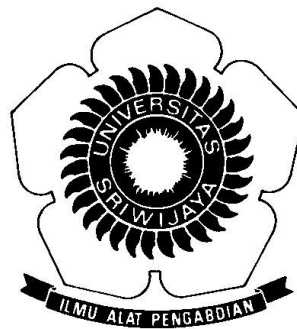


PENGAMANAN AUTENTIKASI PENGGUNA UNTUK *MOBILE*
APPS MENGGUNAKAN METODE *BCRYPT*

Diajukan Untuk Menyusun Skripsi

di Jurusan Teknik Informatika Fakultas Ilmu Komputer Unsri



Oleh:

Muhammad Farras
NIM : 09021281924158

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

Tahun 2023

LEMBAR PENGESAHAN TUGAS AKHIR

Pengamanan Autentikasi Pengguna Untuk *Mobile Apps* Menggunakan Metode BCrypt

Oleh:

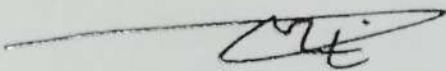
Muhammad Farras

NIM : 09021281924158

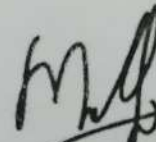
Palembang, 7 Juli 2023

Pembimbing 1

Pembimbing 2



Osvari Arsalan, M.T.
NIP. 198806282018031001



M. Qurhanul Hizqie, M.T., Ph.D.
NIP. 198712052022031006

Mengetahui,

Ketua Jurusan Teknik Informatika



Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Senin tanggal 19 Juni 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Muhammad Farras
NIM : 09021281924158
Judul : Pengamanan Autentikasi Pengguna Untuk *Mobile Apps* Menggunakan Metode Bcrypt

dan dinyatakan **LULUS**.

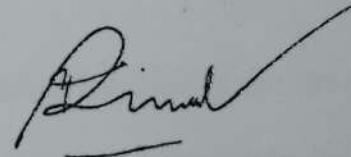
1. Ketua Penguji

Kanda Januar Miraswan, M.T.
NIP 199001092019031012



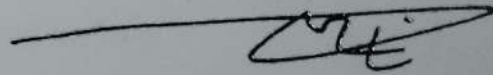
2. Penguji

Mastura Diana Marieska, M.T.
NIP 198603212018032001



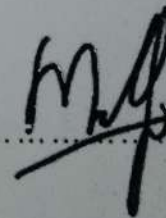
3. Pembimbing I

Osvari Arsalan, M.T.
NIP 198806282018031001



4. Pembimbing II

M. Qurhanul Rizqie, M.T., Ph.D.
NIP 198712032022031006



Mengetahui,

Ketua Jurusan Teknik Informatika



Alvi Syahrini Utami, M.Kom.
NIP 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Farras

NIM : 09021281924158

Program Studi : Teknik Informatika Reguler

Judul Skripsi : Pengamanan Autentikasi Pengguna Untuk *Mobile Apps*
Menggunakan Metode Bcrypt

Hasil Pengecekan *iThenticate/Turnitin*: 12%

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapa pun.

Palembang, 7 Juli 2023



Muhammad Farras
NIM 09021281924158

MOTTO DAN PERSEMBAHAN

Don't limit yourself. Many people limit themselves to what they think they can do. You can go as far as your mind lets you. What you believe, remember, you can achieve.

- Mary Kay Ash-

Kupersembahkan karya tulis ini kepada :

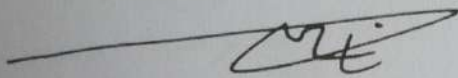
- Ibu Rina Atmajawati
- Mas Fauzi, Mas Ipan, Mbak Maya
- Seluruh Teman dan Sahabat yang kupunyai
- Fakultas Ilmu Komputer, lingkungan yang terbaik
- Universitas Sriwijaya

ABSTRACT

The increasing popularity of Mobile Applications comes with the increasing number of security breaches. User Authentication in a mobile application acts as the first defenses of application security, This means that applying preventive techniques against security attacks with hashing becomes a necessity. Bcrypt is a password hashing algorithm created using adaptive Expensive Key Blowfish encryption where a high number of encryption iterations proves to be effective against common security attack bruteforce. This study aims to implement Bcrypt hashing algorithm on user authentication in a mobile-based application. To test the effectiveness of Bcrypt algorithm, Hashing is done to a collection of texts 60 times with gradual changes in letter/words in each text. Comparisons were made against two control passwords by calculating the average avalanche effect of each sample. The average avalanche effect value obtained in the hashing test is 64.14%. From the test results it can be concluded that the implementation of Bcrypt algorithm in the user authentication feature is considered effective because it meets the SAC (Strict Avalanche Criterion) standard.

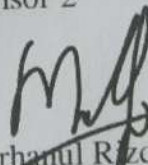
Keywords: User Authentication, Expensive Key Blowfish, Bcrypt, Mobile Application

Supervisor 1



Osvari Arsalan, M.T.
NIP. 198806282018031001

Supervisor 2

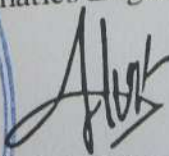


M. Qurhanul Rizqie, M.T., Ph.D.
NIP. 198712032022031006

Approved,



Head of Informatics Engineering Department



Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

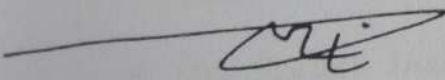
ABSTRAKSI

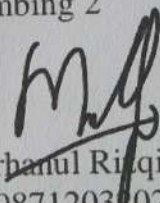
Meningkatnya popularitas teknologi berbasis mobile beriringan dengan peningkatan jumlah serangan keamanan digital. Autentikasi Pengguna didalam aplikasi mobile bertindak sebagai pengamanan pertama keamanan aplikasi, teknik pencegahan terhadap serangan keamanan yang diterapkan di autentikasi pengguna adalah *hashing*. Bcrypt adalah algoritma *hashing* yang dibuat menggunakan enkripsi *Expensive Key Blowfish*. Bcrypt bersifat adaptif dimana jumlah iterasi enkripsi yang tinggi terbukti efektif terhadap serangan umum seperti *brute force*. Penelitian ini bertujuan untuk mengimplementasikan algoritma *hashing* Bcrypt didalam fitur autentikasi pengguna aplikasi berbasis mobile. Pengujian efektifitas *hashing* Bcrypt dilakukan dengan melakukan *hashing* terhadap kumpulan teks sebanyak 60 kali dengan perubahan huruf/kata pada setiap teks. Perbandingan diterapkan terhadap dua buah *password* kontrol dengan menghitung rata-rata *Avalanche Effect* dari setiap sampel. Rata-rata nilai *avalanche effect* yang diperoleh pada pengujian *hashing* adalah sebesar 64.14%. Dari hasil pengujian dapat disimpulkan bahwa implementasi algoritma Bcrypt didalam fitur autentikasi pengguna dinilai efektif karena telah memenuhi standar SAC.

Kata Kunci: Autentikasi Pengguna, *Expensive Key Blowfish*, Bcrypt, *Avalanche Effect*, Aplikasi Mobile

Pembimbing 1

Pembimbing 2



Osvari Arsalan, M.T.
NIP. 198806282018031001


M. Qurhanul Riqie, M.T., Ph.D.
NIP. 198712031022031006

Mengetahui,

Ketua Jurusan Teknik Informatika




Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Puji syukur kehadiran Allah Swt., yang telah melimpahkan rahmat-Nya dan karunia-Nya ke manusia se alam semesta. Berkat ridha-Nya lah penyusunan Tugas Akhir ini dapat diselesaikan dengan baik dan benar sesuai ketentuan yang diberikan kepada penulis.

Terima kasih tak lupa penulis berikan kepada seluruh pihak yang mendukung penulis selama ini dalam mengerjakan Studi Independen serta laporannya, Terutama kepada keluarga dan teman-teman yang tanpa dukungan mereka rasanya mustahil menyelesaikan program yang penulis jalankan. Diantaranya :

1. Ibu Rina Atmajawati yang selalu menemani, mendengarkan cerita, memberi ketenangan dan kenyamanan kepada penulis sejak penulis masih dalam kandungan sampai menekuni perguruan tinggi sekarang.
2. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
3. Ibu Alvi Syahrini Utami, M.Kom selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya
4. Ibu Mastura Diana Marieska, M.T. selaku Penguji Tugas Akhir dan Sekretaris Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya
5. Bapak Osvari Arsalan, M.T. selaku Pembimbing Akademik dan Pembimbing Tugas Akhir serta Dosen Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

6. Bapak M. Qurhanul Rizqie, M.T., Ph.D. selaku Pembimbing Tugas Akhir serta Dosen Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya
7. Rekan-rekan satu kelas Teknik Informatika Reguler A dan teman-teman Perkuliahan, terutama teman-teman yang selalu membantu penulis dalam pelaksanaan maupun penyusunan Tugas Akhir ini.

Penulis juga berterima kasih kepada segala bantuan yang diberikan kepada penulis, baik secara fisik maupun emosional. Penulis berharap Tugas Akhir ini dapat bermanfaat baik dan sadar bahwa pastinya masih ada kesalahan atau ketidakcocokan pada laporan ini maka penulis menerima kritik dan saran. Semoga penelitian ini bisa memberi wawasan lebih serta meningkatkan ilmu pengetahuan para pembaca.

Palembang, 7 Juli 2023

Penulis,

Muhammad Farras
NIM. 09021281924158

DAFTAR ISI

HALAMAN COVER.....	i
LEMBAR PENGESAHAN TUGAS AKHIR	ii
TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI.....	iii
HALAMAN PERNYATAAN	vii
MOTTO DAN PERSEMBAHAN	v
ABSTRACT.....	vi
ABSTRAKSI	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN.....	I-1
1.1 Pendahuluan	I-1
1.2 Latar Belakang Masalah	I-1
1.3 Rumusan Masalah	I-3
1.4 Tujuan Penelitian.....	I-3
1.5 Manfaat Penelitian.....	I-4
1.6 Batasan Masalah.....	I-4
1.7 Sistematika Penulisan.....	I-4
1.8 Kesimpulan.....	I-6
BAB II KAJIAN LITERATUR	II-1
2.1 Pendahuluan	II-1
2.2 Autentikasi.....	II-1
2.3 Kriptografi	II-2
2.4 Hashing.....	II-3
2.5 Blowfish	II-4
2.6 BCrypt	II-7
2.7 Avalanche Effect	II-8
2.8 Scrum.....	II-9

2.9	Penelitian Lain yang Relevan	II-10
2.9.1	Implementation and Performance Analysis of PBKDF2, Bcrypt, Script Algorithms (Ertaul., Kaur., & Gudise. 2018)	II-10
2.9.2	A Comparative Study MD5 and SHA1 Algorithms to Encrypt REST API Aunthetication on Mobile-based Application (Setiadi et al., 2019) ...	II-10
2.9.3	Cryptanalysis of BCrypt and SHA-512 using distributed processing over the cloud (Aggarwal., Chaphekar., & Mandrekar. 2017).....	II-11
2.9	Kesimpulan.....	II-11
BAB III METODOLOGI PENELITIAN		III-1
3.1	Pendahuluan	III-1
3.2	Pengumpulan Data	III-1
3.2.1	Jenis dan Sumber Data	III-1
3.3	Tahapan Penelitian.....	III-2
3.3.1	Kerangka Kerja	III-2
3.3.2	Kriteria Pengujian	III-3
3.3.3	Alat Bantu Pengembangan	III-3
3.3.4	Flowchart Pengujian.....	III-4
3.3.5	Format Data Pengujian.....	III-5
3.3.6	Pengujian Penelitian	III-5
3.3.7	Analisis Hasil Pengujian Penelitian	III-5
3.4	Metode Pengembangan Perangkat Lunak.....	III-6
3.5	Manajemen Proyek Penelitian	III-7
3.6	Kesimpulan	III-10
BAB IV PENGEMBANGAN PERANGKAT LUNAK.....		IV-1
4.1	Pendahuluan	IV-1
4.2	Fase Perencanaan	IV-1
4.3	Fase Implementasi	IV-4
4.3.1	Use-Case Diagram	IV-4
4.3.2	Sequence Diagram	IV-11
4.3.3	Class Diagram.....	IV-14
4.4	Fase Review	IV-15
4.5	Fase Pengujian	IV-18
4.5.1	Rencana Pengujian.....	IV-18

4.5.2 Kasus Uji	IV-20
4.6 Kesimpulan	IV-22
BAB V HASIL DAN ANALISIS PENELITIAN.....	V-1
5.1 Pendahuluan	V-1
5.2 Data Hasil Percobaan/Penelitian	V-1
5.2.1 Konfigurasi Pengujian	V-1
5.2.2 Hasil Pengujian Avalanche Effect Ciphertext	V-2
5.3 Analisis Hasil Penelitian	V-14
5.4 Kesimpulan	V-15
BAB VI KESIMPULAN DAN SARAN	VI-1
6.1 Kesimpulan	VI-1
6.2 Saran	VI-1
DAFTAR PUSTAKA	xxii

DAFTAR TABEL

Tabel III-1. Rancangan Tabel Pengujian Avalanche Effect	III-5
Tabel III-2. Tabel Penjadwalan Penelitian dalam format WBS.....	III-7
Tabel IV-1. Use Case Skenario Login	IV-6
Tabel IV-2. Use Case Skenario Register	IV-7
Tabel IV-3. Use Case Skenario Pengujian Hashing	IV-9
Tabel IV-4. Rencana Pengujian Fitur Login.....	IV-18
Tabel IV-5. Rencana Pengujian Fitur Register	IV-18
Tabel IV-6. Rencana Pengujian Fitur Pengujian Hashing	IV-19
Tabel IV-7. Pengujian Fitur Login.....	IV-20
Tabel IV-8. Pengujian Fitur Register.....	IV-20
Tabel IV-9. Pengujian Fitur Pengujian Hashing.....	IV-21
Tabel V-1. Tabel Hasil Pengujian Avalanche Effect Perbedaan Satu Huruf pada Password Kontrol 'Muhammad Farras'	V-2
Tabel V-2. Tabel Hasil Pengujian Avalanche Effect Perbedaan Kata pada Password Kontrol 'Muhammad Farras'	V-5
Tabel V-3. Tabel Hasil Pengujian Avalanche Effect Perbedaan Satu Huruf pada Password Kontrol 'Merdeka atau Mati'	V-8
Tabel V-4. Tabel Hasil Pengujian Avalanche Effect Perbedaan Kata pada Password Kontrol 'Merdeka atau Mati'	V-11

DAFTAR GAMBAR

Gambar I-1.	Average Weekly Cyber Attacks per Organization by Region.....	I-1
Gambar II-1.	Struktur Feistel Algoritma Blowfish.....	II-5
Gambar II-2 .	Visualisasi Metodologi Scrum.....	II-9
Gambar III-1 .	Diagram Alur Kerangka Kerja Penelitian.....	III-2
Gambar III-2 .	Skema Flowchart Pengujian	III-4
Gambar IV-1.	Project Story Board	IV-2
Gambar IV-2.	Use Case Diagram Sistem Autentikasi Pengguna	IV-5
Gambar IV-3.	Sequence Diagram Login	IV-11
Gambar IV-4.	Sequence Diagram Register	IV-12
Gambar IV-5.	Sequence Diagram Pengujian Hashing.....	IV-13
Gambar IV-6.	Class Diagram Project	IV-14
Gambar IV-7.	Laporan Sprint 1	IV-15
Gambar IV-8.	Laporan Sprint 2.....	IV-15
Gambar IV-9.	Laporan Sprint 3.....	IV-16
Gambar IV-10.	Laporan Sprint 4.....	IV-16
Gambar IV-11.	Laporan Sprint 5.....	IV-17
Gambar IV-12.	Laporan Sprint 6.....	IV-17

BAB I

PENDAHULUAN

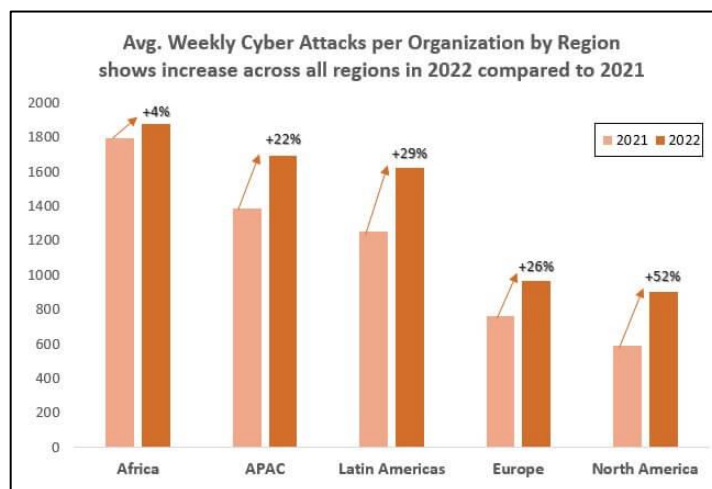
1.1 Pendahuluan

Bab I membahas latar belakang dan rumusan dari permasalahan penelitian, tujuan serta manfaat dari penelitian, batasan masalah, sistematika penulisan dan kesimpulan berdasarkan penelitian yang dilakukan.

1.2 Latar Belakang Masalah

Smartphone terbukti semakin populer setiap tahun di Indonesia, Dengan jumlah pengguna *smartphone* yang meningkat pesat dari 170 juta pengguna di tahun 2021 menjadi 192.15 juta pengguna di tahun 2022 (Laricchia., 2022).

Menurut Check Point Research (2023), peningkatan pengguna yang cepat seiring dengan meningkatnya serangan *cyber attack* terhadap aplikasi-aplikasi *Mobile* seperti yang ditunjukkan pada grafik I-1.



Gambar I-1. Average Weekly Cyber Attacks per Organization by Region

Dari gambar grafik I-1, dapat diambil kesimpulan bahwa dibutuhkan peningkatan keamanan aplikasi berbasis mobile untuk menjaga data-data sensitif didalam aplikasi-aplikasi yang digunakan oleh masyarakat secara umum.

Keamanan terhadap *cyber attack* merupakan tanggung jawab dari penyedia dan pengembang aplikasi berbasis mobile. Salah satu implementasi mekanisme keamanan yang dilakukan adalah melakukan autentikasi. Autentikasi merupakan hal penting untuk menjamin hanya pengguna yang sudah disetujui yang bisa mengakses fitur didalam aplikasi berbasis mobile.

Metode autentikasi yang paling banyak digunakan adalah password. Tetapi, pengguna internet masih banyak yang menggunakan password secara tidak aman sehingga dibutuhkan implementasi sistem keamanan yang dapat menjaga kerahasiaan password tersebut. (Boonkrong et al., 2016).

Salah satu implementasi umum untuk menjaga kerahasiaan password adalah melakukan *hashing*. Bcrypt diusulkan oleh penulis untuk digunakan didalam fitur autentikasi pengguna aplikasi berbasis mobile dikarenakan Bcrypt terbukti efektif terhadap serangan *rainbow table* dan *brute force* (Batubara et al., 2021).

Untuk menentukan keamanan dari algoritma *hashing* yang digunakan, *Avalanche effect* akan dihitung berdasarkan ciphertext hasil *hashing* Bcrypt. Nilai *Avalanche effect* yang baik membuktikan algoritma kriptografi tersebut memiliki tingkat randomisasi yang tinggi (Vadaviya et al., 2015).

Pada penelitian ini, Bcrypt akan diimplementasikan ke dalam aplikasi berbasis mobile yang nantinya akan melakukan autentikasi serta diuji keamanan

autentikasi penggunaanya dengan menghitung nilai *Avalanche effect* dari teks yang sudah di *hashing* oleh Bcrypt.

1.3 Rumusan Masalah

Rumusan masalah dari penelitian yang dilakukan adalah sebagai berikut:

1. Bagaimana membangun fitur autentikasi pengguna pada aplikasi berbasis mobile dengan menggunakan algoritma Bcrypt.
2. Bagaimanakah keamanan hasil implementasi autentikasi pengguna didalam aplikasi berbasis mobile yang dibuat dengan algoritma Bcrypt.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan dari penelitian yang dilakukan adalah sebagai berikut:

1. Membangun aplikasi berbasis mobile dengan mengimplementasikan fitur autentikasi pengguna menggunakan algoritma Bcrypt
2. Melakukan pengujian keamanan fitur autentikasi pengguna yang telah dibuat dengan menghitung nilai *avalanche effect* dari ciphertext hasil password *hashing* yang dilakukan oleh Bcrypt

1.5 Manfaat Penelitian

Penelitian yang dijalankan diharapkan memberi manfaat sebagai berikut:

1. Penelitian ini dapat menghasilkan fitur autentikasi pengguna pada aplikasi berbasis mobile dengan menggunakan algoritma Bcrypt
2. Penelitian ini dapat menjadi rujukan dalam penelitian lebih lanjut mengenai keamanan autentikasi pengguna Mobile Application

1.6 Batasan Masalah

Untuk mencegah penelitian ini terlalu meluas dan tidak terarah, penulis membatasi lingkup masalah pada penelitian ini dengan rincian sebagai berikut: Mobile Application yang dibangun hanya memiliki fungsionalitas autentikasi pengguna, halaman utama, dan penampilan ciphertext hasil password *hashing*.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut:

(i) **BAB I. PENDAHULUAN**

Bab ini membahas secara rinci tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan, dan kesimpulan.

(ii) **BAB II. TINJAUAN PUSTAKA**

Bab ini membahas tentang landasan teori yang menjadi dasar penelitian, seperti deskripsi tentang kriptografi, autentikasi data,

hashing, avalanche effect, algoritma Bcrypt, algoritma Blowfish, dan beberapa kajian literatur yang relevan dengan penelitian.

(iii) **BAB III. METODOLOGI PENELITIAN**

Bab ini membahas secara rinci mengenai kerangka kerja, instrumen penelitian, data yang digunakan dalam penelitian, dan perencanaan dari kegiatan – kegiatan penelitian.

(iv) **BAB IV. PENGEMBANGAN PERANGKAT LUNAK**

Bab ini membahas secara rinci mengenai proses pengembangan perangkat lunak yang sudah direncanakan pada BAB III, dan melakukan pengujian pada perangkat lunak yang digunakan untuk penelitian.

(v) **BAB V. HASIL DAN ANALISIS PENELITIAN**

Bab ini membahas secara rinci mengenai hasil dari perangkat lunak yang digunakan pada penelitian dan melakukan analisa pada hasil tersebut.

(vi) **BAB VI. KESIMPULAN DAN SARAN**

Bab ini membahas secara rinci mengenai kesimpulan yang dapat ditarik dari hasil penelitian yang telah dilakukan serta saran – saran yang dapat digunakan untuk mengembangkan penelitian tersebut.

1.8 Kesimpulan

Bab I menjelaskan terkait latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, Batasan masalah dan sistematika penulisan. Berdasarkan penjelasan diatas, penelitian dalam pengamanan autentikasi pengguna untuk aplikasi berbasis mobile menggunakan metode Bcrypt memberikan hasil yang baik sesuai hipotesis

DAFTAR PUSTAKA

- Boonkrong, Sirapat., & Soombonpattanakit, Chaovalit. (2016). Dynamic Salt Generation and Placement for Secure Password Storing. *IAENG International Journal of Computer Science*. 43, 27-36
- Sriranya, P., & Karthika, R.A. (2015). Providing Password Security By Salted Password Hashing Using Bcrypt Algorithm. *ARPN Journal of Engineering and Applied Sciences*. 10(13), 5551-5556
- Ertaul, Levant., Kaur, Manpreet., & Gudise, Venkata Arun Kumar R. (2018). Implementation and Performance Analysis of PBKDF2, Bcrypt, Scrypt Algorithms. *2016 International Conference of Wireless Networks (ICWN)*, 66-72.
- Batubara, Toras Pangiduan., Efendi, Syahril., & Nabanan, Erna Budhiarti. (2021). Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force. *J. Phys.: Conf. Ser.* **1811** 012129.
- Batubara, Toras Pangiduan., Efendi, Syahril., & Nabanan, Erna Budhiarti. (2021). Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force. *J. Phys.: Conf. Ser.* **1811** 012129.
- Laricchia, Frederica. (2022). Smartphone users by country worldwide 2021. Diambil dari <https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/>. Diakses pada 15 Februari 2023
- Newzoo. (2022). Top Countries by Smartphone Users. Diambil dari <https://newzoo.com/insights/rankings/top-countries-by-smartphone-penetration-and-users>. Diakses pada 15 Februari 2023
- Patil, Priyadarshini., Narayankar, Prasahant., G, Narayan D., & M, Meena S. (2015). A Comprehensive Evaluation of Cryptographic Algorithms : DES, 3DES, AES, RSA, And Blowfish. *International Conference on Information Security & Privacy (ICISP2015)*. 617-624
- Maqsood, Faiqa., Ahmed, Muhammad., Ali, Muhammad M., Munam, Ali Shah. (2017). Cryptography : A Comparative Analysis for Modern Techniques. (*IJACSA*) *International Journal of Advanced Computer Science and Applications*. 8(6), 442-447

- Kuhlreshta, Anuhi., Kumar Dubey, Sanjay. (2014). A Literature Review on Sniffing Attacks in Computer Network. (*IJAERS*) *International Journal of Advanced Engineering Research and Science*. 1(2), 32-37
- Aggarwal, Kirti., Saini, Jaspal Kaur., Verma, Harsh K. (2013). Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers.) *International Journal of Computer Applications*. 68(25), 10-16
- Chi, Lianhua., & Zu, Xinquan. (2017). Hashing Techniques: A survey and taxonomy. *ACM Computing Surveys (CSUR)*, 50(1), 1-36
- Usmonov, M. (2021). Identification and Authentication. *International Journal of Academic Pedagogical Research (IJAPR)*. 5(1), 39-47
- Paul, A., Nalwaya, A. (2019). React Native for Mobile Development: Harness the Power of React Native to Create Stunning IOS and Android Applications Apress. 2-21
- Ruby, S., Copeland, D. B., & Thomas, D. (2020). Agile Web Development with Rails 6. Pragmatic Bookshelf.
- Subramanian, H., & Raj, P. (2019). Hands-On RESTful API Design Patterns and Best Practices: Design, develop, and deploy highly adaptable, scalable, and secure RESTful web APIs. Packt Publishing Ltd.
- Harba, H. S. (2015). Design and Implementation of Multilevel Secure Database in Website. *Journal of Information Engineering and Applications*, 5(12), 11-18.
- Najib, A. F., Rachmawanto, E. H., Sari, C. A., Sarker, K., & Rijati, N. (2019, July). A comparative study MD5 and SHA1 algorithms to encrypt REST API authentication on mobile-based application. *2019 International Conference on Information and Communications Technology (ICOIACT)*, 206-211.
- Aggarwal, A., Chaphekar, P., & Mandrekar, R. (2015). Cryptanalysis of bcrypt and SHA-512 using distributed processing over the cloud. *International Journal of Computer Applications*, 128(16).
- Check Point Research. (2023). 38% Increases in 2022 Global Cyberattacks. Diambil dari <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>. Diakses pada 15 Februari 2023
- Muthavhine, K. D., & Sumbwanyambe, M. (2018, March). An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect. *2018 International Conference on Information and Communications Technology (ICOIACT)*, 114-119.

Keiser, J., & Lemire, D. (2021). Validating UTF-8 in less than one instruction per byte. *Software: Practice and Experience*, 51(5), 950-964.

Webster, A. F., & Tavares, S. E. (1985). On the design of S-boxes. *Conference on the theory and application of cryptographic techniques*, 523-534.