Jurnal Ilmiah Wahana Pendidikan, Juli 2023, 9(13), 81-95
DOI: https://doi.org/10.5281/zenodo.8145614
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Analisis Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) dan Zero-Knowledge Proof Pada Aplikasi Whatsapp Mod

Andika Abadi Pamungkas[1] , Agung Susilo Yuda Irawan[2], Purwantoro[3]

[1,2,3]Universitas Singaperbangsa Karawang

Received: 17 Juni 2023
Revised: 23 Juni 2023
Accepted: 04 Juli 2023

Abstract

With the rapid development of technology and the large amount of digitization in various fields of human life, it is necessary to pay attention to the security and certainty of privacy so that there is no leakage of confidential data, both in the private and governmental domains, especially in Indonesia. In this case cyber-attacks will grow and become more numerous; therefore we need a security principle that can prevent these cyber-attacks, especially in sending something that is sensitive which can be called cryptography. One of the applications that can be implemented regarding this cryptography is the Whatsapp application. WhatsApp claims that the application is safe from data theft and messages being intercepted. However, this is doubtful with the presence of Whatsapp Mod which offers more features than the official application. The security of the modified Whatsapp is questionable, so in this study a test was carried out using the MobSF Framework to find out whether there were security holes that could endanger its users. The results of this research are in the form of a report issued by MobSF regarding the level of danger of the Whatsapp Mod Application. With this research, it is hoped that it will be able to make Whatsapp Mod users aware of the dangers of modified applications and Whatsapp can provide advice and strict action against the Whatsapp Mod developers.

Keywords: *Whatsapp Mod, MobSF, Cryptography*

(*) Corresponding Author: *Andika.abadi18182@student.unsika.ac.id,agung@unsika.ac.id, purwantoro.masbro@staff.unsika.ac.id*

How to Cite: Pamungkas A.A., Irawan A.S.Y., & Purwantoro. (2023). Analisis Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) dan Zero-Knowledge Proof Pada Aplikasi Whatsapp Mod. https://doi.org/10.5281/zenodo.8145614.

PENDAHULUAN

Teknologi saat ini merupakan hal yang tidak dapat dipisahkan dalam kehidupan sehari-hari manusia. Dengan pesatnya perkembangan teknologi dan banyaknya digitalisasi di berbagai bidang kehidupan manusia, maka keamanan dan kepastian privasi perlu diperhatikan agar tidak adanya kebocoran data rahasia baik ranah perseorangan maupun pemerintahan terutama di Indonesia. Menurut Rilis yang dikeluarkan oleh Beta News dalam Antonishyn, M., & Misnik, O. (2019) disebutkan bahwa dari 30 aplikasi terbaik dengan jumlah unduhan sebanyak 500,000 unduhan. 94% berisi setidaknya minimal 3 rata-rata resiko kerentanan, sedangkan 77% berisi seminimalnya dua kerentanan level tinggi. Diantara 30 aplikasi 17% rentan terhadap serangan Man-In-The-Middle (MITM) mengekspos semua data untuk diintersepsi oleh user yang jahat. Selanjutnya, 44% dari aplikasi berisi data rahasia dengan syarat enkripsi yang ketat, termasuk kata sandi atau kunci Application Programming Interface (API) , sementara 66% sisanya memanfaatkan kemampuan fungsional yang dapat membahayakan kerahasiaan pengguna.

Kemudian rilis laporan yang dikeluarkan oleh check point research berjudul "Cyber Attack Trends: 2019 Mid-Year Report" menyatakan bahwa terdapat serangan malware android yang dilakukan 50% lebih banyak dari tahun-tahun sebelumnya, serangan-serangan ini ditujukan oleh pihak peretas dengan iklan-iklan jahat pada perangkat android, pencurian data rahasia, dan pengawasan pengguna. Selain itu, Pada bulan Mei 2019 sebuah aplikasi komunikasi alternatif dari SMS yaitu Whatsapp melaporkan bahwa mereka menghentikan serangan siber yang mengeksploitasi sistem panggilan video untuk mengirim malware ke sejumlah perangkat seluler pengguna Whatsapp. Dalam hal ini serangan siber akan semakin berkembang dan semakin banyak, maka dari itu diperlukan sebuah prinsip keamanan yang dapat mencegah serangan siber tersebut terutama dalam mengirimkan sesuatu hal yang bersifat sensitif yang dapat dinamakan Kriptografi.

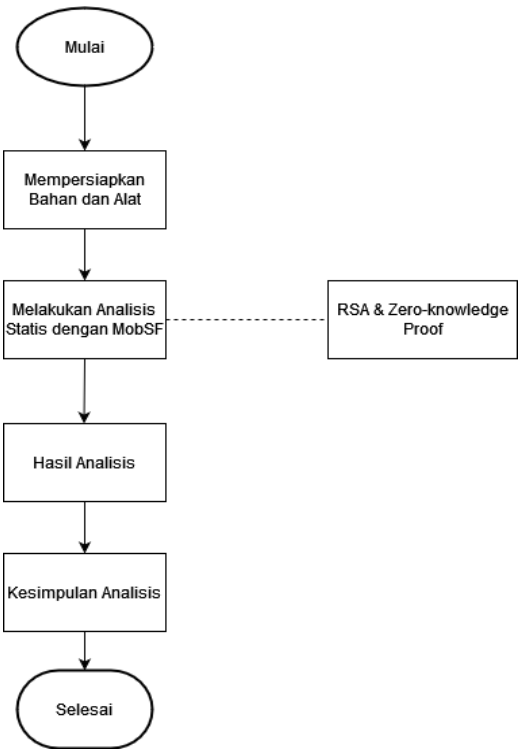
Menurut Hammad (2020) Kriptografi melibatkan penyandian pesan (format terenkripsi) sebelum transmisi sehingga data yang dikirimkan tidak dapat dibaca oleh pihak yang tidak berkepentingan. Banyak Algoritma Kriptografi yang diusulkan dikarenakan pentingnya menjaga keamanan seiring perkembangan teknologi. Algoritma Kriptografi yang umum digunakan adalah Algoritma RSA dan Algoritma Zero-Knowledge, RSA adalah algoritma enkripsi dan merupakan singkatan dari Rivest Shamir Adleman yang dalam hal ini merupakan ciptaan dari professor Leonard Adleman, Adi Shamir, dan Ron Rivest di lab Massachusetts Institute of Technology (MIT) pada tahun 1978. RSA menggunakan kunci enkripsi asimetri yang memiliki dua kunci berbeda, satu kunci dapat diketahui oleh semua orang (public key) sedangkan kunci lainnya (private key) yang digunakan untuk proses dekripsi sebuah pesan. Lalu ada Algoritma Zero-Knowledge yang merupakan suatu protokol yang memungkinkan identifikasi, pertukaran kunci dan operasi-operasi kriptografi dasar lainnya terimplementasikan tanpa membocorkan suatu informasi rahasia dalam "percakapan"nya.

Salah satu aplikasi yang dapat diimplementasikan perihal kriptografi ini merupakan aplikasi Whatsapp. Whatsapp saat ini dapat mengirim dan menerima berbagai macam media seperti teks, foto, video, dokumen, dan lokasi, serta panggilan telepon. Aplikasi ini dilengkapi end-to-end encryption yang memastikan bahwa pesan yang dikirimkan dan diterima hanya tetap di perangkat masing-masing dan tidak ada seseorang yang dapat membaca atau mendengarkan kontennya, bahkan pihak whatsapp sekalipun. Akan tetapi, klaim whatsapp ini patut dipertanyakan dengan kehadiran whatsapp yang telah dimodifikasi oleh pihak ketiga dengan mengusung fitur lebih banyak dibandingkan whatsapp resmi. Sehingga banyak orang menggunakan whatsapp mod yang mereka rasa memiliki keunggulan lebih dibandingkan whatsapp resminya.

Karena Whatsapp yang telah dimodifikasi ini belum terbukti perihal keamanan dan privasinya dalam berkirim pesan maka diperlukan sebuah pengecekan apakah Whatsapp telah menerapkan kedua algoritma kriptografi ini pada aplikasinya atau belum dengan dilakukannya analisis dengan beberapa parameter.

METODOLOGI PENELITIAN

Pada penelitian ini, metode yang digunakan yaitu metode Analisis Statis dengan tahapan-tahapan yang telah disebutkan sebelumnya. Metodologi tersebut di dalam penelitian sebelumnya terbukti dapat mengetahui kerentanan dari sebuah aplikasi.



Gambar 1. Rancangan Penelitian

Langkah-langkah yang ditempuh untuk menyelesaikan penelitian ini adalah sebagai berikut :

1) Tahap Mempersiapkan Bahan dan alat
   Di tahap pertama ini akan dipersiapkan bahan-bahan dan alat-alat termasuk seperti instalasi MobSF dan mempersiapkan aplikasi Whatsapp Mod yang akan dilakukan pengujian
2) Tahap Melakukan Analisis Statis dengan MobSF
   Pada tahap ini, dilakukannya analisis statis dengan menggunakan Aplikasi MobSF dan aplikasi whatsapp Mod yang telah dipersiapkan sebelumnya. Aplikasi MobSF dipilih dikarenakan MobSF (*Mobile Security Framework*) merupakan *framework* yang digunakan untuk melakukan pengujian untuk aplikasi *mobile* Android dan iOS. Selain itu, MobSF dipilih karena dapat melakukan analisis statis, dinamis, dan menganalisis malware dan mendukung binary dari aplikasi *mobile* seperti APK, XAPK, IPA dan APPX Bersama dengan format .zip yang berkaitan dengan penerapan RSA dan Zero-Knowledge Proof didalamnya.

3) Tahap Hasil Analisis
Setelah analisis dilakukan maka didapatkan hasil analisis yang mana akan dianalisis parameter yang telah ditentukan pada MobSFnya yaitu : *Reconnaissance, Security Analysis,* dan *Malware Analysis.*
4) Tahap Kesimpulan Analisis
Pada tahap terakhir, disimpulkan dari hasil analisis yang telah diuji menggunakan MobSF kemudian akan dianalisis apakah Algoritma RSA dan Zero-Knowledge Proof telah diterapkan pada Aplikasi Whatsapp Mod yang kemudian akan dijadikan sebuah kesimpulan yang berupa report dan dijadikan ringkasan agar dapat dipahami dan mudah dibaca.

HASIL DAN PEMBAHASAN

Berikut merupakan hasil dari tiap tahap yang dilakukan pada penelitian ini. bentuk hasil yang didapatkan dapat berbeda tergantung pada spesifikasi mesin yang digunakan, pada penelitian ini digunakan mesin virtual yaitu Virtual Box dengan spesifikasi sebagai berikut:

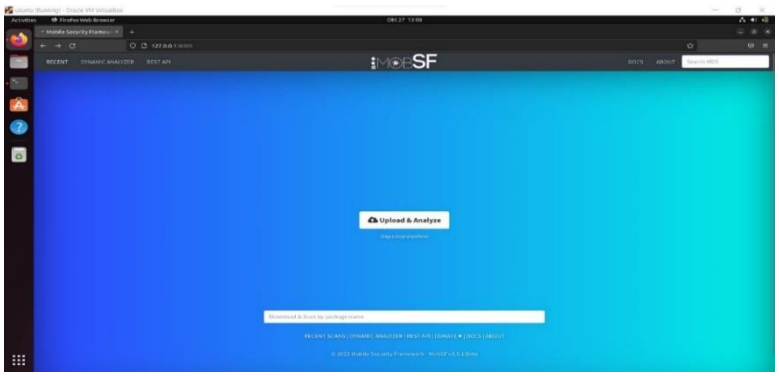
1. 3 CPU Processor
2. 6GB RAM
3. Sistem Operasi Ubuntu 22.04.1

Tahap 1 – Mempersiapkan Bahan Dan Alat

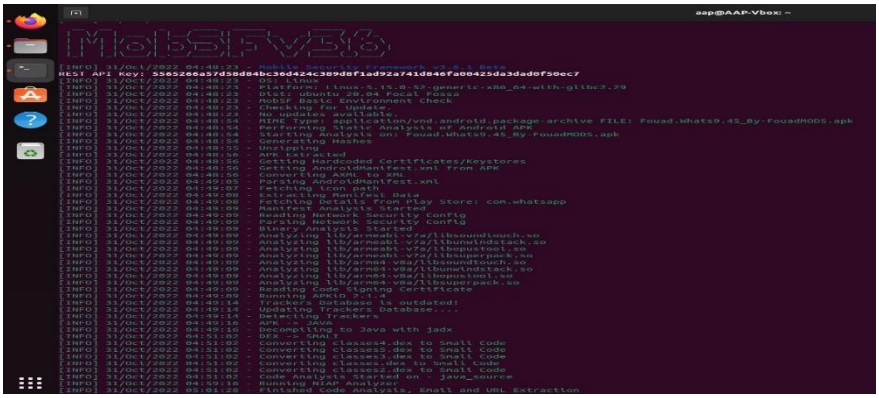
Tahapan mempersiapkan bahan dan alat ini melibatkan pengumpulan sumber daya untuk bahan yang akan dilakukan pengujian yaitu aplikasi Whatsapp Mod yang telah dimodifikasi dan akan ada 3 versi aplikasi Whatsapp Mod yang akan dilakukan pengujian antara lain : Fouad Whatsapp, GB Whatsapp, dan Yo Whatsapp yang ketiganya diunduh melalui situs resmi pihak ketiga. Sementara itu, untuk alat yang menjadi sarana pengujian yaitu MobSF akan diunduh melalui situs GitHub dan akan dipasang pada mesin virtual yang sudah dipersiapkan sebelumnya dan pada Gambar 2 terlihat tampilan utama MobSF

Gambar 2 Tampilan Utama MobSF ketika dijalankan

Tahap 2 - Melakukan Analisis Statis dengan MobSF



Pada tahapan analisis ini akan dilakukan pengujian terhadap ketiga aplikasi Whatsapp Mod, Untuk memulai melakukan analisis yang diperlukan hanyalah mengunggah fail yang diinginkan dan setelah itu MobSF dengan sendirinya akan memulai proses analisis fail APKnya secara menyeluruh seperti yang terlihat pada Gambar 3



Gambar 3 Proses Analisis Statis dengan MobSF

Tahap 3 – Tahap Hasil Analisis

Setelah mengunggah file yang aplikasi maka MobSF memberikan laporan hasil analisis statis yang telah dilakukan akan diperlihatkan pada hasil tes aplikasi Whatsapp Mod dengan parameter yang telah ditentukan

A. Fouad Whatsapp

Pada parameter Reconnaissance yang dilakukan pada Whatsapp versi Fouad Whatsapp terdapat beberapa hal yang mengindikasikan bahwa adanya modifikasi terhadap aplikasi Whatsapp seperti adanya tautan ke situs pihak ketiga. Selain itu, terdapat pelacak yang diketahui milik pihak Google serta teks-teks yang ditambahkan ke dalam aplikasi Whatsappnya. Kemudian, dilanjutkan dengan hasil analisis pada parameter Security Analysis yang ditampilkan pada Tabel 1

Tabel 1 Hasil Analisis Statis Fouad Whatsapp Parameter *Reconnaissance*

	Deteksi	Keterangan
URLs	YES	Situs yang tidak terafiliasi kepada pihak Whatsapp
Trackers	YES	Pelacak yang dimiliki oleh pihak Google
Hardcoded Secrets	YES	Terdapat teks yang sudah ditambahkan di dalam aplikasi yang tidak terdapat di dalam aplikasi Whatsapp yang resmi

Tabel 2 Hasil Analisis Statis Fouad Whatsapp Parameter *Security Analysis*

	Isu Keamanan	Tingkat Keparahan Keamanan
Network Security	Keseluruhan aspek aplikasi	Tinggi
Certificate Analysis	Aplikasi rentan terhadap kerentanan janus & Algoritma pengesahan rentan terhadap tubrukan hash	Tinggi Tinggi

Tabel 4.3 Analisis Statis Fouad Whatsapp Parameter *Malware Analysis* (Lanjutan)

Manifest Analysis	*Launch Mode of activity is not standard*	Tinggi

Di Parameter *Security Analysis* terdapat beberapa poin yang dianalisis oleh MobSF seperti pada *Network Security* yang terdapat tingkat keparahan tinggi dari keseluruhan aspek aplikasi khususnya di bagian keamanan jaringannya. Sementara itu, di poin *Certificate Analysis* terdapat 2 isu keamanan yang menjadi kekhawatiran seperti Aplikasi Whatsapp yang rentan terhadap Kerentanan Janus yang disebabkan oleh aplikasi yang ditandatangani dengan *v1 signature scheme* pada Android 5.0-8.0. selain itu, terdapat isu algoritma pengesahan yang rentan terhadap tubrukan hash. Dikarenakan aplikasi ini ditandatangani dengan *SHA1withRSA* yang diketahui Algoritma Hash SHA1 memiliki isu tubrukan.

Kemudian, pada *Manifest Analysis* hanya terdapat isu yang berulang dengan tingkat keparahan yang tinggi dan ini disebabkan oleh sebuah *Activity* yang tidak boleh memiliki *Launch Mode* yang disetel ke "*singleTask/singleInstance"* karena menjadi *root Activity* dan memungkinkan aplikasi lain untuk membaca konten dari *Intent* yang dipanggil. Jadi, diharuskannya memakai *Launch Mode* yang standar saat informasi sensitive disertakan dalam *Intent*.Selanjutnya akan dibahas Analisis Statis pada Paarameter *Malware Analysis* yang ditampilkan pada tabel 3

Tabel 3 Analisis Statis Fouad Whatsapp Parameter *Malware Analysis*

	Deteksi	Status *Malware*
Domain Malware Check	Twitter.fouadmods.com	OK
	Telegram.fouadmods.com	OK
	www.lassovideos.com	OK
	theyocraft.com	OK
	yousefalbasha.com	OK
	www.cielo.com.br	OK

Seperti yang terlihat pada tabel 4.3 terdapat beberapa Situs yang tidak berafiliasi dengan Whatsapp meskipun status cek *malware* mereka aman. Seperti situs dengan kata kunci fouadmods.com yang merupakan situs pihak ketiga tempat mengunduh aplikasi Whatsapp Mod ini yang dinyatakan oleh hasil pemeriksaan MobSF aman dari *Malware check*. Akan tetapi, hal ini tidak dapat dijadikan acuan dikarenakan menurut MobSF Skor Keamanan Aplikasi didapatkan senilai 41/100 pada Fouad Whatsapp sehingga dapat dikategorikan sebagai *Medium Risk*.

B. GB Whatsapp

Sama halnya dengan Fouad Whatsapp, pada GB Whatsapp dilakukan hal serupa dengan langkah-langkah yang telah dilakukan sebelumnya yang ditampilkan pada tabel 4 – tabel 6.

Tabel 4 Analisis Statis GB Whatsapp Parameter *Reconnaissance*

	Deteksi	Keterangan
URLs	YES	Situs yang tidak terafiliasi kepada pihak Whatsapp
Trackers	YES	Pelacak yang dimiliki oleh pihak Google
Hardcoded Secrets	YES	Terdapat teks yang sudah ditambahkan di dalam aplikasi yang tidak terdapat di dalam aplikasi Whatsapp yang resmi

Tabel 4 Analisis Statis GB Whatsapp Parameter *Reconnaissance* (Lanjutan)

Pada hasil analisis statis aplikasi GB Whatsapp tidak terdapat perubahan terhadap hasil dari parameter *reconnaissance* ini. Sehingga, bisa dikatakan tidak terdapat resiko keamanan terhadap aplikasi GB Whatsapp yang dianalisis. Selanjutnya akan ditampilkan hasil Analisis Statis pada parameter *Security Analysis* terhadap GB Whatsapp pada tabel 5.

Tabel 5 Analisis Statis GB Whatsapp Parameter *Security Analysis*

	Isu Keamanan	Tingkat Keparahan Keamanan
Network Security	Keseluruhan Aspek Aplikasi	Tinggi
Certificate Analysis	Aplikasi rentan terhadap kerentanan janus & Algoritma pengesahan rentan terhadap tubrukan hash	Tinggi Tinggi
Manifest Analysis	*Launch Mode of activity is not standard*	Tinggi

Seperti terlihat pada Tabel 5, hasil analisis statis pada GB Whatsapp di Parameter *Security Analysis* Tidak Berbeda dengan Hasil analisis statis pada Fouad Whatsapp di tabel 2 dengan tingkat keparahan keamanan yang tinggi dalam hal ini selalu berkaitan dengan poin-poin seperti *Network Security, Certificate Analysis,* dan *Manifest Analysis*.

Tabel 6 Analisis Statis GB Whatsapp Parameter *Malware Analysis*

	Deteksi	Status *Malware*
Domain Malware Check	down.fouadmods.com	OK
	Twitter.fouadmods.com	OK
	Telegram.fouadmods.com	OK
	www.lassovideos.com	OK
	yousefalbasha.com	OK
	theyocraft.com	OK

Kemudian, pada tabel 4.6 dapat dilihat bahwa hasil analisis statis pada aplikasi GB Whatsapp parameter *Malware Analysis* dalam poin *Domain Malware Check* memiliki hasil yang mirip. Akan tetapi, situs www.cielo.com.br tidak terdapat pada hasil analisis statis GB Whatsapp parameter ini. Meskipun tidak ada akan tetapi keseluruhan hasil *Malware Analysis* pada GB Whatsapp tidak ditemukannya masalah yang berarti selain disisipkannya situs-situs yang tidak berafiliasi dengan Pihak Whatsapp. Selanjutnya, Menurut MobSF Skor Keamanan Aplikasi didapatkan senilai 41/100 pada GB Whatsapp sehingga dapat dikategorikan sebagai *Medium Risk*.

C. Yo Whatsapp

Sama halnya dengan Versi Whatsapp sebelumnya, pada versi ini juga diambil hasil dari parameter *Reconnaissance*, *Security Analysis*, dan *Malware Analysis* yang akan ditampilkan pada tabel 7-9.

Tabel 7 Analisis Statis Yo Whatsapp Parameter *Reconnaissance*

	Deteksi	Keterangan
URLs	YES	Situs yang tidak terafiliasi kepada pihak Whatsapp
Trackers	YES	Pelacak yang dimiliki oleh pihak Google
Hardcoded Secrets	YES	Terdapat teks yang sudah ditambahkan di dalam aplikasi yang tidak terdapat di dalam aplikasi Whatsapp yang resmi

Pada tabel 7 terdapat beberapa hal yang bisa dianalisis seperti adanya situs-situs yang tidak terafiliasi dengan pihak Whatsapp seperti situs tempat mengunduh aplikasi whatsapp mod yaitu http://down,fouadmods.com. Selain itu, terdapat situs http://cielo.com.br yang diketahui berada pada hasil analisis statis Fouad Mods dan tidak ada pada hasil analisis statis GB Whatsapp. Lalu akan dilanjutkan Analisis Statis Yo Whatsapp Parameter *Security Analysis* pada tabel 8.

Tabel 8 Analisis Statis Yo Whatsapp Parameter *Security Analysis*

	Isu Keamanan	Tingkat Keparahan Keamanan
Network Security	Keseluruhan Aspek Aplikasi	Tinggi
Certificate Analysis	Aplikasi rentan terhadap kerentanan janus & Algoritma pengesahan rentan terhadap tubrukan hash	Tinggi Tinggi
Manifest Analysis	*Launch Mode of activity is not standard*	Tinggi

Dapat dilihat bahwa pada Hasil analisis statis Yo Whatsapp Parameter *Security Analysis* hasilnya memiliki persamaan dengan hasil analisis aplikasi sebelumnya. Ini dapat terjadi apabila pihak *developer* dan *publisher* merupakan satu pihak yang sama dan dalam contoh kasus ini adalah pihak Fouadmods.com.

Tabel 9 Analisis Statis Yo Whatsapp Parameter *Malware Analysis*

	Deteksi	Status
Domain Malware Check	Down.fouadmods.com	OK
	Theyocraft.com	OK
	Twitter.fouadmods.com	OK
	www.lassovideos.com	OK
	Yousefalbasha.com	OK
	www.cielo.com.br	OK
	Telegram.Fouadmods.com	OK

Pada tabel 9 terlihat bahwa terdapat situs yang tidak terafiliasi dengan pihak Whatsapp meskipun status *malware* nya bersih atau OK. Sama halnya dengan hasil analisis statis Whatsapp Mod versi lainnya, situs-situs yang tidak terafiliasi dengan pihak Whatsapp sebagian besar mengarah ke situs dimana ketiga Whatsapp Mod ini diunduh yaitu pada domain fouadmods.com. Selain itu, Berdasarkan hasil yang dikeluarkan oleh MobSF Yo Whatsapp memiliki skor keamanan 41 dari 100 dengan tingkat *Medium Risk* yang sama dengan 2 versi Whatsapp Mod yang telah dilakukan analisis statis sebelumnya. Hal ini dapat terjadi dikarenakan pihak yang merilis Whatsapp Mod yang dianalisis statis merupakan pihak yang sama.

4.2 Pembahasan

Telah dilakukannya analisis statis dengan menggunakan MobSF dan ditampilkan hasilnya dan didapatkan beberapa poin yang menjadi topik pembahasan ini. Pada hasil analisis statis dengan parameter *Reconnaissance* masing-masing aplikasi, meskipun memiliki beberapa *URLs* yang terdeteksi tidak berafiliasi dengan pihak Whatsapp dan *String* yang disisipkan ke dalam aplikasi. Akan tetapi, terkait dengan penerapan Algoritma Kriptografi RSA dan Zero-Knowledge Proof tidak terdapat pelanggaran prinsip dari kedua algoritma tersebut dikarenakan pada hasil analisis statis pada parameter *Reconnaissance* yang didapatkan tidak adanya pertukaran informasi rahasia yang dapat membahayakan perangkat terlepas adanya pelacakan yang dilakukan oleh Pihak *Google Analytics*.

Tabel 10 Perbandingan Hasil Analisis Statis pada Ketiga Aplikasi Whatsapp Mod Parameter *Reconnaissance*

	Fouad Whatsapp	GB Whatsapp	Yo Whatsapp
URLs	http://down.fouadmods.com/ http://www.yousefalbasha.com/yr.html http://theyocraft.com/wmapp	http://down.fouadmods.com/ http://www.yousefalbasha.com/yr.html http://theyocraft.com/wmapp	Yousefalbasha.com/yr.html http://down.fouadmods.com www.sharechat.com http://www.cielo.com.br
Trackers	Google Analytics https://reports.exodus-privacy.eu.org/trackers/48	Google Analytics https://reports.exodus-privacy.eu.org/trackers/48	Google Analytics https://reports.exodus-privacy.eu.org/trackers/48
Hardcoded Secrets	"donations__bitcoin" : "Bitcoin"	"donations__bitcoin" : "Bitcoin"	"donations__bitcoin" : "Bitcoin"

Kemudian, parameter kedua yang telah dilakukan analisis adalah parameter *Security Analysis* yang apabila dikaitkan dengan penerapan kedua Algoritma yaitu RSA dan Zero-Knowledge Proof memiliki hal-hal riskan yang melanggar tujuan dari Algoritma Kriptografi tersebut dan membahayakan perangkat seperti pada yang ditunjukkan pada tabel 11

Tabel 11 Perbandingan Hasil Analisis Statis pada Ketiga Aplikasi Whatsapp Mod Parameter *Security Analysis*

	Nama Aplikasi	Isu Keamanan	Tingkat Keparahan Keamanan
Network Security	Fouad Whatsapp	Keseluruhan Aspek Aplikasi	Tinggi
	GB Whatsapp		
	Yo Whatsapp		
Certificate Analysis	Fouad Whatsapp	Aplikasi rentan terhadap kerentanan janus & Algoritma pengesahan rentan terhadap tubrukan hash	Tinggi Tinggi
	GB Whatsapp		
	Yo Whatsapp		
Manifest Analysis	Fouad Whatsapp	*Launch Mode of activity is not standard*	Tinggi
	GB Whatsapp		
	Yo Whatsapp		

Apabila dilihat berdasarkan tabel 4.11, terlihat bahwa ketiga aplikasi Whatsapp Mod memiliki isu keamanan dan tingkat keparahan keamanan yang sama yaitu tinggi. Hal ini dapat disebabkan karena pihak ketiga yang membuat versi Modifikasi dari aplikasi Whatsapp merupakan pihak yang sama yaitu seseorang yang Bernama Yousef Al Basha. Selanjutnya apabila dikaitkan dengan Algoritma Kriptografi RSA dan Zero-Knowledge Proof dapat dikatakan bahwa ketiga versi Whatsapp Mod tidak menerapkan algoritma kriptografi RSA dan Zero Knowledge Proof dikarenakan beberapa hal, seperti pada *Network Security* yang memiliki isu keamanan yang tinggi dalam hal ini keseluruhan aspek aplikasi Whatsapp Mod tersebut.

Yang dimaksud dari keseluruhan aspek aplikasi memiliki tingkat keparahan keamanan yang tinggi adalah Konfigurasi dasar dikonfigurasi secara tidak aman untuk mengizinkan lalu lintas teks bersih ke semua domain. Hal ini menyebabkan dapat terjadinya kebocoran pada pesan yang dikirimkan dan diterima yang tentu saja tidak memenuhi tujuan dari Kriptografi yang terdapat di Algoritma Kriptografi RSA yaitu Kontrol Akses dan Kerahasiaan. Sementara itu, dalam Algoritma Kriptografi Zero-Knowledge Proof pun isu keamanan ini sangat berbahaya karena dapat memunculkan pihak *Eavesdropper* yang dapat melakukan tindakan *malice*.

Kemudian pada poin *Certificate Analysis* terdapat kerentanan aplikasi terhadap kerentanan janus / *janus vulnerability* yang merupakan Android *Vulnerability* yang memperbolehkan penyerang untuk memodifikasi sebuah aplikasi secara tidak terdeteksi, Hal ini dapat dilakukan dengan menambahkan fail *Dalvix Executable* (DEX) berbahaya ke file *Android Package Kit* (APK). Dalam hal ini, Ketiga Aplikasi Whatsapp Mod ditandatangani dengan skema *v1 signature*, yang menjadikannya rentan terhadap *Janus vulnerability* pada Android 5.0-8.0

Selanjutnya ada Algoritma Pengesahan rentan terhadap tubrukan hash (*hash collision*) yang memiliki tingkat keparahan keamanan tinggi menurut hasil analisis statis MobSF, *hash collision* merupakan kondisi ketika ada lebih dari satu nilai yang akan di-hash oleh fungsi hash tertentu ke slot yang sama dalam table atau struktur data (tabel hash) yang dihasilkan oleh fungsi hash. *Hash collision* ini dapat menjadi

masalah dikarenakan penyerang dapat melakukan *brute force* untuk mendapatkan akses ke dalam aplikasi dan dapat berpura-pura menjadi pengirim atau penerima pesan, hal ini tidak memenuhi tujuan dari kriptografi yaitu *Non-Repudiation* yang memastikan bahwa pengirim dan penerima mengakui pengiriman pesan dan melanggar tentang hal Kontrol Akses dari kedua belah pihak dimana pihak penyerang dapat melihat dan melakukan tiruan untuk mengirim/menerima pesan. Lalu Isu Keamanan selanjutnya yang memiliki resiko tinggi yaitu tentang *Launch Mode of Activity*, menurut hasil analisis statis MobSF sebuah *activity* tidak seharusnya memiliki *launch mode* yang disetel ke "*singleTask/singleInstance*" karena aktivitas ini menjadi *root* dan aplikasi lain dapat membaca konten dari Intent yang dipanggil. Jadi penggunaan *Launch Mode* "Standar diperlukan ketika informasi sensitive disertakan dalam sebuah Intent.

Terakhir, parameter ketiga yang telah dilakukan analisis statis oleh MobSF adalah parameter *Malware Analysis*. Dalam hasil yang ditunjukkan pada tabel 12 bahwa poin yang diperiksa dan memiliki hal yang mencurigakan terdapat pada poin *Domain Malware Check* yang berisi pendeksian terhadap URL-URL yang tidak berafiliasi dengan pihak Whatsapp dan *Geolocation*nya serta status URL-URL tersebut apakah aman atau tidak dengan status "OK".

Tabel 12 Perbandingan Hasil Analisis Statis pada Ketiga Aplikasi Whatsapp Mod Parameter *Malware Analysis*

	Fouad Whatsapp	GB Whatsapp	Yo Whatsapp	*Geolocation*
Domain Malware Check	Down.fouadmods.com	Down.fouadmods.com	Down.fouadmods.com	IP: 172.67.167.160 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203
	www.lassovideos.com	www.lassovideos.com	www.lassovideos.com	*No Geolocation information available.*
	theyocraft.com	theyocraft.com	Theyocraft.com	IP: 36.86.63.182 Country: Indonesia Region: Jakarta Raya City: Jakarta Latitude: -6.214620 Longitude: 106.845131
	yousefalbasha.com	yousefalbasha.com	yousefalbasha.com	IP: 172.64.104.32 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203

Domain Malware Check	www.cielo.com.br	-	www.cielo.com.br	IP: 104.93.107.232 Country: Indonesia Region: Jakarta Raya City: Jakarta Latitude: -6.214620 Longitude: 106.845131

Seperti yang terlihat pada Tabel 12 rata-rata ketiga aplikasi memiliki situs yang disisipkan ke dalam aplikasi akan tetapi hasil pemeriksaan *Domain Malware Check* menurut MobSF tidak ditemukannya situs yang memiliki *malware* hanya situs pihak ketiga seperti domain situs fouadmods.com yang mengarahkan ke tempat mengunduh Aplikasi Whatsapp Mod ketiga versi ini. Selain itu, apabila mengacu dalam penerapannya terhadap Algoritma Kriptografi RSA dan Zero-Knowledge Proof tidak ditemukannya pelanggaran terhadap keamanan. Akan tetapi, terlihat bahwa pihak ketiga telah mengubah atau mensisipkan situs yang tidak terkait dengan pihak Whatsapp. Selain dari hasil analisis statis menggunakan tiga parameter yang sudah ditentukan, MobSF memberikan skor rata-rata untuk aplikasi Whatsapp mod yang akan diwakilkan oleh Fouad Whatsapp

Gambar 4 Skor Keamanan Aplikasi Fouad Whatsapp

Terlihat dalam gambar 4 bahwa skor keamanan aplikasi dari aplikasi Whatsapp Mod memiliki skor yang cukup rendah yaitu 41/100 dengan status *Medium Risk* yang dalam hal ini memiliki Grade B. Dengan kata lain, ketiga Aplikasi sangat riskan apabila digunakan karena menurut MobSF skor 41/100 merupakan skor yang

rendah dan dapat membahayakan Perangkat apabilla aplikasi dipasang.

CONCLUSION

1. Penelitian ini menggunakan metode analisis statis dan MobSF sebagai alat pengujiannya, pada hasil penelitian diketahui bahwa adanya penerapan Algoritma Rivest Shamir Adleman (RSA) dan Zero-Knowledge Proof pada aplikasi Whatsapp Mod apabila melihat hasil pengujian pada parameter yang telah ditentukan, seperti pada parameter *Security Analysis* poin *Certificate Analysis* yang diketahui bahwa terdapat isu Algoritma pengesahan rentan

terhadap tubrukan hash dikarenakan aplikasi ini ditandatangani dengan SHA1*with*RSA. SHA1*with*RSA ini akan melakukan enkripsi pesan yang dikirimkan dan akan melakukan proses enkripsi dan dekripsi diantara pengirim dan penerima, hal ini dapat menyatakan bahwa Algoritma RSA telah diterapkan pada Aplikasi Whatsapp Mod ini meskipun termasuk dalam kerentanan keamanan.

2. Berdasarkan pengujian yang dilakukan dengan menetapkan tiga parameter yang digunakan sebagai acuan hasil analisis statis menggunakan MobSF diketahui bahwa hasil analisis statis memiliki hasil yang tidak jauh berbeda, hal ini dapat terjadi apabila pihak yang melakukan modifikasi merupakan pihak yang sama. Ketika melihat hasil analisis statis parameter *Reconnaissance* versi Fouad Whatsapp dan membandingkannya dengan versi GB Whatsapp dan Yo Whatsapp dapat dilihat bahwa ketiga apikasi memiliki hasil yang sangat mirip terutama Ketika adanya sisipan situs yang bukan dimiliki oleh Whatsapp, lalu terdapat pelacak yang dilakukan oleh pihak *Google Analytics*. Kemudian pada Parameter *Security Analysis*, Aplikasi Whatsapp Mod memiliki hasil yang sama yaitu memiliki kerentanan tinggi dengan isu keamanan yang sama.isu keamanan tersebut antara lain : Permasalahan pada keseluruhan aspek aplikasi, Aplikasi yang rentan terhadap kerentanan janus dan Algoritma pengesahan yang rentan terhadap *hash collision*, serta *Launch Mode of Activity* tidak standar atau dalam kata lain informasi sensitif dapat bocor Ketika *activity* dijalankan melalui *"singleTask/singleInstance*" yang menyebabkan aplikasi lain dapat membaca konten dari halaman yang dipanggil. Terakhir Parameter yang digunakan sebagai acuan adalah Parameter *Malware Analysis*, di parameter ini dicari apakah terdapat *malware* dalam aplikasi dan pada poin *Domain Malware Check* memang ditemukan hal yang tidak berhubungan dengan pihak Whatsapp yaitu situs pihak ketiga akan tetapi berdasarkan hasil analisis statis MobSF menyatakan bahwa domain atau situs tersebut aman yang dinyatakan dengan kata "OK". Selain ketiga parameter yang digunakan untuk menjadi acuan, secara general MobSF memberikan Skor Keamanan Aplikasi yang menggunakan format CVSS (*Common Vulnerability Scoring System*) dan ditentukan bahwa Skor Keamanan Aplikasi ketiga aplikasi Whatsapp Mod yaitu Fouad Whatsapp, GB Whatsapp, dan Yo Whatsapp adalah 41 dari 100 dimana dalam hal ini dikategorikan sebagai *Medium Risk* dan memiliki tingkat B dalam keamanannya.

REFERENCES

Santoso, B., Ghofur, M. A., & Kuswanto, J. (2021). Analysis of WhatsApp Mod User Awareness Information Security with Static Analysis Methods and Quantitative Methods. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 213–222. https://doi.org/10.54706/senastindo.v3.2021.128

Suseno, A. Y., Sulistiyowati, N., & -, P. (2021). Analisis Peningkatan hybrid Cryptosystem Untuk Enkripsi dan Dekripsi Menggunakan Vigenere Cipher dan RSA Pada Text. In *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)* (Vol. 6, Issue 2). https://doi.org/10.30998/string.v6i2.10309

WhatsApp. (2021). End-to-End Encrypted Backups on WhatsApp. *WhatsApp*, 1–25.https://blog.whatsapp.com/end-to-end-encrypted-backups-on-whatsapp

Morais, E., Koens, T., van Wijk, C., & Koren, A. (2019). A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, *1*(8), 1–17. https://doi.org/10.1007/s42452-019-0989-z

Kuncoro, T. R., & Aditama, R. (2019). Analisis Kombinasi Algoritma Kriptografi Rsa Dan Algoritma Steganografi Least Significant Bit (Lsb) Dalam Pengamanan Pesan Digital. *Statmat : Jurnal Statistika Dan Matematika*, *1*(2), 60–82. https://doi.org/10.32493/sm.v1i2.2947

Narendren, S., Yathish, Y. B., & B, C. M. (2018). *A Cryptosystem using Two Layers of Security - DNA and RSA Cryptography*. *119*(7), 217–224.

Mallouli, F., Hellal, A., Sharief Saeed, N., & Abdulraheem Alzahrani, F. (2019). A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms. *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*,173–176. https://doi.org/10.1109/CSCloud/EdgeCom.2019.00022

Hassan, M. A., Shukur, Z., & Mohd, M. (2022). A Penetration Testing on Malaysia Popular e-Wallets and m-Banking Apps. *International Journal of Advanced Computer Science and Applications*, *13*(5). https://doi.org/10.14569/ijacsa.2022.0130580

Al-Delayel, S. A. (2022). *Security Analysis of Mobile Banking Application in Qatar*. http://arxiv.org/abs/2202.00582

Almohaini, R., Almomani, I., & Alkhayer, A. (2021). Hybrid-based analysis impact on ransomware detection for android systems. *Applied Sciences (Switzerland)*, *11*(22). https://doi.org/10.3390/app112210976

Antonishyn, M., & Misnik, O. (2019). Analysis of testing approaches to Android mobile application vulnerabilities. *CEUR Workshop Proceedings*, *2577*, 270–280.

Kumar, K. A., Raman, A., Gupta, C., & Pillai, R. R. (2020). The recent trends in malware evolution, detection and analysis for android devices. *Journal of Engineering Science and Technology Review*, *13*(4), 240–248. https://doi.org/10.25103/jestr.134.25

Janus Android Vulnerability. (n.d.). NHS Digital. https://digital.nhs.uk/cyber-alerts/2017/cc-1886

Why are hash collisions big news? (2017, July 1). Information Security Stack Exchange.https://security.stackexchange.com/questions/163177/why-are-hash-collisions-big-news

Lake, J. (2022, March 30). What is a collision attack? Comparitech. https://www.comparitech.com/blog/information-security/what-is-a-collision-attack/