APLIKASI ANDROID PROTEKSI KEAMANAN UNTUK MENDETEKSI ILEGAL AKSES: BRUTE FORCE

Suryani Suryani[*1)], Indra Samsie[2)]
[1,2]STMIK Dipanegara Makassar; Jl. Perintis Kemerdekaan No.Km.9, Kec. Tamalanrea, Kota Makassar, Sulawesi Selatan, 90245, Telp/Fax: 0411-587194/0411-588283
Program Studi Teknik Informatika, STMIK Dipanegara, Makassar
e-mail: suryani187@dipanegara.ac.id[1)], indrasamsie@gmail.com[2)]

Abstrak

Proteksi terhadap sistem online khususnya website sangat mengandalkan peran administrator yaitu melakukan monitoring website. Administrator tidak dapat melakukan monitoring secara terus menerus karena keterbatasan waktu yang dimiliki. Sedangkan serangan maupun upaya Illegal access khususnya brute force dari attacker terhadap website bisa terjadi kapan saja. Belum adanya mekanisme penanganan yang dapat dilakukan melalui perangkat mobile terhadap upaya Illegal access pada website, menjadi salah satu kelemahan suatu website. Metode yang digunakan yaitu model proteksi dengan pemanfaatan teknologi firebase dalam notifikasi, dimana aplikasi mendeteksi upaya Illegal access dan secara otomatis mengirimkan notifikasi kepada administrator melalui gawai (peranti teknologi yang diciptakan lebih canggih dari teknologi sebelumnya) yang dimiliki. Idealnya website telah menggunakan teknologi Secure Socket Layer (SSL) yang merupakan standar keamanan website dengan teknologi SSL, semua data akan dienkripsi sebelum dikirim ke server. Selain mengandalkan monitoring berupa notifikasi, untuk mempercepat pengamanan terhadap upaya Illegal access, administrator dapat melakukan proteksi dini melalui aplikasi. Proteksi dini berupa penonaktifan sementara user serta mengaktifkan mode hibernasi (mode yang memungkinkan komputer untuk mematikan daya sepenuhnya) pada sistem apabila ancaman serangan terus meningkat. Dengan demikian hasil dari penerapan metode tersebut diharapkan agar administrator dapat lebih cepat dan mudah melakukan monitoring dan penanganan website dari upaya Illegal access dari attacker.

Kata Kunci—*proteksi keamanan, brute force, aplikasi mobile, Illegal access, website*

Abstract

The protection of online systems, especially websites, relies heavily on the role of the administrator, which is monitoring the website. Administrators cannot monitor continuously because of the limited time they have. While attacks and Illegal access especially brute force attempts from attackers against websites can occur at any time. There is no handling mechanism that can be done through mobile devices to Illegal access efforts on the website, becoming one of the weaknesses of a website. The method used is a protection model with the use of firebase notification technology, where the application detects Illegal access attempts and automatically sends notifications to administrators via their devices (technology devices that are created more sophisticated than previous technologies). Ideally, the website has used Secure Socket Layer (SSL) technology which is a website security standard with SSL technology, all data will be encrypted before sending it to the server. Besides relying on monitoring in the form of notifications, to speed up security on Illegal access efforts, the administrator can do early protection through the application. That is in the form of temporary deactivation of the user and activates hibernation mode (a mode that allows the power of the computer will be turn off completely) on the system if the threat of attack continues to increase. Therefore the result of applying the method is expected that the administrator can monitor and handle websites from Illegal access efforts from attackers more quickly, precisely and easily.

Keywords—*security protection, brute force, mobile application, Illegal access, website*

1. PENDAHULUAN

Perkembangan Aplikasi online saat ini semakin tidak bisa dihindarkan karena kebutuhan untuk mengakses informasi berbanding lurus dengan kebutuhan akan keamanan dari aplikasi online tersebut. Selain itu kebutuhan terhadap tenaga ahli di bidang keamanan jaringan yang semakin tinggi untuk melindungi aplikasi online dari upaya kejahatan yang dilakukan oleh penyerang (*attacker*) dengan menyusup ke dalam suatu sistem *website* secara tidak sah, tanpa izin atau tanpa sepengatahuan dari pemilik aplikasi *online* (*Illegal access*).

Proteksi terhadap sistem online khususnya *website* sangat mengandalkan peran administrator yaitu melakukan monitoring terhadap *website* tersebut. administrator akan melakukan monitoring terhadap semua aktifitas terkait, termasuk aktifitas yang dianggap tidak biasa atau mencurigakan pada *website*.

Administrator tidak dapat melakukan monitoring secara terus menerus terhadap sistem online tersebut. Adanya keterbatasan waktu yang dimiliki administrator menyebabkan upaya *Illegal access* dari *attacker* terhadap *website* bisa terjadi kapan saja dan dimana saja.

Penelitian yang terkait dengan keamanan *website* telah diteliti sebelumnya, peneliti Komarudin dan Asep Ririh Riswaya membangun aplikasi keamanan *website* dengan melakukan enkripsi denga metode Hash MD5 (Message-Digest algorithm 5), semua data yang ada didalam aplikasi dienkripsi terlebih dahulu menggunakan metode MD5. Dan peneliti Rudi Ridho Rohmansyah dan Heru Nurwasito meneliti tentang membangun Aplikasi *Mobile* untuk Sistem Keamanan Kantor Menggunakan NFC (*Near-Field Communication*) Kemudian peneliti Dias Utomo, Muchammad Sholeh, dan Arry Avorizano meneliti tentang membangun sistem *mobile* monitoring keamanan web aplikasi menggunakan *Suricata* dan *Boot Telegram Channel*. Perangkat yang dibuat akan mengirimkan notifikasi ke perangkat mobile, sistem notifikasi dilakukan dengan memicu sensor arduino, sensor arduino terlebih dahulu akan mengirimkan data kedalam *firebase realtime database* lalu diterima oleh aplikasi *mobile* dalam bentuk notifikasi sistem monitoring keamanan *website* dengan teknologi *Suricata* dan *Bot Telegram Channel*, aplikasi akan mengirimkan notifkasi ke akun telegram *messenger* ke ponsel administrator apabila terjadi serangan *website*. Secara umum belum ada mekanisme penanganan yang dapat dilakukan melalui perangkat *mobile*.

Belum adanya mekanisme penanganan yang dapat dilakukan melalui perangkat *mobile* terhadap administrator apabila ada upaya *Illegal access* pada *website* tersebut, menjadi salah satu kelemahan suatu *website*. Selain mengandalkan monitoring yang dilakukan administrator, model proteksi juga bisa memanfaatkan teknologi notifikasi yang terus berkembang hingga saat ini.

Aplikasi yang mendeteksi upaya *Illegal access* secara otomatis akan mengirimkan notifikasi kepada administrator melalui gawai (peranti teknologi yang diciptakan lebih canggih dari teknologi sebelumnya) yang dimiliki administrator. Idealnya *website* telah menggunakan teknologi *Secure Socket Layer* (SSL) yang merupakan standart keamanan *website* dengan teknologi SSL semua data akan dienkripsi sebelum dikirim ke server, dan selain mengandalkan monitoring berupa notifikasi, Untuk mempercepat pengamanan terhadap upaya *Illegal access*, administrator dapat melakukan proteksi dini melalui aplikasi.

Menurut Fithria, N, Brute force attack atau Exhaustive attack adalah sebuah teknik serangan yang menggunakan percobaan terhadap semua kunci yang mungkin untuk mengungkap plainteks/kunci. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan

mottonya: "When in doubt, use brute-force" (jika ragu, gunakan brute-force). Teknik tersebut adalah teknik yang paling banyak digunakan untuk memecahkan password, kunci, kode atau kombinasi. Cara kerja metode ini sangat sederhana yaitu mencoba semua kombinasi yang mungkin.

Proteksi dini dari serangan brute force bisa berupa penonaktifan sementara user yang terdeteksi melakukan upaya *Illegal access* serta mengaktifkan mode *hibernasi* (mode yang memungkinkan komputer untuk mematikan daya sepenuhnya) pada sistem *website* apabila ancaman serangan terus meningkat. Selain itu administrator dapat melakukan pengaktifan kembali user yang telah diblokir serta mengaktifkan kembali sistem *website* melalui aplikasi android administrator.

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah Eksperimental, yaitu penelitian yang mencoba mengimplementasikan mekanisme teknologi notifikasi *firebase* perangkat *mobile* dalam upaya melakukan proteksi dini upaya *Illegal access* : *brute force* terhadap *website*.

Langkah - langkah perancangan dalam penelitian ini dibagi menjadi beberapa bagian, antara lain :

a) Pengumpulan data berupa pengumpulan data penunjang yang dapat membantu perancangan sistem.
b) Desain Logic yaitu pemilihan strategi arsitektur.
c) Pengkodean yaitu implementasi model ke dalam bahasa pemrograman.
d) Pengujian Perangkat Lunak dilakukan setelah proses coding selesai untuk melakukan verifikasi dan validasi perangkat lunak.
e) Implementasi yaitu abstraksi dari penerapan (implementasi) suatu sistem software.

Alat yang digunakan dalam penelitian berupa :

a) Perangkat Keras (Hardware)
    1. Laptop intel(R) core(TM) i5 CPU M380 @ 2.73G.Hz
    2. Perangkat Smartphone Jenis Sony Xperia C3.
b) Perangkat Lunak (Software)
    1. Windows 7 Ultimate 32-bit
    2. Java SE Development Kit 7.
    3. Android Studio 3.0
    4. Xamp
    5. Navicat MySQL
c) Desain Konseptual
    Alat bantu yang digunakan yaitu UML. Dalam perancangan sistem peneliti menggunakan Uses Case Diagram, Activity Diagram, Class Diagram, dan Sequential Diagram.

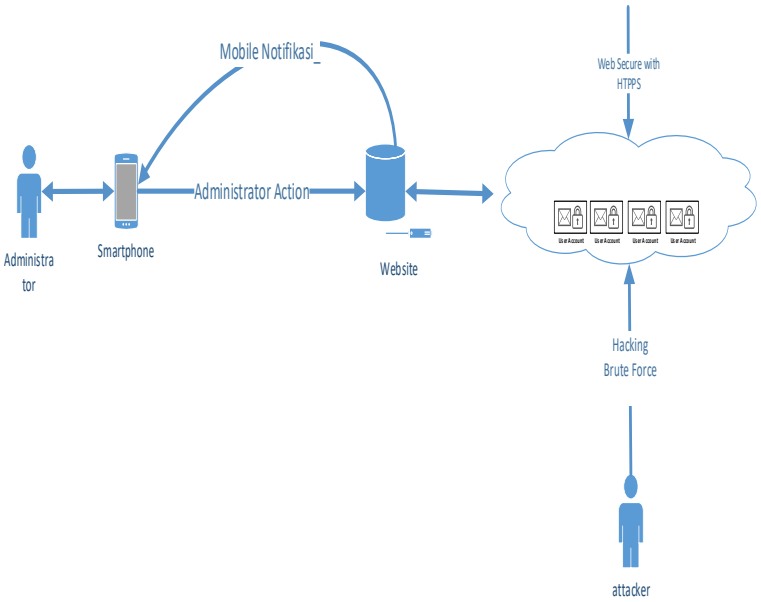
Metode pengujian yang digunakan adalah pengujian *Black-box*, dimana berusaha menemukan kesalahan dalam kategori sebagai berikut :

1. Fungsi-fungsi yang tidak benar atau hilang.
2. Kesalahan interface.
3. Kesalahan dalam struktur data atau akses database eksternal.
4. Kesalahan kinerja

3. HASIL DAN PEMBAHASAN

Desain Sistem yang dibangun :

a) Arsitektur Sistem

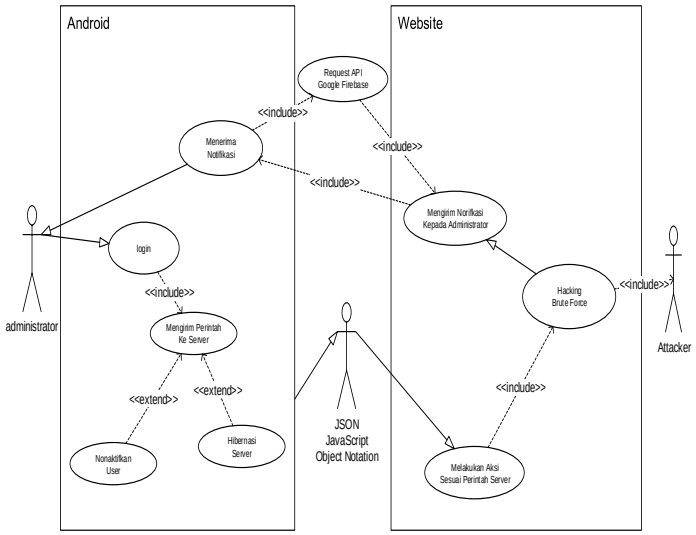


Gambar 1 Arsitektur Sistem

Arsitektur sistem merupakan arsitektur aplikasi proteksi *Illegal access* dari akses *hacking* dengan *brute force*. Apabila *website* terindentifikasi ada upaya serangan *brute force* dari *attacker*, maka sistem secara otomatis akan mengirimkan notifikasi ke aplikasi *mobile* administrator. Aksi dapat dilakukan dari aplikasi *mobile* berupa penonaktifan user/email yang terdientifikasi telah melakukan *brute foce*, serta dapat melakukan penonaktifan *website* sementara melalui aplikasi *mobile*.

Sistem yang dirancang memiliki dua bagian yang akan menggunakan sistem ini yaitu website sebagai prototype website yang akan diserang, serta aplikasi android yang dimiliki oleh *website*, unutk melakukan aksi cepat tanggap dalam mengamankan website tersebut dari upaya *Illegal access*.

b) Use Case Diagram



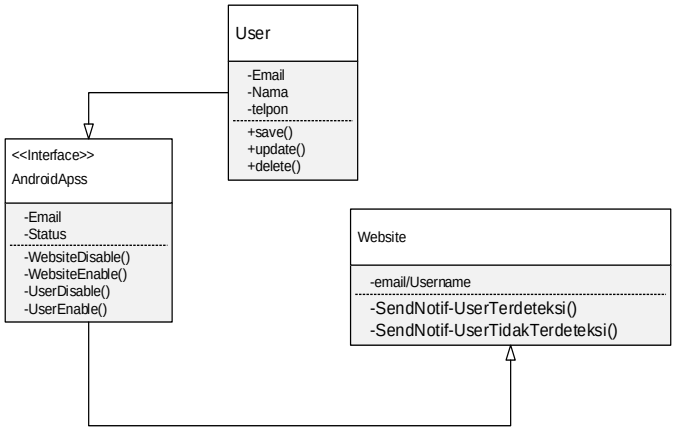
Gambar 2 Use Case Diagram

Usecase diagram menggambarkan proses dari sistem yang dibangun, yang memiliki dua platform yaitu plafrom *website* sebagai prototype dan platform android sebagai aplikasi yang digunakan *administrator* dalam memproteksi dini *website*.

Pada plafrom *website* yang dibangun sebagai prototype uji coba, attacker melakukan hacking brute force dengan mencoba secara berulang-ulang memasukkan user dan password pada website untuk login. Selanjutnya secara otomatis sistem akan mengirim notifikasi kepada administrator jika upaya login gagal atau terdeteksi illegal akses.

Pada platform android administrator dapat melakukan login ke aplikasi, kemudian mengirim perintah ke server untuk melakukan hibernasi server atau menonaktifkan user. Selain itu administrator dapat menerima pemberitahuan atau notifikasi sewaktu-waktu jika terjadi illegal logging khususnya serangan brute force, dengan memanfaatkan Request API Google Firebase.

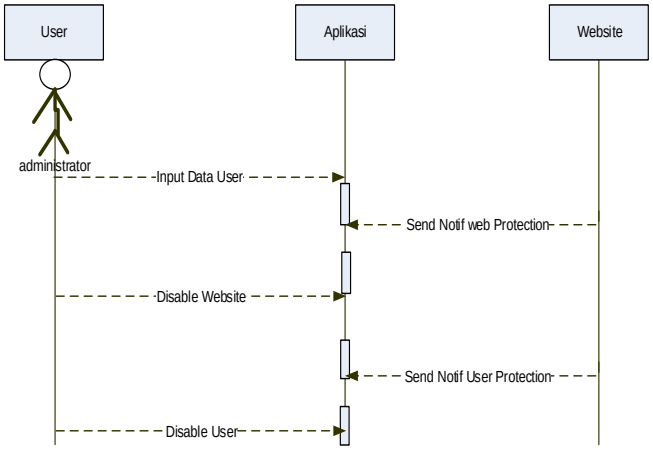
a) Class Diagram



Gambar 3 Class Diagram

Class diagram menggambarkan class-class yang tercipta pada aplikasi baik itu class yang ada di *website* maupun class yang ada di aplikasi android yang memiliki keterhubungan.

b) Sequence Diagram

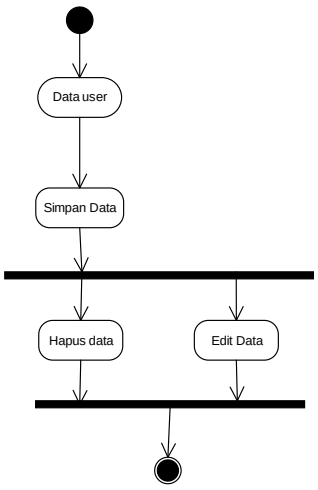


Gambar 4 Sequence Diagram

Sequence diagram di atas menggabarkan arus data yang dikirim dan diterima dari aplikasi dan pengguna sistem atau *user*, maupun data yang dikirim dari aplikasi android ke aplikasi *website*.

c) Activity Diagram

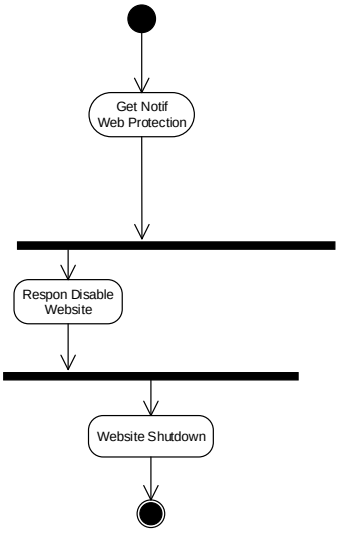
1. Activity diagram Input Data User



Gambar 5 Activity diagram Input User

Class diagram input user adalah class diagram pada aplikasi android yang memperlihatkan proses aktivitas untuk input data *user*, simpan, hapus dan edit data *user*.

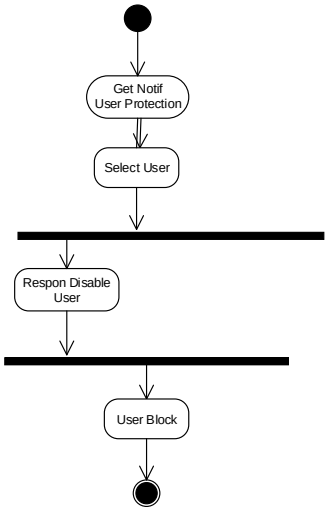
2. *Activity diagram Web protection* dari gangguan *Brute Force*



Gambar 6 Activity diagram *Web Protection*

Class diagram proteksi web adalah class diagram pada aplikasi android yang mengirimkan pesan atau notifikasi proteksi web untuk respon disable website atau penonaktifan *website*.

3. *Activity diagram User protection*



Gambar 7 Activity diagram User Protection

Activity diagram user protection adalah *activity diagram* pada aplikasi android yang mengirimkan pesan ke *website* untuk menonaktifkan user yang dipilih oleh administrator.

Temuan-temuan terbaru yang ditemukan dalam penelitian adalah :

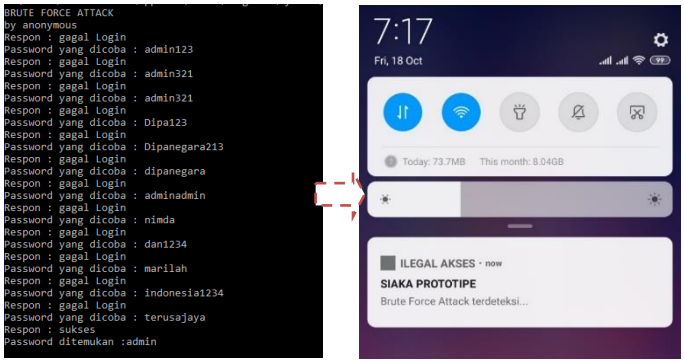
a. Penelitian ini fokus pada bagaimana mengirimkan notifikasi kepada administrator apabila terjadi *illegal access* pada *website*.
b. Aplikasi khusus untuk menerima notifikasi *mobile* serta administrator dapat melakukan penanganan dini terhadap aplikasi berupa penonaktifkan akun, serta melakukan *hibernasi* terhadap *website*.
c. Notifikasi yang diberikan dari fasiltas *firebase* (layanan dari google untuk mempermudah pengembang aplikasi dalam mengembangkan aplikasinya).

4. KESIMPULAN

Kesimpulan yang dapat ditarik berdasarkan hasil penelitian tersebut adalah :

1. Aplikasi berhasil menggunakan teknologi *firebase* dalam penanganan notifikasi ke perangkat *mobile* android administrator.
2. Dengan adanya aplikasi ini, administrator dapat lebih cepat dan mudah melakukan monitoring dan penanganan *website* dari upaya *Illegal access* dari *attacker*.

Adapun Fungsi Notifikasi Serangan Brute Force adalah sebagai berikut :



Gambar 8 Fungsi Notifikasi Brute Force

Pengujian fungsi notifikasi saat serangan brute force pada website, berhasil mengirimkan notifikasi saat serangan brute force terjadi.

Adapun hasil pengujian terhadap sistem adalah sebagai berikut :

Tabel 1 Rekapitulasi Hasil pengujian

No	Spesifikasi		Hasil pengujian
1	Fungsi Menyimpan Biodata Data User	✓	Berhasil Menyimpan dengan indikator aplikasi tampilnya data pada halaman daftar Data User
2	Menguji Notifikasi Web *Protection*	✓	Berhasil Mengirim Pesan Notifikasi ke administrator
3	Menguji Notifikasi *User Protection*	✓	Berhasil Mengirim Pesan Notifikasi ke administrator
4	Fungsi Mengedit data Administrator	✓	Berhasil Mengedit data dan password administrator berhasil diubah
5	Aplikasi harus bisa Mendisable *website* dari Aplikasi Android	✓	Aplikasi berhasil mendisabel *website* dari aplikasi android Aplikasi berhasil mendisabel *website* dari aplikasi android saat *brute force* terjadi
6	Aplikasi harus bisa Mendisable User dari Aplikasi Android	✓	Aplikasi berhasil mendisable User dari aplikasi android
7	Aplikasi harus dapat menampilkan menu utama	✓	Setelah login aplikasi berhasil menamppilkan menu beranda pada aplikasi web
8	Menguji fungsi Logout	✓	Berhasil Logout dengan indikator bahwa akan tampil Halaman Login
9	Menguji fungsi Login Android	✓	Berhasil Login ke android dengan indikator tampil ke halaman utama android
10	Menguji fungsi input url *website*	✓	Berhasil menambahkan url *website* dengan indikator tampil pada halaman daftar *website*
11	Menguji fungsi notifikasi saat serangan *brute force*	✓	Berhasil mengirimkan notifikasi saat serangan *brute force* terjadi

Dari tabel rekapitulasi hasil pengujian dapat disimpulkan bahwa hasil keseluruhan pengujian input output dari aplikasi yang dibuat sudah sesuai dengan spesifikasi yang diinginkan, ini bisa dilihat dari ke sebelas fungsional yang diinginkan dapat bekerja sesuai dengan spesifikasi yang diharapkan.

5. SARAN

Dari keterbatasan pengembangan aplikasi ini, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan aplikasi selanjutnya, yakni:

1. Implementasikan *mobile* notifikasi untuk jenis serangan yang lebih beragam tidak hanya terbatas pada serangan *Illegal access: brute force*.
2. Untuk menyempurnakan sistem ini, pengembangan berikut dapat meliputi mekanisme notifikasi lain.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada semua pihak yang telah memberikan kesempatan dan informasi bermanfaat baik secara langsung maupun tidak langsung, khususnya kepada STMIK Dipanegara Makassar, terima kasih atas dukungan finansialnya sehingga Peneliti dapat melakukan dan melaksanakan penelitian ini.

DAFTAR PUSTAKA

[1] Komarudin, & Asep Ririh Riswaya. (2013). *Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5 Pada Koperasi Mitra Sejahtera Bandung*, Jurnal Computech & Bisnis, Vol. 7, No. 1, Juni 2013, ISSN 2442-4943.

[2] Rudi Ridho Rohmansyah, & Heru Nurwasito. (2018). *Pengembangan Aplikasi Mobile untuk Sistem Keamanan Kantor Menggunakan NFC (Near Field Communication) dan Wi-Fi (Studi Kasus : PT. Rahmi Ida Nusantara),* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol. 2, No. 1, Januari 2018, e-ISSN: 2548-964X.

[3] Dias Utomo, Muchammad Sholeh, Arry Avorizano. (2017). *Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel*, Seminar Nasional TEKNOKA, Vol. 2, 2017, ISSN No. 2502-8782.

[4] Fithria, N. (2007). *Jenis-Jenis Serangan terhadap Kriptografi. Teknik Informatika Institut Teknologi Bandung*.

[5] Gunawan, I. (2016). Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan CSA-Rainbow Tool Untuk Mencari BISS. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *1*(1), 52-55.

[6] Agarwal, B. B.; Tayal, S.P.; Gupta, M. (2010). Software Engineering & Testing. Sudbury, Massachusetts: Johanes and Bartlett Publishers.

[7] Christianini, Nello & John S. Taylor. (2010). *An Introduction to Support Vector Machines and Other Kernel-based Learning Methods*. Cambridge University Press.

[8] Kiktenko, E. O., Kudinov, M. A., & Fedorov, A. K. (2019). *Detecting brute-force attacks on cryptocurrency wallets. arXiv preprint arXiv:1904.06943*.

[9] Momot, Falcon, Lorne Schell, and Duncan Smith. (2019) *System and method for bruteforce intrusion detection*. U.S. Patent No. 10,180,867. 15 Jan.

[10] Sadikin, & Rifki. (2014). *Kriptografi untuk Keamanan Jaringan*. Yogyakarta.

[11] Sholiq (2012). *Pemodelan Sistem Informasi Berorientasi Objek Dengan UML*. Graha Ilmu. Jakarta.

[12] Hammim Tohari. (2014). *Analisis Serta Perancangan Sistem Informasi Melalui Pendekatan UML*, Penerbit Andi, Yogyakarta.

[13] Lukmanul, & Hakim. (2012). *Cara Cerdas Menguasai Layout, Desain, dan Aplikasi Web*. Penerbit Elex Media Komputindo. Jakarta.