Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 6 (2020) 1157 – 1164 ISSN Media Elektronik: 2580-0760

Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data *Internet of Things* (IoT) Tanaman Hidroponik

Roiya Ravida[1], Heru Agus Santoso[2]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[1]roiyaravida36@gmail.com, [2]heru.agus.santoso@dsn.dinus.ac.id*

Abstract

It is easier to grow vegetables using hydroponic techniques in the era of globalization. In hydroponic techniques, the need for certain plants to grow is very important to note. Manually, controlling and checking conditions is difficult to measure, so a system that can check plant needs is needed. Internet of Things (IoT) is known to be used to manage hydroponic plants. The drawback of IoT is the use of the system in general, resulting in confusion in the process of detecting plant needs. In IoT, it is important to implement system security with the aim of limiting interested users. In this study, the IoT security process was carried out using cryptographic techniques, namely the 128-bit Advanced Encryption Standard (AES) algorithm. This algorithm was chosen because it has a safer encryption result compared to similar symmetrical algorithms such as Blowfish, Caesar cipher and faster than the Data Encryption Standard (DES). Cryptography is used in securing the input data for plant needs designed using the ESP 8266 version of the Arduino Uno SoC microcontroller. Several criteria for selected plant needs include Total Dissolve Solid (TDS), Potential Hydrogen (PH), temperature, and distance that have been captured through Sensors and stored in the database before cryptography processing. Experimental results to prove data security in the IoT system have been done by analyzing plaintext and ciphertext, calculating the Avalanche Effect (AE), entropy and Bit Error Ratio (BER) values. AE obtained 58.01% as the highest yield, the highest entropy was 6.3566 while all data resulted in BER = 0. Based on the results obtained, it can be concluded that 128-bit Advanced Encryption Standard (AES) cryptography on IoT systems is good and according to standards.

Keywords: Advanced Encryption Standard, Internet of Things, Hydroponic Plants, Avalanche Effect, Entropy

Abstrak

Model bercocok tanam sayuran lebih mudah menggunakan teknik hidroponik di era globalisasi. Dalam teknik hidroponik, kebutuhan tanaman akan zat tertentu untuk tumbuh sangat penting untuk diperhatikan. Secara manual, pengaturan dan pengecekan kondisi menjadi hal yang sulit diukur sehingga diperlukan sistem yang dapat mengecek kebutuhan tanaman. *Internet of Things (IoT)* dikenal dapat digunakan untuk melakukan pengelolaan terhadap tanaman hidroponik. Kekurangan IoT yaitu penggunaan sistem secara umum sehingga mengakibatkan kerancuan dalam proses deteksi kebutuhan tanaman. Dalam IoT penting diterapkan keamanan sistem dengan tujuan membatasi user yang berkepentingan. Pada penelitian ini, proses pengamanan IoT dilakukan menggunakan teknik kriptografi yaitu algoritma *Advanced Encryption Standard (AES)* 128 bit. Algoritma ini dipilih karena mempunyai hasil enkripsi lebih aman dibanding algoritma simetris sejenis misalnya Blowfish, Caesar cipher serta lebih cepat dibanding *Data Encryption Standard (DES)*. Kriptografi digunakan dalam mengamankan data kebutuhan tanaman yang dirancang menggunakan mikrokontroler *Arduino Uno SoC* versi ESP 8266. Beberapa kriteria kebutuhan tanaman yang di pilih antara lain *Total Dissolve Solid (TDS), Potential Hydrogen (PH),* temperatur, dan jarak telah ditangkap melalui Sensor2 dan disimpan dalam database sebelum diolah dengan kriptografi. Hasil percobaan untuk membuktikan keamanan data dalam sistem IoT telah dilakukan dengan menganalisis teks dan *cipher-text*, menghitung nilai *Avalanche Effect (AE),* entropi *dan Bit Error Ratio (BER).* AE memperoleh 58,01% sebagai hasil tertinggi, entropi tertinggi 6,3566, sedangkan semua data menghasilkan BER = 0. Berdasarkan hasil yang telah diperoleh, dapat disimpulkan bahwa kriptografi *Advanced Encryption Standard (AES)* 128 bit pada sistem *IoT* sudah baik dan sesuai *standard.*

Kata kunci: *Advanced Encryption Standard, Internet of Things*, tanaman hidroponik, *Avalanche Effect*, entropi

Diterima Redaksi : 17-09-2020 | Selesai Revisi : 03-11-2020 | Diterbitkan Online : 20-12-2020

1. Pendahuluan

Secara umum, keuntungan penggunaan IoT adalah peningkatan *customer engagement*, optimasi teknologi, minimalisasi pemborosan, serta *enchanced data collection*. Namun keamanan IoT sangat lemah, seperti pada kejadian yang menimpa perusahaan Cina Orvibo yang menjalankan *smarthome platform.* Perusahaan tersebut menawarkan *smarthome* untuk mempermudah aktivitas *user* di dalam rumah. Data yang disimpan tidak diberikan pengamanan apapun sehingga sekelompok peretas bernama "*hacktivis*" dapat membaca dan mengakibatkan pelanggaran keamanan. Dengan demikian keamanan data sangat penting karena menyangkut privasi pengguna *smarthome* [1]. Kemananan kunci sistem IoT merupakan hal mendasar dalam pertukaran informasi [2]. Model keamanan data dapat dilakukan menggunakan teknik penyandian data, dalam bentuk enkripsi dan dekripsi [3]. Hanya pengirim dan penerima sajalah yang dapat mengetahui kunci dari proses penyandian [4]. Teknik penyandian ini dikenal dengan kriptografi.

Berdasarkan kunci yang digunakan, kriptografi terbagi menjadi dua yaitu simetris dan asimetris [5]. Kriptografi simetris menggunakan kunci yang sama antara proses enkripsi dan dekripsi sedangkan asimetris menggunakan kunci yang berbeda. Kunci asimetris dinilai lebih aman dibanding simetris namun algoritma yang dapat digunakan masih terbatas dan membutuhkan waktu operasi lebih lama. Kriptografi simetris dapat dikatakan aman apabila kunci yang digunakan merupakan kombinasi angka dan huruf yang rumit. Semakin panjang kunci yang digunakan tentu dapat meningkatkan keamanan. Salah satu algoritma simetris dengan operasi yang cepat adalah *Advanced Encryption Standard (AES)* [6].

AES lebih cepat dibanding *Data Encryption Standard (DES)* dalam proses enkripsi-dekripsi [8], hal ini diperoleh dari 10 putaran kunci sebelum proses enkripsi. Secara realtime, AES juga terbukti dapat mengirim pesan melalui sistem [9]. Menurut [10], AES 128-bit dapat mengenkripsi file dokumen dengan mengkonversinya menjadi kode *Standard Code for Information Interchange (ASCII)* selama 10 putaran sehingga data yang dihasilkan akan sulit untuk dikonversi ke aslinya apabila tidak menggunakan kunci asli. Hal ini seperti yang terjadi pada pengamanan data untuk *smarthome* menggunakan AES, diketahui bahwa protokol jaringan harus tahan terhadap serangan [11]. Berdasarkan [12], AES telah terbukti aman untuk diimplementasikan ke dalam jaringan karena integritas data, kerahasiaan dan efisiensi tetap terjaga. Menurut [13], AES terbukti mempunyai waktu enkripsi dan dekripsi lebih cepat di banding *Blowfish*. File teks AES hasil dekripsi dan file asli tidak mengalami perubahan [14], dan apabila dibandingkan dengan *Caesar cipher* maka AES lebih aman setelah dilakukan pengujian menggunakan teknik *brute force*.

Pada penelitian yang dilakukan oleh [15], proses pengamanan sistem *IoT* telah dilakukan menggunakan DES dan *Data Encryption Standard Lightweight* (DESL). Tetapi dalam peneltian ini hanya dihasilkan perbandingan waktu enkripsi dan dekripsi saja. Penelitian yang dilakukan oleh [16] menjelaskan mengenai perbandingan antara AES dan Blowfish pada kriteria waktu enkripsi, waktu dekripsi dan alokasi penggunaan memori. AES lebih cepat dalam melakukan enkripsi plainteks dibandingkan dengan Blowfish. Penelitian lain yang dilakukan oleh [17], melalui modifikasi S-Box dan ekspansi kunci AES telah berhasil menekan kebutuhan daya dalam proses integrasi sistem IoT.

Berdasarkan kebutuhan model cocok tanam hidroponik yang lebih mudah menggunakan IoT, dan kebutuhan akan keamanan sistem, maka penelitian ini penting dilakukan. Hasil yang diharapkan adalah sistem IoT mampu menangkap data kebutuhan tanaman hidroponik melalui sensor. Disisi lain, model keamanan dengan teknik kriptografi dapat dilakukan pada proses input data dan informasi kebutuhan tanaman melalui platform android. Adapun perbedaan dari penelitian yang telah dilakukan oleh [15] dengan menggunakan DES yang hanya menampilkan hasil waktu enkripsi dekripsi tanpa mengetahui ketahanan terhadap keamanan data dalam IoT. Pada penelitian ini kami menguji ketahanan data menggunakan perhitungan entropy. Merujuk pada [16], maka kami akan menggunakan AES dalam melakukan proses enkripsi dekripsi untuk membuktikan keamanan IoT berbasis kriptografi.

2. Metode Penelitian

2.1. *Advanced Encryption Standard (AES)*

AES adalah algoritma simetris yang menggunakan kunci sama persis pada proses enkripsi dan dekripsi yang diimplementasikan dalam teknik tunggal atau gabungan seperti steganografi [18] atau kompresi data [19]. Berdasarkan panjang kunci yang digunakan, AES memiliki 3 jenis, yaitu AES 128 [8], AES 192 [20] dan AES 256 [21] sesuai Tabel 1.

Tabel 1. Versi AES Berdasarkan Panjang Kunci [22]

AES Version	Key Length (Nk Words)	Block Size (Nb Words)	Number of Rounds (Nb)
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

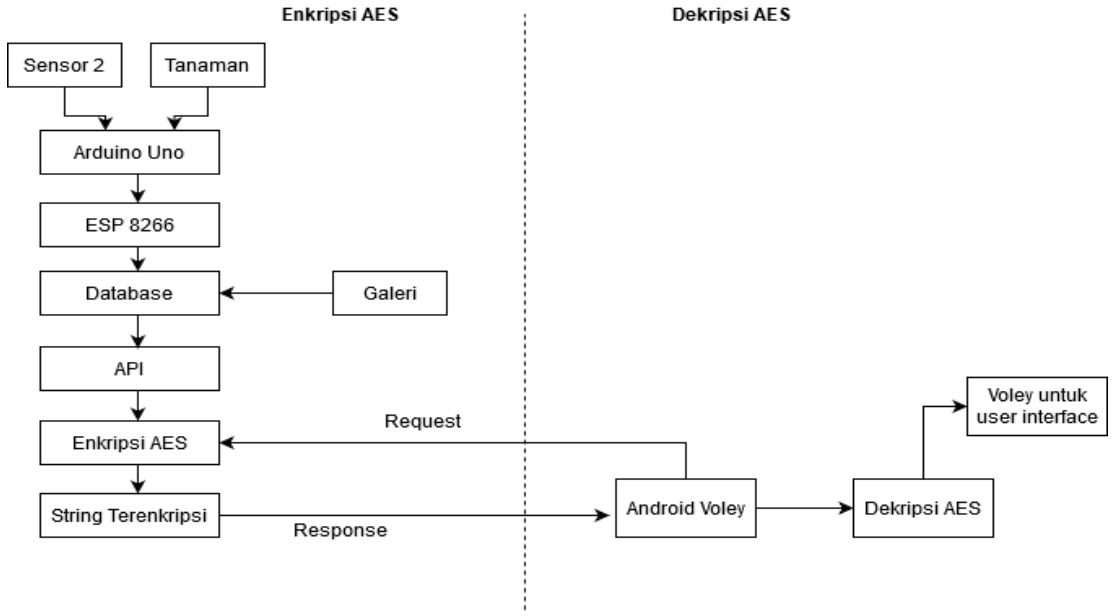
Pada Tabel 1, setiap jenis menggunakan kunci internal yang berbeda dalam menjalankan kunci bulat untuk setiap putaran. Algoritma ini digunakan untuk mengenkripsi suatu dokumen dan file yang berisi teks dengan melakukan proses enkripsi secara paralel, umumnya beroperasi pada 128-bit atau 16 blok karakter. Blok 128-bit dalam teks biasa [23] dimasukkan ke dalam bentuk persegi berukuran 4x4 *byte* dengan operasi XOR kunci dan diproses sebanyak sepuluh kali

menggunakan substitusi *addkey linier* untuk menghasilkan *ciphertext*.

2.2. Skema Penelitian

Berdasarkan Gambar 1, skema penelitian direpresentasikan menjadi dua bagian utama yaitu enkripsi dan dekripsi. Dalam AES, proses enkripsi terdiri dari empat jenis operasi *byte* yaitu *SubBytes*, *ShiftBytes*, *ShiftRows*, *MixColoumns* dan *AddRoundKey*. Enkripsi awal di mulai dari status input yang kemudian akan mengalami transformasi *byte*, setelah itu status *AddRoundKey* akan mengalami perubahan pada *SubBytes*, *MixCloumns* dan *AddRoundKey* secara berulang sebanyak *Nr* (untuk AES-256 bit terdiri dari 14 *loop*). Proses putaran terakhir mengalami transformasi *MixColoumns*, sedangkan proses *AddRoundKey* menggunakan perhitungan XOR menurut rumus 1 berikut [24].

$$M_{ij} = X_{ij} \oplus Y_{ij} \quad (1)$$



Gambar 1. Skema Penelitian

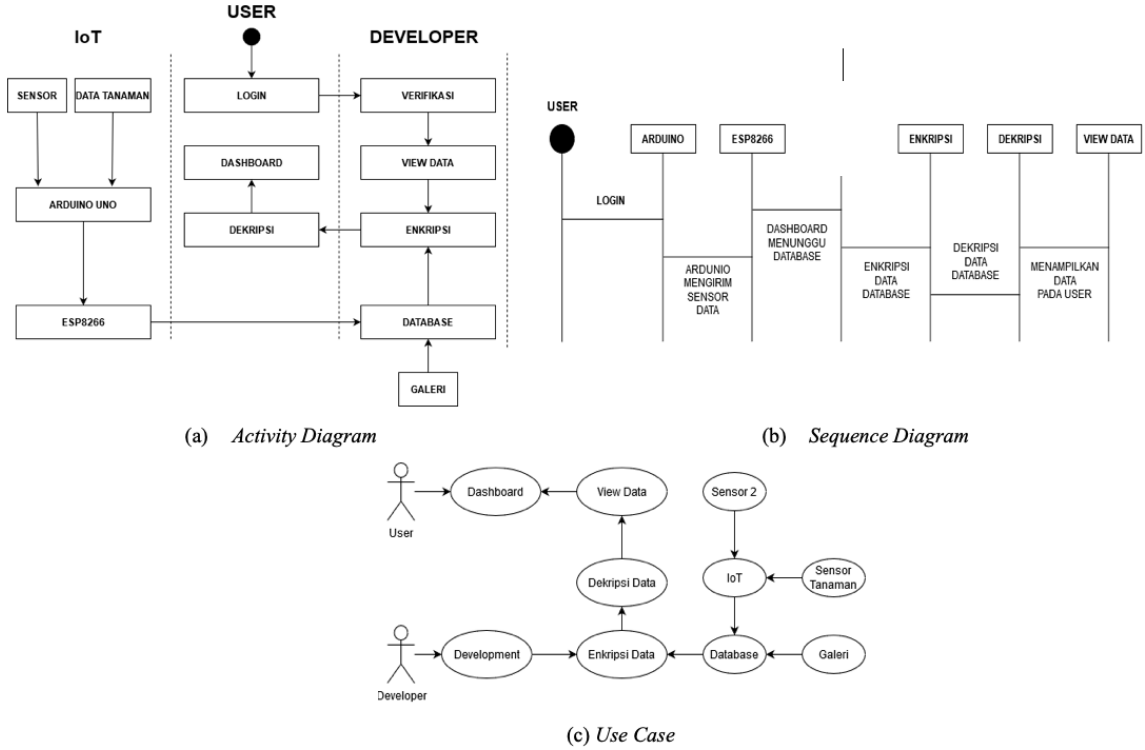
Pada proses dekripsi, luaran yang dihasilkan dengan menggunakan AES-128 berupa *string* dari putaran terakhir yang bersifat heksadesimal. Berdasarkan Gambar 1, dekripsi hanya terjadi pada android data *cipher text* yang akan dikirim ke android saat android meminta data terenkripsi dari server. Tahapan penelitian keamanan sistem IoT tanaman menggunakan AES sesuai Gambar 1 dapat dijabarkan menjadi bebrapa langkah sebagai berikut. Pertama proses *inverse Add Round Key*, sama seperti selama enkripsi, dilakukan dengan mengoperasikan XOR. Kedua, *inverse Mix Columns* menggunakan metode yang hampir sama dengan *Mix Columns* pada saat enkripsi. Perbedaannya adalah yang digunakan *a(x)* yaitu *invers (a-1)*. Selanjutnya pada langkah ketiga, *inverse Shift Row* merupakan kebalikan dari proses enkripsi *ShiftRows*, jika pada saat enkripsi dilakukan proses dari atas dengan baris kedua bergeser 1 *byte*, baris 3 bergeser 2 *byte*, baris 4 bergeser 3 *byte*. Pada proses dekripsi, baris 4 bergeser 1 *byte*, baris ke 3 bergeser 2 *byte* dan baris 2 bergeser 3 *byte*. Langkah ke empat yaitu *inverse Sub Byte* yang memiliki cara kerja yang sama dengan *Sub Bytes* saat melakukan enkripsi. Perbedaannya terletak pada S-Box yang digunakan saat mengubah *state* yang harus diganti. Langkah ke lima yaitu *inverse Add Round Key*. Sama seperti saat enkripsi, yaitu dengan mengoperasikan XOR kunci. Hasil akhir luaran menggunakan *voley library* untuk mendapatkan akses dari *API website*. Kemudian hasil proses dekripsi ini berupa *string JSON* dimana *JSON* ini berisi data yang diambil dari *database* yang berguna untuk membantu menampilkan informasi yang terdapat pada *Android*.

2.3. Rancangan Sistem Hidroponik

Mikrokontroler mengambil data tumbuhan hidroponik yang telah diberi sensor, sehingga *Arduino* dapat memperoleh data tentang kebutuhan tumbuhan. Selanjutnya data tersebut diolah menggunakan ESP 8266. *ESP 8266 on Chip System (SoC)* untuk mengolah data yang telah diambil oleh *Arduino*, sehingga data tersebut dapat di kirim ke *database*. *Database* adalah data yang telah dikelompokkan dalam satu memori tertentu berisi data yang saling berhubungan. Data tersebut berfungsi mempermudah akses terkomputerisasi dalam perawatan tumbuhan hidroponik berbasis *IoT*. Secara *realtime*, data tanaman telah tertanam pada Sensor2 dan tersimpan di Galeri. Data pada Sensor2 terdiri dari suhu, jarak, *Potensi Hidrogen (PH)*, dan *Total Dissolve Solid (TDS)* yang merupakan padatan terlarut dalam air. Pada Galeri, terdapat

kumpulan gambar *realtime* perkembangan tanaman hidroponik. Gambar yang dihasilkan akan di kirim ke *database* dan akan di hapus secara berkala selama seminggu dengan tujuan mengurangi penumpukan data dalam *database*. Jenis tanaman dan tempat serta spesifikasinya (model hidroponik horizontal dan model vertikal) digunakan sebagai input data. *Database* harus dapat dibaca oleh *android* sehingga diperlukan *Application Programming Interface (API)* digunakan untuk melakukan integrasi data dari *database*.

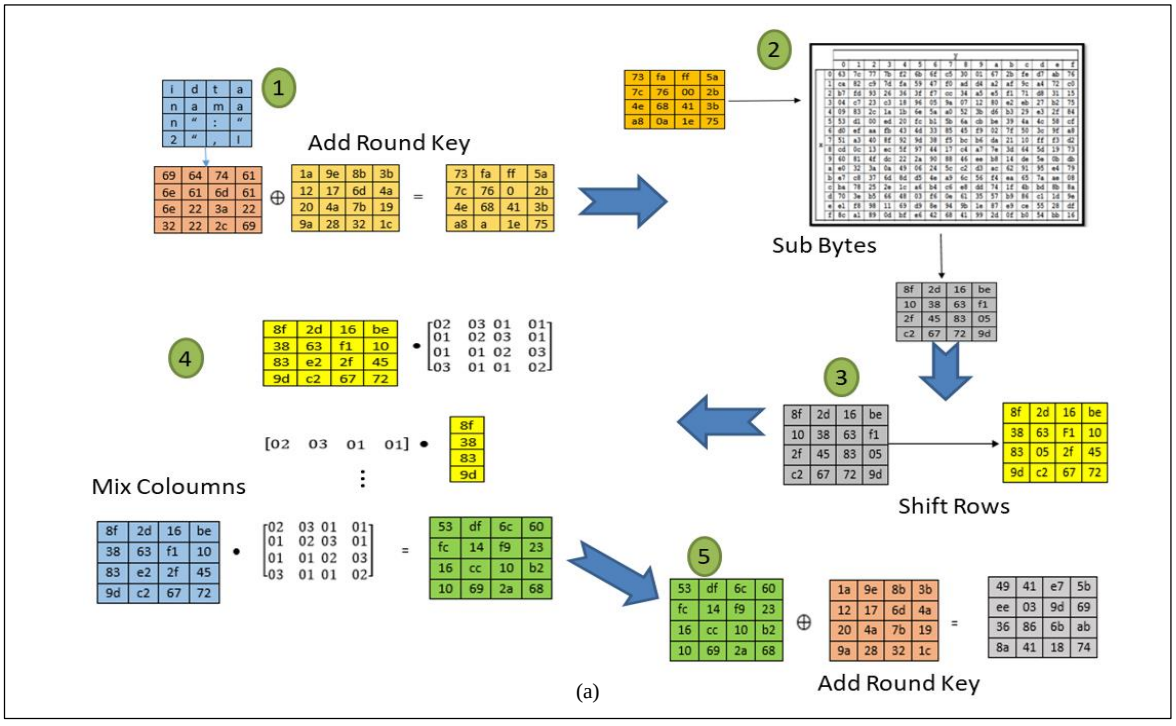
Pada Gambar 2 dapat dilihat rancangan sistem yang telah diimplementasikan. Gambar 2 (a) merupakan *activity diagram*. Pada *activity diagram* digambarkan bahwa user memerlukan login melalui *dashboard*. Proses pencocokan user menggunakan arduino uno. Selanjutnya, sistem akan memproses data dari *database.*



(a) *Activity Diagram* (b) *Sequence Diagram*

(c) *Use Case*

Gambar 2. Rancangan Sistem Kriptografi Hidroponik



(a)

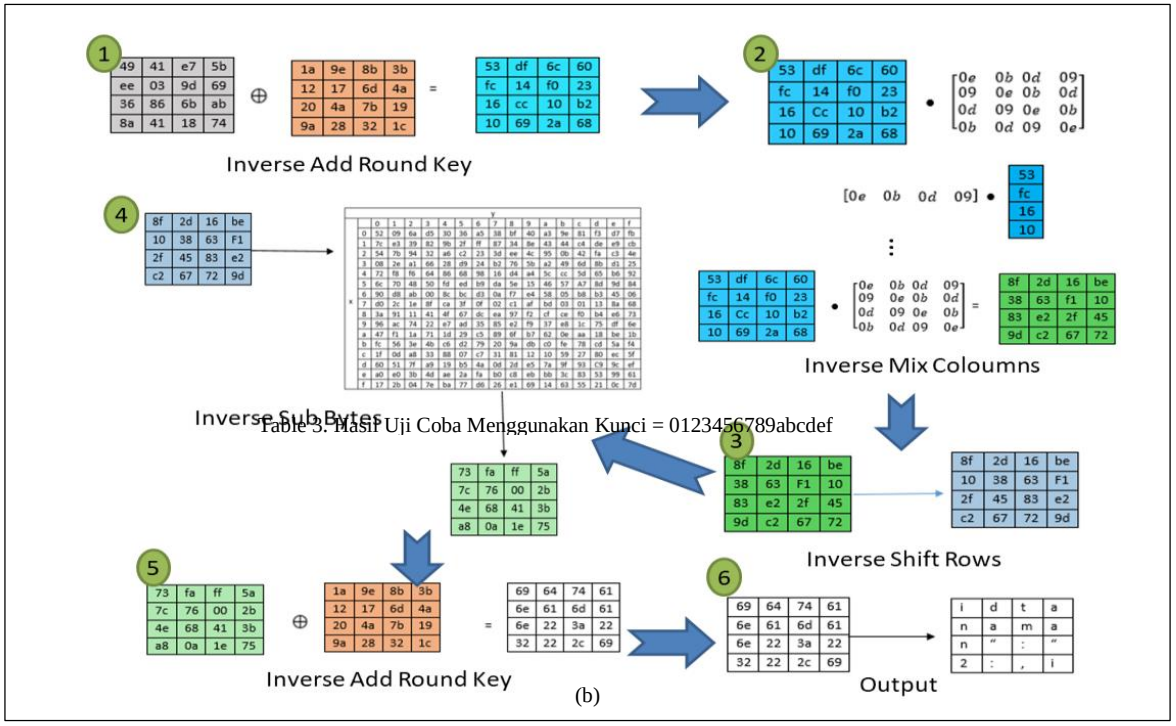


Table 3. Hasil Uji Coba Menggunakan Kunci = 0123456789abcdef

Gambar 3. Perhitungan manual (a) enkripsi, (b) dekripsi

Proses enkripsi dan dekripsi menggunakan kunci yang sama dan dilakukan secara *realtime.* Pada Gambar 2 (b), terdapat sequence diagram yang menggambarkan alur *Arduino* dalam mengoleksi data dari sensor, kemudian dikirim ke *ESP8266* sehingga data bisa di upload ke *database*. Sebelum data dikirimkan kepada *user*, data telah melewati proses enkripsi dengan kunci tertentu. Ketika user mengambil data, proses dekripsi secara realtime terjadi. Gambar 2 (c) adalah *use case* dari aplikasi IoT hidroponik berbasis kriptografi AES. Pemakai dan pengembang aplikasi saling berinteraksi dalam proses pengambilan data hingga proses pemantauan kebutuhan tanaman hidroponik dapat selesai dilakukan dengan baik.

2.3. Proses Enkripsi dan DekripsDalam penelitian ini, perhitungan manual AES telah di uji coba untuk pengecekan terhadap hasil kriptografi sesuai Gambar 3. Pada Gambar 3, dijelaskan bahwa kunci yang digunakan untuk proses enkripsi dekripsi hingga dihasilkan sebuah ciphertext. Pada Gambar 3, terdapat proses perhitungan kunci awal yang dihitung menggunakan sejumlah putaran. Kunci awal berupa bilangan heksadesimal seperti kunci yang digunkaan pada Tabel 3. Proses perhitungan *sub bytes* menggunakan bantuan *sub box* yang digunakan untuk mencari perpotongan antara nilai pada kedua bilangan heksadesimal.

3. Hasil dan Pembahasan

3.1. Pengumpulan Data

Data yang dienkripsi dan didekripsi diambil melalui subsistem *Sensor2*, tanaman dan galeri. Pada *Sensor2* ditangkap informasi yang berisi data mengenai kebutuhan tanaman hidroponik yang ditanam yaitu suhu air, jarak tanam, *Potensial Hidrogen (PH)* dan *Total Dissolve Solid (TDS).* Sensor tanaman berisi model atau penataan tanaman hidroponik yang dilakukan baik secara verikal maupun horizontal. Sedangkan pada galeri berisi gambar tentang kesehatan tanaman hidroponik yang ditanam. Semua data diambil melalui *database* web Udinus *Hydroponic IoT* berupa *JSON* yang akan dienkripsi dalam bentuk *API* bertipe data string. Gambaran mengenai parameter dalam implementasi sistem dapat dilihat pada Gambar 3.

```
Format data sensor
[
  {
     “id_tanaman“: “2“,
     “id“: “9292“,
     “ph“: “20.65“,
     “jarak“: “3.55“,
     “tds“: “0.00“,
     “temperatur“: “29.20“,
     “humidity“: “90.80“,
     “waktu“: “2020-03-03 04:58:47“,
     “jam“: “00:00:00:0000“
  },
  {
     “id_tanaman“: “2“,
     “id“: “9291“,
     “ph“: “20.52“,
     “jarak“: “3.55“,
     “tds“: “0.00“,
     “temperatur“: “29.20“,
     “humidity“: “90.80“,
     “waktu“: “2020-03-03 04:58:24“,
     “jam“: “00:00:00:0000“

  },
```

Berdasarkan parameter pada format data di atas, data dari database akan diolah oleh android melalui teknik enkripsi-dekripsi. Dalam penelitian ini digunakan 100 buah tanaman kangkung. Terdapat keterangan mengenai

jarak, ph, id tanaman, tds, temperatur, humidity, waktu dan jam pengambilan data.

3.2. Analisis Keamanan Data

Uji coba hasil sistem IoT dalam aspek keamanan dilakukan dengan menghitung beberapa alat uji yaitu *Avalanche Effect* (AE) sesuai rumus (2), Entropy sesuai rumus (3), dan hasil enkripsi dekripsi berupa teks asli dari sistem yang telah di buat.

$$AE = \frac{bit\ yang\ berubah}{total\ bit} \text{ x } 100\% \quad (2)$$

Tabel 2. Hasil AE dan Entropi

Contoh Pesan	AE	Entropi
Hydroponic Plant	56.21%	6.2120
Kale Plant	57.12%	6.3128
Android System Hydroponic	50.37%	6.1470
Sensor IoT esp8266	52.88%	6.3566
Kale Testing Equipment	58.01%	6.4521

AE adalah metode untuk mengetahui berapa persen perubahan pesan selama proses enkripsi dilakukan dengan melihat rasio antara jumlah bit *ciphertext* [25] karena adanya perubahan *plaintext* pada jumlah bit [26]. Jika konversi bit adalah setengah dari jumlah bit di *ciphertexts* atau 50%, maka algoritma telah memenuhi proses enkripsi dan dekripsi yang benar [27]. Pada Tabel 2, dipaparkan perolehan nilai AE dan entropy. Pada Tabel 2 dapat dilihat bahwa pesan yang digunakan dalam percobaan tidak hanya satu. Terdapat lima pesan yang digunakan untuk lima buah proses berbeda dengan tujuan untuk membandingkan nilai AE dan entropy saja.

Table 3. Hasil Uji Coba Menggunakan Kunci = 0123456789abcdef

Objek	Keterangan	
Sensor2	Plainteks	"id_tanaman": "2", "Id": "9292", "ph": "20.65", "jarak": "3.55", "Tds": "0.00", "temperatur": "29.20", "huminity": "90.80", "Waktu": "2020-03-03 04:58:47", "jam": "00:00:00.00000" "id_tanaman": "2", "Id": "9291", "ph": "20.52", "jarak": "3.55", "Tds": "0.00", "temperatur": "29.20", "huminity": "90.80", "Waktu": "2020-03-03 04:58:24", "jam": "00:00:00.00000"
	Enkripsi	Do9Bk7atu99shOt4vcO3rG92G/GtuEVxOaaTwSIpXr1onE5Dh6ylONWJ6rmtPZsSfNAm8QQAMGgZP7UxYdn cw2wpPGp218aWKdCOZFcmetVgb9sijTTrmngJbDjUfiPcSR0SMasBnVb9gVlHqiq3xIZHYezwgnQOrUE0D5k XGExPXSwUNXCU3K5XWty7n3By5DoqaFAK69fHrYA9wOlRSQuMBkqP98KmWCUR08P+7kqLBGM1Pf+ 8Oxel/riaW1MVmWMl1/312Bj6OO5mmOizBAqViJkXUFQzJS81rEHOcrwrIxRLKLirtB0ekPTaXa8A75gL+/fC KXmmi8qpecMwxON39PhPCyyCNfV38eWycCzQ2uyG68DsGPwzAli8D2jnf+pHnnrHIoLHQu2n+IMYFmdGg 34KHLATDUTMjW8Zn0/qnOiAZOLvrhsuDZWhbAvGEK2jzr++ttB/Es8udPUpjNpr/4cipJ7hDtNQsHCUAZaR8 XewRIEbihL5zhEg2HXtuBreNtaiiGAx+kkPUylD2a6+xPSp1kQEVq/IrS1Z/nK9keuABw5zOkwGZmoXb3+pc+j GBRgRP7K8tp8MwOIl/Yo41SclKN7mXnoNkCX4h0ZeXodV00QKVWcEGQF9+ggTqcHcax6JhkFIEeCpFdmc mSylblaAbM
	Dekripsi	"id_tanaman": "2", "Id": "9292", "ph": "20.65", "jarak": "3.55", "Tds": "0.00", "temperatur": "29.20", "huminity": "90.80", "Waktu": "2020-03-03 04:58:47", "jam": "00:00:00.00000" "id_tanaman": "2", "Id": "9291", "ph": "20.52","jarak": "3.55", "Tds": "0.00", "temperatur": "29.20", "huminity": "90.80", "Waktu": "2020-03-03 04:58:24", "jam": "00:00:00.00000"
Tanaman	Plainteks	[{"id":"1","nama_tanaman":"Kangkung","tempat":"D.2.F","spesifikasi":"Vertikal","id_user_input":"1","created_a ":"2019-09-18 11:00:00","update_at":"2019-11-25 3:11:10"},{"id":"2","nama_tanaman":"Sawi","tempat":"D.2.A","spesifikasi":"Horizontal","id_user_input":"2","cr ated_at":"2019-09-18 13:00:00","update_at":"2019-11-25 04:47:58"}]
	Enkripsi	i/dAwrlruJ4TEy30bzEDrOfZVdqr0eXYoHDlGPVBlcWHVZpsI7OzUY0WoWcM53+9d5ROe5M8oRMhinnRM A+6W7YLSaEwqdCJ3jAn/9JWF7bj1/oQBdbcYFXq7BFL8T58Y4lnrIl2qjY+GRcG71jniCuIw0B99ii/mhf8uJpvI FtDk929dJP2kXAcRZmvIREVlv2c3NPBJS/I19Dr4V3fjDNLx+zqz887rmT7twQVPN3ILY4OzIuyc5osufZzuFPV mxon/i7MBF3hLGix+SbSLnUu49T0zM8qDJ
	Dekripsi	[{"id":"1","nama_tanaman":"Kangkung","tempat":"D.2.F","spesifikasi":"Vertikal","id_user_input":"1","created_a ":"2019-09-18 11:00:00","update_at":"2019-11-25 03:11:10"},{"id":"2","nama_tanaman":"Sawi","tempat":"D.2.A","spesifikasi":"Horizontal","id_user_input":"2","c eated_at":"2019-09-18 13:00:00","update_at":"2019-11-25 04:47:58"}]
Galeri	Plainteks	"RGB_id": "3", "id_tanaman": "1", "RGB_name_file": "image/2020-05-1_2248masking.png","path_file": "rgbImage/image/2020-05-31_2248masking.png" "RGB_timestamp": "2020-05-31 22:48:57" "RGB_value_extract": "rgbImage/2020-05-31_2249histogram.jpg","RGB_id": "2", "id_tanaman": "1", "RGB_name_file": "image/2020-05-31_2245masking.png"."path_file": "rgbImage/image/2020-05-31_2245masking.png", "RGB_timestamp": "2020-05-31 22:45:26", GB_value_extract": "rgbImage/2020-05-31_2245histogram.jpg", "RGB_id": "1", "id_tanaman": "1", "RGB_name_file": "1", "path_file": "1", "RGB_timestamp": "2020-05-31 22:31:28","RGB_value_extract":"1"
	Enkripsi	VoehOhGV1Jc4lC006csEfawGBQi4Y6AcO/lJ/9o2vUW3JW5ktHJbXYzbICNGFZ0pbQ0hWi5kWSbVCM8Wm aeiyzqUsE9b3AQ+KePdILIiZRmhbvacJ717vrXFHM2RtTLu2+wJoqN8RLoRpL2UxVkqWz3+uWc7S82YBIEp oSFCm7fnTKupXstlP3sNYgTDno9NcP5pp7DExqYkOlg218dDV+RHbtQ2aV3uJNnLJIK26UntPJbRtRlO8f+cM Y9xSBW3tl99NBWQYH7FAqebG3tWUktcTaDutg2uzN4Rko+/0PUKGXE4WZZ2yzYI9B2ENJwEgtcx+8hxE3 O5TOvYHDgtMNlpVAdK6pPOrYaLD6nno/lREGhKbFODBwmf3RBYBdILpzRAfQKssN1dU93uvzWjj2V93S GkbczyysLQZbSWUh9rz1PVBUl030muzB7/H/m6oitCaFQyQ3M4wrxJAoKvipEal874//cwGIZUzIGtpY+SNb17 R8FM+U6G3Oau3Me7KiDDhrEXUZx/IOkNRxxLXbQqT7mhd5ZxXTC:ZmVkY2JhOTg3NjU0MzIxMA==
	Dekripsi	"RGB_id": "3", "id_tanaman": "1", "RGB_name_file": "image/2020-05-31_2248masking.png","path_file": "rgbImage/image/2020-05-31_2248masking.png" "RGB_timestamp": "2020-05-31 22:48:57" "RGB_value_extract": "rgbImage/2020-05-31_2249histogram.jpg","RGB_id": "2", "id_tanaman": "1", "RGB_name_file": "image/2020-05-31_2245masking.png"."path_file": "rgbImage/image/2020-05-31_2245masking.png", "RGB_timestamp": "2020-05-31 22:45:26", GB_value_extract": "rgbImage/2020-05-31_2245histogram.jpg", "RGB_id": "1", "id_tanaman": "1", "RGB_name_file": "1", "path_file": "1", "RGB_timestamp": "2020-05-31 22:31:28","RGB_value_extract":"1"

Setiap proses enkripsi dekripsi IoT android dilakukan menggunakan sebuah kunci yang sama. Seluruh data uji coba menghasilkan AE di atas 50%, di mana AE terendah yaitu 50,37% dan tertingi 58,01%. Nilai entropy seluruh data uji coba .atas enam dengan nilai tertinggi yaitu 6.4521. Tetapi pada penelitian ini belum dicapai entropy sempurna mendekati nilai 8. Alat uji lain yang digunakan adalah entropy. Eksperimen dengan entropy menunjukkan hasil mendekati nilai tertinggi. Metode ini memiliki ukuran ruang kunci K di mana nilai entropy terbaik adalah 8 [30]. Semakin besar nilai entropy [31], maka semakin sulit memecahkan *ciphertext*. Perhitungan entropy dapat dilakukan dengan rumus (3).

$$H\ (X) = \sum_{i=0}^{n} a_i\ ^2 log(p(S_i)) \quad (3)$$

Menurut rumus 3, *X* adalah pesan, *Si* adalah simbol pada pesan, $p(S_i)$ adalah peluang terjadinya S_i dan a_i adalah banyaknya kemunculan S_i.

Alat uji ketiga yaitu *Bit Error Ratio (BER)*. *BER* digunakan untuk menghitung jumlah perbedaan bit pada teks dekripsi dengan *plaintext* asli. Dalam penelitian ini dihasilkan nilai BER = 0. Berdasarkan [32], nlai 0 menunjukkan bahwa tidak terdapat kesalahan dalam proses dekripsi dan teks dekripsi sama persis dengan dengan teks asli. Pada Tabel 3, pengujian menggunakan teks asli dari *database* telah diuji coba. Berdasarkan tabel tersebut dapat dibandingkan *plaintext* dan teks hasil dekripsi. Seluruh data dari sampel tool *Sensor2*, tanaman dan Galeri menghasilkan tampilan *plaintext* dan teks dekripsi yang sama persis.

4. Kesimpulan

Berdasarkan hasil pengujian sistem enkripsi yang diimplementasikan pada aplikasi hidroponik menggunakan algoritma 128-bit *Advanced Encryption Standard (AES)*, dapat disimpulkan bahwa algoritma AES cocok untuk diterapkan dalam mengamankan data yang terdapat pada sistem/*database*. Proses enkripsi dilakukan untuk menghasilkan data yang tidak mudah dibaca dan tidak mudah diretas oleh orang lain kecuali mereka memiliki kunci untuk mendekripsi data tersebut. Kunci yang digunakan untuk mengenkripsi dan mendekripsi sama. Jika kunci yang digunakan sama maka data dapat digunakan, tetapi jika berbeda maka hasilnya tidak akan terbaca. Pada penelitian ini, telah dilakukan uji coba dan evaluasi *Advanced Encryption Standard (AES)*. Algoritma tersebut dapat bekerja secara lintas *platform* yaitu menyembunyikan data pada saat proses pengiriman dari server ke *Android* dengan benar dan aman. Berdasarkan penelitian yang telah dilakukan, terdapat hasil yang kurang maksimal yaitu nilai entropy yang belum sempurna yaitu masih berkisar pada angka 6.1 sampai 6.4 dan diharapkan dapat menghasilkan nilai sempurna yaitu 8. Pada penelitian selanjutnya diharapkan nilai pengujian dapat optimal dengan menggunakan algoritma simetris atau asimetris lain. Jumlah data yang lebih banyak dan pengukuran hasil dalam rentang waktu yang lebih lama. Penelitian selanjutnya juga dapat dilakukan dengan menggabungkan AES dan algoritma transposisi untuk melakukan teknik super enkripsi dengan tujuan peningkatan keamanan data.

Ucapan Terimakasih

Penelitian ini terselenggara atas bantuan Universitas Dian Nuswantoro dalam memberikan kesempatan pada penulis untuk menggunakan Laboratorium Rekayasa Perangkat Lunak dan *Database* (RPLD) khususnya dalam pengembangan metode tepat guna *IoT* Tanaman Kangkung.

Ucapan Terimakasih

Penelitian ini terselenggara atas bantuan Universitas Dian Nuswantoro dalam memberikan kesempatan pada penulis untuk menggunakan Laboratorium Rekayasa Perangkat Lunak dan *Database* (RPLD) khususnya dalam pengembangan metode tepat guna *IoT* Tanaman Kangkung.

Daftar Rujukan

[1] Winder Davey. (2019, July) Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach. [Online]. https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/#230e8b36411c

[2] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, 2017.

[3] Sarada Prasad Gochhayat et al., "Reliable and Secure Data Transfer in IoT Networks," *Wireless Networks : The Journal of Mobile Communication,Computation and Information*, 2019.

[4] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, and Rabah Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Computer Networks Vol 133, Issue 14*, pp. 141-156, 2018.

[5] Xinlei Wang, Jianqing Zhang, Eve M. Schooler, and Mihaela Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," in *IEEE International Conference on Communications (ICC)*, Sydney, NSW, Australia, 2014.

[6] Kun Lin Tsai et al., "AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments," *IEEE Access Vol 6, Topic: Security and Trusted Computing for Industrial Internet of Things*, pp. 45325-45334, 2018.

[7] Ritambhara, Alka Gupta, and Manjit Jaiswal, "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT)," in *International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, India, 2017.

[8] Ali Akbar Pammu, Kwen-Siong Chong, Weng-Geng Ho, and Bah-Hwee Gwee, "Interceptive side channel attack on AES-128 wireless communications for IoT applications," in *IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Jeju, South Korea, 2016.

[9] Weize Yu and Selcuk Kose, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers (Volume: 64 , Issue: 11)*, 2017.

[10] Noveline Aziz Fauziah, Eko Hari Rachmawanto, De Rosal Ignatius Moses Setiadi, and Christy Atika Sari, "Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application," in *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia, 2018, pp. 146-151.

[11] B.K.S. Rajaram and Krishna Prakash N, "Secure MQTT using AES for Smart Homes in IoT Network," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, pp. 483-485, 2019.

[12] Turki Ali Alghamdi, Ishtiaq Ali, Nadeem Javaid, and Muhammad Shafiq, "Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain," *IEEE Access Vol 8*, pp. 1048-1061, 2019.

[13] Wiwin Styorini and Dwi Harinitha, "Analisis Performansi Algoritma AES dan Blowfish Pada Aplikasi Kriptografi," in *Seminar Nasional*, pp. 1-6.

[14] Aji Fitrah Marisman and Anita Hidayati, "PEMBANGUNAN APLIKASI PEMBANDING KRIPTOGRAFI DENGAN CAESAR CIPHER DAN ADVANCE ENCRYPTION STANDARD," *Jurnal Penelitian Komunikasi dan Opini Publik*, vol. 19, no. 3, pp. 213-222, Desember 2015.

[15] Fernando Fernando and Lukas Lukas, "IMPLEMENTASI DAN ANALISIS LIGHTWEIGHT CRYPTOGRAPHY UNTUK INTERNET OF THINGS (IOT)," *JURNAL ELEKTRO*, vol. 10, no. 2, pp. 85-94, Oktober 2017.

[16] Resianta Perangin-angin, Indra Kelana Jaya, Benget Rumahorbo, and Berlian Juni R. Marpaung, "Analisa Alokasi Memori dan Kecepatan Kriptograpi Simetris Dalam Enkripsi dan Dekripsi," *INFORMATION SYSTEM DEVELOPMENT [ISD]*, vol. 4, no. 1, pp. 11-16, Januari 2019.

[17] Duy-Hieu Bui, Diego Puschini, Simone Bacles-Min, Edith Beigné, and Xuan-Tu Tran, "Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications," in *International Conference on IC Design and Technology (ICICDT)*, Ho Chi Minh City, Vietnam, 2016, pp. 1-4.

[18] Eko Hari Rachmawanto, Khabib Prasetyo, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, and Nova Rijati, "Secured PVD Video Steganography Method based on AES and Linear Congruential Generator," in *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia, 2018, pp. 163-167).

[19] Mutia Rizky Ashila, Nur Atikah, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, and Christy Atika Sari, "Hybrid AES-Huffman Coding for Secure Lossless Transmission," in *Fourth International Conference on Informatics and Computing (ICIC)*, Semarang, Indonesia, 2019.

[20] Ioannis Georgiadis, Michael Dossis, and Sotirios Kontogiannis, "Performance evaluation on IoT devices secure data delivery processes," in *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, Athens, Greece, 2018, pp. 306–311.

[21] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić, "Distinguisher and Related-Key Attack on the Full AES-256," in *Advances in Cryptology - CRYPTO 2009. Lecture Notes in Computer Science, vol 5677*. Berlin, Heidelberg: Springer, 2009, pp. 231-249.

[22] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir, "Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds," in *nternational Conference on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg., 2010, pp. 299-319.

[23] Bawna Bhat, Abdul Wahid Ali, and Apurva Gupta, "DES and AES performance evaluation," in *International Conference on Computing, Communication & Automation*, Noida, India, 2015, pp. 887-890.

[24] Simon Heron, "Advanced Encryption Standard (AES)," *Network Security Vol 2009 Issue 12*, pp. 8-12, 2010.

[25] Ibnu Utomo Wahyu Mulyono, Ajib Susanto, Muhamad Rizky Fajar Febrian, and Ghaitsa Ardelia Rosyida, "A Combination of Hill Cipher and LSB for Image Security," *Scientific Journal of Informatics, Vol. 7, No. 1*, pp. 155-165, 2020.

[26] Amish Kumar and Namita Tiwari, "Effective Implementation and Avalanche Effect of AES," *International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4*, pp. 31-35, 2012.

[27] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect," *IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1*, pp. 106-111, 2011.

[28] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature Communications*, pp. 1-11, 2018.

[29] Bobby Jasuja and Abhishek Pandya, "Crypto-Compression System: An Integrated Approach," *International Journal of Computer Applications, Vol 116, No 21*, pp. 34-41, 2015.

[30] Amandeep Singh, Praveen Agarwal, and Mehar Chand, "Image Encryption and Analysis using Dynamic AES," in *5th International Conference on Optimization and Applications (ICOA)*, Kenitra, Morocco, 2019, pp. 1-6.

[31] Georgios Makris and Ioannis Antoniou, "Chaos Cryptography with prescribed Entropy Production," in *International Electronic Conference on Entropy and Its Applications*, 2015, pp. 1-17.

[32] O. Shoewu and Segun O. Olatinwo, "Securing Text Messages using Elliptic Curve Cryptography and Orthogonal," *The Pacific Journal of Science and Technology, Volume 14. Number 2*, pp. 220-227, 2013.