JESSI
Journal of Embedded System Security and Intelligent System

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

Data *Confidentiality* Pada Kontrol Smart PDAM Menggunakan AES *Algorithm*

Satria Gunawan Zain[1], Abdul Wahid[2], Iin Rahmawati[3]
[1*]Sg.zain@gmail.com, [2]wahid@unm.ac.id, [3]iinrahmawati78@gmail.com
[123]Universitas Negeri Makassar

Received : 10 Apr 2023
Accepted : 12 May 2023
Published : 19 May 2023

Abstract

This study aims to apply cryptographic techniques to the control of smart PDAM data communication and to find out the comparison of security before and after using cryptographic techniques on smart PDAM data communication. The research method used is the R&D (Research and Development) method. The AES algorithm is applied to code request data to produce chippertext which is then transmitted to a digital water meter. Digital water meters also apply the same AES algorithm with the same private key so they can translate encrypted commands. The spinner consists only of the telemetry device lora is only able to get chippertext commands and does not know the code request data. Cryptographic techniques applied at the hardware level can guarantee code requests from monitoring stations cannot be detected by third parties or snippers. And by applying cryptographic techniques with the AES algorithm on smart PDAM data communication controls it is safer than not implementing these techniques.

Keywords: AES Data, Security, Communication, Cryptography

Abstrak

Penelitian ini bertujuan untuk menerapkan teknik kriptografi pada kontrol komunikasi data smart PDAM dan mengetahui perbandingan keamanan sebelum dan sesudah menggunakan teknik kriptografi pada komunikasi data smart PDAM. Adapun metode penelitian yang digunakan adalah metode R&D (Research and Development). Algoritme AES diterapkan pada code request data menghasilkan chippertext kemudian ditransimisikan pada meteran air digitial. Meteran air digital juga menerapkan algoritme AES yang sama dengan kunci private yang sama sehingga dapat menerjemahkan perintah yang telah terenscripsi. Snippeer hanya terdiri dari perangkat telemetry lora hanya mampu mendapatkan perintah chippertex dan tidak mengetahui code request data. Teknik kriptografi yang diterapkan pada level hardware dapat menjamin code request dari stasiun monitoring tidak dapat diketahui oleh pihak ketiga atau snipper. Dan dengan menerapkan teknik kriptografi dengan algoritma AES pada kontrol komunikasi data smart PDAM lebih aman dibandingkan tidak menerapkan teknik tersebut.

Kata Kunci: AES Data, Keamanan, Komunikasi, Kriptografi

This is an open access article under the CC BY-SA license

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

1. Pendahuluan

Perkembangan teknologi berkembang di masyarakat sangat pesat. Masayarakat dimanjakan dengan perkembangan teknologi saat ini[11]. Perkembangan teknologi dapat kita rasakan secara langsung dengan adanya perangkat-perangkat cerdas yang diciptakan untuk memantu ataupun mengerjakan pekerjaan sehari-hari. Seperti teknologi smart home, smart parking, tandan tangan digital, smart PDAM atau meteran digital dan perangkat-perangkat cerdas lainnya yang dapat membantu serta mengerjakan tugas manusia sebelumnya. Smart PDAM merupakan salah satu teknologi yang mulau dikembangkan untuk memberikan kemudahan dalam pengelolaan air bersih. Teknoligi ini dengan mengubah cara kerja meteran air konvensional menjadi digital mulai dari pemakaian air yang dapat di kontrol dan di pantau oleh pengguna, pelayanan serta pembayaran dapat dilakukan secara digital melalui smart phone. Dari berbagai inovasi yang telah banyak diciptakan tentunya tujuannya untuk menjadi sebuah produk yang bernilai dan dapat merasuki jajaran pasar berbasis teknologi di era industry 4.0. Namun untuk dapat menjadi sebuah produk berbasis teknologi tentunya harus memenuhi aspek-aspek bedasarkan International Standart Oraginzation (ISO).

Meteran digital ini dilengkapi dengan sensor-sensor seperti sensor tekanan air, sensor water flow, dan selenoid. Berbeda dengan meteran analog yang segala kegiatan seperti memantau penggunaan air, mematikan pemakaian air yang yang dilakukan langsung ke rumah-rumah pelanggan, meteran digital dapat melakukan

Pemantauan sekaligus pengontrolan dari jarak jauh tanpa harus meninggalkan stasiun pengendali. Meteran bekerja dengan cara membaca setiap aliran air yang mengalir tiap satuan waktu oleh sensor water flow, kemudian setiap aliran air akan dikalkulasikan untuk mendapatkan total harga dari penggunaan air. Selain itu meteran dapat dimatikan atau dihidupkan oleh petugas PDAM melalui telecommand atau perintah yang dikirimkan melalui jarak jauh dari stasiun pengendali (pihak PDAM) sebagai fitur penertiban pemnayaran air. Perintah yang diberikan dari stasiun pengendali menggunakan jarigan radio melalui perangkat telemetri LoRa. Telecommand dapat berupa perintah instruksi dimana pihak penerima akan mengirimkan request data kepada pihak pengirim menggunakan beberapa inisial khusus seperti kode 101, 111, atau 102. Kode – kode khusus ini berisikan instruksi untuk meminta data sensor, penggunaan air perjam, perhari dan perbulan serta perintah untuk memutuskan aliran air. Setiap kali stasiun pusat membutuhkan data maka dikirimkan data request data, lalu meteran digital akan mengirimkan balik data penggunaan sesuai dengan request sebelumnya. Demikian juga untuk menonaktifkan meteran digital dikirimkan perintah mematikan.

Smart PDAM mempunyai keunggulan utama yaitu sistemnya dapat di operasikan tanpa menggunakan internet walaupun alat ini berbasis Internet Of Things (IOT). Sistem dari produk ini juga menerapkan model jaringan telemetri untuk penerapan di daerah yang minim jarigan untuk mengirimkan perintah atau request dengan jarak jauh atau telecommand. Perkembangan teknologi telemerti telah dimanfaatkan dalam pemantauan dan distribusi data/informasi secara tepat. Pada teknologi telemetri remote collecting data merupakan sebuah metode pengambilan data-data pengukuran dari jarak jauh yang dapat menghasilkan data digital [16].

Data yang akan diamankan adalah data sensor yang dikirimkan melalui frekuensi gelombang radio menggunakan modul LoRa dengan seri SX1262. Tujuannya adalah untuk mencegah pihak ketiga membaca data sensor yang dikirimkan yang masuk pada jaringan dengan frekuensi yang sama. Namun hal ini dapat ditangani dengan menerapkan protokol kemanan[10] dengan menggunkan teknik kriptografi. Penelitian kali ini akan berfokus pada aspek keamanan pengiriman data sistem smart PDAM dengan mengangkat judul “Penerapan Kriptografi pada Kontrol Komunikasi Data Smart PDAM”.

Kriptografi adalah bidang ilmu yang mempelajari cara menjaga kemanan dalam proses kemanan data dalam sebuah pengiriman, Kriptografi memiliki dua konsep penting yaitu enkripsi dan dekskripsi. Enkripsi mengubah informasi atau data kedalam bentuk yang tidak dikenali menggunakan algoritma tertentu sedangkan dekskirpsi adalah mengubah dari bentuk samar tersebut menjadi informasi awal. Terdapat berbagai metode dalam kriptografi seperti Caesar chipper, Affine, Monoalphabethic, Polyaphabetic, Vigenre, Transposisi dan banyak metode-metode dalak kriptografi ini (Permana, 2018). Algrtima kriptografi ini diterapkan melalui bahasa pemgrograman arduino atau Arduimo Integrated Development Environment (IDE). Ada banyak algoritma kriptografi yang telah didukung oleh Aruino IDE seperti Authenticated Encryption with Associated Data (AEAD), Block Chiper AES, HASH, Public Key, Random Number Generation (RNG). Dalam penelitian kali ini penulis mencoba menerapkan algoritma AES untuk melakukan enkripsi dan dekripsi data sensor. Untuk mengakses protokol ini kita dapat menggunakan libraies yang ada dalam Arudino IDE.

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

Implementasi kriptografi pada sistem smart PDAM sangat penting untuk meningkatkan keamanan dalam pertukaran data atau komunikasi antar sensor dalam mengolah data agar data tidak dapat terbaca ketika ada pihak ketiga yang mencoba masuk kedalam jaringan. Algoritma AES menrapkan metode enkripsi dan deskripsi data. Data sensor dari perangkat pengirim akan di enkripsi berarti data tersebut akan berubah menjadi karakter acak yang tidak dapat dibaca lalu dikirimkan ke perangkat penerima. Data tersebut dikirimkan melalui frekuensi radio menggunakan telemtri LoRa, dan perangkat tersebut akan menerima data acak yang sudah terenkripsi menggunakan telemetri LoRa, modul ini dapat menggunakan komunikasi dua arah yaitu sebagai transmitter dan reciver kemudian data yang terenkripsi akan dideskripsikan kembali untuk mengembalikan kebentuk semula agar terbaca oleh penerima, proses deksripsi terjadi pada saat perangkat penerima telah menerima paket data yang dikirim. Oleh karena itu pihak ketiga tidak dapat melihat data apalagi memanipulasi paket data yang dikirimkan. Hasil yang didapatkan penelitian dapat menjadi solusi dari permasalahan yang ada pada sistem smart PDAM saat ini.

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah yang dapat dirumuskan dalam penelitian ini antara lain: yang pertama Bagaimana menerapkan teknik kriptografi pada kontrol komunikasi data smart PDAM dan yang kedua Bagaimana perbandingan tingkat keamanan sebelum dan setelah menggunakan teknik Kriptografi pada komunikasi data smart PDAM

Dari masalah tersebut penelitian ini berinisiatif untuk Memahami cara menerapkan teknik kriptografi pada kontrol komunikasi data smart PDAM.dan mengetahui perbandingan keamanan sebelum dan sesudah menggunakan tekik kriptografi pada komunikasi data smart PDAM.

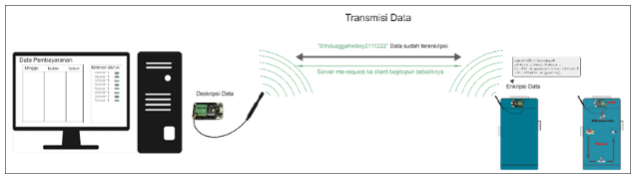
2. METODE PENELITIAN

Adapun metode penelitian yang diimplementasikan ialah metode R&D dikarenakan dalam penelitian penulis akan mengembangkan sistem dengan yang telah ada sebelumnya.

2.1. Desain Sistem

Sistem keamanan dibentuk menggunakan teknik kriptografi dengan mengimplementasikan algortima AES pada kode program arduino. Algoritma ini mengubah plaintext menjadi ciphtext menggunakan metode enkripsi. Yaitu metode untuk mengubah data plaintext menjadi kode acak yang tidak bisa dibaca kode acak tersebut kita sebut dengan ciphertext. Kode program akan ditulis dan dijalankan pada module LoRa dalam modul tersebut sudah terdapat mikrokontroler khususnya yang mengatur bagaimana pengiriman atau penerimaa data dapat berlangsung.

Dalam sistem yang dibangun tiap perangkat smart PDAM memiliki module LoRa ini yang bertugas mengirim sekaligus dapat menerima data dari/ke LoRa utama (server). Semua perangkat yang terhubung dapat saling berkomunikasi. Penerapan teknik kriptografi ini bertujuan agar data yang dikirim atau diterima aman dari gangguan luar atau pihak ke-3 yang bisa kapan saja masuk ke dalam jaringan yang berusaha masuk dengan mencari frekuensi gelombang radio yang sama di jalurnya.



Gambar 1. Desain Sistem

2.2. Teknik Pengumpulan Data

Penulis menyusun langkah-langkah penelitian dalam pengambilan data untuk mengukur tingkat keamanan yang dihasilkan setelah menerapkan teknik kriptografi. Dalam teknik pengambilan data langkah-langkah tersebut dengan beberapa parameter teknik analisis data dan observasi. Teknik observasi digunakan untuk melakukan pengamatan langsung kepada objek penelitian bertujuan untuk mengumpulkan data hasil pengamatan.

Oleh karena itu teknik observasi dilakukan untuk mengumpulkan data dari hasil uji coba yang telah dilakukan. Dalam penelitian tidak harus melibatkan seorang atau lebih partisipan karena objek penelitiannya sendiri adalah sub sistem yaitu kontrol komunikasi data yang akan diuji keamanannya. Dalam simulasinya dilakukan oleh penulis dengan tim yang riset smart PDAM yang telah ada sebelumnya. Data yang diambil untuk membandingkan tingkat keamanan dengan kondisi sistem sebelum dan sesudah menggunakan kriptografi. Data yang akan diobservasi dikategorikan dalam beberapa parameter dalam sebuah tabel, berikut tabel parameter yang dibutuhkan:

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

Tabel 1. Parameter Keamanan Data Menggunakan Kriptografi

No	Parameter	Output	Jenis
1	Karakter	Tipe Data	*Number, String*
2	Jenis Data	Jenis	Jenis
3	Enkripsi	*Ciphertext*	*Random Key*
4	Deskripsi	*Plaintext*	*Number, String*

2.3. Teknik Analisis Data

Teknik analisis data yang digunakan adalah analisis kualitatif menggabarkan kualitas subjek berdasarkan parameter yang telah didkomentasikan pada tabel 2.2. Berdsarkan parameter data yang dikumpulkan dari hasil observasi. Data disajikan dalam bentuk tabel pengamatan. Oleh karena itu dibutuhkan sebuah tabel untuk mendokumentasikan data yang dikumpulkan, berikut tabel data yang dibutuhkan.

Tabel 2. Kisi-kisi variabel pengamatan dari hasil observasi

No	Variabel Pengamatan	Keterangan
1	Request data	Permintaan akses data
2	Data kunci	Kunci enkripsi
3	Generate kode request	Membuat data *request* sesuai permintaan server pada meteran
4	Generate code comand	Membuat data perintah sesuai dengan *key* yang diberikan oleh meteran
5	Respon meteran	Respon atau *action* dari meteran setelah menerima *request*

2.4. Teknik pengujian

Parameter yang ditinjau dalam teknik pengujian kali ini adalah pengujian terhadap kemanan sistem komunikasi data. Pengujian keamanan dilakukan dengan simulasi penyerangan saat smart PDAM sedang beropeasi. Percobaan dilakukan untuk membaca data sensor melalui pihak ke tiga. Jika data berhasil dibaca dapat disimpulkan bahwa data tersebut tidak aman dan rentan pembobolan. Oleh karena itu akan diterapkan teknik kriptografi menggunakan metode AES yang akan di terapkan langsung melalui program arudino IDE sebagai pertahanan dari percobaan pembacaan data sensor saat pengiriman paket data. Selama proses transmisi berlangsung, sniffer melakukan sniffing terhadap pesan yang dikirim. Kemudian sniffer juga akan mencoba untuk mendapatkan pesan asli.

Tabel 3. Model Default Tanpa Keamanan

No	Jenis Data	Tipe Data	Data Kiriman	Data Terima
1	Data Sensor / Data Waktu	Int/ Char/ String	Plain Text / Chipper Text	Plain Text / Chipper Text

Tabel 4. Pengujian Enkripsi Dengan AES

No	Jenis Data	Tipe Data	Data Kiriman	Data Terima
1	Data Sensor / Data Waktu	Int/ Char/ String	Plain Text / Chipper Text	Plain Text / Chipper Text

Tabel 5. Pengujian Deskripsi AES

No	Jenis Data	Tipe Data	Data Kiriman	Data Terima
1	Data Sensor / Data Waktu	Int/ Char/ String	Plain Text / Chipper Text	Plain Text / Chipper Text

Tabel 6. Status pengujian

No	Mode	Kondisi
1	Mode *default* tanpa keamanan	*Sniffer* dapat melihat *plaintext*
2	Enkripsi AES	*Sniffer* melihat pesan *ciphertext*

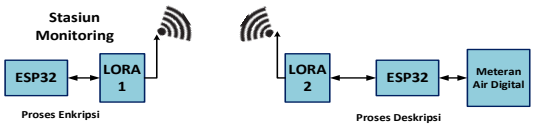
ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

3. HASIL DAN PEMBAHASAN

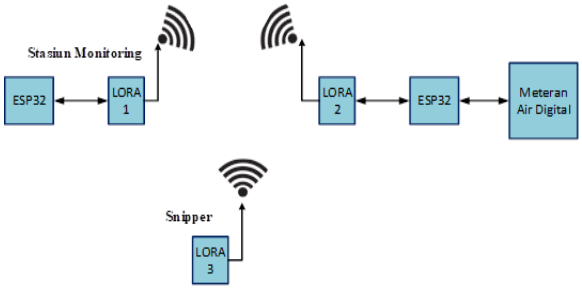
3.1. Hasil Perancangan

Dari peneltitian yang telah dilakukan ditemukan dua model perancangan skema dalam pengujian keamanan menggunakan teknik kriptografi algoritma AES dan pengujian tanpa keamanan. Skema pertama menggunakan dua mudol LoRa dan dua mikrokontroler. Request data akan di lakukan pada salah satu mikrokontroler yang berperan sebagai stasiun monitoring. Kemudian mikrokontroller ini berkomunikasi dengan LoRa menggunakan pin RX/TX lalu hasil request akan di kirimkan ke lora lainnya menggunakan telemteri. Request ini akan bersisi kode perintah yang akan dienkripsi pula Setelah menerima request LoRa akan meneruskan ke mikrokontroler yang memproses data. Paket data yang diterima akan dideskripsi dulu untuk mengetahui apa isi paket data tersebut. Setalah data berisikan perintah terdeskripsi, permintaan tersebut akan di proses kembali dan direspon untuk mengirimkan data yang diminta. Data akan dienkripsi kemudian dikirimkan ke tujuan melalui modul LoRa. Ketika paket data sampai ke mikrokontroler tujuan data tersebut harus dideskripsi untuk diketahui hasilnya.



Gambar 2. Skema Pengujian Pertama

Skema kedua dengan menerapkan skema pertama namun ditambah satu sniffer. Sniffer berperan sebagai pihak ketiga yang bertujuan untuk membaca data yang dikirimkan antar LoRa. Skema kedua ini bertujuan untuk membuktikan apakah implementasi kriptografi pada komunikasi data ini dapat berjalan dengan baik atau tidak. Skema ini yang akan menjadi patokan akhir untuk menentukan apakah komunikasi yang dilakukan itu aman atau tidak. Itulah ketiga hasil perancangan untuk kemanan komunikasi data pada sistem Smart PDAM yang hasil penelitiannya akan didokumentasikan dalam bentuk tabel.



Gambar 3. Skema Kedua Pengujian Menggunakan Sniffer

Adapun daftar perintah pada stasiun monitong yang diamankan sebelum dikirim ke meteran air digital dapat ditunjukkan pada Tabel 7 Pada sistem smart PDAM dengan LoRa sebagai media komunikasi menggunakan perintah untuk meminta data dari pada setiap meteran air digital. Agar perintah tersebut aman dan dapat dibuka oleh meteran tujuan saja maka perintah tersebut di enkripsi terlebih dahulu.

Tabel 7. Daftar Perintah Yang Di Amankan

No.	Daftar Perintah Stasiun Monitoring	Keterangan
1	111	Meminta Debit Perjam pada Meteran 1
2	112	Meminta Debi Perhari pada Meteran 1
3	113	Meminta Debit perbulan pada Meteran 1
4	12	Meteran 1 OFF
5	13	Meteran 1 ON

Pada Tabel 7 daftar tersebut menggunakan angka satu sebagai kode meteran air digital tujuan. Angka pertama pada perintah tersebut merupakan kode pada meteran air digital. Daftar perintah pada stasiun monitoring yang diamankan pertama yaitu 111 merupakan kode perintah untuk meminta data debit perjam pada meteran air digital pertama Kemudian pada

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

perintah kedua 112 merupakan perintah untuk meminta data debit perhari pada meteran air digital pertama. Lalu kode 113 merupakan perintah untuk meminta data debit perbulan pada meteran air digital pertama. Selanjutnya kode perintah 12 perintah untuk mematikan meteran air digital pertama. Kemudian kode 13 perintah untuk meyalakan meteran air digital pertama.

3.2. Hasil Pengujian

3.2.1 Pengujian Model Default tanpa Keamanan

Pada pengujian model dafault tanpa keamanan, penulis melakukan pengujian program komunikasi data pada LoRa tanpa menerapkan teknik kriptografi. Dengan hasil pengujian seperti pada Tabel 4.2 dibawah ini yang menunjukkan bahwa jika teknik kriptografi tidak diimplementasikan maka data yang diterima adalah plaintext. Tabel 8 merupakan hasil pengujian yang dilakukan sebanyak lima kali pengiriman data request dari stasiun monitoring ke meteran air digital.

Tabel 8. Hasil Pengujian Model Default tanpa Kamanan

No	Jenis Data	Tipe Data	Data Kiriman	Data Terima
1	Data *Request* 111	*String*	111	*111*
2	Data *Request* 112	*String*	112	112
3	Data *Request* 113	*String*	113	113
4	Data *Request* 12	*String*	12	12
5	Data *Request* 13	*String*	*13*	*13*

3.2.2 Pengujian Enkripsi menggunakan AES

Pengujian enkripsi dengan teknik kriptografi menggunakan algoritma AES yang diimplementasikan pada stasiun monitoring. Pada Tabel 9 merupakan hasil pengujian yang dilakukan untuk mengetahui bahwa data request berhasil di enkripsi. Seperti pada Tabel 9 data request berhasil dienkripsi dengan tipe data string dikirim dalam bentuk chipertext dan berhasil diterima oleh meteran air digital dalam bentuk chipertext.

Tabel 9. Hasil Pengujian Enkripsi menggunakan AES

No	Jenis Data	Tipe Data	Data Kiriman	Data Terima
1	Data *Request* 111	*String*	P4qVLkbs5sqYDbvcyXw70Q==	P4qVLkbs5sqYDbvcyXw70Q==
2	Data *Request* 112	*String*	P2YkGRgji5vDn81Ozw2NMA==	P2YkGRgji5vDn81Ozw2NMA==
3	Data *Request* 113	*String*	ARN98hc6ZCIR3WnhSEFmcw==	ARN98hc6ZCIR3WnhSEFmcw==
4	Data *Request* 12	*String*	O1C9y04jRHa82JMSokpZUA==	O1C9y04jRHa82JMSokpZUA==
5	Data *Request* 13	*String*	jrY2Z43E9vBhI4Gij5OhQ==	jrY2Z43E9vBhI4Gij5OhQ==

3.2.3 Pengujian Deskripsi menggunakan AES

Setelah menerapkan deskripsi menggunakan algoritma AES pada meteran air digital, sebelum diterapkan deskripsi meteran air digital menerima data dalam bentuk chipertext, namun setelah deskripsi diterapkan maka data yang diterima berbentuk plaintext. Hal ini dapat membuktikan bahwa penerapan deskripsi pada meteran air digital berhasil. Tabel 10 menunjukkan hasil pengujian tersebut berhasil.

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

Tabel 10. Hasil Pengujian Deskripsi menggunakan AES

No	Jenis Data	Tipe Data	Data Kiriman	Data Terima
1	Data *Request* 111	*String*	P4qVLkbs5sqYDbvcyXw70Q==	111
2	Data *Request* 112	*String*	P2YkGRgji5vDn81Ozw2NMA==	112
3	Data *Request* 113	*String*	ARN98hc6ZCIR3WnhSEFmcw==	113
4	Data *Request* 12	*String*	O1C9y04jRHa82JMSokpZUA==	12
5	Data *Request* 13	*String*	jrY2Z43E9vBhI4Gij5OhQ==	13

3.3. Pembahasan

Penerapan teknik kriptografi pada kontrol komunikasi data smart PDAM merupakan pengembangan dari sistem komunikasi smar PDAM yang menggunakan LoRa sebagai media komunikasi data. Penelitian ini mengamankan data request dari stasiun monitoring ke meteran air digital dengan menerapkan teknik kriptografi menggunakan algoritma AES.

Penerapan teknik ini bertujuan untuk memahami cara menerapkan Teknik kriptografi pada control komunikasi data smart PDAM dan mengetahui perbandingan keamanan sebelum dan sesudah menggunakan teknik kriptografi pada komunikasi smart PDAM. Penelitian ini menggunakan metode penelitin Research and Development (R&D). Model pengembangan yang diterapkan yaitu metode eksperimen yang dilakukan langsung dan melakukan uji coba untuk mengetahui tingkat keamanan pada komunikasi data smart PDAM.

Penelitian ini dibatasi pada pengujian penerapan teknik kriptografi pada stasiun monitoring, data request dari stasiun montoring akan diamankan sebelum dikirim ke meteran air. Penelitian ini menggunaka dua model perancangan skema dalam pengujian keamanan menggunakan teknik kriptografi algoritma AES. Skema pertama menggunakan dua mudol LoRa dan dua mikrokontroler dan skema kedua dengan menerapkan skema pertama namun ditambah satu sniffer.

Pada sistem smart PDAM menggunakan LoRa sebagai media komunikasi menerapkan perintah untuk meminta data dari pada setiap meteran air digital. Angka pertama pada perintah tersebut merupakan kode pada meteran air digital. Daftar perintah pada stasiun monitoring yang diamankan pertama yaitu 111 merupakan kode perintah untuk meminta data debit perjam pada meteran air digital pertama Kemudian pada perintah kedua 112 merupakan perintah untuk meminta data debit perhari pada meteran air digital pertama. Lalu kode 113 merupakan perintah untuk meminta data debit perbulan pada meteran air digital pertama. Selanjutnya kode perintah 12 perintah untuk mematikan meteran air digital pertama. Kemudian kode 13 perintah untuk meyalakan meteran air digital pertama.

Teknik kriptografi menggunakan algoritma AES ini diimpelentasikan melalui teknik coding menggunakan software Arduino IDE. Hasil pengujian skema pertama dengan dua mudol LoRa dan dua mikrokontroler ESP32 yaitu dari enam kali percobaan pengiriman data lima diantaranya data requet yang telah didaftarkan pada program dan satu data yang tidak terdaftar ada program. Setelah melakukan uji coba tersebut didapatkan bahwa program berhasil mengenali perintah request yang diinput dan menolak untuk memproses data yang tidak terdaftar dalam program. Data request berhasil dienkripsi yang menghasilkan data chipertext kemudian dikerim ke meteran air digital. Meteran air digital yang menerima data tersebut juga berhasil melakukan deskripsi pada chipertext yang diterima.

Kemudian hasil pengujian skema kedua dengan menambahkan sniffer atau pihak ketiga. Pada pengujian mode default tanpa keamanan didapatkan kondisi sniffer dapat melihat data request dalam

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

bentuk plaintext. Dan pada pengujian enkripsi dan deskripsi AES dengan teknik kriptografi atau keamanan, kondisi sniffer hanya dapat melihat data request yang dikirim dalam bentuk pesan ciphertext.

4. Kesimpulan

Berdasarkan hasil penelitian, kesimpulan pertama telah diterapkan teknik kriptografi pada control komunikasi enkripsi data smart PDAM yaitu dengan menggunakan program algoritma AES pada mikrokontroler ESP32 di stasiun monitoring dan algoritma dekripsi AES pada sisi meteran air digital kesimpulan kedua berdasarkan hasil penelitian dengan menerapkan teknik kriptografi dengan algoritma AES pada kontrol komunikasi data smart PDAM lebih aman dibandingkan tidak menerapkan keamanan, karena jika tidak menerapkan teknik kriptografi maka sniffer dapat melihat data asli yang dikirim sedangkan jika menerapkan teknik tersebut maka sniffer hanya dapat melihat data dalam bentuk ciphertext.

DAFTAR PUSTAKA

[1] Abdul Rahman, A., Nur Aini Muzasyaroh, A., & Andriana. (2020). Perancangan Sistem Telemetri Data Meteorologi Pertanian dengan Menggunakan LoRa secara Realtime. Tiarsie, 17(4), 137–142.

[2] Abraham, F. Z., Santosa, P. I., & Winarno, W. W. (2018). Tandatangan Digital Sebagai Solusi Teknologi Informasi Dan Komunikasi (Tik) Hijau: Sebuah Kajian Literatur (Digital Signature As Green Information and Communication Technology (Ict) Solution: a Review Paper). Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi, 9(2), 111. https://doi.org/10.17933/mti.v9i2.120

[3] Ambarita, R. (2017). Sistem Pakar Diagnosa Kerusakan Mainboard Komputer. IJIS - Indonesian Journal On Information System, 2(1). https://doi.org/10.36549/ijis.v2i1.20

[4] Asiyanik. (2017). Studi Terhadap Advanced Encryption Standard (Aes) DanAlgoritma Knapsack Dalam Pengamanan Data. Santika, 7(Jurnal Ilmiah Sains dan Teknologi), 553–561.

[5] Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001. Jurnal Tekno Kompak, 11(2), 41. https://doi.org/10.33365/jtk.v11i2.162

[6] Utama, DW. (2000). Sistem Kontrol Pada Modul Aliran Distribusi Bahan Baku Dengan Menggunakan Progammable Logic Controller. Seminar Nasional Mesin Dan Industri (SNMI3) 2007, Jurusan Te, 1–12.

[7] Faris, M. H. (2017). Pengaruh Tingkat Penerimaan Penggunaan Teknilogi Terhadap Minat Masyarakat Kota BanjarBaru menggunakan Teknologi Smart Home.

[8] Gunawan, S. S. (2021). Buku Paduan Aplikasi Smart PDAM. Teknologi, IOT, 1–15.

[9] Hasyim, A. (2016). Perencanaan dan analisis kehandalan sistem komunikasi radio microwave tampak pandang pada pita frekuensi 12750-13250 MHz [Planning and analysis of the reliability of line of sight microwave radio communication system on 12750-13250 MHz band]. Buletin Pos Dan Telekomunikasi, 14(2), 147. https://doi.org/10.17933/bpostel.2016.140206

[10] Hidayat, R. F., Akbar, S. R., & Kusyanti, A. (2018). Implementasi dan Analisa Performansi Protokol Keamanan TinySec pada Wireless Sensor Network dengan Media Pengiriman Data NRF24L01 melalui Frekuensi Radio. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2(9), 2858–2865.

[11] Meinarni, N. P. S. (2019). Tinjauan Yuridis Cyber Bullying Dalam Ranah Hukum Indonesia. … : Jurnal Ilmu Sosial Dan Humaniora, 5, 577–593. http://jayapanguspress.penerbit.org/index.php/ganaya/article/view/225

[12] Nurdiansyah, M., Sinurat, E. C., Bakri, M., & Ahmad, I. (2020). Sistem Kendali Rotasi Matahari Pada Panel Surya Berbasis Arduino UNO. Jurnal Teknik Dan Sistem Komputer, 1(2), 7–12. https://doi.org/10.33365/jtikom.v1i2.14

[13] Pangestu, S. (2017). Persepsi Masyarakat Tentang Pelayanan Listrik Prabayar Dan Pascabayar Oleh Pt Pln (Persero) Di Desa Karya Bhakti Kecamatan Muara Wahau Kabupaten

ISSN cetak 2745-925X
ISSN online 2722-273X
DOI:http://dx.doi.org/10.26858/jessi.v4i1.42841

JESSI Volume 04 Nomor 1 May 2023

Kutai Timur. EJournal Pemerintahan Integratif, 5(2), 296–307.

[14] Permana, A. A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI, 4(3), 110. https://doi.org/10.36722/sst.v4i3.280

[15] Susandi, D., Nugraha, W., & Rodiyansyah, S. F. (2017). Perancangan Smart Parking System Pada Prototype Smart Office Berbasis Internet Of Things. Prosiding Semnastek, November, 1–2.

[16] Wahjono, H. D. (2018). Penerapan Teknologi Online Monitoring Kualitas Air Untuk Das Prioritas Di Sungai Ciliwung Dan Sungai Cisadane. Jurnal Air Indonesia, 9(1). https://doi.org/10.29122/jai.v9i1.2476

[17] Widayanto, A. (2018). Modul Perkuliahan Jaringan Komputer. Pelatihan Pemanfaatan Tik Untuk Pembelajaran, 4–12. https://repository.bsi.ac.id/index.php/unduh/item/237028/Modul-Jaringan-Komputer.pdf