# METODE ONE TIME PASSWORD MODIFIED SEBAGAI SISTEM KEAMANAN MONITORING IOT

**Dewa Gde Eka Krisna Adinatha, Gusti Made Arya Sasmita, I Putu Agus Eka Pratama**
Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana, Bukit Jimbaran, Bali, Indonesia, telp (0361) 701806
e-mail: [1]adinatha24@gmail.com, [2]aryasasmita@unud.ac.id, [3]eka.pratama@unud.ac.id

## Abstrak

Monitoring merupakan suatu aktivitas yang dilakukan untuk mengetahui proses jalannya suatu program atau sistem yang telah dirancang, apakah berjalan dengan baik sesuai dengan yang diharapkan atau tidak, mengetahui hambatan yang terjadi dan bagaimana cara mengatasi hambatan tersebut. Skema kriptografi untuk mengamankan protokol komunikasi merupakan salah satu pertahanan paling efektif terhadap berbagai serangan, termasuk penyadapan dan serangan routing yang sederhana, pada layer komunikasi. Salah satu teknik yang dipelajari dalam kriptografi adalah enkripsi-deskripsi. Penelitian ini bertujuan untuk menerapkan algoritma *one time password* atau OTP modified ke dalam sistem monitoring suhu dan kelembaban berbasis IoT menggunakan perangkat mikrokontroller Raspberry PI dan sensor DHT 11. Proses enkripsi pada sistem keamanan diawali dengan melakukan hashing menggunakan metode SHA pada plaintext, dilanjutkan dengan memproduksi *private key* dan *public key* untuk enkripsi RSA Signature, hasil hashing akan di enkripsi menggunakan algoritma RSA Signature, hasil enkripsi RSA Signature akan di gabungkan dengan *public key* RSA Signature dan *plaintext*, dilanjutkan dengan memproduksi OTP yang akan digunakan sebagai kunci AES. Selanjutnya proses enkripsi AES dijalankan, kunci OTP akan dienkripsi RSA, hasil ciphertext RSA dan ciphertext AES digabungkan dan di encoding dengan metode Base64. Penerapan sistem keamanan ini mendapatkan hasil test durasi rata-rata proses enkripsi data 435,163ms dan proses pengiriman data dengan enkripsi 123,705ms

**Kata Kunci** : Monitoring, Kriptografi, *One Time Password Modified, Rivest Shamir Adleman, Advanced Encryption Standard.*

## *Abstract*

Monitoring is an activity carried out to find out the process of running a program or system that has been designed, whether it runs well as expected or not, find out the obstacles that occur and how to overcome these obstacles. The cryptographic scheme to secure communication protocols is one of the most effective defenses against a variety of attacks, including eavesdropping and simple routing attacks, at the communication layer. One of the techniques studied in cryptography is encryption-description. This study aims to apply a one time password (OTP) modified algorithm into an IoT based temperature and humidity monitoring system using a Raspberry PI microcontroller device and a DHT 11 sensor. . The encryption process begins with hashing using the SHA method on the plaintext, followed by producing a private key and public key for RSA Signature encryption, the hashing results will be encrypted using the RSA Signature algorithm, the RSA Signature encryption results will be combined with the RSA Signature public key and plaintext, followed by producing an OTP that will be used as an AES key. Next the AES encryption process is executed, the OTP key will be encrypted RSA, the results of the RSA ciphertext and the AES ciphertext are combined and encoded with the Base64 method. The implementation of this security system gets the test results of the average duration for data encryption process is 435,163ms, and the data transmission with encryption process is 123,705ms

***Key Word** : Monitorring, Cryptography, One Time Password Modified, Rivest Shamir Adleman, Advanced Encryption Standard*

# 1. PENDAHULUAN

Keamanan data menjadi hal yang sangat penting pada jaman sekarang ini. Hal ini dikarenakan dalam setiap pengambilan keputusan, kebijakan, dan lain-lain harus berdasarkan data, agar keputusan atau kebijakan yang dikeluarkan sesuai dengan kondisi yang diharapkan [1]. Metode pengamanan data sangat diperlukan di berbagai sektor, diantaranya pada sektor militer untuk mengamankan data-data penting militer yang bersifat rahasia, kemudian di sektor perbankan untuk mengamankan data-data personal nasabah, yang ketiga pada sektor informasi publik dimana pengamanan data diperlukan untuk mencegah beredarnya berita-berita palsu (*hoax*) pada publik, dan yang tidak kalah penting adalah pada sektor penggunaan teknologi *internet of things* (IoT).

Konsep IoT diartikan sebagai sebuah kemampuan untuk menghubungkan objek-objek cerdas dan memungkinkannya untuk berinteraksi dengan objek lain, dengan lingkungan, maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet [2]. Dari sisi pengguna perorangan, IoT sangat terasa pengaruhnya dalam bidang domestik seperti pada aplikasi rumah dan mobil cerdas. Dari sisi pengguna bisnis, IoT sangat berpengaruh dalam meningkatkan jumlah produksi, efisiensi, kualitas produksi, pemantauan distribusi barang, mencegah pemalsuan, mempercepat waktu ketersediaan barang pada pasar retail, manajemen rantai pasok, hingga sistem *monitoring* gudang atau ruangan [3].

*Monitoring* merupakan suatu aktivitas yang dilakukan untuk mengetahui proses jalannya suatu program atau sistem yang telah dirancang, apakah berjalan dengan baik sesuai dengan yang diharapkan atau tidak, mengetahui hambatan yang terjadi dan bagaimana cara mengatasi hambatan tersebut. Selain itu, *monitoring* juga bertujuan untuk memastikan apakah suatu proses yang dilakukan telah sesuai dengan prosedur yang berlaku [4]. Sebuah sistem *monitoring* akan mempermudah suatu pekerjaan jika dirancang dan dilakukan secara efektif, terlebih jika diterapkan sistem IoT di dalamnya.

Salah satu tantangan yang harus diatasi untuk mendorong implementasi IoT secara luas adalah faktor keamanan. IoT merupakan sebuah sistem kompleks yang melibatkan banyak komponen. Kompleksitasnya bukan hanya berkaitan dengan berbagai entitas seperti data, perangkat, jalur komunikasi, sensor, dan lain-lain, tetapi juga melibatkan berbagai peralatan dengan beragam kemampuan komunikasi dan pengolahan data. Penggunaan skema kriptografi untuk mengamankan protokol komunikasi merupakan salah satu pertahanan paling efektif terhadap berbagai serangan, termasuk penyadapan dan serangan routing yang sederhana, pada layer komunikasi. Salah satu teknik yang dipelajari dalam kriptografi adalah enkripsi-deskripsi. Enkripsi merupakan proses mengacak atau mengubah pesar awal menjadi bentuk dan susunan lain, atau dalam bentuk *chipertext* sedemikian rupa sehingga tidak dapat dikenali oleh pihak lain. Sedangkan deskripsi adalah proses mengubah *chipertext* tersebut menjadi pesan asli yang dapat dibaca kembali [5].

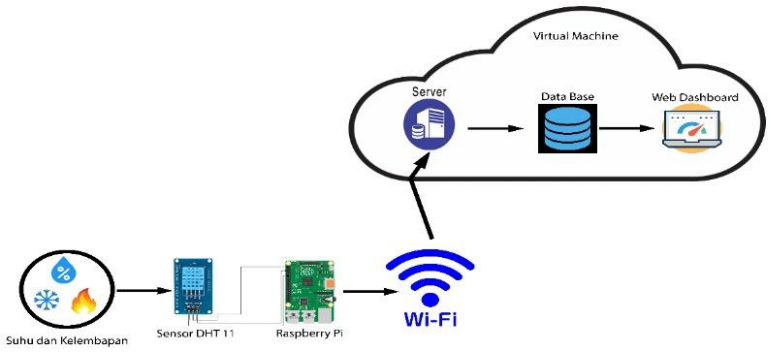
Algoritma *one time password* (OTP) merupakan algoritma kriptografi yang kuat dan aman apabila memenuhi kriteria pengoperasian dalam mengecek kunci secara random dan tidak menggunakan kunci untuk operasi lain. OTP melakukan proses dengan enkripsi dan dekripsi yang menjadi kelebihannya dalam menyamarkan pesan yang termuat pada media tertentu. Karena kecepatan yang cukup tinggi ini. Memungkinkan untuk dapat digunakan pada sistem real-time, salah satu contohnya adalah pada penerapan IoT [6]. Berdasarkan latar belakang di atas, maka tugas akhir ini bertujuan untuk menerapkan algoritma *one time password* atau OTP *modified* ke dalam sistem *monitoring* suhu berbasis IoT menggunakan perangkat komputer mini yaitu *Raspberry PI*. Algoritma OTP digunakan untuk autentikasi penerima informasi dengan algoritma RSA yang menggunakan bahasa pemrograman *python*.

# 2. METODOLOGI

Pada bagian ini akan dijelaskan mengenai metode, tahapan-tahapan, maupun model penelitian yang digunakan untuk memperoleh data.

## 2.1 Gambaran Umum Sistem

Perancangan desain proses merupakan penjabaran dari tahapan-tahapan yang dilakukan dalam pembuatan penerapan keamanan sistem monitoring berbasis IOT dapat dilihat pada Gambar 1.

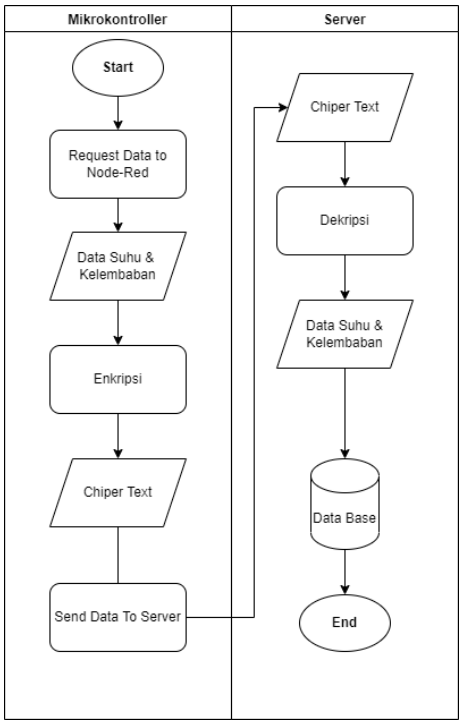



Gambar 1. Gambaran Umum Sistem

Gambar 1 merupakan gambaran umum sistem yang diawali dengan data suhu dan kelembaban pada suatu ruangan akan diambil oleh sensor DHT11 dan di kirim menuju mikrokontroler yakni *Raspberry PI*. Kemudian, pada *Raspberry PI* data suhu dan kelembaban akan di enkripsi menggunakan bahasa pemrograman *Phyton*, setelah itu data enkripsi akan dikirim menuju *cloud* menggunakan wifi dengan menggunakan *protocol hypertext trasfer-transfer protocol* (HTTP). Setelah itu, hasil enkripsi yang sudah diterima di *server* akan dideskripsi menggunakan bahasa pemrograman *Python*. Selanjutnya, hasil deskripsi akan dilanjutkan ke *database* dan web *dashboard* akan mengambil data tersebut dari *database* untuk di perlihatkan sebagai informasi.

## 2.2 Perancangan Sistem

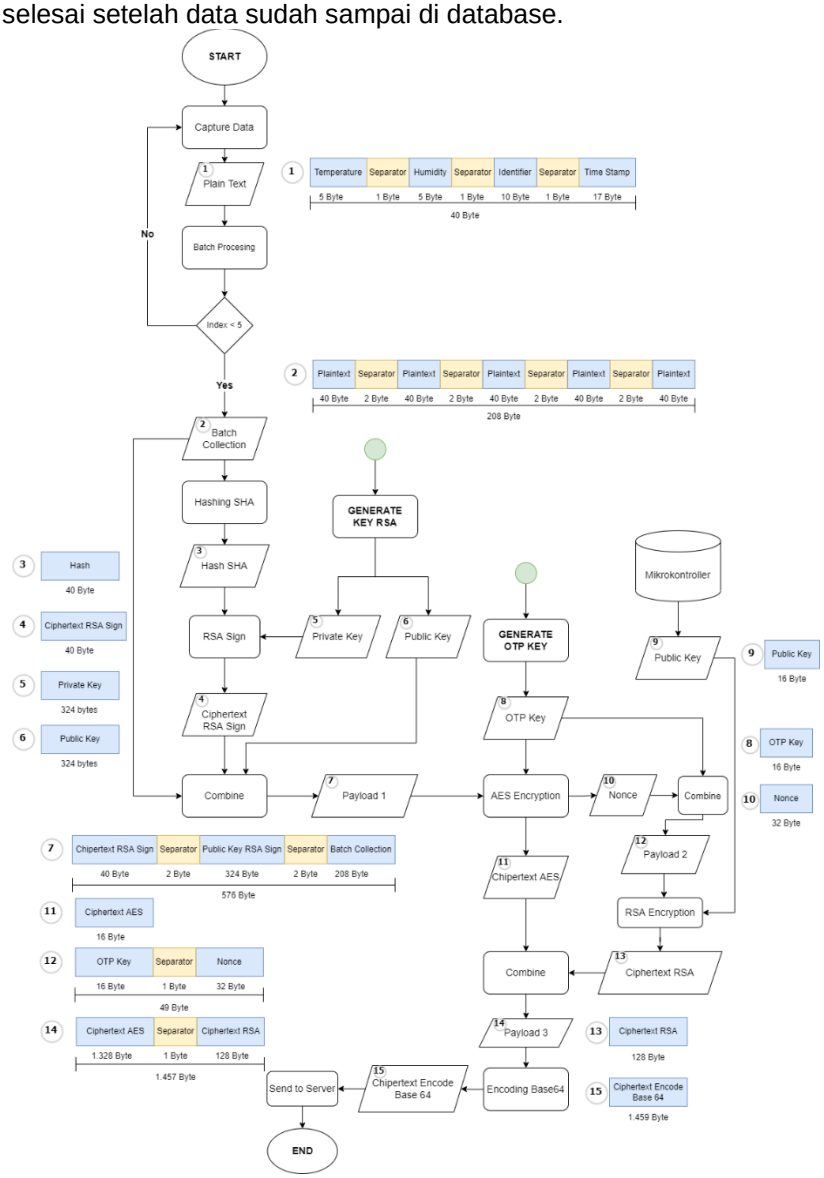
Desain sistem dibuat dengan menggunakan bahasa pemrograman *python*, pengiriman data menggunakan jaringan lokal, *portainer* juga digunakan sebagai *docker* untuk membuat, menguji dan menerapkan aplikasi, serta dalam perancangan *dashboard*. Untuk desain proses fungsional merupakan penjabaran dari proses merancang sistem yang digambarkan dengan diagram alur (*flowchart*) berikut.




Gambar 2. *Flowchart* Sistem Keamanan IoT

Gambar 2 merupakan flowchart sistem keamanan IoT yang akan dibuat, pada flowchart di jelaskan ada dua proses yang terjadi pada mikrokontroller dan pada server proses pertama yang dijalankan pada mikrokontroller adalah proses request data ke node-red, ini dilakukan karena terjadinya eror saat menghubungkan sensor yang sudah di pasang pada port GPIO ke python, setelah mendapatkan data suhu dan kelembaban proses dilanjutkan dengan meng-enkripsi data suhu dan kelembaban menggunakan metode yang sudah ditetapkan.

Setelah data berhasil di enkripsi maka akan mendapatkan hasil ciphertext (data yang telah di enkripsi) dan setelah itu ciphertext ini akan dikirimkan ke serever. Pada server data yang diterima akan berupa ciphertext, ciphertext ini akan dideskripsikan menggunakan metode yang sudah ditetapkan, proses deskripsi ini akan mengeluarka output berupa palin text yang memuat data suhu dan kelembaban, setelah itu data suhu dan kelembaban ini akan dikirim ke database, proses akan selesai setelah data sudah sampai di database.



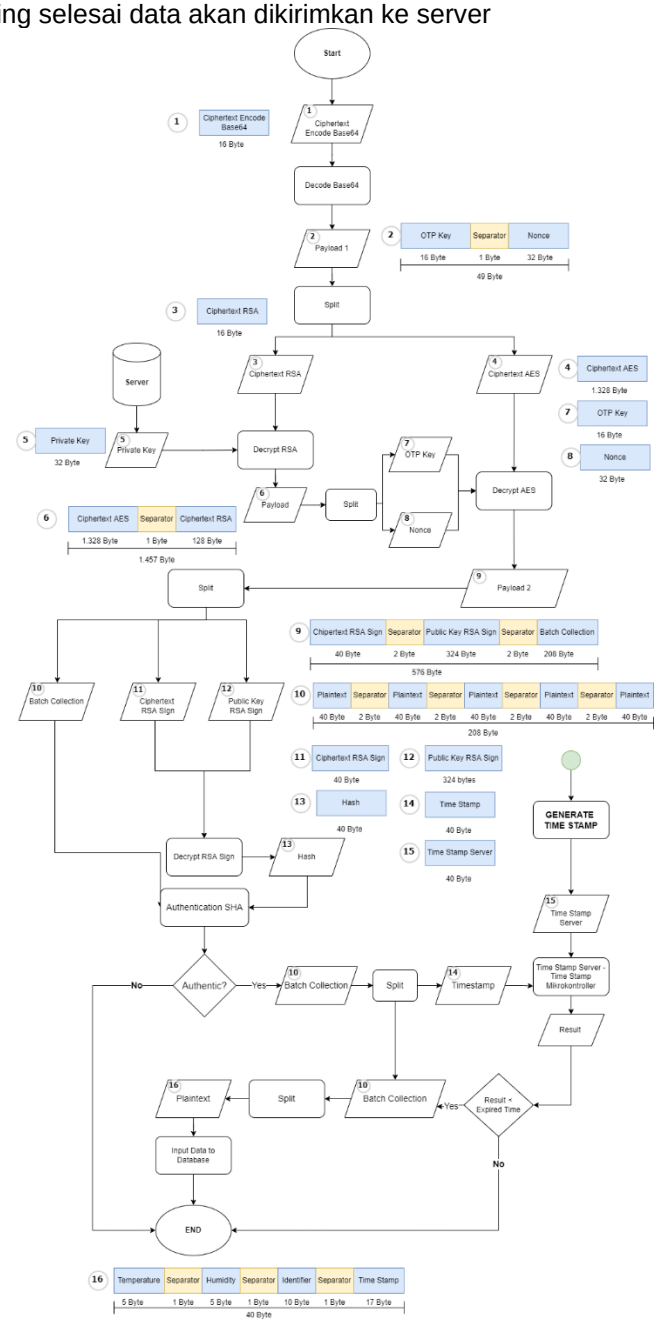

**Gambar 3** *Flowchart* Sistem Keamanan

Gambar 3 merupakan flowchart sistem keamanan yang diterapkan pada tugas akhir ini, diawali dengan proses menangkap plaintext yang berupa data sensor suhu, kelembaban, 10 bilangan awal mac address sebagai identifier, dan time stamp. Setelah itu plain text akan dikumpulkan terlebih dahulu dengan metode append dan akan di proses menjadi data arrat, sebelum data berjumlah 5 maka proses capture akan di ulang terus-menerus. Dilanjutkan hashing dengan algoritma SHA, hasil dari hashing SHA dibuatkan RSA Sign yang bertujuan mendapatkan tanda tangan digital dengan algoritma RSA sign yang mempunyai private key dan public key,

proses ini akan mengenkripsi hasil hashing SHA dengan private key yang dihasilkan algoritma RSA.

Selanjutnya plaintext, public key dari algoritma RSA Sign dan hasil tanda tangan dari pemrosesan RSA Sign sebelumnya disatukan menjadi satu payload yang dinamakan ciphertext RSA sign. Proses dilanjutkan dengan membuat one time password atau OTP key yang memuat bilangan acak berformat string. OTP key akan digunakan sebagai kunci pada proses enkripsi AES. Selanjutnya ciphertext RSA sign diproses enkripsi menggunakan algoritma AES dengan OTP key yang sudah disiapkan sebelumnya. Hasil dari enkirpsi AES ini dinamakan ciphertext AES.

OTP key yang dibuat untuk enkripsi AES dan nonce yang merupakan atribut tambahan dari enkripsi AES, akan dikombinasikan serta diamankan dengan metode enkripsi RSA.hasil enkripsi ini dinamakan ciphertext RSA. Ciphertext AES dan ciphertext RSA akan dikombinasikan dan diencoding dengan metode Base64 ini bertujuan agar hasil enkripsi tidak mengandung simbol-simbol terlarang yang akan menjadi hambatan pada saat pengiriman data ke server. setelah hasil encoding selesai data akan dikirimkan ke server




**Gambar 4** *Flowchart* Sistem Keamanan

Gambar 4 merupakan flowchart tahap autentifikasi data dari mikrokontroller ke server yang diawali dengan menerima kumpulan data ciphertext dari mikrokontoller dan dilanjutkan decoding menggunkan metode Base64. Selanjutnya hasil decode di pisahkan yang akan menghasilkan dua ciphertext yaitu ciphertext RSA dan ciphertext AES. Ciphertext RSA akan diproses terlebih dahulu karena ciphertext ini mengandung OTP key yang berfungsi untuk mendeskripsi ciphertext AES. Setelah ciphertext RSA dideskripsi dengan private key yang sudah di-set pada server, hasil deskripsi yang berupa OTP key akan digunakan untuk mendeskripsikan ciphertext AES. Hasil ciphertext AES akan dipisahkan dan mendapatkan data batch collection, ciphertext RSA sign, dan public key RSA sign.

Proses dilanjutkan dengan mendeskripsikan ciphertext RSA sign dengan public key RSA sign, hasil dari deskripsi ini berupa hash SHA yang akan di authentikasi dengan plaintext. Pada proses ini batch collection akan di hashing dan dicocokan dengan nilai hash yang didapatkan dari proses sebelumnya. Jika hasilnya sama maka batch collection akan diteruskan pada proses selanjutnya. Batch collection pada tahap ini memiliki lima plaintext yang setiap datanya terdiri dari data suhu, kelembaban, mac address, dan time stamp. Time stamp pada plaintext akan dipisahkan dan divalidasi masa berlakunya dengan membangkitkan time stamp baru pada server, time stamp mikrokontroller akan dikurangi dengan time stamp yang baru dibangkitkan pada server jika hasil lebih besar dari expired time maka proses akan slesai dan eror, namun jika hasil lebih kecil dari expired time maka proses dilanjutkan dengan memisahkan setiap data plaintext yang berisi pada bacth collection. Setelah data dipisahkan, plaintext yang berisi data suhu, kelembaban, mac address, dan times stamp, yang akan di input ke data base secara berurut.

## 3. KAJIAN PUSTAKA

### 3.1 Internet of Things (IoT)

*Internet of Things* (IoT) adalah sebuah perkembangan teknologi di bidang internet yang memudahkan pengguna untuk mengelola, mengendalikan, dan mengoptimalkan suatu perangkat secara nirkabel menggunakan internet tanpa perantara manusia [7]. IoT biasanya menggunakan beberapa teknologi yang digabungkan menjadi satu kesatuan, diantaranya sensor sebagai pembaca data, koneksi internet dengan beberapa macam topologi jaringan, *radio frequency identification* (RFID), *wireless sensor network* dan masih banyak lagi seiring dengan perkembangan teknologi kedepan.

### 3.2 Confidentiality, Integrity, Availability (CIA)

Keamanan informasi memiliki beberapa aspek yang menjadi perhatian utama yang wajib dipahami dalam penerapannya. Beberapa aspek tersebut sering dipahami sebagai C.I.A triangle model yang terdiri dari confidentiality atau kerahasiaan, integrity atau keaslian data, dan availability atau ketersediaan data.

#### 3.2.1 *Confidentiality*

*Confidentiality* atau kerahasiaan adalah aspek yang biasa dipahami tentang aspek keamanan, aspek *confidentiality* menyatakan bahwa data hanya dapat diakses atau dilihat oleh orang yang berhak. hanya dapat diakses atau dilihat oleh orang yang berhak [8].

#### 3.2.2 Integrity

Aspek *integrity* mengatakan bahwa data tidak boleh berubah tanpa ijin dari yang berhak.

#### 3.3.3 Availability

Ketergantungan kepada sistem yang berbasis teknologi informasi menyebabkan sistem (beserta datanya) harus dapat diakses ketika dibutuhkan. Jika sistem tidak tersedia, *not available*, maka dapat terjadi masalah yang menimbulkan kerugian finansial atau bahkan nyawa. Itulah sebabnya aspek *availability* menjadi bagian dari keamanan.

### 3.3 Kriptografi

Kriptografi adalah suatu ilmu teknik enkripsi dimana pesan asli (plaintext) diacak menggunakan suatu kunci enkripsi menjadi pesan tersandi (ciphertext), yang dimana pesan

tersebut sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Untuk mendapatkan pesan asli kembali maka diperlukan sebuah metode khusus yang disebut dengan metode dekripsi [9].

3.4 Enkripsi dan Deskripsi

Enkripsi adalah sebuah proses penyandian yang mengubah pesan asli (plaintext) menjadi pesan tersandi (ciphertext). Sedangkan dekripsi adalah sebuah proses mengubah pesan tersandi (ciphertext) menjadi pesan asli (plaintext) kembali [10]. Enkripsi dan dekripsi merupakan suatu pesan yang memetakan elemen-elemen antara kedua himpunan tersebut. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim ataupun pesan yang disimpan.

3.5 Algoritma Kriptografi

Algoritma merupakan urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara matematis dan benar.

3.5.1 Algoritma Simetri

Algoritma simetri adalah algoritma yang memakai kunci yang sama untuk kegiatan enkripsi dan deskripsi [11].

3.5.1.1 Advanced Encryption Standar (AES)

Algoritma Rijndael merupakan salah satu algoritma kunci simetri yang tergolong sebagai AES. Algoritma ini mendukung kriptografi dengan panjang kunci 128 bit sampai dengan 256 bit dengan step 32 bit.

3.5.1.2 Algoritma Hash SHA

SHA adalah serangkaian fungsi cryptographic hash yang dirancang oleh National Security Agency (NSA) dan diterbitkan oleh NIST sebagai US Federal Information Processing Standard.

3.5.2 Algoritma Asimetri

Algoritma asimetri adalah algoritma yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi digunakan untuk proses deskripsi, yang dimana algoritma asimetris ini dibagi menjadi dua jenis, yaitu public dan private.

3.5.2.1 Algoritma *One Time Password (OTP)*

One Time Password (OTP) adalah password yang berlaku hanya untuk satu sesi login atau transaksi.

3.5.2.2 Algoritma *Rivest Shamir Adleman (RSA)*

Algoritma ini merupakan salah satu metode kriptografi yang menggunakan private key dan public key untuk proses enkripsi dan dekripsi atau dalam istilahnya sering disebut teknik asimetris, algoritma ini menggunakan private key untuk melakukan enkripsi dan untuk dekripsinya menggunakan public key.

3.6 Mikrokontroller

Mikrokontroler adalah sebuah komputer mikro dalam satu chip tunggal.

## 4 HASIL DAN PEMBAHASAN

Dalam bagian ini akan dijelaskan mengenai implementasi sistem keamanan IoT yang telah dirancang bangun, sistem *dashboard* yang telah berhasil didesain, hasil percobaan keseluruhan prototipe, hasil pengambilan data dari sensor dengan rentang waktu 24 jam, dan analisis hasil dari masing-masing percobaan tersebut.

### 4.1 Menjalankan Program Pada Sistem Keamanan IoT

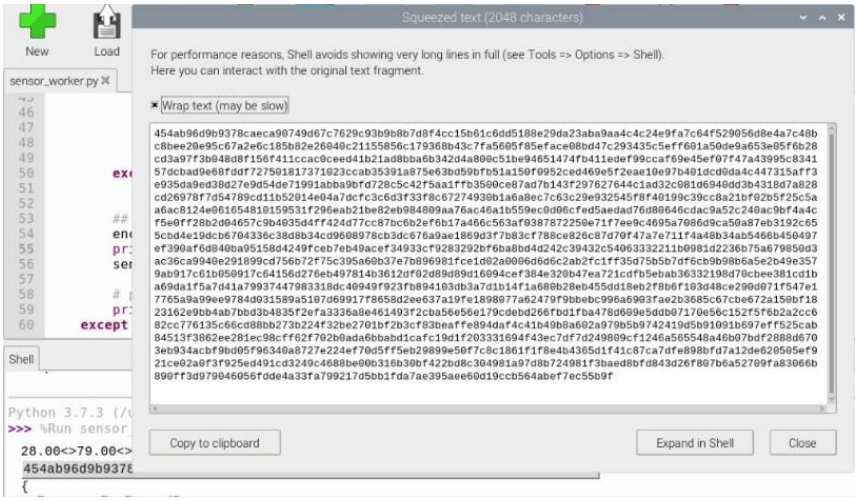
Program akan dijalankan pada mikrokontroller dengan IDE Thonny yang berada pada lingkungan pengembangan bahasa pemrograman python. Pada server yang berada pada laptop, menggunakan IDE Visual Studio Code untuk menjalankan program server. Web view dashboard pada sistem ini menggunakan Grafana yang dapat menampilkan visualisasi data dengan tampilan grafik, untuk menjalankan gafana diperlukan docker engine sebagai aplikasi yang dapat meng-hosting paket data yang berupa container.


**Gambar 4** *Dashboard* Grafana

Gambar 4 merupakan tampilan dari dashboard Grafana yang sudah dijalankan dengan menampilkan grafik data suhu, rata-rata suhu, maximum suhu, dan minimum suhu dalam waktu tertentu. Dashboard juga menampilkan grafik data kelembaban, rata-rata kelembaban, maximum kelembaban, dan minimum kelembaban dalam waktu tertentu.

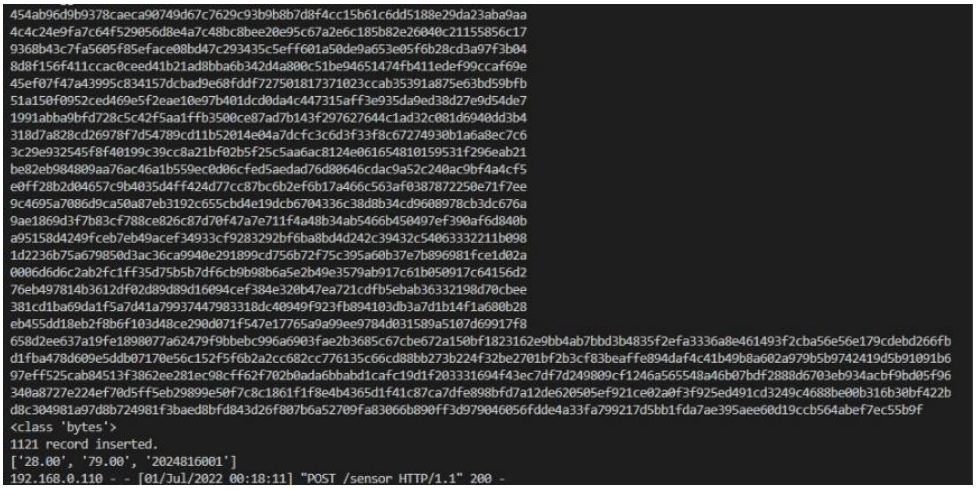
### 4.2 Data Hasil Enkripsi dan Deskripsi

Hasil tangkapan data suhu dan kelembaban akan di enkripsi pada mikrokontroller dengan tujuan mendapatkan paket data yang aman, hasil enkripsi akan berupa bilangan acak yang akan dikirimkan ke server, setelah diterima maka data tersebut akan di deskripsi dan dimasukkan ke database. berikut merupakan hasil tangkapan ciphertext yang akan dikirim pada mikrokontroller, ciphertext yang diterima oleh server, dan ciphertext yang berjalan pada layer komunikasi yang diambil dari tangkapan program wireshark.



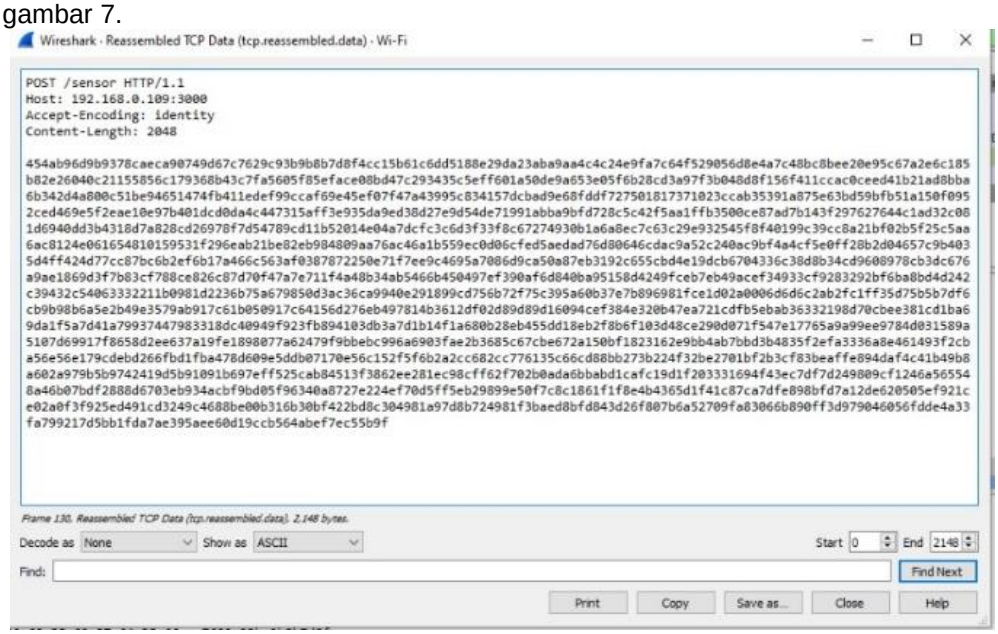

Gambar 5 Ciphertext yang dikirim pada Mikrokontroller

merupakan data hasil enkripsi pada mikrokontroller yang dikirim ke server. Tangkapan data suhu dan kelembaban pada sensor DHT 11 yang dipasang pada mikrokontroller pada sesi ini mendapatkan hasil data suhu 28.00°C dan kelembaban 79%. Selanjutnya server akan menerima paket yang sama dengan apa yang dikirim oleh mikrokontroller dapat dilihat pada gambar 6.




Gambar 6. Ciphertext yang Diterima oleh Server

Gambar 6 merupakan hasil enkripsi yang dikirim dari mikrokontroller dan diterima oleh server. Jika dilihat bilangan awal dan bilangan akhir pada data yang dikirim dan yang diterima, maka mendapatkan hasil yang sama dengan 10 bilangan awal yaitu 454ab96d9b dan 10 bilangan akhir yaitu ef7ec55b9f. Hasil proses deskripsi pada sesi ini menunjukan data suhu 28.00°C dan kelembaban 79%, jika dibandingkan dengan data yang ditangkap pada mikrokontroller. Data yang dienkripsi dan dideskripsi memiliki nilai yang sama. Selain itu jika dilihat berdasarkan tangkapan aplikasi wireshark data yang berjalan di antara mikrokontroller dan server dapat dilihat pada gambar 7.




Gambar 7 Hasil Tangkapan Ciphertext pada Program Wireshark

Gambar 7 merupakan hasil tangkapan data antara mikrokontroller dan server, dapat dilihat data enkripsi yang dikirim memiliki 10 bilangan awal yaitu 454ab96d9b dan 10 bilangan akhir yaitu ef7ec55b9f. Hasil tangkapan data pada aplikasi wireshark sama dengan hasil enkripsi yang dikirim dari mikrokontroller dan paket data yang diterima oleh server.

## 4.3 Hasil Uji Coba Dalam Waktu 24 Jam

Program akan dijalankan satu hari non-stop dari tanggal 25 Juni 2022 sampai dengan 26 Juni 2022 dengan interval waktu pengambilan data berjarak 30 menit, ini bertujuan untuk memantau kinerja keseluruhan sistem. Hasil data yang telah di masukkan pada database dapat dilihat pada Tabel 1.

Tabel 1 Hasil Uji sistem 24 Jam

| No. | Suhu (°C) | Kelembaban (%) | Date and Time |
|---|---|---|---|
| 1 | 28 | 73 | 2022-06-25 09:20:04 |
| 2 | 28 | 72 | 2022-06-25 10:20:30 |
| 3 | 29 | 71 | 2022-06-25 11:20:59 |
| 4 | 30 | 69 | 2022-06-25 12:21:26 |
| 5 | 31 | 65 | 2022-06-25 13:21:49 |
| 6 | 30 | 68 | 2022-06-25 14:22:13 |
| 7 | 30 | 67 | 2022-06-25 15:22:43 |
| 8 | 30 | 65 | 2022-06-25 16:23:25 |
| 9 | 29 | 68 | 2022-06-25 17:24:06 |
| 10 | 28 | 67 | 2022-06-25 18:24:46 |
| 11 | 28 | 64 | 2022-06-25 19:25:18 |
| 12 | 27 | 63 | 2022-06-25 20:25:42 |
| 13 | 27 | 64 | 2022-06-25 21:26:10 |
| 14 | 26 | 64 | 2022-06-25 22:26:39 |
| 15 | 26 | 65 | 2022-06-25 23:27:02 |
| 16 | 26 | 63 | 2022-06-26 00:27:29 |
| 17 | 25 | 64 | 2022-06-26 01:34:35 |
| 18 | 25 | 64 | 2022-06-26 02:34:58 |
| 19 | 25 | 64 | 2022-06-26 03:35:23 |
| 20 | 25 | 63 | 2022-06-26 04:35:45 |
| 21 | 25 | 64 | 2022-06-26 05:36:08 |
| 22 | 24 | 65 | 2022-06-26 06:36:33 |
| 23 | 24 | 63 | 2022-06-26 07:36:53 |
| 24 | 26 | 82 | 2022-06-26 08:37:20 |
| 25 | 25 | 75 | 2022-06-26 09:37:46 |

Tabel 1merupakan hasil input data dari mikrokontroller yang dikirim ke server dan sudah mengalami proses enkripsi, deskripsi, dan input ke database. Proses uji berlangsung dari tanggal 25-06-2022 jam 09:20:04 sampai dengan tanggal 26-06-2022 jam 10:38:10.

4.4 Perhitungan Durasi Proses Enkripsi dan Pengiriman Data

Tahap pengujian juga dilakukan dengan menambahkan kode program yang dapat menangkap waktu durasi proses enkripsi dan pengiriman data dalam mili second.

Tabel 2 Durasi Proses Enkripsi dan Pengiriman Data

| No. | Durasi Proses Enkripsi | Durasi Pengiriman Data |
|---|---|---|
| 1 | 447,464ms | 108,279ms |
| 2 | 572,844ms | 93,852ms |
| 3 | 238,139ms | 121,156ms |
| 4 | 720,686ms | 99,315ms |
| 5 | 725,966ms | 115,720ms |

| | | |
|---|---|---|
| 6 | 619,243ms | 90,575ms |
| 7 | 294,343ms | 127,393ms |
| 8 | 310,990ms | 242,602ms |
| 9 | 263,024ms | 92,338ms |
| 10 | 158,927ms | 145,822ms |
| **Average :** | **435,163ms** | **123,705ms** |

Tabel 2 merupakan hasil tangkapan durasi proses enkripsi dan durasi proses pengiriman data, dari 10 sample data yang di ambil rata-rata waktu proses enkripsi adalah 435,163 mili second dan durasi proses pengiriman data rata-rata adalah 123,705 mili second.

## 5. KESIMPULAN

Berdasarkan percobaan dan penelitian yang telah dilakukan pada penelitian ini, didapatkan beberapa kesimpulan sebagai berikut:

a. Sistem *internet of things* atau IoT yang dirancang bangun pada penelitian tugas akhir ini memiliki tiga bagian utama, yaitu bagian sensor, bagian mikrokontroler, dan bagian server. Bagian sensor terdiri dari satu jenis sensor yaitu sensor suhu dan kelembaban DHT11. Sensor ini terhubung secara langsung ke mikrokontroler dengan komunikasi dua arah. Mikrokontroler yang digunakan pada tugas akhir ini adalah mikrokontroler yang telah tersedia di dalam Raspberry PI 3 Model B+. Setelah data pembacaan sensor diterima oleh mikrokontroler, maka data tersebut diolah dan disesuaikan kembali agar nilai output dari mikrokontroler telah terkonversi menjadi besaran suhu dan kelembaban. Kemudian, data pembacaan suhu dan kelembaban ini kumpulkan dengan proses batching dan dienkripsi sebelum dikirim ke server menggunakan metode: hashing, algoritma enkripsi RSA Signature, algoritma enkripsi AES dengan OTP key, algoritma enkripsi RSA dengan key yang sudah di set pada mikrokontroller dan server, serta encoding base64. Setelah data sampai di server, data yang terenkripsi tersebut dideskripsi dan dipisahkan per-sesi sehingga data pembacaan suhu dan kelembaban dapat di input pada data base serta muncul pada dahsboard web yang dirancang.

b. Penerapan kerahasian data (Confidentiality) pada sistem keamanan ini diterapkan pada proses enkripsi AES yang menerapkan OTP key sebagai kunci enkripsi dan deskripsi, OTP key akan di enkripsi menggunakan algoritma RSA agar pada saat pengiriman tidak berupa plaintext. Keaslian data (Integrity) pada sistem keamanan ini diterapkan pada proses hash dengan metode SHA yang menlakukan enkripsi satu arah dan dapat divalidasi nantinya pada proses deskripsi, serta penerapan enkripsi RSA Signature yang akan mengamankan data hash dengan menlakukan enkripsi yang nantinya hanya dapat dibuka dengan public key yang sudah ada pada paket pengiriman. Ketersediaan data (Availability) pada sistem keamanan ini diterapkan pada proses batching yang akan mengumpulkan plaintext terlebih dahulu, plaintext akan di enkripsi jika jumlahnya sudah mencapai lima data, ini akan menghemat penggunaan CPU, memory, serta dapat menampilkan data secara real-time

c. Dalam uji coba sistem, durasi waktu proses enkripsi rata-rata dengan 10 sample data mendapatkan hasil 435,163 mili second dan durasi waktu pengiriman data dengan proses enkripsi rata-rata dengan 10 sample data mendapatkan hasil 123,705 mili second. Validasi data dilakukan dengan membandingan data sebelum di enkripsi, data yang dikrim dari mikrokontroller raspberry pi, data yang diterima oleh server, data yang dideskripsi pada server, dan data yang dimasukkan pada database. Pengujian pertama dilakukan selama 24 jam dengan interval waktu 1 jam yang menghasil 25 data yang dikirim dari mikrokontroller raspberry pi, semua data berhasil dengan baik di enkripsi, dikirim, dideskripsi, dan dimasukkan ke database, Pengujian kedua dilakukan tanpa interval waktu, dengan 20 data sebagai sample yang mendapatkan hasil seluruh data berhasil diproses dengan baik.

## DAFTAR PUSTAKA

[1] D. A. Pratiwi, “Peningkatan keamanan data dengan metode cropping selection pseudorandom,” *J. TICom*, vol. 4, no. 3, pp. 132–138, 2016.
[2] M. A. Iqbal, O. G.Olaleye, and M. A. Bayoumi, “A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches,” Univ. Louisiana Lafayette, vol. 16, no. 7, pp. 331–333, 2016, doi: 10.1111/j.1399-6576.1984.tb02071.x.
[3] W. Najib, S. Sulistyo, and Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology),” J. Nas. Tek. Elektro dan Teknol. Inf. |, vol. 9, no. 4, pp. 375–384, 2020.
[4] A. Sumarudin, W. P. Putra, E. Ismantohadi, S. Supardi, and M. Qomarrudin, “Sistem Monitoring Tanaman Hortikultura Pertanian Di Kabupaten Indramayu Berbasis Internet of Things,” J. Teknol. dan Inf., vol. 9, no. 1, pp. 45–54, 2019, doi: 10.34010/jati.v9i1.1447.
[5] N. Indahwati and A. Prihanto, “Penerapan Algoritma Kriptografi Asimetris Elgamal dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Dekripsi Gambar Warna,” J. Informatics Comput. Sci., vol. 1, no. 02, pp. 97– 103, 2020, doi: 10.26740/jinacs.v1n02.p97-103.
[6] R. Pasmah, A. J. Lubis, and A. Usman, “Prototipe Sistem Keamanan Ruangan Menggunakan Finger Print dan Keypad Matrix dengan One Time Pad,” Explorer (Hayward)., vol. 1, no. 2, pp. 53–62, 2021, doi: 10.47065/explorer.v1i2.89.
[7] Wilianto and A. Kurniawan, “Sejarah , Cara Kerja Dan Manfaat Internet of Things,” Matrix, vol. 8, no. 2, pp. 36–41, 2018.
[8] B. Rahardjo, “Keamanan Informasi & Jaringan,” p. 47, 2017, [Online]. Available: http://budi.rahardjo.id/files/keamanan.pdf.
[9] E. S. Han and A. goleman, daniel; boyatzis, Richard; Mckee, “Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah,” J. Chem. Inf. Model., vol. 53, no. 9, p. 2, 2019.
[10] Arafat, “Sistem Pengamanan Pintu Rumah Berbasis Internet of Things (IoT) dengan ESP8266,” J. Ilm., vol. 7, no. 4, pp. 262–268, 2016.
[11] N. Azis, “Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Cipher dan Operasi XOR,” Ikraith-Informatika, vol. 2, no. 1, pp. 72– 80, 2018.