

DOI : https://doi.org/10.36341/rabit.v9i1.3666 *Corresponding Author* : Aulyah Zakilah Ifani

Dengan hasil tersebut maka penerapan algoritma AES pada aplikasi ini dapat digunakan karena memiliki kualitas keamanan yang baik dan aman.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan peneliti dapat menyimpulkan bahwa dengan algoritma AES metode keamanan pada aplikasi yang dibangun menunjukkan bahwa aplikasi tersebut menjadi lebih aman karena informasi *login* atau daftar yang dilakukan pengguna, tidak diketahui oleh siapapun baik itu pemilik aplikasi maupun pihak ketiga. Kelemahan dari penelitian yang dilakukan yakni masih belum melakukan ujicoba terhadap percobaan penyerangan peretasan pada informasi pengguna. Sehingga masih belum teruji secara teknis atau percobaan peretasan.

Peneliti berharap pada penelitian selanjutnya dapat melakukan percobaan peretasan pada aplikasi Grant Me pada bagian informasi *login* dan pendaftaran pengguna. Sehingga penggunaan AES dapat dibuktikan lebih lanjut dan mendapatkan hasil yang valid terhadap keamanan yang diterapkan. Untuk pengembangan selanjutnya juga penulis menyarankan tidak hanya menggunakan kriptografi namun juga menggunakan steganografi dalam pengamanan berkas pengguna.

DAFTAR PUSTAKA

[1] "Tren Penelitian Keterampilan Berpikir Kritis Pada Jurnal Pendidikan Dasar Di Indonesia | Juliyantika | Jurnal Basicedu." Https://Jbasic.Org/Index.Php/Basicedu/Article/View/2869/Pdf (Accessed Jul. 05, 2023).

[2] A. Purwanto And H. W. Nugroho, "Analisa Perbandingan Kinerja Algoritma C4.5 Dan Algoritma K-Nearest Neighbors Untuk Klasifikasi Penerima Beasiswa," *Jurnal Teknoinfo*, Vol. 17, No. 1, Art. No. 1, Jan. 2023, Doi: 10.33365/Jti.V17i1.2370.

[3] W. Susanto And A. Mulyani, "Analisa Algoritma C4.5 Terhadap Penentuan Rekomendasi Penerima Beasiswa," *Oktal : Jurnal Ilmu Komputer Dan Sains*, Vol. 1, No. 10, Art. No. 10, Oct. 2022.

[4] R. Wahyuni And Y. Irawan, "Aplikasi E-Book Untuk Aturan Kerja Berbasis Web Di Pengadilan Negeri Muara Bulian Kelas Ii Jambi," *Jurnal Ilmu Komputer*, Vol. 9, No. 1, Pp. 20–26, May 2020, Doi: 10.33060/Jik/2020/Vol9.Iss1.152.

[5] I. Riadi, A. Ifani, And R. Kusuma, "Optimization And Evaluation Of Authentication System Using Blockchain Technology," *Emerging Science Journal*, Vol. 4, Pp. 225–240, Feb. 2022, Doi: 10.28991/Esj-2021-Sp1-015.

[6] I. Riadi, H. Herman, And A. Z. Ifani, "Optimization Of System Authentication Services Using Blockchain Technology," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, And Control*, Nov. 2021, Doi: 10.22219/Kinetik.V6i4.1325.

[7] Aprizaldi * 1 , Mhd Arief Hasan2 , Debi Setiawan3, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma Aes 128 Untuk Enkripsi Dan Dekripsi Data," *Jurnal Teknik Informatika*.

[8] A. Ramadan And P. Painem, "Pengamanan Data Keuangan Menggunakan Algoritma Advanced Encryption Standard 128 Pada Pt. Charise Deo Indonesia," *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (Senafti)*, Vol. 1, No. 1, Art. No. 1, Sep. 2022.

[9] A. Ignasius And D. V. S. Y. Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," *Skanika: Sistem Komputer Dan Teknik Informatika*, Vol. 5, No. 1, Art. No. 1, Jan. 2022, Doi: 10.36080/Skanika.V5i1.2118.

[10] Tiwi Juliyantika, Hamdan Husein

Batubara, “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard”.

[11] R. Marpaung, “Implementasi Pada Sistem Informasi Penyimpanan Data Pribadi Dengan Metode Enkripsi Aes,” Vol. 2, No. 11, Art. No. 11, 2022, Accessed: Jul. 05, 2023. [Online]. Available: Http://Uti.Teknokrat.Ac.Id/Index.Php/Cyberarea/Article/View/274

[12] D. J. S. H. N. A. Bambang Ismanto, "Pengembangan Prototype Aplikasi Notifikasi Jadwal Ujian Berbasis Android," Jurnal Teknologi dan Sistem Informasi Univrab, vol. VII, no. 2, pp. 147-155, 2022.

[13] H. A. Z. I. Imam Riadi, "Pengembangan Layanan Autentikasi Berbasis Teknologi Blockchain," Journal of Applied Informatics and Computing, vol. V, no. 1, pp. 1-8, 2021.

[14] H. A. Z. I. Imam Riadi, "Optimization of system authentication services using blockchain technology," Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, vol. VI, no. 4, pp. 277-286, 2021.

[15] A. S. Muhammad Fahrizal, "Pengamanan M-Commerce Menggunakan One Time Password Metode Pseudo Random Number Generator (PRNG)," Jurnal Teknologi dan Sistem Informasi Univrab, vol. V, no. 2, pp. 108-116, 2020.

[16] E. H. H. H. R. Enggar Novianto, "Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia," Jurnal Teknologi dan Sistem Informasi Univrab, vol. VIII, no. 1, pp. 10-15, 2023.

DOI : https://doi.org/10.36341/rabit.v9i1.3666 *Corresponding Author* : Aulyah Zakilah Ifani