Pembuatan Aplikasi Penyimpanan Password Menggunakan Metode Honey Encryption Pada Android

Nouchka Indra Dewa, Agustinus Noertjahyana, Andreas Handojo
Program Studi Informatika Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131, Surabaya 60236, Indonesia
Telp. (031) – 2983455, Fax. (031) – 8417658
E-mail: C14170021@john.petra.ac.id, agust@petra.ac.id, handojo@petra.ac.id

ABSTRAK

Saat ini, penyimpanan data ini tentu sangat membutuhkan pengamanan untuk menghindari resiko – resiko seperti adanya serangan hacker, kebocoran data, atau kehilangan itu selalu ada. Salah satu tindakan untuk pengamanan ini adalah menggunakan password untuk melindungi informasi. Namun hal ini cukup beresiko dimana password yang memiliki kombinasi sukar, akan susah untuk diingat. Untuk membantu pengguna smartphone android dalam menyimpan dan mengamankan password ini didalam smartphonenya, maka dibuatlah aplikasi penyimpanan password. Aplikasi ini dibuat pada smartphone android dengan menggunakan metode kriptografi yaitu metode Honey Encryption. Dimana aplikasi pada smartphone berbasis android yang bertujuan untuk menyimpan dan mengamankan password. User dapat mengatur secara manual key yang akan digunakan pada proses enkripsi. Proses enkripsi ini dilakukan secara online sehingga user dapat melakukan request dari server untuk data keynya. Langkah online ini dapat memudahkan user saat akan menghapus dan memanage data backup online berupa key dan data text username dan passwordnya. Hasil dari penelitian ini menunjukkan bahwa sistem ini diproteksi dengan Algoritma Honey Encryption yang mampu mengamankan password yang telah disimpan. Juga menunjukkan bahwa sistem ini berhasil menerapkan Algoritma Honey Encryption untuk mengelabui user yang tidak memiliki password dengan menampilkan password yang salah.

Kata Kunci: *Kriptografi, password, Algoritma Honey Encryption*

ABSTRACT

Currently, this data storage certainly really needs security to avoid risks such as hacker attacks, data leaks, or loss that is always there. One measure for this security is to use a password to protect the information. However, this is quite risky where passwords that have difficult combinations will be difficult to remember. To help android smartphone users in storing and securing these passwords in their smartphones, a password storage application was made. This application is made on an android smartphone using a cryptographic method, namely the Honey Encryption method. Where is an application on an Android-based smartphone that aims to store and secure passwords. Users can manually set the key that will be used in the encryption process. This encryption process is done online so that the user can make a request from the server for the key data. This online step can make it easier for users to delete and manage online backup data in the form of keys and text data for their username and password. The results of this study indicate that this system is protected by the Honey Encryption Algorithm which is able to secure the stored passwords. It also shows that this system has successfully implemented the Honey Encryption Algorithm to trick users who do not have a password by displaying the wrong password.

***Keywords**: Cryptography, password, Honey Encryption Algorithm*

1. PENDAHULUAN

Perkembangan teknologi informasi pada saat ini membawa dampak yang sangat besar dalam pengelolaan data dan penyimpanan data. Penyimpanan data ini tentu sangat membutuhkan pengamanan untuk menghindari resiko – resiko seperti adanya serangan hacker, kebocoran data, atau kehilangan itu selalu ada [1]. Salah satu tindakan untuk pengamanan ini adalah menggunakan password untuk melindungi informasi. Namun hal ini cukup beresiko dimana password yang memiliki kombinasi sukar, akan susah untuk diingat. Untuk membantu pengguna smartphone android dalam menyimpan dan mengamankan password ini didalam smartphonenya, maka dibuatlah aplikasi penyimpanan password. Aplikasi ini dibuat pada smartphone android dengan menggunakan metode kriptografi yaitu metode Honey Encryption. [2].

Maka dari itu Skripsi ini membuat "Pembuatan Aplikasi Penyimpanan Password Menggunakan Metode Honey Encryption Pada Android" yaitu aplikasi pada smartphone berbasis android yang bertujuan untuk menyimpan dan mengamankan password. User dapat mengatur secara manual key yang akan digunakan pada proses enkripsi. Proses enkripsi ini dilakukan secara online sehingga user dapat melakukan request dari server untuk data keynya. Langkah online ini dapat memudahkan user saat akan menghapus dan memanage data backup online berupa key dan data text username dan passwordnya.

Aplikasi pengamanan data menggunakan algoritma Honey Encryption yang mempunyai dua teknik pembacaan yaitu teknik enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Program penyimpanan password menggunakan metode honey encryption pada android adalah sebuah program yang dapat enkripsi password di android. Yaitu mengamankan password dalam android. Dekripsi adalah mengubah file yang tidak dapat dibaca hasil proses enkripsi menjadi seperti semula. [3]

Program yang akan diuji adalah honey encryption yang dimana Honey Encryption merupakan salah satu algoritma baru dalam ilmu kriptografi, untuk itu perlu dilakukan analisis kinerja algoritma tersebut pada proses enkripsi dan dekripsi. Disini honey encryption akan diuji ke efektifan dan ke efisiensi nya pada android. Seperti yang ada dalam artikel. Tidak seperti program pada umum nya, program ini menggunakan honey encryption yang merupakan metode baru, berbeda dengan AES/DES yang merupakan metode lama dan sering diuji. Dengan encryption ini, user android akan

lebih mudah dalam mengamankan dan menyimpan password mereka. [4]

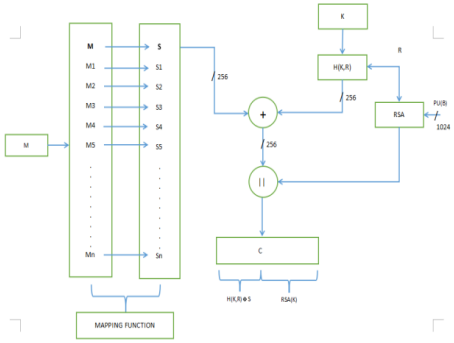
2. LANDASAN TEORI

2.1. Enkripsi

Umpamakan A dan B adalah dua pihak yang berkomunikasi, di mana A ingin mengirim pesan M ke B. Dalam proses enkripsi, pengguna akan memberikan pesan (M) dan kunci simetrik (k). Pesan ditempatkan di ruang pesan yang akan dipetakan ke nilai hash dari pesan (S) yang dihasilkan menggunakan logika SHA256. Ruang juga berisi beberapa string valid yang dipilih secara acak (M1, M2, M3, ..) yang dipetakan ke nilai seed (S1, S2, S3,...). [1]. Nilai kunci dihashkan menggunakan SHA256 dengan nilai (R) yang dihasilkan secara acak. Nilai seed ini dienkripsi dengan kunci public dari penerima B dan digabungkan dengan nilai xor dari nilai yang dipetakan pesan S dan nilai hash kunci dan (R). [5]

$$C= H(K,R)\oplus S \parallel RSA(Pub ,R)$$

Gambar 1 mewakili keseluruhan proses enkripsi yang dilakukan oleh pengirim.



Gambar 1. Proses Enkripsi Honey Encryption

2.2. Dekripsi

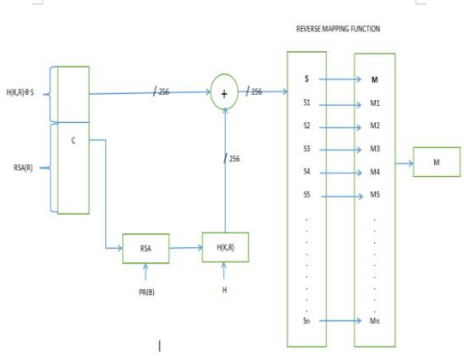
Dalam ciphertext yang dihasilkan oleh pengirim pertama 256 bit memiliki nilai xor, nilai hash kunci dan string acak yang terenkripsi RSA. Pertama di bagian penerima, sebagian RSA diambil dari teks sandi dan didekripsi dengan kunci publiknyauntuk mendapatkan string acak R. [1]. Kemudian penerima akan menggeneratekan nilai hash dengan menggunakan kunci simetrik K dan mendekripsi string acak R. Lalu, nilai yang dihasilkan adalah nilai xor dengan 256 bit pertama dari ciphertext. Hasilnya nanti akan menghasilkan nilai yang akan dipetakan secara reverse untuk mendapatkan pesan yang dihasilkan. [1].

$$H(K,R)\oplus S\oplus H(K,RSA(PRb,RSA(Pub ,R)))=S \quad (1)$$

Ketentuan Khusus

1. Nilai (R) harus mengandung minimal 10 karakter yang mencakup huruf besar, huruf kecil dan bilangan bulat.
2. Dalam perhitungan nilai hash, total jumlah putaran minimal 100000.
3. Kata sandi yang sering digunakan seperti „12345", „password", dll digunakan untuk nilai kunci K1, K2, K3,... sehingga mudah untuk memanipulasi cryptanalist.
4. Jika pengirim menggunakan kunci K yang berada dalam nilai kunci K1, k2, K3, … maka nilai seed yang diperoleh dengan nilai Ki harus diperbarui dengan nilai yang diperoleh oleh K. [1].

Gambar 2 mewakili keseluruhan proses deskripsi yang dilakukan oleh pengirim.



Gambar 2. Proses Dekripsi Algoritma Honey Encryption

3. ANALISA DAN DESAIN SISTEM

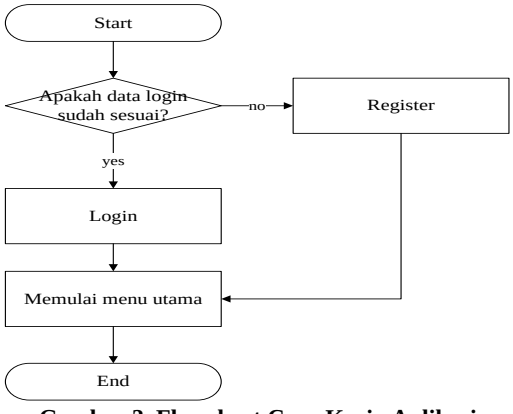
3.1. Analisa Permasalahan

Penelitian ini bertujuan untuk membantu pengguna smartphone android dalam menyimpan dan mengamankan password didalam smartphonenya. Penyimpanan data ini tentu sangat membutuhkan pengamanan untuk menghindari resiko – resiko seperti adanya serangan hacker, kebocoran data, atau kehilangan itu selalu ada. Salah satu tindakan untuk pengamanan ini adalah menggunakan password untuk melindungi informasi. Namun hal ini cukup beresiko dimana password yang memiliki kombinasi sukar, akan susah untuk diingat. Untuk membantu pengguna smartphone android dalam menyimpan dan mengamankan password ini didalam smartphonenya, maka dibuatlah aplikasi penyimpanan password. Aplikasi ini dibuat pada smartphone android dengan menggunakan metode kriptografi yaitu metode Honey Encryption. Dengan berbagai pertimbangan diatas, maka penelitian ini yang diharapkan dapat memudahkan user untuk mengamankan password didalam smartphonenya. Sehingga dapat menghindari serangan hacker, kebocoran data, dan lainnya.

3.2. Desain Flowchart

3.2.1. Flowchart Sistem

Sebelum melakukan pembuatan coding untuk membuat aplikasi, terlebih dahulu dilakukan pembuatan flowchart tentang sistem yang dibuat.

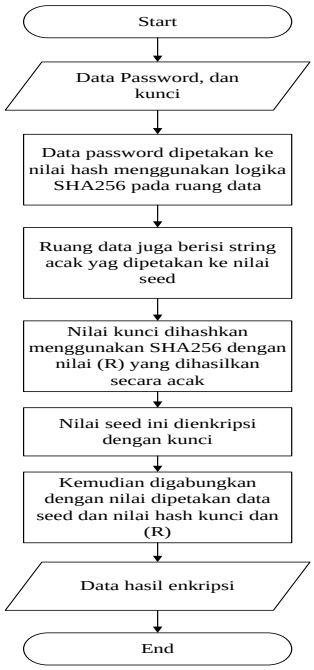


Gambar 3. Flowchart Cara Kerja Aplikasi

Gambar 3 menjelaskan tentang cara kerja aplikasi sebelum user dapat melakukan proses enkripsi dan dekripsi. Pertama, user harus melakukan login terlebih dahulu. Langkah pertama adalah user harus memasukkan data login berupa username dan password. Jika data login sudah sesuai maka user berhasil login. Jika tidak maka

user harus melakukan registrasi terlebih dahulu. Setelah berhasil login maka user dapat masuk ke halaman menu utama.

3.2.2. Flowchart Enkripsi



Gambar 4. Flowchart Enkripsi Honey Encryption

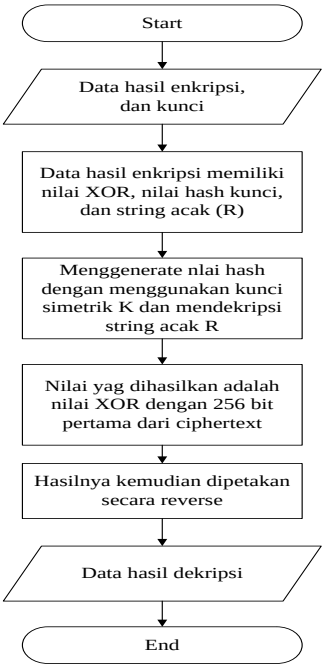
Gambar 4 menjelaskan tentang proses enkripsi Honey Encryption. Berikut adalah langkah-langkahnya:

1. Menginputkan data password yang akan disimpan dan diamankan, kemudian memasukkan kunci untuk proses Honey Encryption
2. Data password dipetakan ke nilai hash menggunakan logika SHA 256 pada ruang data
3. Ruang data juga berisi string acak yang dipetakan di nilai seed
4. Nilai kunci dihashkan menggunakan SHA256 dengan nilai (R) yang dihasilkan secara acak
5. Nilai seed ini dienkripsi dengan kunci
6. Kemudian digabungkan dengan nilai dipetakan data seed dan nilai hash kunci dan (R)
7. Didapatkan data hasil enkripsi

3.2.3. Flowchart Dekripsi

Gambar 5 menjelaskan tentang dekripsi Honey Encryption dimana proses kerjanya adalah sebagai berikut:

1. Menginputkan data password hasil enkripsi dan kunci untuk proses Honey Encryption
2. Data hasil enkripsi memiliki nilai XOR, nilai hash kunci, dan string acak (R)
3. Menggenerate nilai hash dengan menggunakan kunci sinetrik K dan mendekripsi string acak R
4. Nilai yang dihasilkan adalah nilai XOR dengan 256 bit pertama dari ciphertext
5. Hasilnya kemudian dipetakan secara reverse
6. Didapatkan data hasil dekripsi

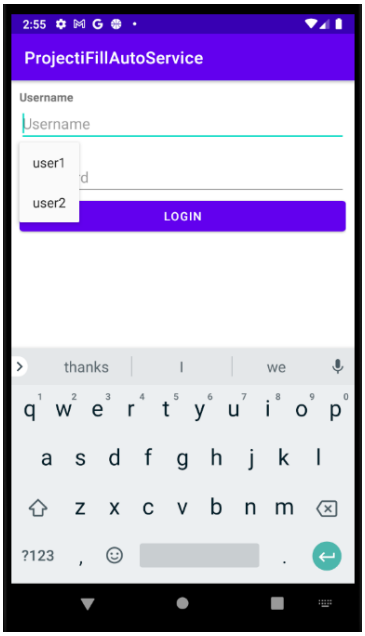


Gambar 5. Flowchart Dekripsi Honey Encryption

4. PENGUJIAN SISTEM

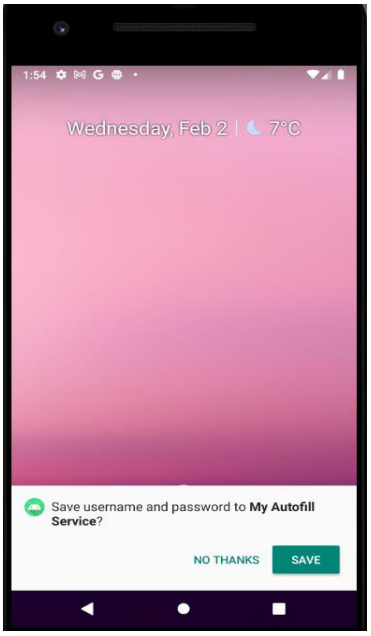
4.1. Pengujian Login

Login wajib dilakukan pada awal membuka aplikasi dengan 2 macam user yaitu user1 dan user2.



Gambar 6. Halaman Login

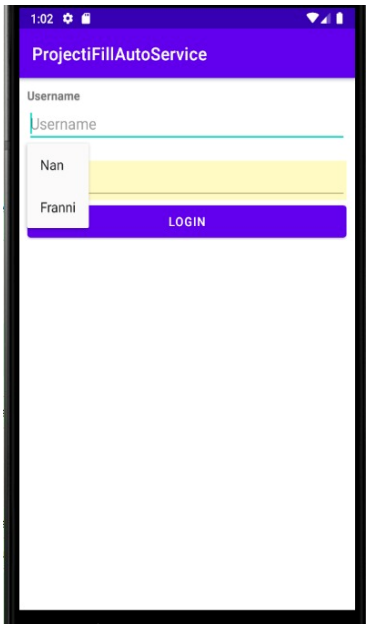
Gambar 6 merupakan halaman login yang apabila setelah berhasil melakukan login maka otomatis akan memunculkan notifikasi menyimpan username dan password pada My Autofill Service. Tampilan tersebut dapat dilihat pada Gambar 7.



Gambar 7. Notifikasi Menyimpan Username Dan Password

4.2. Halaman Enkripsi

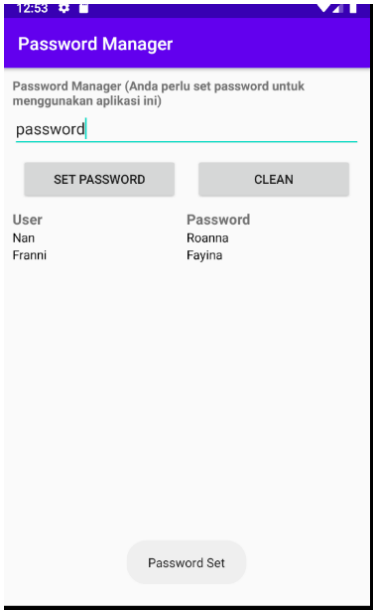
Halaman ini muncul saat menu enkripsi ditekan. Pada tampilan ini user terlebih dahulu menginput data password untuk mulai proses enkripsi. Tampilan ini dapat dilihat pada Gambar 8.



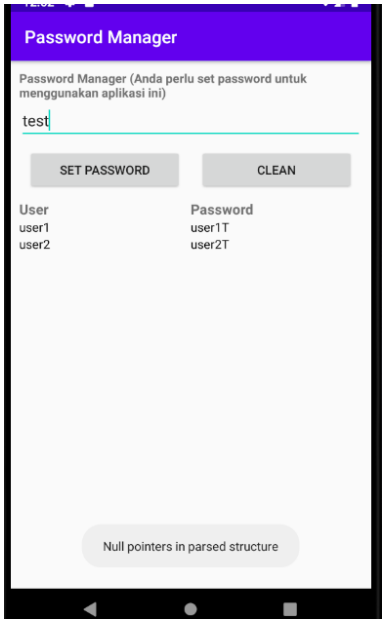
Gambar 8. Tampilan Enkripsi

4.3. Halaman Dekripsi

Halaman ini muncul saat menu dekripsi ditekan. Pada tampilan ini user harus memastikan bahwa password yang digunakan untuk menyimpan data password sama antara proses dekripsi dan enkripsi. Ketika password yang dimasukkan sudah benar maka akan menampilkan nama user dan password yang terdapat pada database dengan benar. Jika password yang dimasukkan salah maka akan menampilkan nama user dan password pada database tidak sesuai. Tampilan dekripsi dengan password yang salah dapat dilihat pada Gambar 9. Tampilan dekripsi dengan password yang benar dapat dilihat pada Gambar 10.



Gambar 9. Tampilan Dekripsi Dengan Password Yang Salah



Gambar 10. Tampilan Dekripsi Dengan Password Yang Benar

4.4. Pengujian dengan Kuesioner

Pengujian kuesioner dilakukan pada 10 mahasiswa dengan jumlah skor dan persentase kelayakannya. Dimana 10 mahasiswa responden ini dipastikan sudah pernah mencoba menggunakan aplikasi setidaknya sekali. Responden tersebut mengisi kuesioner dengan menggunakan tanda centang pada kolom jawaban sesuai dengan pengalaman yang terjadi saat menggunakan Aplikasi Penyimpanan Password menggunakan Metode Honey Encryption pada Android.

Tabel 1. Kuesioner Analisa Kepuasan Pemakaian Aplikasi

No	Pertanyaan	STS	TS	N	S	SS
1	Apakah aplikasi dapat dipasang (di-*install*) dengan mudah			1	8	1
2	Apakah aplikasi dapat melakukan fungsi yang diperlukan			2	8	
3	Bagaimana tampilan aplikasi Aplikasi Penyimpanan Password menggunakan Metode Honey Encryption pada Android			1	8	1
4	Bagaimana kemudahan dan pengoperasian Aplikasi Penyimpanan Password menggunakan Metode Honey Encryption pada Android			3	6	1
5	Bagaimana kecepatan akses Aplikasi Penyimpanan Password menggunakan Metode Honey Encryption pada Android			1	9	
6	Bagaimana fitur yang memadai pada Aplikasi Penyimpanan Password menggunakan Metode Honey Encryption pada Android			1	9	
7	Bagaimana ketepatan fungsi tombol dengan tujuan menu yang diinginkan Aplikasi Penyimpanan Password menggunakan Metode Honey Encryption pada Android			1	8	1
8	Apakah langkah – langkah operasional aplikasi dapat dipelajari dengan mudah			3	7	
9	Apakah kesalahan yang terjadi pada aplikasi dapat diperbaiki dengan mudah			2	8	
10	Apakah aplikasi dapat melanjutkan fungsi kerjanya seperti biasa setelah dilakukan perubahan / perbaikan			1	8	1
	Jumlah	0	0	16	79	5
	Jumlah skor	0	0	48	316	25
	$\sum Skor$	389				
	Persentase (%)	77,8%				

Tabel 1 merupakan hasil pengujian kuesioner analisa kepuasan pemakaian aplikasi yang digunakan untuk mengetahui bagaimana pendapat pengguna mengetahui aplikais yang sudah dibuat. Jumlah skor observasi adalah jumlah dari skor masing – masing butir pernyataan hasil observasi yang dikalikan bobot skor menurut skala likert. Skor maksimal adalah skor maksimal yang dikalikan pada skala likert yang dikalikan dengan jumlah butir soal, sehingga 5 x 10 = 50. Jumlah skor yang diharapkan adalah skor maksimal yang dikalikan dengan jumlah para ahli, sehingga 10 x 50= 500. Perhitungan persentase kelayakan dari data para ahli (tabel 1) menggunakan rumus sebagai berikut :

$$\sum Skor_{observasi} = (jumlah \times skor\ SS) + (jumlah \times skor\ S) + (jumlah \times skor\ N) + (jumlah \times skorTS) + (jumlah \times skor\ STS)$$

$$\sum Skor_{observasi} = (5 \times 5) + (79 \times 4) + (16 \times 3) + (0 \times 2) + (0 \times 1)$$

$$\sum Skor_{observasi} = 389$$

Sedangkan persentase kelayakan dari para ahli adalah sebagai berikut :

$$persentase\ kelayakan = \frac{skor\ observasi}{skor\ yang\ diharapkan} \times 100\%$$

$$persentase\ kelayakan = \frac{389}{500} \times 100\%$$

$$persentase\ kelayakan = 77{,}8\%$$

Total skor observasi dari data ahli perangkat lunak sejumlah 389 (77,8%) dari skor yang diharapkan yaitu 500 (100%). Berdasarkan standar kriteria pada tabel pedoman kriteria penilaian persentase total skor 77,8% termasuk dalam kategori Layak.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Keunggulan dari Algoritma Honey Encryption berdasarkan aplikasi yang sudah dibuat adalah mampu mengamankan password yang telah disimpan dan dapat mengelabui user yang tidak memiliki password dengan menampilkan password yang salah.
2. Kelebihan dari aplikasi menggunakan Honey Encryption adalah aplikasi ini dapat menyajikan informasi tentang password yang tersimpan pada database secara tepat, dan mudah untuk menyajikan informasi tentang password palsu bagi user yang tidak memiliki password untuk mengakses aplikasi ini.
3. Hasil uji media interaktif pada 10 mahasiswa diperoleh 389 dan persentase 77,8% dari skor yang diharapkan yaitu 500 (100%). Dimana 77,8% berdasarkan tabel pedoman kriteria penilaian termasuk dalam kategori Layak.

6. REFERENCES

[1] Elmasri, & Navathe, S. B 2011. *Fundamentals of Database. Systems* (6th Edition). New York: Addison-Wesley.

[2] Muanar. G. B, Nurnawati. E. K & Sholeh. M. (2019). Rancang Bangun Aplikasi Pencarian Perguruan Tinggi. *Jurnal SCRIPT, Vol. 7, No. 2. E-ISSN: 2338-6313*.

[3] Santhi. (2017). Implementation of Enhanced Honey Encryption for IoT Security. *IJNTR, Volume-3, Issue-3, 87-89.*

[4] Sujacka & Hasdyna. (2018). Analisis Kinerja Algoritma Honey Encryption Dan Algoritma Blowfish Pada Proses Enrkipsi dan Dekripsi. *TECHSI, Vol. 10, No. 1.*

[5] Sujacka. Hasdyuna & Mutasar (2020). Algoritma Honey Encryption dalam Sistem Pendataan Sertifikat Tanah dan Bangunan di Universitas Malikussaleh. *Informatics Journal, Volume-5, No. 3.*