**SA2-01A**

**DOKUMEN PRA PROPOSAL SKRIPSI**

|  |  |  |
| --- | --- | --- |
| Nama Mahasiswa | **:** | Winda Ayu Safitri |
| NIM | **:** | 155150207111083 |
| Jurusan | **:** | Teknik Informatika |
| Program Studi | **:** | Teknik Informatika |
| Keminatan | **:** | Jurusan TIF:   1. Prodi TIF Komputasi Berbasis Jaringan |
| Bidang Penelitian | **:** | Jurusan TIF:   1. Komputasi Berbasis Jaringan |
| Jenis Penelitian | **:** | Implementatif / ~~Non-Implementatif~~ \*) |
| Tipe Penelitian | **:** | Implementatif Pengembangan |
| Asal Judul Skripsi | **:** | ~~Usulan Sendiri~~ / Usulan Pembimbing \*) |
| Judul | **:** | IMPLEMENTASI ENKRIPSI PAYLOAD MENGGUNAKAN ALGORITMA GRAIN 128bit DENGAN PUBLISH / SUBSCRIBE BERBASIS IOT MIDDLEWARE |

|  |  |
| --- | --- |
| **Latar Belakang**  **(Maksimal 500 Kata dan Sitasi Penelitian atau fakta lapangan yang ada)** | *Internet of Things (IoT)* merupakan salah satu teknologi paling mutakhir yang ada di dunia saat ini. *IoT* merupakan sebuah konsep yang merujuk kepada suatu objek yang memiliki kemampuan untuk mengirimkan data dari perangkat ke perangkat lain tanpa harus ada campur tangan manusia. Komponen *IoT* terdiri dari sensor, *software*, perangkat (*Raspberry Pi, Arduino*), dan jaringan internet. Semua komponen tersebut saling terhubung untuk berkomunikasi dan melakukan pertukaran data (Xia, et al., 2012). *Internet of Things (IoT)* mengumpamakan dimana benda fisik dan benda digital (ponsel, tv, mobil) dapat dihubungkan melalui teknologi informasi dan komunikasi yang sesuai untuk memungkinkan berbagai aplikasi dan layanan (Razzaque, et al., 2016).  Upaya yang dilakukan untuk mengamankan data yang telah dikirim dalam komunikasi tersebut yakni melalui kriptografi. Kriptografi merupakan suatu ilmu yang digunakan untuk mengamankan data, mengacak data sedemikian rupa hingga data tidak dapat di baca oleh pihak yang tidak berwenang (Ekklesia, 2016). Algoritme yang dapat digunakan dalam proses enkripsi yaitu Algoritma Grain 128 bit. Algoritme 128 bit dipilih karena merupakan algotritme baru yang telah disahkan oleh NIST sebagai standart baru Stream cipher (NISTIR, 2016). Stream cipher merupakan jenis algoritme enkripsi simetri, enkripsi ini dilakukan dengan cara data plain text (data asli yang belum tersandi) diolah per satuan bit, data terkecil (Chitra Windayasari, 2008).  Untuk mengatasi masalah ini dibutuhkan sebuah *middleware* yang mampu mendukung interoperabilitas. Mohamed (2012), Fersi (2015) dan M. A. Razzaque (2016) mengartikan interoperabilitas sebagai kemampuan *middleware* untuk dapat digunakan oleh beragam jenis perangkat/teknologi/ aplikasi sebagai perantara untuk saling berkomunikasi dan bertukar data. *Middleware* menyediakan satu jenis *interface* bagi semua sensor untuk mengirimkan data serta menyediakan *service discovery* beserta API bagi aplikasi atau perangkat yang hendak membaca data dari sensor.  Dari penelitian sebelumnya yang dilakukan oleh Ala Al-Fuqaha (2015) dan (Tuwanut, 2015) tentang protokol pada IoT menyebutkan bahwa setidaknya terdapat tiga protokol utama yang digunakan dalam IoT. Protokol pertama yakni CoAP karena dapat digunkan pada perangkat dengan *resource* yang sangat terbatas.Selain itu protokol ini juga menerapkan semantik yang sama dengan HTTP. Protokol kedua yakni MQTT, protokol ini sangat tepat digunakan untuk komunikasi *Machine-to-Machine* atau untuk keperluan *real-time*. Protokol ini menerapkan pola *publish/subscribe* dalam implementasinya. Protokol ketiga yakni Websocket dimana protokol ini sangat tepat ketika digunakan untuk menghubungkan perngkat IoT seperti *middleware* dengan internet atau *cloud*.  Secara umum, middleware dapat memudahkan proses pengembangan dengan mengintegritaskan komputasi heterogen dan perangkat komunikasi dan pendukung interoperabilitas dalam beragam aplikasi dan layanan. Middleware mengabstraksikan kompleksitas system atau perangkat keras yang memungkinkan pengembangan aplikasi untuk memfokuskan semua usahanya pada tugas yang harus diselesaikan tanpa gangguan kekhawatiran *orthogonal* pada system atau perangkat keras Pada system ini juga menyediakan proses authentikasi untuk mengetahui bahwa seseorang / sender tersebut itu asli. (Razzaque, et al., 2016). |
| **Landasan Kepustakaan**  **(Maksimal 250 Kata)** | Pada beberapa penelitian yang berkaitan dengan topik penelitian yang akan dilakukan oleh penulis, yang pertama terdapat judul “*Implementasi Algortime Grain V1 Dan 128 Bit Pada Raspberry PI*”. Penelitian tersebut menggunakan algoritme Grain dalam pengaplikasian terhadap *hardware* yang berbeda kemudian menghasilkan *keystream*, tetapi tidak diterapkan untuk proses pengiriman data, yang kedua yaitu penelitian yang berjudul “*Implementasi Algoritma V1 Pada Protokol MQTT Menggunakan Raspberry Pi untuk Mengamankan Data IOT”* yang bertujuan untuk menghasilkan keystream dan diterapkan untuk proses pengiriman data. Sebelumnya juga terdapat penelitian yang berjudul “*Pengembangan IOT Middleware sebagai Gateway untuk Protokol COAP, MQTT, dan Websocket”* tetapi tidak sebagai pengiriman data yang telah diamankan. Landasan kepustakaan ini yang akan menjadi dasar pengembangan dan pengujian *middleware* pada penelitian kali ini. |
| **Rumusan Masalah**  **(diisi dalam bentuk numbering)** | 1. Bagaimana hasil dari test vector yang dihasilkan oleh algoritma grain 128 bit? 2. Bagaimana hasil autentikasi enenkripsi yang menerapkan algoritma grain 128 bit dengan publish / subscribe berbasis IoT middleware? 3. Bagaimana cara menerapkan algoritma grain 128 bit pada proses enkripsi berbasis IoT middleware? |
| **Metode yang digunakan untuk menyelesaikan permasalahan**  **(Maks 250 kata dan 1 Gambar Metode** | Metode yang digunakan dalam penelitian ini yaitu menggunakan middleware dan menyusun sebagaimana fungsinya. Hal yang pertama dilakukan adalah mengkonfigurasi media publisher dan menghubungkan *publisher* agar bias terhubung dengan *middleware* yang telah terpasang. *Publisher* nantinya akan menghasilkan gambar yang akan di enkripsi dengan algoritma yang telah ditentukan dan nantinya akan dikirim ke middleware sebagai pengujian apakah *middleware* tersebut mampu menerima file yang telah dikirim. Untuk memastikan apakah *publisher* itu dengan benar, maka akan rancang dengan *autentikasi*. *Autentikasi* ini dilakukan agar *subscriber* dapat benar – benar tau bahwa yang mengirim adalah *publisher.*  Identifikasi Masalah  Analisis Kebutuhan  Perancangan Sistem  Implementasi  Pengujian  Mulai  Kesimpulan dan Saran  Selesai |
| **Daftar Pustaka** | Chitra Windayasari, S. E. A., 2008. “*Analisis Dan Implementasi Algoritma Kriptografi Kunci Simetri Mickey-128 Untuk Kasus Penyandian Data Multimedia”*. p. 6  Ekklesia, D., 2016. “*Kriptografi. Studi dan Implementasi Pengamanan Basis Data Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 1445 Fakultas Ilmu Komputer, Universitas Brawijaya dengan Teknik Kriptografi Stream Cipher”*. pp. 1 -7.  Hell, Martin, Johansson, Thomas, and Meier, Willi. 2006. “Grain - *A Stream Cipher for Constrained Environments*”, in *Informations Theory*, 2006 *IEEE International Symposium* on, July, pp. 1614-1618.  Kamal, Raj. 2017. “*Internet of Things Architecture and Design Principles”.* India. Mc Graw Hill Education.  Razzaque, Muhammad, Member, IEEE, Jevric, Marija, Palade, Andre and Clarke, Siobhan. 2016. “*Middleware for Internet of Things: A Survey”.* IEEE Internet of Things Journal. Vol. 3. No. 1.  Rochman, Hudan Abdur, Primananda, Rakhmadhany, Nurwasito, Heru. 2017. “*Sistem Kendali Berbasis Mikrokontroler Menggunakan Protokol MQTT pada Smartphone*”, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Vol. 1 No. 6.  Xia, Feng, Yang, Laurence T., Wang, Lizhe, and Vinel, Alexey. 2012. “*Internet of Things*”, *International Journal of Communication System.* 25:1101-1102. |
| **Status Usulan** | *Diteruskan Menjadi Proposal / Ditolak\*)*  Keterangan : (apabila ditolak) |
| **Masukan pembimbing untuk penulisan proposal:** | *(diisi oleh calon dosen pembimbing)* |
| **Tanda Tangan Mahasiswa** |  |
| **Tanda Tangan Calon Dosen Pembimbing** |  |

\*) Coret yang tidak perlu