Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202296767
Vol. 9, No. 7, Desember 2022, hlm. 1787-1794 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

IMPLEMENTASI ALGORITMA MICKEY 2.0 UNTUK MENGAMANKAN KOMUNIKASI DATA PADA PERANGKAT *BLUETOOTH LOW ENERGY*

Amelia Dwi Rochani[1], Ari Kusyanti*[2], Fariz Andri Bakhtiar[3]

[1,2,3]Universitas Brawijaya, Malang
Email: [1]ameliadwirochani27@gmail.com, [2]ari.kusyanti@ub.ac.id, [3]fariz@ub.ac.id
*Penulis Korespondensi

(Naskah masuk: 08 Desember 2022, diterima untuk diterbitkan: 27 Desember 2022)

Abstrak

Kondisi *Internet of Things* saat ini yang cenderung tanpa menggunakan fitur keamanan dapat menjadi tantangan untuk realisasi *Internet of things* terutama di bidang privasi dan kerahasiaan data, khususnya pada modul sensorik berdaya rendah yaitu *Bluetooth Low Energy*. Adanya celah keamanan pada *Bluetooth Low Energy* menjadi perhatian besar di jaringan *Internet of Things* saat ini, terutama yang terhubung dengan jaringan *public*. Data dari perangkat dapat diretas dan dimodifikasi oleh peretas. Dengan menerapkan algoritma enkripsi pada perangkat *Bluetooth Low Energy* dapat menjamin aspek *confidentiality* data serta dapat mencegah peretas menyadap dan mencuri data. Pada penelitian ini digunakan algoritma Mickey 2.0 untuk melakukan enkripsi. Algoritma ini berhasil melewati proyek eStream dan menjadi kandidat ideal untuk perangkat berkonsumsi daya rendah. Data yang diamankan berasal dari sensor DHT11 yang dikirim menggunakan protokol *Bluetooth Low Energy*. Sebelum dikirim dilakukan enkripsi pada sisi *server* menggunakan algoritma Mickey 2.0 dan proses dekripsi akan dilakukan pada sisi *Client.* Hasil *keystream* akan divalidasi terlebih dahulu pada pengujian *test vector*. Untuk mengetahui tingkat keamanan dilakukan pengujian serangan pasif *sniffing* dan serangan aktif *Known Plaintext Attack* (KPA). Serangan pasif dan serangan aktif yang dilakukan tidak berhasil mendapatkan *plaintext*.

Kata kunci: *Algoritma Mickey 2.0, Bluetooth Low Energy, confidentiality, enkripsi*

IMPLEMENTATION OF THE MICKEY 2.0 ALGORITHM TO SECURE DATA COMMUNICATIONS ON BLUETOOTH LOW ENERGY DEVICES

Abstract

The current condition of the Internet of Things tends to be without the use of security features, especially in the field of privacy and data confidentiality, especially in the low power sensor module i.e. Bluetooth Low Energy. The existence of security holes in Bluetooth Low Energy is a big concern for Internet of Things networks, especially those connected to public networks. Data from the device can be hacked and modified by hackers. By implementing encryption algorithms on Bluetooth Low Energy devices it can guarantee data confidentiality aspects and can prevent hackers from eavesdropping and stealing data. In this research, Mickey 2.0 algorithm is used for encryption. This algorithm successfully passed the eStream project and became an ideal candidate for low power consumption devices. The secured data comes from the DHT11 sensor which is sent using the Bluetooth Low Energy protocol. Before sending data, encryption is performed on the server side using the Mickey 2.0 algorithm and the decryption process will be carried out on the Client side. The keystream results will be validated first in the test vector test. To determine the level of security, a passive sniffing attack and an active Known Plaintext Attack (KPA) were tested. Passive attacks and active attacks do not get the plaintext.

Keywords: *Mickey 2.0, Bluetooth Low Energy, confidentiality, encryption*

1. PENDAHULUAN

Enkripsi merupakan bagian penting dalam penerapan jaringan berbasis *Internet of things*. Dalam skema enkripsi, pengirim mengenkripsi data yang hanya dapat didekripsi dan dibaca oleh penerima dengan tujuan agar data yang dikirim aman dari penyerang. Meningkatnya jumlah perangkat yang terhubung melalui *Internet of Things* menyebabkan tingginya kemungkinan gangguan digital atau kekacauan selama perangkat tersebut

beroperasi (Nawir et al., 2016). Tidak adanya proteksi pada perangkat IoT bukanlah pilihan yang tepat, pesan yang tidak terenkripsi seharusnya tidak boleh digunakan untuk mentransfer data yang berharga bagi pengguna (Zhang & Liang, 2017).

Kondisi *Internet of Things* saat ini yang cenderung tanpa menggunakan fitur keamanan dapat menjadi tantangan utama untuk realisasi *Internet of things* terutama di bidang privasi dan kerahasiaan data. Proses enkripsi pada perangkat *Internet of Things* juga membutuhkan sumber daya komputasi dan memori khususnya modul sensorik yang menggunakan *Bluetooth* (Weber & Boban, 2016). Penelitian yang berjudul *"Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey"* menyajikan taksonomi komprehensif untuk masalah keamanan dan privasi BLE. Proses *pairing* yang tidak aman, otentikasi yang tidak tepat, dan kurangnya kriptografi yang sesuai membuat perangkat BLE rentan terhadap penyadapan, *Man-In-The-Middle* (MITM), dan serangan lainnya (Barua et al., 2022). Adanya kerentanan pada perangkat BLE, keamanan telah menjadi perhatian besar untuk perangkat BLE di jaringan *Internet of Things* saat ini, terutama yang terhubung dengan jaringan *public.* Data dari perangkat dapat diretas dan dimodifikasi oleh peretas yang ada di jaringan *public* maupun jaringan *private*.

Berdasarkan permasalahan di atas diperlukan mekanisme keamanan pada komunikasi *Bluetooth Low Energy* yang dapat mencegah *attacker* menyadap dan mencuri data pribadi pengguna. Setidaknya perangkat harus memenuhi fitur *Pairing,* Enkripsi, dan*, Informative UI* untuk melindungi transmisi data (Zhang & Liang, 2017). *Pairing* melibatkan pertukaran paket *Security Manager Protocol (SMP)* untuk menghasilkan kunci sementara yang disebut *Short Term Key* (STK). STK ini akan digunakan untuk mengenkripsi koneksi & komunikasi antara dua perangkat (Townsend et al., 2014).

Penelitian yang berjudul "*Bluetooth Low Energy Security Vulnerability and Improvement Method*" mengusulkan metode peningkatan keamanan dengan meningkatkan panjang *Temporary Key*. Penelitian tersebut menyatakan bahwa *Bluetooth Low Energy* memiliki kerentanan pada *Temporary Key* karena ukurannya yang pendek. *Temporary Ke*y sendiri digunakan untuk menghasilkan *Short Term Key* (STK) yaitu kunci enkripsi dalam proses *pairing.* Butuh waktu lama untuk memecahkan *encryption key* ketika metode tersebut digunakan. Meskipun butuh waktu lama untuk memecahkan *encryption key, attacker* masih bisa menemukan celah pada *encryption key* tersebut (Giwon et al., 2016). Hal ini dapat diartikan bahwa proses *pairing* pada *Bluetooth Low Energy* tidak mengatasi masalah keamanan komunikasi data dan beresiko keamanan pada perangkat *Bluetooth Low Energy.*

Dalam *Bluetooth Low Energy* hampir semua konsep keamanan seperti *Authentication, Integrity, dan Confidentiality* didasarkan pada proses *pairing.* Namun komunikasi pesan antara perangkat BLE dan aplikasi pada *gateway* tidak terenkripsi berarti penyerang bisa saja menyadap data dengan menggunakan *packet sniffer* (Zhang, 2017). Algoritma Mickey 2.0 dapat mengatasi masalah keamanan sistem khususnya pada perangkat berdaya rendah seperti BLE, algoritma ini berhasil melewati proyek eStream dan menjadi kandidat ideal untuk perangkat berkonsumsi daya rendah. Mickey 2.0 merupakan algoritma *synchronous stream cipher* dirancang untuk diimplementasikan pada perangkat keras. Pada web eStream terdapat artikel, *source code* yang didalamnya terdapat *test vector,* serta berbagai informasi dari algoritma Mickey 2.0. Artikel tersebut berjudul "*The Stream cipher Mickey 2.0"* oleh Steve Babbage & Matthew Dodd mengenai *stream cipher* Mickey 2.0 tertulis bahwa Mickey 2.0 memiliki 80-bit key dan Inisialisasi vector dengan panjang hingga 80 bit. Mickey 2.0 tidak dirancang untuk perangkat lunak berkecepatan tinggi, dan implementasinya cukup efisien (Babbage & Dodd, 2006).

Penerapan algoritma enkripsi pada perangkat *Bluetooth Low Energy* bertujuan menjamin aspek *confidentiality* data. Data dari sensor yang dikirim menggunakan protokol *Bluetooth Low Energy* akan diamankan sebelum dikirim dengan melakukan enkripsi pada sisi *server* menggunakan Algoritma Mickey 2.0 dan proses dekripsi akan dilakukan pada sisi *client.* Sistem BLE yang digunakan terdiri dari mikrokontroler *server* yang akan mengirimkan data sensor dan mikrokontroler *client* yang menerima data sensor.

2. LANDASAN KEPUSTAKAAN

2.1. Kriptografi

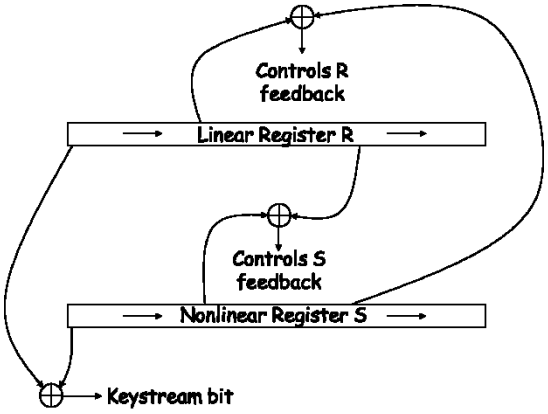
Kriptografi dapat didefinisikan sebagai seni menulis atau memecahkan kode. Definisi dari kriptografi tidak hanya berfokus pada kode–kode yang telah digunakan berabad–abad untuk memungkinkan komunikasi rahasia, melainkan kriptografi saat ini mencakup banyak hal yaitu berkaitan dengan mekanisme untuk memastikan integritas, teknik bertukar kunci rahasia, uang digital, dan untuk autentikasi (Katz & Lindell, 2015). Dalam buku yang berjudul *HandBook of Applied Crypthography* dijelaskan ada empat tujuan dari keamanan informasi yaitu:

1. *Confidentiality*, menjamin kerahasiaan untuk menjaga informasi.
2. *Integrity,* menjamin integritas data untuk menghindari manipulasi data.
3. *Authentication,* mengidentifikasi dua pihak yang saling melakukan komunikasi.

4. *Non-repudiation,* mencegah suatu entitas untuk menyangkal komitmen dari tindakan yang sebelumnya dilakukan (Menezes et al., n.d.).

2.2. Algoritma Mickey 2.0

Mickey 2.0 salah satu portofolio dari proyek eSTREAM yang bertujuan untuk mengidentifikasi *stream cipher* baru, Mickey 2.0 merupakan algoritma kriptografi *synchronous stream cipher* dirancang oleh Steve Babbage dan Matthew Dodd. Algoritma Mickey 2.0 ditujukan untuk platform perangkat keras yang memiliki sumber daya terbatas serta dimaksudkan untuk memiliki kompleksitas perangkat keras yang rendah dan memberikan tingkat keamanan yang tinggi. Mickey 2.0 memiliki dua parameter input 80-bit *secret key* dan *Initialisation variable* panjangnya antara 0 dan 80 bit.



Gambar 1. Arsitektur Variabel *Clocking* Algoritma Mickey 2.0

Gambar 1 merupakan variabel arsitektur *clocking* pada algorima Mickey 2.0 terdapat dua register sebagai komponen dasar untuk *keystream generation,* register ini di inisialisasi dengan menggabungkan 80-bit *key* dan 80-bit *Initialization Value* (IV). Register R merupakan register linier, register S merupakan register non linier. Register didefinisikan sebagai n, untuk Mickey 2.0 terdapat 100 register yang berarti panjang register $R = r_0 \dots r_{99}$ dan $S = s_0 \dots s_{99}$ untuk bit register. Dalam setiap siklus *clock* dikendalikan oleh bit *control* yang terdapat dalam setiap register, masing – masing yaitu C_R C_S. Proses *clock* dari register R dan S akan menghasilkan *keystream* bit.

2.3. *Bluetooth Low Energy*

Bluetooth Low Energy (juga disebut *Bluetooth Smart*) adalah teknologi inovatif yang dikembangkan oleh *Bluetooth Special Interest Group* (SIG), bertujuan untuk menjadi alternatif terbaik dari teknologi nirkabel yang sudah ada seperti IEEE 802.11b (Wi-Fi), Zigbee, ANT+, dan *Bluetooth Classic* (*Bluetooth* 3.0, BR/EDR). Karena memiliki kinerja yang baik dalam segi konsumsi daya yang rendah maupun fungsionalitasnya, menjadikan BLE sangat tepat diterapkan dalam *teknologi Internet of Things* (Tosi et al., 2017).

Dalam *Bluetooth Low Energy* terdapat *Security Manager (SM)* yang merupakan protokol dan serangkaian algoritma keamanan yang dirancang untuk menghasilkan dan bertukar kunci keamanan. Dalam *Security Manager* mendefinisikan dua peran yaitu sebagai *Initiator* dan *Responder,* selain itu terdapat 3 prosedur keamanan di *Security Manager* antara lain :

1. *Pairing*, prosedur di mana *Temporary Key* dihasilkan.
2. *Bonding*, merupakan serangkaian *pairing* yang diikuti oleh pembuatan dan pertukaran kunci permanen yang disimpan dalam memori non-volatile
3. *Encryption Re-establishment,* prosedur ini menentukan cara menggunakan kunci–kunci dalam koneksi berikutnya untuk membangun kembali koneksi yang aman dan terenkripsi tanpa harus melalui prosedur *pairing* atau *bonding* lagi (Townsend et al., 2014).

2.4. ESP32

ESP32 merupakan serangkaian chip mikrokontroler dengan daya rendah, memiliki kemampuan *Bluetooth* dan Wi-Fi maka dari itu ESP32 sangat populer di berbagai proyek yang terkait dengan IoT. ESP32 dirilis untuk menggantikan mikrokontroler sebelumnya yaitu ESP8266, ESP32 memiliki kinerja jauh lebih baik daripada ESP8266 (Maier et al., 2017). Pada Gambar 2 merupakan wujud dari modul ESP32.

Gambar 2. Perangkat ESP32

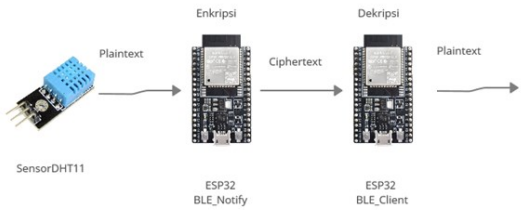
3. METODE PENELITIAN

Bab metodologi penelitian kerangka penelitian yang digunakan meliputi studi literatur, analisis kebutuhan dan perancangan sistem, implementasi sistem, pengujian dan sistem, pengambilan kesimpulan dan saran.

3.1. Perancangan Sistem

Sistem yang digunakan dalam penelitian ini merupakan perangkat *Bluetooth Low Energy* yang

terhubung secara *node to node* karena komunikasi yang digunakan berupa *Client* untuk menerima data dan *server* yang mengirimkan notify kepada *Client.*



Gambar 3. Gambaran umum sistem

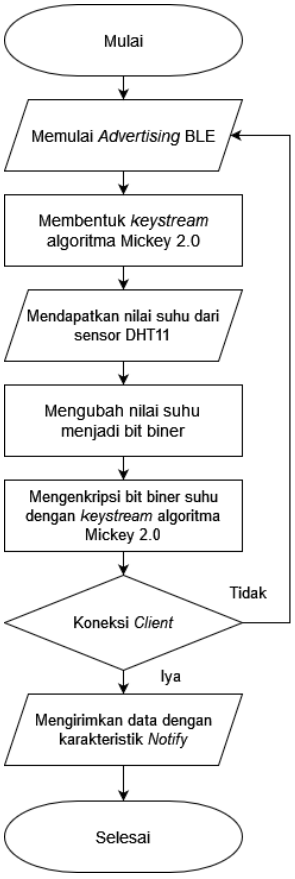
Gambar 3 adalah gambaran umum sistem. Sensor DHT11 digunakan untuk menghasilkan data suhu yang diamankan dengan algoritma Mickey 2.0. Terdapat perangkat esp32 BLE_Notify digunakan sebagai *server* yang akan mengirimkan data sensor DHT11 berupa *plaintext* ke BLE_*Client*. Penggunaan sensor DHT11 dikarenakan mempunyai stabilitas pembacaan nilai yang baik dan kalibrasi nilai yang akurat, DHT11 memberikan nilai suhu dan kelembapan yang sangat tepat dan memastikan *reliability* tinggi dan stabilitas dalam jangka panjang. Sensor ini memiliki komponen pengukur kelembapan tipe resistif dan komponen pengukur suhu tipe NTC *(Negative Temperature Coefficient)* yang memiliki respon cepat dan hemat biaya (Srivasta et al., 2018). Didalam BLE_Notify terdapat proses menghasilkan *keystream* algoritma Mickey 2.0 untuk mengenkripsi nilai dari sensor DHT11 dan perangkat esp32 BLE_*Client* berperan sebagai *client*. Hasil enkripsi dari BLE_Notify selanjutnya akan dikirimkan ke BLE_*Client* berupa *ciphertext*. Lalu BLE_*Client* mendekripsi mengunakan *key* yang sama dengan proses enkripsi dan hasil dekripsi ditampilkan ke *client*.

4. IMPLEMENTASI

Implementasi terbagi menjadi implementasi sistem *Bluetooth Low Energy* dan implementasi algoritma Mickey 2.0. Implementasi sistem meliputi Implementasi *Ble_notify* sebagai *server* dan *Ble_ Client* sebagai *client.*

4.2. BLE_Notify

Sistem Ble_Notify berperan sebagai *server* bertugas untuk proses menghasilkan *keystream* dan enkripsi berupa data yang diambil dari sensor DHT11. Alur dari sistem akan dijelaskan pada Gambar 4 di bawah ini:

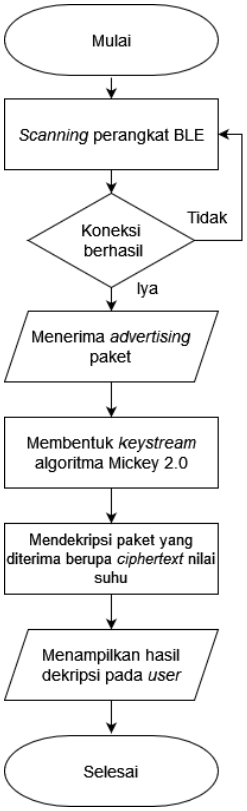


Gambar 4. Alur BLE_Notify

Gambar 4 merupakan alur sistem BLE_Notify, diawali dengan memulai *advertising* BLE untuk memberitahu keberadaannya. Setelah itu membentuk *keystream* algoritma Mickey 2.0 yang berupa bit biner dan mendapatkan nilai suhu dari sensor DHT11, data dari sensor yang didapatkan berupa *integer* dan diubah terlebih dahulu menjadi bit biner untuk proses enkripsi dengan meng-xor kan nilai suhu dan *keystream* algoritma mickey 2.0. Setelah *ciphertext* didapatkan sistem akan memulai koneksi ke *client*. Jika koneksi *client* tidak terhubung maka akan mengulang dari proses *advertising* BLE, sebaliknya jika terhubung dengan *client* maka sistem akan mengirimkan data dengan karakteristik Notify().

4.3. BLE_*Client*

Sistem Ble_*Client* berperan sebagai *client* bertugas untuk proses menghasilkan *keystream* dan dekripsi berupa *ciphertext* yang diterima dari *server.* Alur dari sistem akan dijelaskan pada Gambar 5 di bawah ini:



Gambar 5. Alur BLE_*Client*

Gambar 5 merupakan alur sistem BLE_*Client*, diawali dengan proses *scanning* bertujuan untuk memindai atau mencari layanan di sekeliling untuk menemukan *server*. Lalu akan dilakukan pencarian karakteristik dari layanan *server* sekitar dan setelah menemukan perangkat yang dicari maka sistem akan menerima paket dari *server* berupa *ciphertext*. Sistem akan membentuk *keystream* algoritma mickey 2.0 untuk mendekripsi paket yang diterima. Proses dekripsi dilakukan dengan meng-xor-kan *ciphertext* dengan *keystream* untuk selanjutnya ditampilkan hasil dekripsi pada *user*. Jika proses *scanning* tidak menemukan perangkat dengan layanan dan karakteristik yang dicari maka sistem akan mengulang proses *scanning* kembali.

5. PENGUJIAN DAN PEMBAHASAN

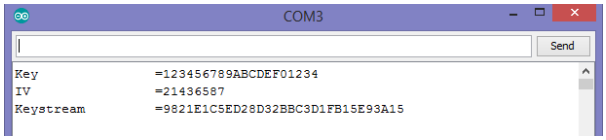
5.1 Pengujian *Test Vector*

Prosedur pengujian *test vector* untuk algoritma Mickey 2.0 dengan cara memasukkan nilai *Key* dan IV yang sesuai dengan jurnal algoritma Mickey 2.0 oleh Steve Babbage & Matthew Dodd ke dalam sistem.

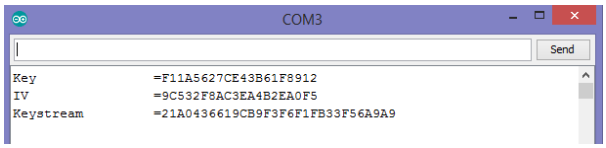
Tabel 1 adalah skenario pengujian *test vector* yang dimasukkan sebagai variabel masukan yang merujuk pada jurnal Mickey 2.0.

Tabel 1. Skenario Pengujian *Test Vector*

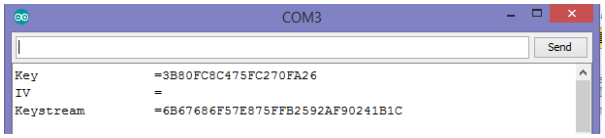
Skenario	*Key*	IV	*Keystream*
1	12 34 56 78 9a bc de f0 12 34	21 43 65 87	98 21 e1 0c 5e d2 8d 32 bb c3 d1 fb 15 e9 3a 15
2	f1 1a 56 27 ce 43 b6 1f 89 12	9c 53 2f 8a c3 ea 4b 2e a0 f5	21 a0 43 66 19 cb 9f 3f 6f 1f b3 03 f5 6a 09 a9
3	3b 80 fc 8c 47 5f c2 70 fa 26	-	6b 67 68 6f 57 0e 87 5f fb 25 92 af 90 24 1b 1c



Gambar 6. Hasil *Test Vector* Skenario 1



Gambar 7. Hasil *Test Vector* Skenario 2

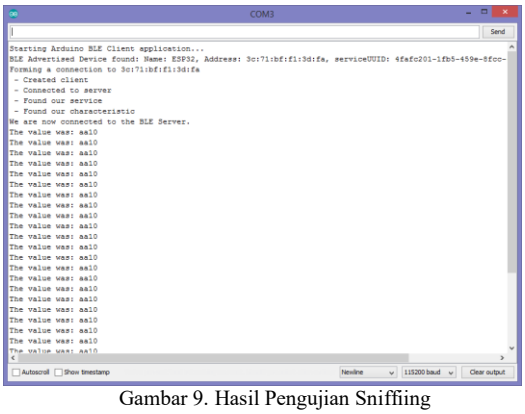


Gambar 8. Hasil *Test Vector* Skenario 3

Gambar 6, 7, dan 8 adalah hasil pengujian *test vector*, dari tiga skenario yang telah dilakukan *keystream* yang dihasilkan sama dengan *test vector* yang ada pada jurnal Mickey 2.0 dan pengujian ini dapat dinyatakan valid.

5.2 Pengujian Keamanan Serangan Pasif

Pengujian keamanan pasif dilakukan *sniffing* pada perangkat *server* dengan menggunakan mikrokontroler sebagai *Client* yang tidak memiliki *keystream* dari algoritma Mickey 2.0.



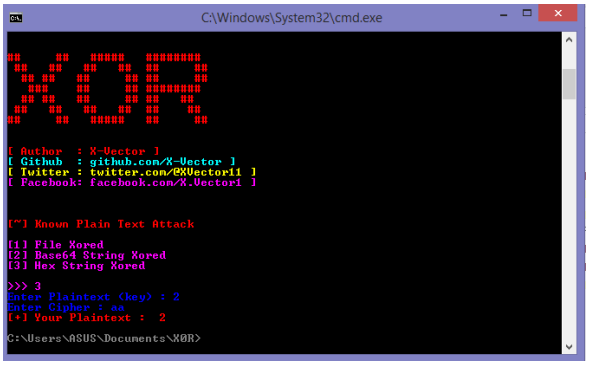
Gambar 9. Hasil Pengujian Sniffiing

Hasil pengujian *sniffing* pada gambar 9 berupa *ciphertext* heksadesimal yaitu aa10, akan tetapi *sniffer* tidak memiliki *keystream* yang sesuai untuk melakukan dekripsi, sehingga data yang diterima tidak dapat didekripsikan menjadi *plaintext.*

5.3 Pengujian Keamanan Serangan Aktif

Pengujian keamanan serangan aktif dilakukan untuk memastikan keamanan sistem dari serangan aktif. Serangan aktif yang digunakan yaitu KPA (*Known Plaintext Attack*).

Penyerangan *Known Plaintext Attack* dilakukan dengan memasukan *plaintext* beserta *ciphertext* yang telah diketahui. Tujuannya adalah untuk mendapatkan *keystream* dari *ciphertext* dan bagian-bagian *plaintext* yang telah diketahui.



Gambar 10. Hasil Pengujian Serangan *Known Plaintext Attack*

Gambar 10 menunjukkan hasil pengujian serangan *Known Plaintext Attack*, serangan yang dilakukan tidak berhasil, karena dari beberapa *plaintext* dan *ciphertext* yang digunakan tidak menunjukkan nilai *plaintext* yang sesunguhnya pada sistem BLE.

6. KESIMPULAN DAN SARAN

6.1 KESIMPULAN

Dari keseluruhan penelitian yang dilakukan kesimpulan yang didapat sebagai berikut :

1. Mekanisme implementasi algoritma Mickey 2.0 pada perangkat *Bluetooth Low Energy* dimulai dari inisialisasi sampai proses clocking dari register S dan register R untuk menghasilkan bit *keystream*, dengan menggunakan dua sistem *Bluetooth Low Energy* yang berperan sebagai *Client* dan *server. Server* mengirimkan notifikasi data berupa *ciphertext* yaitu nilai suhu yang terenkripsi dengan algoritma Mickey 2.0 serta *Client* menerima data berupa *plaintext* yang terdekripsi dengan algoritma Mickey 2.0. Algoritma Mickey 2.0 telah dijalankan sesuai dengan prosedur yang ada pada jurnal Mickey 2.0 oleh Steve Babbage & Matthew Dodd
2. Hasil dari *test vector* terhadap *keytsream* yang dihasilkan oleh algoritma Mickey 2.0 sesuai dengan *test vector* jurnal Mickey 2.0 oleh Steve Babbage & Matthew Dodd sehingga pengujian *test vector* dinyatakan valid dan algoritma yang diimplementasikan pada sistem BLE berjalan dengan baik.
3. Algoritma Mickey 2.0 berhasil di implementasikan untuk pengamanan. Data dari *server* berhasil terenkripsi dan dapat didekripsi pada sisi *client* sehingga dapat melindungi dari serangan pasif *sniffing* dan serangan aktif *Known Plaintext Attack*.

6.2 SARAN

Berdasakan proses penelitian yang telah dilakukan untuk pengembangan penelitian selanjutnya, terdapat beberapa saran, yaitu:

1. Penelitian selanjutnya dapat mengembangkan variasi metode keamanan saat menggunakan algoritma Mickey 2.0 terutama untuk mencegah dari serangan *Known Plaintext Attack*.
2. Pengujian yang diterapkan untuk algoritma Mickey 2.0 lebih bervariasi.
3. Pada penelitian ini sistem masih dijalankan secara manual pada Arduino IDE, untuk penelitian selanjutnya diharapkan sistem ini dapat berjalan secara otomatis, sehingga mempermudah *user* untuk menggunakan sistem.

DAFTAR PUSTAKA

BABBAGE, S. & DODD, M., 2006. The stream cipher Mickey 2.0.

BARUA, A., AL AMIN, M.A., HOSSAIN, M.S. & HOSSAIN, E., 2022. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. *Barua, A., Al Alamin, M. A., Hossain, M. S., & Hossain, E. (2022). Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. IEEE Open Journal of the Communications Society.*

GIWON , K., JEEHYONG , K., JAEWON, N. & SUNGHYUN, C., 2016. Bluetooth low energy security vulnerability and improvement method. *IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, pp.(pp. 1-4).

KATZ, J. & LINDELL, Y., 2015. Chapman & Hall/CRC Cryptography and Network Security. In *INTRODUCTION TO MODERN CRYPTOGRAPHY (Second Edition)*.

MAIER, A., SHARP, A. & VAGAPOV, Y., 2017. Comparative analysis and practical implementation of the microcontroller module for the Internet of Things. *Proc.7th IEEE Int.Conference on Internet*

Technologies and Applications.

MENEZES, A.J., OORSCHOT, P.C.V. & VANSTONE, S.A., 1997. *HANDBOOK of APPLIED CRYPTOGRAPHY*. London NewYork: CRC Press.

NAWIR, M., AMIR, A., YAAKOB, N. & LYNN, O., 2016. Internet of Things (IoT): Taxonomy of security attacks. *International Conference on Electronic Design (ICED)*, pp.321-26.

SRIVASTA, D., KESARWANI, A. & DUBEY, S., 2018. Measurement of Temperature and Humidity by using Arduino Tool and DHT11. *International Research Journal of Engineering and Technology (IRJET)*, (5.12), pp.876-78.

TOSI, J. et al., 2017. Performance Evaluation of Bluetooth Low Energy:A Systematic Review. *Sensors*.

TOWNSEND, K., CUFFI , C., AKIBA & DAVIDSON, R., 2014. *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking*. O'Reilly Media, Inc.

WEBER, M. & BOBAN, M., 2016. Security challenges of the internet of things. *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp.638-43.

ZHANG, Q..&.L.Z., 2017. Security analysis of bluetooth low energy based smart wristbands. *International Conference on Frontiers of Sensors Technologies (ICFST)*, pp.(pp. 421-425).