Journal of Information Technology and Computer Science (INTECOMS)
Volume 6 Nomor 2, Desember 2023
e-ISSN : 2614-1574
p-ISSN : 2621-3249

SKEMA OTENTIKASI RINGAN UNTUK PERANGKAT IOT DENGAN MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN

LIGHTWEIGHT AUTHENTICATION SCHEME FOR IOT DEVICES USING THE RIVEST SHAMIR ADLEMAN METHOD

Boy Sampetua Sipahutar[1], Aulia Khamas Heikhmakhtiar[2], Rinaldi Munir[3], Akhmad Farid Wadjdi[4]
[1]Fakultas Sains Dan Teknologi Pertahanan Universitas Pertahanan Republik Indonesia, [2]Prodi Informatika, Fakultas Sains dan Teknologi Pertahanan, Unhan RI, [3]Institut Teknologi Bandung, [4]BRIN, Pusat Riset Geospasial
boy.sipahutar@tp.idu.ac.id

ABSTRACT
Internet of Things (IoT) connects various types of devices to the internet, creating intelligent and integrated systems. However, security is becoming a significant challenge in IoT development, as internet-connected devices are vulnerable to cyber-attacks. To solve security problems in IoT, authentication schemes are an important solution. This study aims to develop a lightweight authentication scheme using RSA encryption for IoT devices. The research method used is experimental research, by developing and testing the implementation of authentication schemes on IoT devices. The data used is primary data from testing the implementation of authentication schemes on IoT devices. Tests on the implementation of the authentication scheme show that this scheme can provide an adequate level of security for IoT devices with low overhead. The conclusion of this study is that a lightweight authentication scheme using RSA encryption can be an effective solution to increase security on IoT devices. This research contributes to the development of IoT technology by offering a secure and efficient authentication scheme for IoT devices.

Keywords: *IoT Security, IoT Authentication, IoT RSA*

ABSTRAK
Internet of Things (IoT) menghubungkan berbagai jenis perangkat ke internet, menciptakan sistem yang cerdas dan terintegrasi. Namun, keamanan menjadi tantangan yang signifikan dalam pengembangan IoT, karena perangkat yang terhubung ke internet rentan terhadap serangan cyber. Untuk mengatasi masalah keamanan pada IoT, skema otentikasi menjadi salah satu solusi yang penting. Penelitian ini bertujuan untuk mengembangkan skema otentikasi ringan menggunakan enkripsi RSA untuk perangkat IoT. Metode penelitian yang digunakan adalah penelitian eksperimental, dengan mengembangkan dan menguji implementasi skema otentikasi pada perangkat IoT. Data yang digunakan adalah data primer dari pengujian implementasi skema otentikasi pada perangkat IoT. Hasil pengujian implementasi skema otentikasi menunjukkan bahwa skema ini dapat memberikan tingkat keamanan yang memadai untuk perangkat IoT dengan overhead yang rendah. Kesimpulan dari penelitian ini adalah skema otentikasi ringan menggunakan enkripsi RSA dapat menjadi solusi yang efektif untuk meningkatkan keamanan pada perangkat IoT. Penelitian ini memberikan kontribusi untuk pengembangan teknologi IoT dengan menawarkan skema otentikasi yang aman dan efisien untuk perangkat IoT.

Kata Kunci: Keamanan IoT, Otentikasi IoT, IoT RSA

PENDAHULUAN

Telah banyak laporan yang menunjukkan bahwa perangkat IoT rentan peretasan (YASMINE HARBI, 2021). Dengan meningkatnya popularitas perangkat IoT dalam kehidupan sehari-hari, bahasan masalah keamanan dan risikonya perlu mendapat perhatian serius, misalnya, kebocoran informasi sensitif, penolakan serangan layanan, dan akses jaringan yang tidak sah (Minhaj Ahmad Khan, 2018); masalah ancaman saluran sisi daya, yang memungkinkan pembongkaran tingkat instruksi dari program tingkat perakitan perangkat (Tyagi, 2017); dan (Zhang L. Z., 2019) (Varma, 2019).

Eksplorasi berbagai riset lainnya yang dilakukan Jiang et al. menunjukkan

bahwa kerentanan yang umum terjadi pada perangkat IOT adalah penolakan layanan dan akses jaringan yang tidak sah (Jiang, 2020) Selain hal yang diatas, Buffer Overflow (Calatayud, IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)), dan kebocoran privasi pengguna juga menjadi keamanan yang perlu diatasi (Alladi, 2020).

Penelitian terdahulu juga menunjukkan bahwa solusi untuk menjaga keamanan jaringan IoT adalah tugas yang kompleks (Voas, 2016). Misalnya, perlunya modifikasi arsitektur aplikasi IoT untuk lingkungan end-to-end dan membahas teknologi-teknologi baru seperti blockchain, fog computing, edge computing, dan machine learning yang dapat digunakan untuk meningkatkan keamanan penggunaan perangkat IoT (Hassija, 2019); pentingnya upaya standardisasi untuk mengadaptasi dan meningkatkan *Datagram Transport Layer Security* untuk aplikasi IoT (Keoh, 2014); dan penggunaan pembelajaran mesin dalam gateway IoT untuk membantu mengamankan sistem - jaringan syaraf tiruan di gateway untuk mendeteksi anomali dalam data yang dikirim dari perangkat edge (Canedo, 2016).

Sementara itu untuk perangkat dengan sumber daya kecil, banyak riset yang mengusulkan solusi keamanan IoT melalui skema autentikasi ringan yang aman untuk berbagai aplikasi seperti aplikasi e-health dalam konteks Internet of Things (Khemissa, 2015); pengguna seluler (Anwar, 2015); skema autentikasi ringan yang mendukung pencabutan kartu pintar dan efisien secara komputasi dibandingkan skema yang ada (Mishra D. D., 2015).

Otentikasi adalah salah satu prinsip keamanan jaringan yang kuat, khususnya untuk jaringan kecil seperti server lokal atau untuk jaringan besar seperti server cloud pusat (Salah, 2012) dan skema otentikasi ringan memiliki beberapa manfaat, termasuk peningkatan keamanan, pengurangan konsumsi energi, dan autentikasi yang lebih cepat (Lee, 2014). Dalam prakteknya, skema otentikasi adalah suatu cara untuk memastikan bahwa pengguna atau perangkat yang terhubung pada jaringan IoT adalah benar-benar yang seharusnya. Beberapa contoh penggunaan skema otentikasi ringan misalnya, (Fan, 2019), pengendalian lampu dari jarak jauh menggunakan Raspberry Pi (Efendi, 2018), sistem keamanan rumah menggunakan ESP8266 (Hutabarat, 2018), sistem deteksi kebakaran menggunakan Arduino (Sasmoko, 2017), dan kontrol lampu otomatis menggunakan Arduino dan Platform Cayenne IoT (Tayef, 2021).

Sementara itu skema otentikasi yang kompleks dan memakan banyak sumber daya dapat menjadi beban tambahan bagi perangkat IoT yang memiliki keterbatasan sumber daya.

Penelitian sebelumnya telah mengembangkan beberapa skema otentikasi ringan pada IoT, namun masih terdapat beberapa kelemahan dalam skema tersebut, misalnya rentan peretasan akses sandi (Kumar, 2022), rentan serangan peniruan identitas pengguna dan memiliki biaya penyimpanan yang besar (Zhou, 2019). Oleh karena itu, ada kebutuhan riset pengembangan skema otentikasi ringan yang lebih aman dan efisien untuk perangkat IoT. Dengan demikian kami memandang bahwa studi ini memiliki relevansi kuat terhadap upaya memberikan solusi masalah kerentanan perangkat IoT yang menerapkan skema otentikasi ringan.

Atas dasar pemikiran tersebut, penelitian ini Tujuan: mengembangkan skema otentikasi ringan yang aman dan tanpa memberikan beban tambahan pada perangkat IoT.

Manfaat: meningkatkan keamanan jaringan IoT dan mengurangi risiko pencurian data, peretasan perangkat, dan penyalahgunaan perangkat pada jaringan tersebut. Selain itu, penelitian ini juga dapat menjadi acuan bagi para peneliti untuk mengembangkan skema otentikasi ringan yang lebih aman dan efisien untuk perangkat IoT di masa depan.

Berdasarkan uraian latar belakang dan tujuan diatas, kami merumuskan pertanyaan sebagai berikut:

Bagaimana pengembangan skema otentikasi ringan yang aman untuk perangkat IoT? Untuk mengetahui bagaimana mengembangkan skema otentikasi yang dapat memenuhi dua hal penting dalam penggunaan perangkat IoT, yaitu keamanan dan efisiensi sumber daya. Penelitian ini akan mengeksplorasi beberapa metode otentikasi yang dapat digunakan pada perangkat IoT, serta mengevaluasi keamanan dan efisiensi masing-masing metode.

Apa saja keterbatasan sumber daya pada perangkat IoT yang harus diperhatikan dalam pengembangan skema otentikasi ringan? Perangkat IoT memiliki keterbatasan sumber daya, seperti daya, memori, dan kecepatan prosesor, yang harus diperhatikan dalam pengembangan skema otentikasi ringan. Pertanyaan ini akan mengeksplorasi keterbatasan sumber daya pada perangkat IoT dan bagaimana mempertimbangkan keterbatasan tersebut dalam pengembangan skema otentikasi.

Bagaimana mengatasi masalah keamanan pada jaringan IoT tanpa memberikan beban tambahan pada perangkat IoT? Bagaimana cara mengoptimalkan keamanan pada jaringan IoT tanpa memberikan beban tambahan pada perangkat IoT. Penelitian ini akan mengeksplorasi bagaimana mempertahankan keamanan pada jaringan IoT tanpa menambahkan beban pada perangkat IoT, serta bagaimana mengatasi risiko keamanan pada perangkat IoT yang sudah terkoneksi ke jaringan

METODE

Dalam penelitian ini, metode penelitian yang akan digunakan adalah *mixed-method* yakni dibagi menjadi Studi literatur mengenai apa saja yang dibutuhkan terkait penelitian ini dan selanjutnya melakukan Analisis Dan Desain Sistem berisi perancangan Arsitektur system dengan menggunakan pengendali mikro dengan papan tunggal yang berfungsi dalam proyek perangkat lunak sumber terbuka (Arduino) dan hasil akhir penelitian akan disajikan dalam bentuk tabel berupa perbandingan sebelum dan sesudah penambahan otentikasi.

Pada studi kasus penelitian kali ini, kami menggunakan perangkat IoT unutk kebutuhan pengecekan jumlah liter yang dimasukan ke tangki bahan bakar truk ekspedisi untuk menghitung total penggunaan bahan bakar truk tersebut per satuan waktu (hari/minggu atau bulan) sehingga bisa validasi dengan laporan penggunaan bahan bakar yang di laporkan oleh pengemudi.

Skema yang Diusulkan

Dalam penelitian ini skema yang diusulkan adalah skema otentikasi sederhana dengan mengirimkan idPerangkat (alat pengurkur jumlah) yang sudah di enkrpsi dengan menggunakan RSA. Selain idPerangkat, data jumlah liter (output alat) yang akan dikirim ke komputer server juga akan di enkripsi terlebih dahulu dengan menggunakan kunci publik yang sudah dibuat sebelumnya untuk selanjutnya dikirim melalui HTTP POST ke server online (aplikasi yang sudah di publish sebelumnya).

HASIL DAN PEMBAHASAN

1. Hasil Pengembangan

Sesuai dengan skema yang diusulka pada metode penelitan. Selanjutnya peneliti mengembang kode yang asli yang sudah dibuat sebelumnya dengan menambahkan enkripi RSA pada data yang dikirim sehingga dengan modifikasi request (http post) data yang dikirim ke server lebih sulit untuk di ubah oleh orang yang tidak berwenang dan membatasi kemungkinan untuk mengirimkan reques ke server dengan menggunakan tools http post biasa seperti postman, dll tanpa melalui enkripsi.

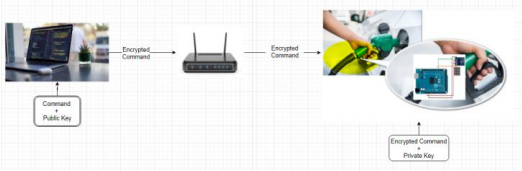
Data yang diterima oleh komputer pengendali (server) yang sudah dalam bentuk data terenkripsi tersebut selanjutnya

akan di dekripsi kembali menjadi data asli untuk di proses lebih lanjut.
Adapun data yang dikirim dalam perancangan ini berupa data jumlah liter dan idPerangkat (device ID).

Tabel 1. Data Yang Dikirim Dari Perangkat

No	Data yang dikirim	Keterangan
1.	totalLiter	Data jumlah liter yang dihasilkan oleh sensor.
2.	idPerangkat	ID Peragkat yang set di dalam perangkat.

Desain skema otentikasi ringan pada IoT didasarkan pada beberapa aspek keamanan, yaitu enkripsi, hashing, dan algoritma otentikasi. Skema ini didesain agar dapat memberikan tingkat keamanan yang memadai pada perangkat IoT tanpa mengorbankan kinerja dan penggunaan sumber daya yang berlebihan. Dalam penelitian ini akan menggunakan metode RSA satu arah dari komputer ke IoT device.



Gambar 1. Skema Otentikasi Ringan IoT

a) Fase Perancancangan Perangkat (IoT Device)

Dalam fase ini penulis dengan dibantu oleh teknisi hardware membuat perangkat pengukur debit cairan sederhanan yang berfungsi untuk mengukur jumlah liter yang di keluarkan dari nozzle pengisian bahan bakar. Adapun spesifikasi perangkat yang dirancang adalah sebagai berikut:

Tabel 2. Spesifikasi Perangkat Iot Sederhana

No.	Spefikasi	Keterangan
1.	Adafruit_Sensor-master	Sensor yang digunakan untuk mengumpulkan data berupa jumlah liter yang di keluaran dari nozzle
2.	ESP8266	Microchip Wi-Fi, dengan perangkat lunak jaringan TCP/IP bawaan, dan kemampuan mikrokontroler
3.	LiquidCrystal I2C	Untuk menampilkan jumlah liter yang di keluarkan di layar sederhana

Gambar 2. Perangkat Pengukur Debit Cairan Sederhana

b) Fase Penulisan Kode sumber

Dalam fase ini penulis mengembangakan kode sumber yang digunakan pada perangkat yang dibuat agar berfungsi, dalam hal ini kode sumber di buat dengan menggunakan bahsa pemrograman C Basic

```
IF time period 1 second

    //Hitung total Liter Per Detik

    total_liter = total_mili / 1000;



    //Print di serial monitor

    print (Debit %kec_air% ml/sec dan
Total %total_liter% L");

    count = 0;



  //Cek data sudah di sync

  IF total_liter > 1 AND debit_air == 0

    postData();

  count = 0;
```

Gambar 3. Pseudo Code Untuk Mengecek Total Liter per Detik

c) Fase Pembangkitan kunci public dan kunci private

Selanjutnya penulis membangkitkan kunci public dan kunci private dengan menggunakan RSA.

Kunci private akan digunakan oleh komuter server untuk melakukan dekripsi data yang diterima melalui HTTP POST yang dikirim oleh perangkat. Kunci pubilc akan disematkan pada perangkat untuk melakukan enkripsi data yang akan di kirim ke komputer server.

Baik kunci public dan kunci private akan di generate oleh applikasi server dengan menggunakan kode PHP.

d) Fase penerapan metode dekripsi perintah didalam perangkat.

Kunci pubic yang di bangkitkan disematkan di dalam perangkat untuk melakukan nkripsi data sebelum melakukan post data ke komputer server.

```
IF WiFi is not Connected
    connectToWifi();
  IF WiFi is Connected
      data = "totalLiter=";
      data += total_liter;
      data += "&idPerangkat=";
      data += idPerangkat;
       data = encrypData(data);
       //POST data to Server
      http.POST(data);
      resetTotalLiter();
  ELSE
    print ("WiFi Not Connected");
```

Gambar 4. Pseudo Code Untuk Melakukan Postdata()

```
String encDt;
Array char_code;
FOR looping on dt.length
    encDt+=char_code[i]
RETURN encDt;
```

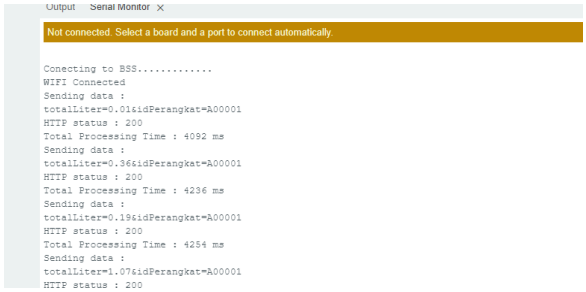
Gambar 5. Pseudo Code Untuk Encrypdata()

2. Pengujian dan Evaluasi Skema Otentikasi Ringan

Setelah perangkat dan kode sumber selasi dekembangkan, proses selanjutnya adalah pengujian skema. Pengujian dilakukan dengan mengaliri sensor (IoT Device) yang buat dengan air untuk mendapatkan data berupa jumlah liter air yang dilalui sensor untuk. Setelah perangkat berhenti dialiri air selanjutnya perangkat tersebut akan melalukan otomatis melakukan posting data ke komputer server melalui HTTP POST ke API komputer server yang sudah dibuat sebelumnya, untuk selanjutnya di dekripsi dan di validasi lebih lanjut, jika idPerangkat dan data valid maka server akan memproses data tersebut lebih lanjut.

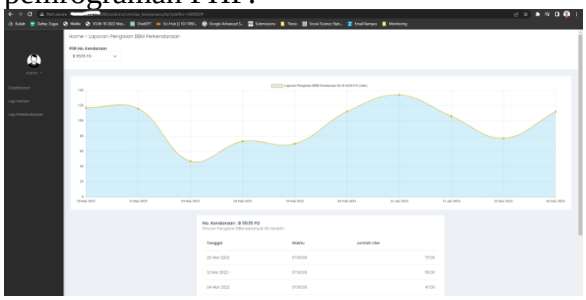
Dalam pengujian peneliti menggunakn tools Arduino IDE untuk mengembangkan code sumber dan melakukan pengujian pengiriman data ke komputer server Hasilnya sebagaimana gambar berikut:

Gambar 6. Pengujian Dengan Mengirimkan Data Enkripsi



Gambar 7. Pengujian Tanpa Enkripsi

Setelah data di proses dan di simpan di database selanjutnya ditampilkan dalam dashboard serderhana yang dibuat sebelumnya dengan menggunakan Bahasa pemrograman PHP.



Gambar 8. Dashboard Data Yang Dikirim Dari Perangkat

3. Keterbatasan Sumber Daya Pada Perangkat IoT yang Harus Diperhatikan.

Perangkat IoT seringkali dibatasi sumber daya dan memiliki daya pemrosesan, memori, dan energi yang terbatas. Oleh karena itu, mereka memerlukan algoritma otentikasi ringan yang dapat diimplementasikan dengan overhead minimal1. Kriptografi ringan adalah metode enkripsi yang memiliki footprint kecil dan/atau kompleksitas komputasi rendah. Hal ini bertujuan untuk memperluas aplikasi kriptografi ke perangkat terbatas (Okamura Toshihiko, 2017).

4. Fungsi Perangkat dan Cara Kerja.

Perangkat ini ditujukan untuk perusahaan expedisi yang memiliki banyak kendaraan dalam hal ini adalah truk, fungsi alat yang di buat adalah untuk mengukur berapa liter bahan bakar yang diisi oleh pengemudi pada saat melakukan pengisian bahan bakar baik pada saat pengisian di kantor maupun pengisian di lapangan. Hal ini bertujuan untuk meminimalisir penggelapan bahan bakar oleh pengemudi.

Adapun cara kerja alat ini adalah dengan mengurukur jumlah liter air yang melewati corong pengisian bahan bakar, karena alat ini akan di tempatkan pada corong tangki bahan bakar, sehingga otomatis akan menghitung jumlah bahan bakar yang melewati alat tersebut dan disimpan dalam memory alat. Setelah pengemudi kembali ke pangkalan truk dan terhubung dengan wifi kantor, secara otomatis alat tersebut akan mengirimkan data yang ada di memory ke server kantor untuk kemudian server akan menyimpan data tesebut ke dalam database untuk di proses lebih lanjut. Karena dalam penelitian ini penulis telah melakukan pengecekan data yang dikirim oleh alat melalui log server, setelah alat tersebut terhubung dengan wifi dan mengirimkan data ke server. Maka penulis mengetahui bahwa data yang dikirim telah dienkripsi.

5. Analisis Perbandingan

Tabel 3. Tabel Perbandingan Hasil Pengujian

No.	Parameter pengukuran	Tanpa Enkripsi Otentikasi	Dengan Enkripsi Otentikasi
1.	Total waktu proses (dalam milisecond)	4181.467 ms (CI 95% : 4092 –4254)	4188.667 ms(CI 95% : 41.56 – 4211)
2.	Ukuran kode sumber	4.44 KB	6.37 KB
3.	Enkrpsi	Data tidak di enkripsi	Data di enkripsi
4.	Tingkat keamanan (sesuai dengan penjelasan …sitasi…)	Kurang aman karena data tidak di enkripsi sehingga lebih mudah untuk di serang.	Lebih aman karena data tidak mudah di untuk di salah gunakan
5.	Protokol	HTTP POST ke http://xxx.xxx.xxx.217:8080/arduino/post.php	HTTP POST ke http://xxx.xxx.xxx.217:8080/arduino/post.php
6.	Format data transaksi	totalLiter=2.4&idPerangkat=A0001	data=0000005700000031006000010001002800000060000100310000004100010000000000000001003700280001005100410047005100470051004700510047003100410057000100370001006000010037000000000001000100310028000000570001003700000060000100280028000100470031002800000047004700470051005900590059005900590059

Setelah di lakukan pengujian(Uji T) diperoleh hasil perbandingan antara perangkat yang ditambahkan Enkripsi Otentikasi dengan perangkat tanpa enkripsi

otentikasi, dengan perbandingan seperti table diatas, dimana diperolah hasil uji T dengan Confidence Interval 95% dengan hasil sebagai betikut:

Tabel 4. t-Test: Two-Sample Assuming Equal Variances

	Variable 1	*Variable 2*
Mean	4181.466667	4188.666667
Variance	2177.838095	136.952381
Observations	15	15
Pooled Variance	1157.395238	
Hypothesized Mean Difference	0	
df	28	
t Stat	-0.579591867	
P(T<=t) one-tail	0.283412274	
t Critical one-tail	1.701130934	
P(T<=t) two-tail	0.566824547	
t Critical two-tail	2.048407142	

Untuk data detail data pengukuran secara terlampir.

Tabel 5. Data Sample with encryption

No.	Original Data	Time Process
1.	idPrengkat=A0001&totalLiter=0.00	4156 ms
2.	idPrengkat=A0001&totalLiter=0.00	4190 ms
3.	idPrengkat=A0001&totalLiter=0.07	4185 ms
4.	idPrengkat=A0001&totalLiter=0.19	4186 ms
5.	idPrengkat=A0001&totalLiter=1.67	4197 ms
6.	idPrengkat=A0001&totalLiter=1.47	4185 ms
7.	idPrengkat=A0001&totalLiter=1.58	4187 ms
8.	idPrengkat=A0001&totalLiter=1.35	4183 ms
9.	idPrengkat=A0001&totalLiter=2.65	4196 ms
10.	idPrengkat=A0001&totalLiter=1.96	4197 ms
11.	idPrengkat=A0001&totalLiter=0.00	4183 ms
12.	idPrengkat=A0001&totalLiter=1.36	4190 ms
13.	idPrengkat=A0001&totalLiter=2.34	4211 ms
14.	idPrengkat=A0001&totalLiter=1.79	4188 ms
15.	idPrengkat=A0001&totalLiter=1.47	4196 ms

Table 6. Data Sample without encryption

No	Original Data	Time Process
1.	totalLiter=0.01&idPerangkat=A0001	4092 ms
2.	totalLiter=0.36&idPerangkat=A0001	4236 ms
3.	totalLiter=0.19&idPerangkat=A0001	4254 ms
4.	totalLiter=1.07&idPerangkat=A0001	4203 ms
5.	totalLiter=0.00&idPerangkat=A0001	4169 ms
6.	totalLiter=0.51&idPerangkat=A0001	4154 ms
7.	totalLiter=2.57&idPerangkat=A0001	4204 ms
8.	totalLiter=0.48&idPerangkat=A0001	4143 ms
9.	totalLiter=0.78&idPerangkat=A0001	4203 ms
10.	totalLiter=0.28&idPerangkat=A0001	4235 ms
11.	totalLiter=0.44&idPerangkat=A0001	4160 ms
12.	totalLiter=0.28&idPerangkat=A0001	4159 ms
13.	totalLiter=0.62&idPerangkat=A0001	4230 ms
14.	totalLiter=0.63&idPerangkat=A0001	4120 ms
15.	totalLiter=0.70&idPerangkat=A0001	4160 ms

Diskusi Hasil

Dari uji coba yang dilakukan maka diperolah hasil berupa:

1. Skema otentikasi ringan yang aman untuk perangkat IoT dengan memperhatikan keamanan dan efisiensi sumber daya yakni dengan dengan melakukan ekripsi ringan pada device dengan jumlah parameter yang diminimalisasi sehingga tidak membutuhkan sumberdaya yang banyak untuk melakukan enkripsi.
2. Keterbatasan sumber daya pada perangkat IoT yang harus diperhatikan dalam pengembangan skema otentikasi ringan ykni memory karena perangkat IoT umumnya memiliki memory yang minim.
3. Untuk mengatasi masalah keamanan pada jaringan IoT tanpa memberikan beban tambahan pada perangkat IoT yakni dengan melakukan autentikasi ringan dengan resource yang minim baik dengan menggunakan enkripsi sederhana dengan menggunakan kunci publik

SIMPULAN

Dari pengujian diperoleh hasil dengan sedikit usaha lebih untuk menambahkan enkripsi data akan meningkatkan keamanan pengiriman data ke komputer server tanpa harus membebani perangkat baik secara performa maupun secara ukuran kode sumber yang disematkan di perangkat.

Berikut adalah beberapa hal yang dapat di pertimbangkan sebagai saran dalam penelitian selanjutnya:

- Perlu adanya pengujian lebih lanjut dengan memperbanyak variansi test case untuk menguji akibat yang ditimbulkan dari jenis-beberapa jenis serangan yang mungkin bisa dilakukan, seperti serangan man in the middle, data spoofing, and data inject.

- Perlu adanya pengujian lebih lanjut dengan menggunakan metode enkripsi agar diperoleh hasil perbandingan antara setiap metode enkripsi.
- Masih terdapat kemungkinan pengembangan system yang sedang diteliti dengan model multi sensor yang di tempatkan dimasing-masing unit kendaraan

DAFTAR PUSTAKA

Alladi, T. C. (2020). Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*.

Anwar, M. &. (2015). A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. *In MAICS*.

Calatayud, B. M. (IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)). A comparative analysis of Buffer Overflow vulnerabilities in High-End IoT devices. *2022*.

Canedo, J. &. (2016). Using machine learning to secure IoT systems. *IEEE*.

Efendi, Y. (2018). Internet of Things (IOT) sistem pengendalian lampu menggunakan Raspberry PI berbasis mobile. *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar*.

Fan, K. Z. (2019). A lightweight authentication scheme for cloud-based RFID healthcare systems. *IEEE*.

Hassija, V. C. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*.

Hutabarat, D. P. (2018). Development of home security system using ESP8266 and android smartphone as the monitoring tool. *IOP Publishing*.

Jiang, X. L. (2020). An experimental analysis of security vulnerabilities in industrial IoT devices. *ACM Transactions on Internet Technology (TOIT)*.

Keoh, S. L. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of things Journal*.

Khemissa, H. &. (2015). A lightweight authentication scheme for e-health applications in the context of internet of things. *IEEE*.

Kumar, V. M. (2022). Light weight authentication scheme for smart home iot devices. *Cryptography*.

Lee, J. Y. (2014). A lightweight authentication protocol for internet of things. *IEEE*.

Liu, J. R. (2019). A novel secure authentication scheme for heterogeneous internet of things. *IEEE International Conference on Communications (ICC)*.

Minhaj Ahmad Khan, K. S. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*.

Mishra, D. B. (2021). An efficient and secure RSA-based authentication scheme for Internet of Things (IoT) using smart card. *Journal of Ambient Intelligence and Humanized Computing*.

Mishra, D. D. (2015). A secure password-based authentication and key agreement scheme using smart cards. *Journal of Information Security and Applications*.

Nguyen, T. H. (2021). A zero-knowledge proof based blockchain authentication scheme for internet of things. *International Journal of Communication Systems*.

Qin, J. L. (2019). A Lightweight and Secure Authentication Scheme for Internet of Things Devices. *IEEE Access*.

Salah, K. C.-M. (2012). Using cloud computing to implement a security overlay network. *IEEE security & privacy*.

Sasmoko, D. &. (2017). Rancang bangun sistem pendeteksi kebakaran berbasis

iot dan sms gateway menggunakan arduino. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*.

Tayef, S. H. (2021). Design and Implementation of IoT based Smart Home Automation System. *International Conference on Computer and Information Technology (ICCIT) (pp. 1-5). IEEE*.

Tyagi, J. P. (2017). Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly. *IEEE Consumer Electronics Magazine*.

Voas, J. (2016). NIST Special Publication 800-183. Networks of 'Things'. Gaithersburg. *National Institute of Standards and Technology (NIST)*.

Wang, Q. C. (2020). An Improved Lightweight Authentication Protocol for Internet of Things. *IEEE Access*.

Yang, W. L. (2020). A review of the Internet of Things (IoT) for smart home: Challenges and solutions. *International Conference on Robotics and Automation Engineering (ICRAE)*.

Yang, X. Z. (2018). A Lightweight Authentication Scheme for Internet of Things. *IEEE Access*.

YASMINE HARBI, Z. A. (2021). Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE*.

Zhang, L. Z. (2019). A Survey of Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access*.

Zhang, Y. X. (2019). A novel secure and efficient authentication scheme for the internet of things. *Future Generation Computer Systems*.

Zhou, L. L. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future generation computer systems*.