Pengamanan Restful API Web Service Menggunakan Json Web Token (Studi Kasus: Aplikasi Siakadu Mobile Unesa)

Jihad Satrio Utama[1], Aries Dwi Indriyanti[2]

[1,2] Sistem Informasi, Fakultas Teknik, Universitas Negeri Surabaya
[1]jihad.20114@mhs.unesa.ac.id
[2]ariesdwi@unesa.ac.id

***Abstrak*— Penerapan teknologi informasi bertujuan untuk membantu manusia dalam melakukan pekarjaan sampai mengatasi masalah yang muncul dalam kehidupan selain itu juga memudahkan dalam pengaksesan informasi yang tidak dibatasi oleh waktu dan ruang, hal ini juga berdampak pada instansi perusahaan contohnya pada Universitas Negeri Surabaya sudah menerapkan sistem informasi akademik berbasis *website* dan android akan yaitu berisi tentang informasi akademik suatu sistem yang dibuat guna keperluan pengolahan data-data *akademik*. Didalam aplikasi tersebut memanfaatkan arsitektur *REST API* dimana memiliki pola untuk menyediakan standar antara komunikasi yang tidak kompatibel untuk aplikasi *web* dan juga diciptakan untuk menyederhanakan proses pertukan data antara sistem yang berbeda dalam jaringan, akan tetapi telah ditemukan sebuah celah pada arsitektur *restful api* di aplikasi tersebut maka dari itu diterapkanlah sebuah pengamanan terhadap aplikasi menggunakan *son web token algoritma hmac-sha 512* untuk pengamanan 3 komponen *header, payload* dan *signature* sehingga seseorang tidak akan bisa mengubah dan melihat data yang terenkripsi ketika melakukan request ke server.**

***Kata Kunci*— Siakadu, Rest, Api, Json, Website, Token.**

I. PENDAHULUAN

Penerapan teknologi informasi bertujuan untuk membantu manusia dalam melakukan pekerjaan sampai mengatasi masalah yang muncul dalam kehidupan. Selain itu teknologi informasi memudahkan dalam pengaksesan informasi yang tidak dibatasi oleh waktu dan ruang [1]. Hal ini juga berdampak pada instansi, perusahaan, dan lapisan masyarakat dituntut untuk maju menggunakannya [2]. Sudah banyak sekali sebuah lembaga atau instansi yang menerapkan kemudahan teknologi, dalam contohnya pada aktivitas akademik pada dunia instansi pendidikan membutuhkan suatu sistem informasi dalam mengatur kegiatan akademik yang sangat cepat, efektif, efisien dan akurat guna meningkatkan standar mutu pendidikan pada universitas tersebut salah satunya adalah sistem informasi akademik.

Universitas Negeri Surabaya adalah perguruan tinggi negeri yang memiliki 7 fakultas, 90 jurusan dan 152 prodi, sudah menerapkan aplikasi berbasis website Siakadu (Sistem Informasi Akademik UNESA) berisi tentang informasi akademik suatu system yang didesain untuk keperluan pengelolaan data-data akdemik dengan penerapan teknologi informasi di lingkungan pergeruan tinggi Universitas Negeri Surabaya [3].

Kemudian dalam perkembangan waktu siakadu dihadirkan dalam fitur mobile pada tahun 2019 aplikasi yang dihadirkan memanfaatkan arsitektur *RESTful API (Representational State Transfer)* adalah sebuah arsitektur dimana memiliki pola untuk menyediakan standar antara komunikasi yang tidak kompatibel untuk aplikasi *web*, *REST* adalah jenis *RPC (Remote Procedure Call)* sebuah protokol yang diciptakan guna menyederhanakan proses pertukaran data antara sistem yang berbeda pada jaringan [4]. Membangun *API (Application Programming Interface)* untuk aplikasi *mobile* bukanlah masalah yang mudah terkait dengan hadirnya bahasa, alat, *framework* dan keamanannya [5].

Pada penelitian sebelumnya yang berjudul "Analisis Keamanan Data Pada Aplikasi Android Menggunakan HTTP Canary (Studi Kasus : Siakadu UNESA Mobile)" dilakukan perekaman terhadap seluruh aktifitas pada aplikasi siakadu mobile menggunakan bantuan alat *Http Cannary* telah ditemukan ketika melakukan request terhadap *server* bahwa tidak adanya autentikasi atau *session* pengguna dan *server* merespon apa yang diminta, sehingga siapa saja bisa meniru request dengan melakukan mengambil data tanpa adanya autentikasi [6].

Dengan memanfaatkan *framework laravel* dikarenakan kemudahan penggunaannya dan menyedikan banyak fitur untuk menangani pembuatan *API* [7]. Kemudian menggunakan *JWT (Json Web Token)* sebuah arsitektur untuk membantu dalam pengamanan *RESTful API* serta melindungi seluruh komunikasi, integrasi dan kerahasiaan data [8]. Didalam arsitektur JWT terdapat algoritma HMAC SHA-512 untuk melakukan enkripsi token ketika melakukan proses autentikasi [9]. algoritma ini memiliki kinerja yang baik jika diterapkan pada arsitektur 64-bit memiliki kecepatan dan ukuran data pada keamaanan REST [10].

Maka berdasarkan pada masalah yang diuraikan diatas dan dibuatlah suatu judul untuk penulisan skripsi ini adalah "Pengamanan Restful Api Web Service Menggunakan Json Web Token (Studi Kasus: Aplikasi Siakadu Mobile Unesa)" dengan penerapan keamanan pada arsitektur *RESTful API* diharapkan memberikan manfaat bagi seluruh civitas akademika UNESA untuk keamanan data di aplikasi siakadu *mobile*.

II. PENELITIAN TERKAIT

Penelitian terdahulu bertujuan agar mendapatkan sebuah bahan dasar perbandingan dan acuan pada penulisan skripsi ini. Selain itu untuk menghindari pandangan penelitian yang

berkesan sama, maka dalam kajian Pustaka ini peneliti mencamtumkan hasil dari penelitian sebelumnya sebagai berikut:

Penelitian tentang keamanan dan privasi pada Restful Api telah dilakukan sebelumnya oleh Muhammad A. Rahman Irmansyah Putra pada tahun 2022 dengan judul "Analisis Keamanan Data Pada Aplikasi Android Menggunakan HTTP Canary (Studi Kasus: SIAKADU UNESA Mobile)" dalam penelitian tersebut dijelaskan dengan menggunakan bantuan alat *HTTP Canary* telah dilakukan perekeman aktivitas *traffic* pada aplikasi tersebut dan telah dilakukan percobaan ratusan request dengan ip yang sama *server* telah merespon semua bentuk request terhadap *API* sehingga ditakutkan terjadinya *scrapping* data dalam sekala besar, kemudian tidak adanya autentikasi kepada pengguna dan langsung meresponse apa yang diminta oleh pengguna sehingga siapapun dapat mengambil data berdasarkan *request* terhadap *server* tanpa adanya autentikasi.

Kemudian penelitian selanjutnya tentang pengamanan dan privasi telah dilakukan sebelumnya pada tahun 2020 oleh Aal Hibsy dengan judul "Implementasi Fitur Keamanan dengan JSON Web Token dan Fitur Geo-tagging pada Aplikasi Web Service Training From Home" penelitian ini memiliki tujuan dari penerapan terhadapap kemanan pada *Json Web Token (JWT)* pada *web service* pada mode autentikasi sistem dan mengembangkan fitur *geo-tagging* untuk mendukung proses *check in* (presensi) dari berbagai lokasi. Kemudian hasil dari implementasi penelitian tersebut bahwa *web service* berbasis android dengan kemanan *JWT* dan *geo-tagging* mampu menghasilkan token sebagai bentuk autentikasi pengguna yang berhak melakukan request data terhadap aplikasi tersebut. Dan jika *email* atau *password* salah maka akses *token* tidak diberikan[11].

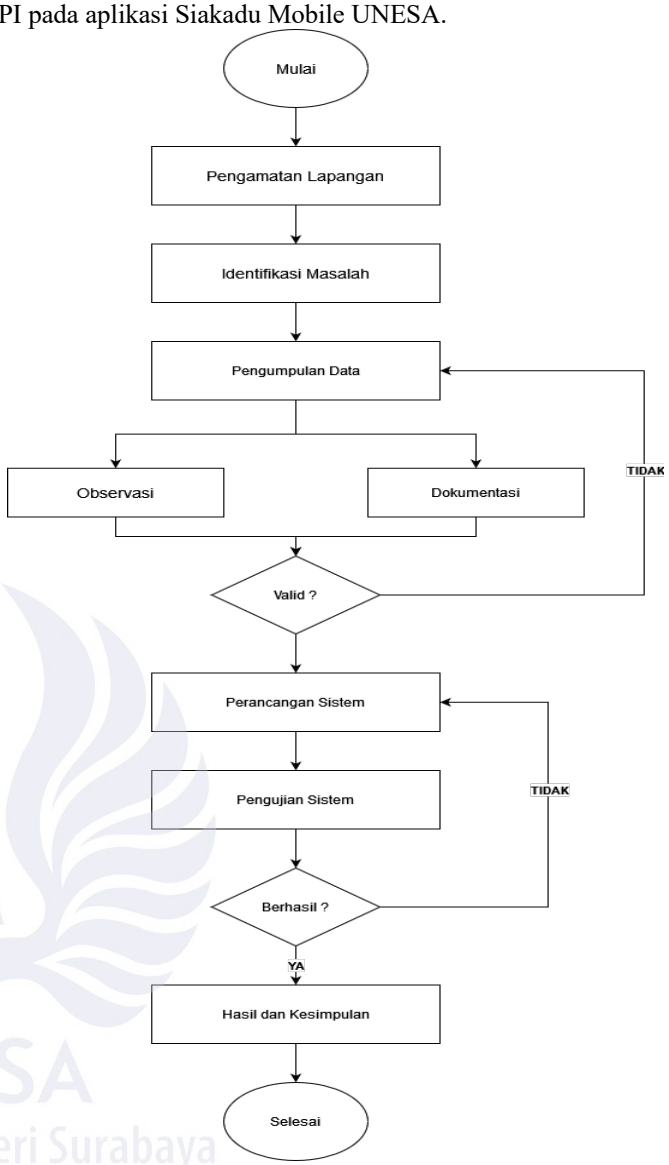
Pada penelitian selanjutnya membahas tentang pengukuran kecepatan pengamanan menggunakan algoritma *HMAC SHA-512* oleh Alam Rahmatulloh pada tahun 2018 dengan judul "Keamanan Restful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA 512" dalam penelitian tersebut telah dilakukan perbandingan kecepatan antara *token* yang dihasilkan oleh *HMAC SHA-256* dan *HMAC SHA-512* dan hasil penerapan algoritma *HMAC SHA-512* pada *JWT* memiliki kinerja yang sangat baik jika dinjalankan pada arsitektur 64-*bit* dibandingkan dengan *SHA-256*. Akan tetapi token yang dihasilkan oleh *SHA-512* memiliki ukuran nilai hash 2% tentunya memiliki keamanan pertukan data yang lebih baik karena ukuran token lebih banyak atau panjang.

III. METODOLOGI PENELITIAN

A. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan penelitian kualitatif, dimana penelitian ini dilakukan merbaksud untuk memahami gejala atau fenomena tentang apa yang dialami oleh subjek penelitian dan juga bisa dipahami sebagai metode memakai data deskriptif seperti wawancara, observasi, sumber dokumen [12].

Pendekatan penelitian kualitatif memili prosedur penelitian yang menghasilkan data yang deksriptif dalam artian pendekatan ini tidak menggunakan angka-angka dan menggambarkan tentang implementasi keamanan pada Restful API pada aplikasi Siakadu Mobile UNESA.



Gbr. 1 Alur Penelitian

B. Sumber Data dan Data Penelitian

Subjek penelitian memeiliki tujuan yang akan dijadikan analaisis atau fokus dalam sebuah masalah. Subjek penelitian disini menjelaskan bahwa fokus yang nantinya dikaji dari penelitian, dalam hal ini adalah siakadu Universitas Negeri Surabaya.

1. Sumber Data

a. Informan

Informan dalam penelitian merupakan narasumber yang berarti seseorang yang sangat memahami dengan keterkaitan subjek penelitian serta mampu

memberikan penjabaran yang sangat mendalam tentang penilitian yang diangkat.

b. Dokumen

Dokumen adalah suatu teks, bukum foto yang berkaitan dengan penelitian. Pada bagian dokumen dimanfaatkan oleh penulis untuk sumber data yang dapat diuji juga digunakan sebagai bukti analisis data.

2. Data Penelitian

a. Data Primer

Data primer adalah data fundamental didapatkan dengan cara langsung oleh penulis dari sumber tanpa melampaui perantara. Data primer dikumpulkan melalui informasi perkataan dan perilaku subjek yang diamati yakni Pusat Pengembangan Teknologi Informasi Universitas Negeri Surabaya.

b. Data Sekunder

Data yang didapatkan bukan hasil dari usaha penulis sendiri atau tidak didapat secara langsung dari sumber data. Data sekunder ini berguna untuk sarana pendukung informasi utama yang dapat diperoleh melalui arsip, laporan, publikasi, dan lain sebagainya

C. Instrumen Pengumpulan Data

Ciri dari penelitian kualitatif yaitu peneliti bertindak sebagai instrument sekaligus pengumpul data. Selain manusia instrumen juga dapat dari hal lain seperti angket, pedoman wawancara, pedoman observasi dan lain sebagainya akan tetapi fungsinya hanya sebagai alat pendukung dalam penelitian dikarenakan tugas peneliti sebagai instrument kunci[13].

1. Observasi

Sebuah teknik untuk mengumpulkan data-data dengan cara langsung terjun pada lapangan dengan mengamati setiap masalah yang terjadi di tempat kejadian.

TABEL I
INSTRUMEN OBSERVASI

No.	Sarana	Ada	Tidak ada
1.	Kantor PPTI		
2.	Program Kerja		
3.	Visi dan Misi		
4.	Daftar Pegawai		
Catatan :			

2. Dokumentasi

Dilakukan dengan cara mengumpulkan sebuah data-data dengan segala referensi atau turun langsung dengan tujuan mengetahui keadaan yang sebenarnya dari dokumen-dokumen yang memiliki keterkaitan dengan penelitian.

TABEL II
INSTRUMEN WAWANCARA

No.	Aspek	Butir Pertanyaan
1.	Keamanan Restful API	Apakah aplikasi siakad mobile menggunakan Restful API?
		Apakah proses API RESTful pada aplikasi siakad mobile memilki hambatan selama digunakan, jika ada tolong jelaskan. Sistem keamanan data saat ini sangat ramai rentan di bobol, menurut bapak apakah aplikasi siakad mobile saat ini sudah aman, jika tidak jelaskan.
		Apakah Restful API pada siakad mobile memiliki metode autentikasi untuk data seperti data NIK dan nomer handphone, jelaskan
		Bagaimana pendapat bapak tentang JSON WEB TOKEN apakah cocok untuk system pengamanan RESTFUL API WEBSERVICE, jelaskan
2.	Algoritma HMAC	Fungsi metode kriptografi pada keamanan data sangat dibutuhkan untuk kemanan data, apakah siakad mobile sudah menerapkan fungsi tersebut?
		Apakah algoritma HMAC menurut anda efektif digunakan untuk siakad mobile?

D. Analisa Kebutuhan

Berdasarkan studi literatur yang telah didapatkan dari penelitian terkait maka dijabarkan sebagai berikut :

TABEL III
ANALISA KEBUTUHAN

Permasalahan	Dampak	Solusi
Tidak ada verifikasi terhadap *token* ketika melakukan *request* terhadap server (Arief, 2022).	Orang lain dapat melakukan *request* data kepada *server* tanpa adanya proses	Melakukan pengamanan dengan menggunakan *Json Web Token.*

	verifikasi (Arief, 2022).	
Perbedaan ketika menggunakan pengamanan algoritma *hmac sha-512* dan *hmac sha-256* didalam penerapan *json web token* (Alam, 2018).	Memiliki dampak jika *algoritma hmac sha-512* dijalankan pada arsitektur 64*bit*. (Alam, 2018).	Penulis menggunakan algoritma *hmac sha-512* dikarenakan sesuai dengan arsitektur yang dipakai adalah 64*bit*.

E. Klasifikasi Data

Dilakukan dengan membaca seluruh data secara mendalam dan mengelompokkan data sesuai pemahaman peneliti berdasarkan dari hasil wawancara dengan informan.

TABEL IV
KLASIFIKASI KEAMANAN

NO	Fitur	REST		Keamanan	
		Get	Post	Firewall	JWT Hmac sha
1	Biodata		✓	✓	
2	Jadwal Kuliah		✓	✓	
3	KRS		✓	✓	
4	KHS		✓	✓	
5	History UKT		✓	✓	
6	Rekap Absen		✓	✓	

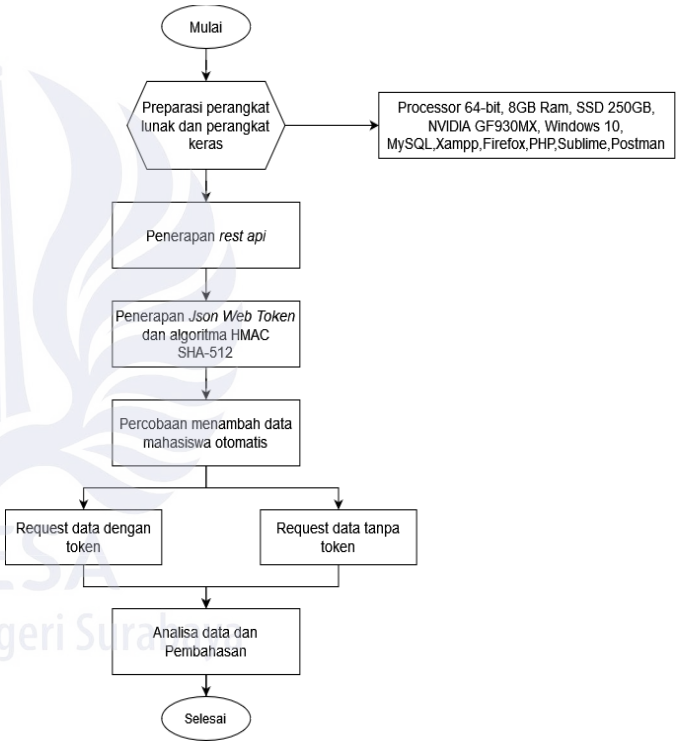
Pada klasifikasi celah keamanan didapatkan menggunakan *software postman* terletak pada url http://siakadu.unesa.ac.id/api/apiunggun dengan melakukan *request* dengan *key* dan *value* dapat diakses tanpa adanya autentikasi.

TABEL V
KLASIFIKASI CELAH KEAMANAN

NO	*Parameter*		*Key and Value*	
	GET	POST	kondisi	nipd
1		✓	biodatamhsmobile	NIM
2		✓	jadwalperkuliahan	NIM
3		✓	krs_mahasiswa	NIM
4		✓	khs_mahasiswa	NIM
5		✓	history_ukt	NIM
6		✓	rekap_absen	NIM

F. Desain Pengujian

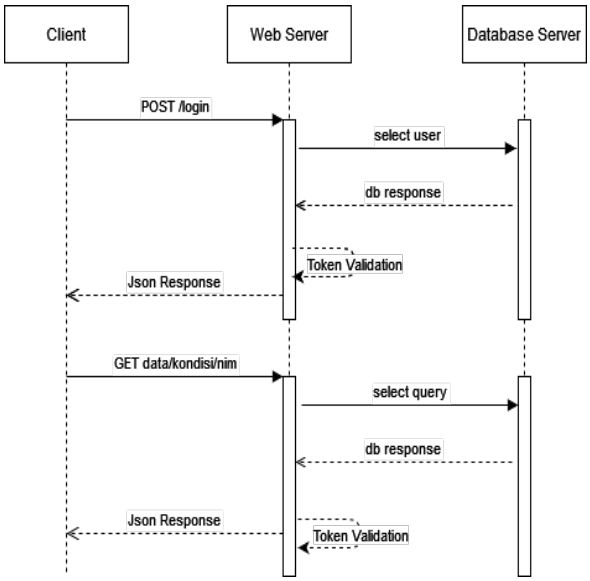
Penulis melakukan pengujian melakukan penerapan *Json Web Token* & memakai prosedur pemecahan *hmac sha-512* didalamnya dan menggunakan *script* yang sanggup menambah data secara *realtime* lalu dilakukan pengetesan terhadap sistem bermaksud menguji coba memakai data aktif.



Gbr. 2 Alur Pengujian

1. Rest Api

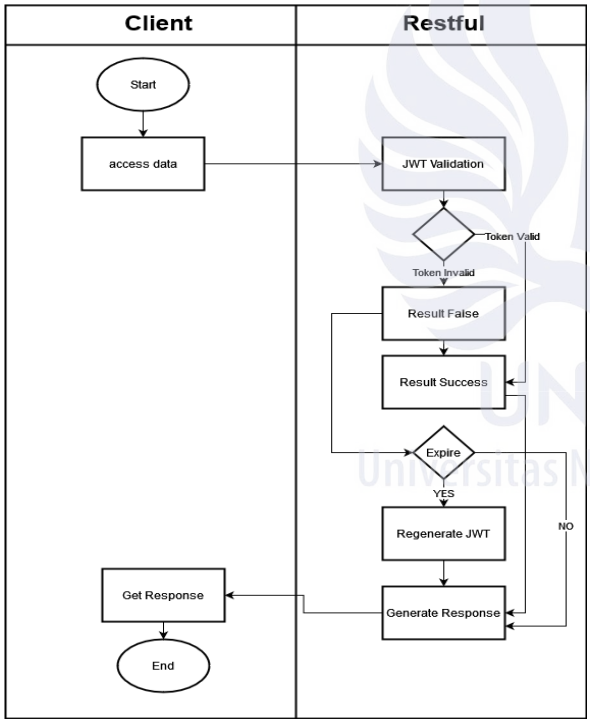
Proses arsitektur *rest api* memiliki sebuah rangkaian terstruktur klien melakukan serangkaian operasi yang dapat dipanggil oleh *client http* operasi yang diliki *rest api* adalah *GET, POST, DElETE. web server* bekerja untuk mengidentifikasi apa yang diinginkan oleh klien kemudian dilanjutkan pada *database server* dan menghasilkan *response* sesuai apa yang diminta oleh klien.



Gbr. 3 *Rest Api*

2. *Json Web Token Validation*

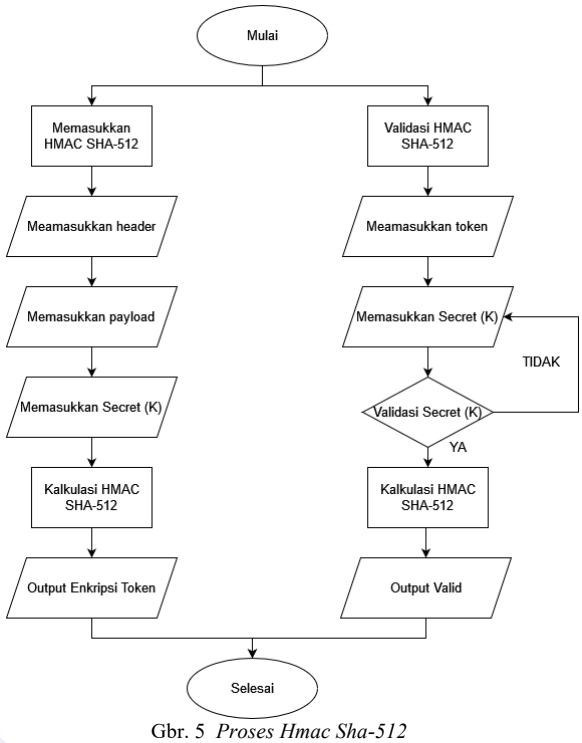
ketika klien mengakses data pada aplikasi dan akan ada proses autentikasi dan pertukaran informasi, dengan mengirim *token* melalui *url* parameter *HTTP* jika proses autentikasi berhasil maka *server* akan merespon apa yang diminta oleh klien.



Gbr. 4 *Json Web Token Validation*

3. *Hmac Sha-512*

klien menggunakan rest api maka akan adanya validasi signature dan pengirimannya melalui header *http* jadi untuk proses verifikasi klien perlu membagikan kunci yang digunakan untuk membuatnya dan mengirim pesan dan penerima harus memiliki kunci yang sama.



Gbr. 5 *Proses Hmac Sha-512*

F. Alat Pendukung Penelitian

Dalam membangun sebuah sistem maka dibutuhkanlah peralatan yang mendukung terdiri dari perangkat keras *(hardware)* dan perangkan lunak *(software)*. Perangkat yang digunakan dalam penlitian antara lain dijabarkan sebagai berikut:

1. *Hardware*

   Komputer yang memiliki spesifikasi:
   a. *Architecture Processor* 32/64 *bit*
   b. 8GB *RAM (Random Access Memory)*
   c. *SSD* 250GB
   d. *NVIDIA Geforce* 930MX
2. *Software*

   Agar sistem yang dibangun dapat berjalan baik dan benar maka diperlukan beberapa perangkat lunak yang membantu dalam pengerjaan sistem sebagai berikut :
   a. *Operating System Windows 10*
   b. *Database : MysQl*
   c. *Browser Internet : Firefox*
   d. *Programming language : PHP (Hypertext Preprocessor)*
   e. *Editor : Sublime Text*
   f. *Tool HTTP Client : Postman*

IV. HASIL DAN PEMBAHASAN

Hasil penelitian dan pembahasan penelitian merupakan hasil analisis data. Di bagian ini akan adanya proses pembahasan berdasarkan rumusan masalah dan tujuan penelitian. Pada tahapannya akan dijelaskan bahwa sistem siap untuk dijanlakan pada keadaan yang sebenarnya, sehingga akan mengetahui

hasil apakah yang diperoleh dari sistem sesuai dengan tujuan yang diharapkan.

A. *Hasil Pengujian*

Hasil akan dijelaskan berdasarkan pengujian yang telah dilakukan proses enkripsi dan deskripsi pada *json web token* menggunakan *algoritma hmac sha-512* terhadap sistem yang telah dibuat. Pengujian ini dilakukan dengan melakukan penginputan data secara *realtime* menggunakan fitur *seeder* yang ada pada *laravel framework* dan memanfaatkan *bash script* untuk automasi penginputan data melalui *seeder*, hasil Analisa dan pengujian yang diperoleh dapat dilihat berdasarkan perbandingan ketika melakukan request menggunakan token dan tidak menggunakan token sebagai berikut.

1. *Penginputan data realtime*

Pada bagian ini dilakukan penginputan data mahasiswa secara *realtime* dengan menggunakan *seeder* pada *laravel framework,* proses ini menggunakan aturan penginputan dengan berapa kali *looping* yang diinginkan dan memberi waktu *sleep* per-detik.

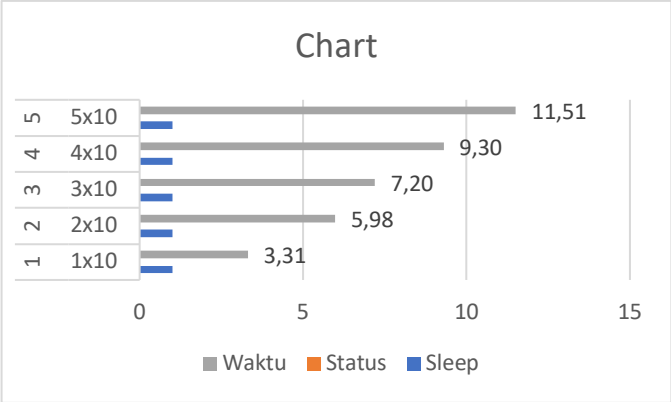
```
abrisam@abrisam MINGW64 /c/xampp/htdocs/skripsi
$ ./hasnain.sh
#========================#
#Satu kali seeder 10 data #
# LoopSeeder Data Laravel #
#   by @Jihadsatrio      #
#========================#
masukan berapa kali loop
1
masukan berapa detik untuk loop example: 5
1

 menjalankan seeder[!] per 1 detik

  INFO  Seeding database.

{
    "name": "Susanna Krajcik",
    "nipd": 22988,
    "email": "awunsch@example.org",
    "email_verified_at": "2022-11-13T16:45:22.000000Z",
    "jk": "lk",
    "nm_agama": "konghucu",
    "nm_ayah": "Shyanne Bednar",
    "nm_ibu": "Melany King",
    "tgl_lahir": {
        "date": "1997-03-20 21:20:34.000000",
        "timezone_type": 3,
        "timezone": "UTC"
    },
    "tmpt_lahir": "Iraq",
    "ipk": "4",
    "picture": "Dr. Dan Haley II",
    "updated_at": "2022-11-13T16:45:22.000000Z",
```

Gbr. 6 *Proses Penginputan Data Realtime*

TABEL VI
HASIL WAKTU INPUT DATA

No	Jumlah Inputan	*Sleep*	Status	Waktu
1	1x10	1	Sukses	3.31
2	2x10	1	Sukses	5.98
3	3x10	1	Sukses	7.20
4	4x10	1	Sukses	9.34
5	5x10	1	Sukses	11.51
Total data	150 data	Total waktu per-detik:		37.34

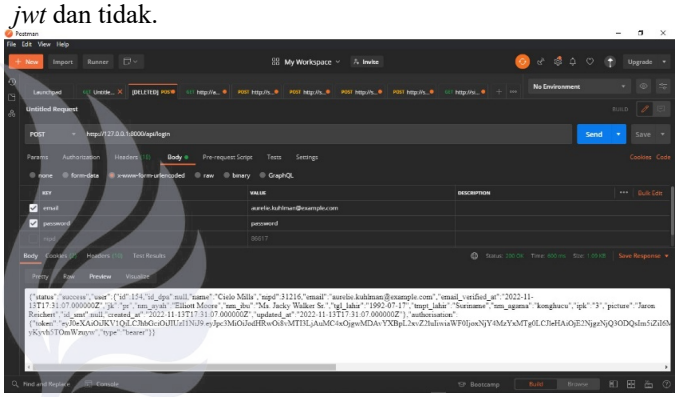
Tabel VI menerangkan bahwa ketika melakukan penginputan data menggunakan *seeder* dan memanfaatkan automasi *bash script* memiliki waktu yang berbeda disetiap lama waktu penginputan datanya bergantung pada banyak data yang dimasukkan.



Gbr. 7 *Chart Hasil Input Data*

2. *Pengujian Request Data*

Berdasarkan hasil pengujian terhadap *request user* memiliki *role admin* dan *user* terdapat sebuah perbedaan hak dalam pengaksesan data dimana *role admin* dapat melihat data seluruh mahasiswa maka sebaliknya *role user* hanya dapat melihat data biodatanya sendiri, pada bagian ini juga dilakukan melakukan *request* menggunakan *token jwt* dan tidak.



Gbr. 7 *Login Dengan Fitur Rest API*

TABEL VII
HASIL RESPONSE LOGIN

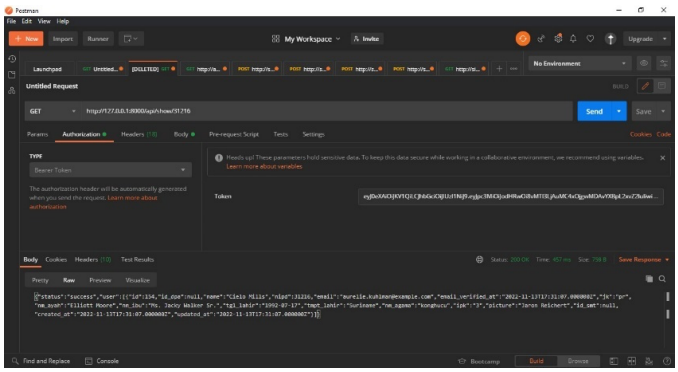
Email	***Password***
aurelie.kuhlman@example.com	*****
Token	
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTI3LjAuMC4xOjgwMDAvYXBpL2xvZ2luIiwiaWF0IjoxNjcxMTQ2NjU2LCJleHAiOjE2NzExNTAyNTYsIm5iZiI6MTY3MTE0NjY1NiwianRpIjoiZDNVZ3k1NGlRWjM3WmZjcSIsInN1YiI6IjEiLCJwcnYiOiIyM2JkNWM4OTQ5ZjYwMGFkYjM5ZTcwMWM0MDA4NzJkYjdhNTk3NmY3In0.dNeil68KFA8jM05FWleCQ5gfuDSTEs9l1BlGN-WwQac	
Token Type	*Bearer*
Role	*Admin*
Url	127.0.0.1/api/login
Method	*POST*

Tabel VII memiliki hasil informasi berupa token yang nanti akan dipakai guna proses autentikasi ketika melakukan *request* data terhadap *server.*

TABEL VIII
HASIL RESPONSE LOGIN

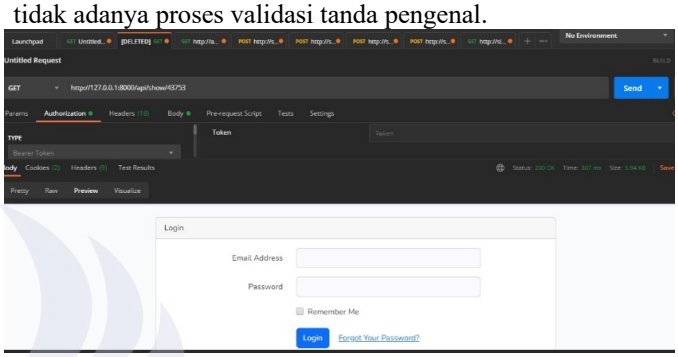
Hasil *Encoded Token*	
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vMTI3LjAuMC4xOjgwMDAvYXBpL2xvZ2luIiwiaWF0IjoxNjcxMTQ2NjU2LCJleHAiOjE2NzExNTAyNTYsIm5iZiI6MTY3MTE0NjY1NiwianRpIjoiZDNVZ3k1NGlRWjM3WmZjcSIsInN1YiI6IjEiLCJwcnYiOiIyM2JkNWM4OTQ5ZjYwMGFkYjM5ZTcwMWM0MDA4NzJkYjdhNTk3NmY3In0.dNeil68KFA8jM05FWleCQ5gfuDSTEs9l1BlGN-WwQac	
Hasil *Decoded Token*	
Header (Algorithm & Token Type)	***Payload (Data)***
{ "typ": "JWT", "alg": "HS512" }	{ "iss": "http://127.0.0.1:8000/api/login", "iat": 1671146656, "exp": 1671150256, "nbf": 1671146656, "jti": "d3Ugy54iQZ37Zfcq", "sub": "1", "prv": "23bd5c8949f600adb39e701c400872db7a5976f7" }
Verify Signature	
HMACSHA512(base64UrlEncode(header) + "." + base64UrlEncode(payload), eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJodHRwOi8vMTI3LjAuMC4xOjgwMDAvYXBpL2xvZ2luIiwiaWF0IjoxNjcxNTQ2NDIyLCJleHAiOjE2NzE1NTAwMjIsIm5iZiI6MTY3MTU0NjQyMiwianRpIjoiWldsTjh2ZzRhUUhidlZtNiIsInN1YiI6IjEiLCJwcnYiOiIyM2JkNWM4OTQ5ZjYwMGFkYjM5ZTcwMWM0MDA4NzJkYjdhNTk3NmY3In0.SUQz9k966FQUfCzTSrZNsfratUnPcIhR5_Y_7FEmN9sN6PVV68oKhoxmSz1SKZJcddgOlOMjix_SF0JVwmIbgQ)	

Tabel VIII dijelaskan pada penerapan algoritma *hmac sha-512* yang ada pada *json web token* terdapat sturktur yang memiliki *header, payload* dan *signature,* kemudian pada *header* memiliki dua bagian seperti jenis *token* yang digunakan yaitu *jwt* dan bagian selanjutnya adalah algoritma yang digunakan *hmac sha-512* sebagai penanda tanganan. Pada bagian *payload* berisi informasi atau data yang akan dikirim memiliki sifat data yang unik bagi *user* berkaitan dengan *authorization* karena data tersebut digunakan tanda pengenal oleh pengirim *token*, hasil dari penggabungan ketiga bagian tersebut akan dikelompokkan dan ototmatis dilakukan *encode* menjadi *token random.*



Gbr. 8 *Request Data Dengan Token Pada Rest API*

Tahap selanjutnya adalah melakukan pengujian terhadap *request* data pada fitur *rest api* tanpa menggunakan token dan memiliki hasil *output* berupa halaman *login* karena tidak adanya proses validasi tanda pengenal.



Gbr. 9 *Request Data Tanpa Token Pada Rest API*

B. *Pembahasan*

Berdasarkan hasil pengujian yang telah dilaksanakan di kantor PPTI (Pusat Pengembangan Teknologi Informasi) Universitas Negeri Surabaya Lidah Wetan dengan hasil wawancara kepada narasumber atau pakar yaitu ketua PPTI UNESA didapatkan beberapa point yaitu siakad *mobile* telah menerapkan *restful api* pada pengamanan sistem data yang berupa *token* dan dari sisi *server* menggunakan *firewall protection*. Akan tetapi temuan pada studi literatur berupa artikel ilmiah masih ditemukan celah pada fitur *rest api* berdasarkan hal tersebut penulis melakukan penerapan pengaman *restful api* menggunakan *json web token hmac sha-512 algorithm* dan memiliki hasil uji dengan table sebagai berikut :

TABEL IX
RATA-RATA TIME RESPONSE ROLE USER

No	RU	DT	TT	RNML
1.	501	403	226	338
2.	572	324	213	330
3.	468	356	222	269
4.	430	298	227	278
5.	433	302	223	269
6.	373	292	281	274
7.	393	588	214	297
8.	413	252	279	485

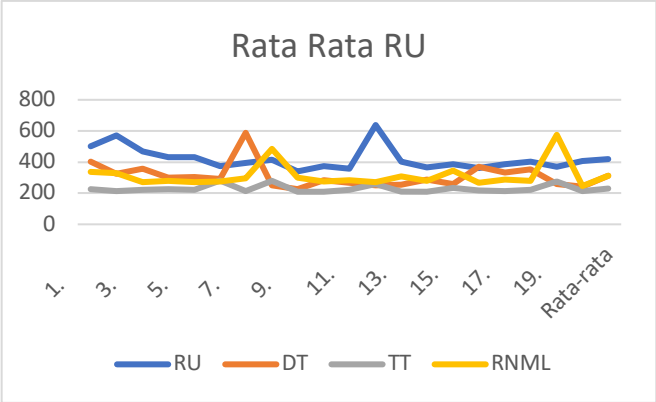
9.	340	226	211	299
10.	375	282	211	274
11.	357	267	223	283
12.	638	250	260	270
13.	403	253	210	309
14.	365	289	211	278
15.	386	260	233	344
16.	360	371	218	267
17.	386	332	213	289
18.	401	353	221	281
19.	370	260	277	575
20.	405	244	215	246
Rata-rata	418,45	310,1	229,4	312,75

TABEL X
RATA-RATA TIME RESPONSE ROLE ADMIN

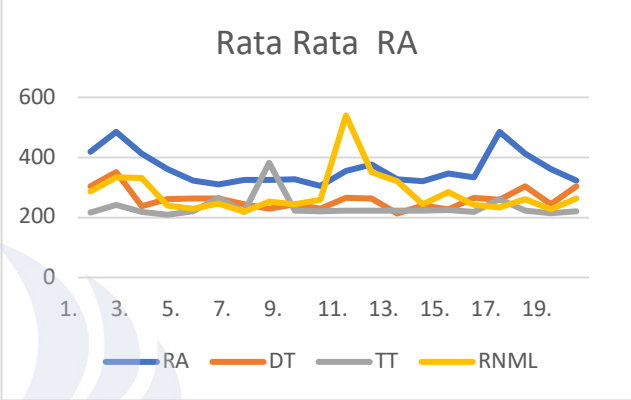
No	RU	DT	TT	RNML
1.	419	304	217	286
2.	485	351	241	334
3.	413	238	219	332
4.	361	260	209	239
5.	323	264	221	230
6.	311	263	266	247
7.	326	244	218	219
8.	326	229	382	252
9.	327	244	222	243
10.	305	230	220	259
11.	355	265	223	540
12.	377	263	222	350
13.	328	213	222	321
14.	320	240	223	245
15.	346	226	224	285
16.	333	265	218	241
17.	485	258	262	234
18.	413	304	222	262
19.	361	258	215	227
20.	323	304	221	263
Rata-rata	361,85	260,45	233,35	280,45

Dari hasil Tabel diatas memiliki keterangan sebagai berikut :

1. RU : Role user
2. RA : Role admin
3. DT : Dengan token
4. TT : Tanpa token
5. RNML: Request nim mahasiswa lain
6. Hijau : Berhasil
7. Merah : Gagal



Gbr. 10 *Chart Rata Rata Time Respone RU*



Gbr. 10 *Chart Rata Rata Time Respone RA*

Pada gambar diatas dijelaskan terdapat hasil uji coba pada request menggunakan role admin menggunakan postman terdapat grafik yang terdapat hasil yang acak terdapat waktu pengujian request time pada role admin. kemudian pada gambar rata-rata RU dijelaskan bahwa hasil time response pengujian pada pengguna yang memiliki hak user memiliki keluaran waktu yang berbeda beda hasil tercepat didapatkan ketika melakukan pengujian tanpa token dan hasil memakan waktu yang lebih tinggi didapatkan ketika melakukan login.

V. KESIMPULAN

Berdasarkan hasil uji coba yang telah dilakukan oleh peneliti mengenai pengamanan restful api menggunakan *json web token* dan algoritma *hmac sha 512*, kesimpulan yang diperoleh dari seluruh proses dan hasil pembahasan pada penelitian yang telah dilakukan sebagai berikut :

1. Hasil wawancara pada ahli atau ketua ppti menjelaskan bahwa aplikasi siakadu *mobile* aman tetapi di dalam studi literatur berupa artikel ilmiah sebelumnya di dapati bahwa masih ada celah keamanan data dengan cara melakukan request data tanpa adanya login terhadap aplikasi siakadu *mobile*.
2. Dengan menerapkan *jsonweb token* algoritma *hmac sha-512* pada rest api ketika melakukan request diketahui bahwa user atau pengguna harus melakukan login terlebih dahulu sehingga token akan diberikan kepada user yang nantinya akan digunakan untuk

melakukan request dan pencocokan token atau private key pada server.
3. Dari hasil pengujian penginputan data secara ulang dan menghasilkan data yang real time kemudian dilakukan proses pengujian request terhadap *rest api* tidak ada perbedaan ketika melakukan *request* dalam segi keamanan.

VI. SARAN

Pada penelitian yang telah dilakukan ini semua proses sudah berjalan dengan semestinya namun berdasarkan penelitian yang dilakukan, saran yang dibutuhkan dari pengembangan sistem ketika melakukan pengamanan restful api menggunakan *json web token* algoritma *hmac sha-512* lebih lanjut adalah sebagai berikut:

1. Penulis menyadari bahwa penerapan keamanan data menggunakan *json web token* algoritma *hmac sha-512* belum sempurna oleh karena itu, untuk kedepanya penelitian selanjutnya diharapkan dapat mengimplentasikan pada siakadu (Sistem Informasi Akademik Unesa) mobile.
2. Pada penereapan keamanan data menggunakan *json web token hmac sha-512 algorithm* ini masih sangat sederhana pada fitur pengambilan data mahasiswa, dikarenakan data real mahasiswa pada perguruan tinggi sangatlah banyak maka dari itu dibutuhkan pengembangan sistem agar dapat dijalankan secara tepat dan sesuai dengan kebutuhan yang diinginkan.

VII. UCAPAN TERIMAKASIH

Alhamdulillah, atas segala Rahmat dan Hidayah-Nya dan pada akhirnya saya mampu menyelesaikan Skripsi ini dengan baik. Adanya karya kecil yang sudah saya buat, saya sangat amat berterima kasih kepada:

1. Allah SWT yang selalu memberikan rahmat dan pertolongannya untuk saya serta atas ridho-Nya pula skripsi ini bisa diselesaikan dengan baik.
2. Kedua orang tua tercinta saya Bapak Mulyo Santoso dan Almarhumah Ibunda Indah Kurniawati beserta adik Dimas Falah Setiawan yang tak pernah henti mendoakan dan mendukung saya didalam berbagai segala keadaan.
3. Paman dan bibi tercinta saya Bapak Surya dan Ibu Yulaena yang selama ini mendidik dan membantu saya agar menjadi anak yang berguna bagi kedua orang tua.
4. Ibu Aries Dwi Indriyanti, S.Kom., M.Kom. selaku dosen pembimbing skripsi yang telah banyak memberikan ilmunya, membantu saya selama proses perkuliahan dan memberikan motivasi sehingga saya dapat menyelesaikan skripsi ini.
5. Bapak Aditya Prapanca, S.T., M.Kom. dan Bapak Dodik Arwin Dermawan, S.ST., S.T., M.T. selaku dosen penguji skripsi saya yang memberikan masukan-masukan agar skripsi saya menjadi lebih baik.
6. Seluruh Civitas Akademik Universitas Negeri Surabaya terutama dosen-dosen saya tercinta semoga ilmu nya berkah dan penulisan skripsi dan tugas akhir dengan studi kasus di kampus UNESA sebagai bentuk khidmah saya pada perguruan tinggi ini.
7. Keluarga besar Jurusan Teknik Informatika Angkatan 2017 yang telah melewati proses mencari ilmu dan susah senang bersama selama perkuliahan, serta mendukung ketika mengalami kesusahan hingga detik akhir menjadi mahasiswa.
8. Teman hidup saya Elmawati yang selalu menemani dan memberi semangat dalam penyusunan skripsi ini.
9. Teman teman Warkop DKI yang senantiasa menemani dikala susah senang dan senda gurau mereka yang menguatkan saya untuk menjalani penyelesaian skripsi ini.

REFERENSI

[1] Utami, S. S. (2010). Pengaruh Teknologi Informasi Dalam Perkembangan Bisnis. Jurnal Akuntansi dan Sistem Teknologi Informasi, 8(1).

[2] Simarmata, J., Chaerul, M., Mukti, R. C., Purba, D. W., Tamrin, A. F., Jamaludin, J., ... & Meganingratna, A. (2020). Teknologi Informasi: Aplikasi dan Penerapannya. Yayasan Kita Menulis.

[3] Praditya, A. R., & Yustanti, W. (2019). Pengaruh Kualitas Layanan Sistem Informasi Akademik Terpadu (Siakadu) Terhadap Kepuasan Mahasiswa (Studi Kasus: Fakultas Teknik Universitas Negeri Surabaya). In Jurnal Manajemen Informatika (Vol. 10, Issue 01).

[4] Surwase, V. (2016). REST API modeling languages-a developer's perspective. Int. J. Sci. Technol. Eng, 2(10), 634-637.

[5] Chen, X., Ji, Z., Fan, Y., & Zhan, Y. (2017). Restful API Architecture Based on Laravel Framework. In Journal of Physics: Conference Series (Vol. 910). https://doi.org/:10.1088/1742-6596/910/1/

[6] Rahman, M. A., & Agus Prihanto. (2022). Analisis Keamanan Data Pada Aplikasi Android Menggunakan HTTP Canary (Studi Kasus : Siakadu UNESA Mobile). In Journal of Informatics and Computer Science (JINACS) (Vol. 03, Issue 03).

[7] Somya, R., & Nathanael, T. M. E. (2019). Pengembangan Sistem Informasi Pelatihan Berbasis Web Menggunakan Teknologi Web Service Dan Framework Laravel. Techno Nusa Mandiri: Journal of Computing and Information Technology, 16(1), 51-58.Jones, M., Bradley, J., & Sakimura, N. (2015). Json web token (jwt) (No. rfc7519).

[8] Turner, J. M. (2008). The keyed-hash message authentication code (hmac). Federal Information Processing Standards Publication, 198(1), 1-13.

[9] Setiawan, A., & Purnamasari, A. I. (2020). Implementasi JSON Web Token Berbasis Algoritma SHA-512 untuk Otentikasi Aplikasi BatikKita. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(6), 1036-1045.

[10] Rahmatullah, A., Sulastri, H., & Nugroho, R. (2018). Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512.
[11] Hibsy, A., & Wibowo, A. (2020). Implementation of Security Features with JSON Web Tokens and Geo-tagging Features in Web Service Training From Home Applications. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(4), 618-626.
[12] Harahap, N. (2020). Penelitian Kualitatif.
[13] Anufia, B., & Alhamid, T. (2019). Instrumen Pengumpulan Data.