IMPLEMENTASI *MAN IN THE MIDDLE ATTACK* PADA ALGORITME BLAKE2S BERBASIS LoRa

Nurovi Andiyani[1], Ari Kusyanti[2], Reza Andria Siregar[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]noroviandiyani98@gmail.com, [2]ari.kusyanti@ub.ac.id, [3]reza.jalin@ub.ac.id

Abstrak

Long Range (LoRa) merupakan teknologi *Low Power Wide Arean Network* (LPWAN) yang digunakan untuk transmisi menggunakan spectrum gelombang radio dengan transmisi jangkauan jarak yang jauh dan konsumsi daya yang rendah. Data yang ditransmisikan belum memiliki keamanan sehingga integritasnya tidak terjamin. Metode yang telah digunakan untuk keamanan integritas data yaitu algoritme SHA-256 yang sudah tidak aman untuk digunakan karena serangan *collison attack* dan *second preimage.* Oleh karena itu, algoritme BLAKE2S digunakan sebagai alternatif untuk menjaga integritas data yang ditransmisikan. BLAKE2S telah terbukti sebagai algoritme yang memiliki tingat keamanan yang lebih baik. Dari penelitian yang dihasilkan, algoritme BLAKE2S berhasil melakukan keamanan yang diimplementasikan untuk menjamin keamanan data pada LoRa. Pengamanan data dilakukan dengan mengubah menjadi *message digest* melalui proses *hashing.* Keamanan data dengan pengujian serangan aktif menggunakan teknik *Man In The Middle Attack* berhasil dilakukan. Ketika *attacker* melakukan serangan, *gateway* mampu melakukan pengecekan terhadap data dari *node* asli dan *attacker* yang dicocokan dengan data dari *gateway* sehingga menghasilkan data yang tidak valid yang berarti integritas datanya terjamin.

Kata kunci: LoRa, IoT, Algoritme BLAKE2S, *Man In The Middle Attack,* Integritas data, keamanan

Abstract

Long Range (LoRa) is a Low Power Wide Arean Network (LPWAN) technology used for transmission using radio wave spectrum with long range transmission and low power consumption. The transmitted data does not have security so the integrity is not guaranteed. The method that has been used for data integrity security is the SHA-256 algorithm that is no longer safe to use due to collison attacks and second preimage. Therefore, the BLAKE2S algorithm is used as an alternative to maintaining the integrity of transmitted data. BLAKE2S has been proven to be an algorithm that has better security. From the resulting research, BLAKE2S algorithm successfully performs security implemented to ensure data security on LoRa. Data security is done by converting into message digest through hashing process. Data security with active attack testing using techniques Man In The Middle Attack was successfully performed. When the attacker performs an attack, the gateway is able to check the data from node's original and the attacker be matched with the data from the gateway and generating invalid data which means the data integrity is guaranteed.

Keywords: *LoRa, IoT, BLAKE2S Algorithm, Man In The Middle Attack, Integrity, Security*

1. PENDAHULUAN

Perkembangan dari teknologi internet yang disebabkan oleh *Internet of Things* (IoT) yang mengubungkan setiap objek agar dapat berkomunikasi. Konsep IoT menggunakan daya yang sedikit, data *rate* yang rendah serta efektivitas biaya. *Long Range* (LoRa) merupakan salah satu teknologi *Low Power Wide Area Network* (LPWAN) yang memiliki konsumsi daya rendag, transmisi jarak jauh serta biaya yang sedikit. LoRa atau *Long Range* merupakan sebuah Teknik modulasi yang memungkinkan transfer informasi jarak jauh dengan transfer *rate* yang rendah (Farooq and Pesch, 2018). LoRa menyediakan konektivitas jarak jauh dengan jangkauan komunikasi lebih dari 2 km. LoRa menggunakan spektrum gelombang radio untuk melakukan pengiriman data. Selain itu LoRa merupakan solusi terbaik untuk IoT yang membutuhkan berbagai komunikasi data dengan tetap menjaga penggunaan daya yang sedikit.

Penelitian yang dilakukan oleh Semiconductors (2018) melakukan keamanan data yang dikirimkan pada LoRa menggunakan algoritme SHA-256. Algoritme SHA256 yang merupakan algoritme *hashing* untuk menjaga keamanan integritas data. Namun pada algoritme SHA-256 telah ditemukan serangan pada tahun 2011 yaitu *preimage attack* (Khovratovich et. al., 2012).

Berangkat dari uraian sebelumnya, maka digunakan algoritme *hashing* alternatif sebagai pengganti algoritme SHA256 yaitu Algoritme BLAKE2S. Algoritme BLAKE2S merupakan salah satu dari algoritme BLAKE2 yang dikembangkan dari BLAKE. Dimana BLAKE memiliki susunan algoritme yang ringan sehingga lebih cepat diterapkan pada perangkat lunak dan keras. Algoritme BLAKE2 dapat digunakan untuk algoritme *hashing* yang dirilis pada tahun 2012. Algoritme BLAKE2 diketahui tidak memiliki masalah keamanan serta tahan terhadap *collison attack* dan *second preimage*. Oleh karena itu algoritme BLAKE2S jika dibandingkan dengan algoritme SHA-256 tingkat keamanannya lebih baik dan lebih cepat (Aumasson et al., 2013).

Penelitian ini menggunakan algoritme BLAKE2S sebagai keamanan integritas data yang akan dikirimkan oleh *node* ke *gateway* dengan menggunakan modul komunikasi LoRa. Untuk memastikan keamanan integritas data, pada penelitian ini akan dilakukan pengujian keamanan agar data yang dikirimkan tidak diubah oleh pihak yang tidak berwenang sehingga integritas datanya terjamin. Pengujian yang dilakukan adalah pengujian keamanan integritas pada data yang dikirimkan dengan melakukan serangan *Man In The Middle Attack* (MITM).

2. LANDASAN KEPUSTAKAAN

Pada Pada penelitian yang dilakukan oleh Arijuddin dengan judul "Pengembangan Sistem Perantara Pengiriman Data Menggunakan Modul Komunikasi LoRa dan Protokol MQTT Pada *Wireless Sensor Network"* menghasilkan yaitu komunikasi pengiriman data antara *node* ke dengan menggunakan modul komunikasi LoRa kemudian meneruskannya ke server. Pada penelitian tersebut komunikasi yang terjadi antara *node* dan *gateway* yang menggunakan

LoRa masih rentan terhadap serangan pihak yang tidak berwenag. Oleh karena itu, pada penelitian ini peneliti akan menambahkan keamanan terhadap data yang dikirimkan pada modul komunikasi LoRa.

Penelitian yang dilakukan oleh NXP Semiconductors dengan judul "*IoT Device Secure Connection with LoRa"* mendapatkan hasil yaitu menerapkan keamanan pada LoRa. Penelitian tersebut melakukan keamanan pada integritas datanya dengan menggunakan algoritme SHA256. Namun algoritme tersebut sudah tidak aman lagi sehingga peneliti menggunakan alternatif lain dengan menggunakan algoritme BLAKE2S. Penelitian selanjutnya yang dilakukan oleh Aumasson dengan judul "BLAKE2: simpler, smaller, fast as MD5" merupakan penjelasan secara detail dan jelas mengenai algoritme BLAKE2S yang akan digunakan dalam penelitian ini.

2.1 *Internet of Things*

IoT pada dasarnya merupakan sebuah teknologi yang dapat menghubungkan apapun, IoT menghubungkan setiap objek untuk dapat berkomunikasi antara perangkat satu dengan perangkat yang lain. IoT juga sebagai perkembangan keilmuan yang sangat menjanjikan untuk mengoptimalkan kehidupan dengan menggunakan teknologi cerdas dan peralatan pintar yang terhubung melalui jaringan internet.

2.2 *Long Range* (LoRa)

Long Range (LoRa) merupakan teknik modulasi yang memungkinkan untuk melakukan transfer data dengan jarak yang jauh dan transfer *rate* yang rendah. LoRa menggunakan teknik modulasi *Chirp Spread Spectrum* (CSS) dimana teknik ini terdiri dari penggunaan *chirp signal* yang kuat terhadap gangguan saluran karena *bandwidth* dialokasikan untuk memancarkan data atau informasi.

2.3 Algoritme BLAKE2S

Algoritme BLAKE2S merupakan sebuah algoritme kriptografi fungsi *hash* yang didesain berjalan pada perangkat 32 bit. BLAKE2S bekerja dengan 10 rounds yang dapat menghasilkan *message digest* dengan panjang hingga 32 bytes. Inputan yang masuk berupa data dan *key*. Data yang masuk kemudian dilakukan *padding* dengan menambahkan 0 hingga memenuhi panjang blok yaitu 16 blok dengan panjang *digest* minimal 1 byte dan *key* hingga 32byte yang opsional. Hal pertama yang dilakukan yaitu *initialization vector*. *Initialization Vector* merupakan nilai konstan yang nilainya diberikan secara statis dimana masing-masing nilai IV tersebut menghasilkan 32bit yang diberikan pada Tabel dibawah ini.

Tabel 1. Nilai *Initialization Vector* BLAKE2S

IV_0 = 6a09e667	IV_4 = 510e527f
IV_1 = bb67ae85	IV_5 = 9b05688c
IV_2 = 3c6ef372	IV_6 = 1f83d9ab
IV_3 = a54ff53a	IV_7 = 5be0cd19

Lalu menginisialisasi nilai *h* atau *chain value*. Nilai masing-masing *chain value* atau *h* awal akan menghasilkan *output* 32 bit terdapat pada Tabel dibawah ini.

Tabel 2. Nilai *Chain Value* Awal

h_0 = 6B08E647
h_1 = BB67AC85
h_2 = 3C6EF372
h_3 = A45FF53A
h_4 = 510E527F
h_5 = 9B05688C
h_6 = 1F83D9AB
h_7 = 5BE0CD19

Kemudian menginisialisasi nilai permutasi. Setelah itu masuk pada tahap *Initialization* dimana tahap ini akan memproses inisialiasi IV, permutasi, dan *chain value* awal yang akan diproses pada fungsi *compress* yang akan menghasilkan nilai v awal. Setelah nilai v ditentukan, maka masuk tahap *round function*. Proses *round* akan mengelompokkan nilai v_0 …… v_{15} kedalam G_0 …… G_7 dengan menggunakan 2 teknik yaitu *column step* dan *diagonal step.* Setelah itu melakukan proses *G function* dimana nilai v didalam G direpresentasikan kedalam a, b, c, d sehingga menjadi G_i (a, b, c, d). Dimana *r, G_i (a, b, c, d)* algoritme G *function* diatur sebagai berikut:

$a \leftarrow a + b + m_{\sigma\tau}(2i)$

$d \leftarrow (d \oplus a) \ggg 16$

$c \leftarrow c + d$

$b \leftarrow (b \oplus c) \ggg 12$

$a \leftarrow a + b + m_{\sigma\tau}\,(2_i{+}1)$

$d \leftarrow (d \oplus a) \ggg 8$

$c \leftarrow c + d$

$b \leftarrow (b \oplus c) \ggg 7$

Sesudah proses *round* pada *G function* maka masuk tahap terakhir yaitu *finalization.* Proses ini akan menghasilkan nilai *chain value* baru yang disebut *message digest* dimana *chain value* awal akan di-XOR kan dengan nilai v yang diatur sebagai berikut:

$h'_0 \leftarrow h_0 \oplus v_0 \oplus v_8$

$h'_1 \leftarrow h_1 \oplus v_1 \oplus v_9$

$h'_2 \leftarrow h_2 \oplus v_2 \oplus v_{10}$

$h'_3 \leftarrow h_3 \oplus v_3 \oplus v_{11}$

$h'_4 \leftarrow h_4 \oplus v_4 \oplus v_{12}$

$h'_5 \leftarrow h_5 \oplus v_5 \oplus v_{13}$

$h'_6 \leftarrow h_6 \oplus v_6 \oplus v_{14}$

$$h_7' \leftarrow h_7 \oplus v_7 \oplus v_{15}$$

2.4 *Man In The Middle Attack* (MITM)

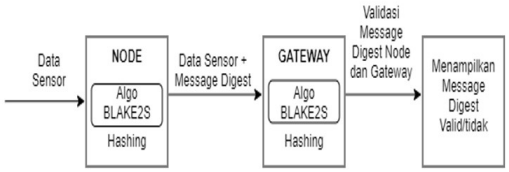
Man In The Middle Attack (MITM) merupakan serangan yang dilakukan oleh penyerang atau *attacker* dimana *attacker* melakukan serangan dengan cara menyampaikan dan mengubah pesan saat dua pihak yang berwenang sedang berkomunikasi secara berlangsung.

3. PERANCANGAN SISTEM

Tahap perancangan sistem akan dilakukan perancangan terhadap sistem yang dibuat agar dapat melakukan koneksi dan komunikasi untuk pengiriman data. Sistem akan terdiri dari *node* da *gateway* yang dirancang dengan menggunakan modul LoRa dimana *node* digunakan sebagai pengirim dan *gateway* digunakan sebagai penerima.

3.1 Perancangan Pengamanan pada Sistem

Tahap perancangan pengamanan pada sistem akan menggunakan algoritme BLAKE2S untuk proses pengamanan data yang diimplementasikan pada *node* dan *gateway.*



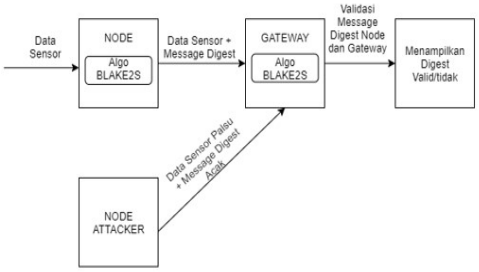
Gambar 3. Rancangan Umum Pengamanan Sistem

Pada Gambar diatas menjelaskan rancangan umum pengamanan pada sistem yang akan diimlementasikan pada *node* dan *gateway. Node* akan menerima data berupa suhu dan kelembaban. Data tersebut kemudian dilakukan proses *hashing* dengan menggunakan BLAKE2S. *Hashing* digunakan untuk keamanan integritas data. proses *hashing* akan menghasilkan *message digest*. Kemudian *node* akan mengirim data asli dan hasil *message digest* ke *gateway. Gateway* akan menerima data dari *node* yang berupa data asli dan hasil *message digest* yang dihasilkan *node.* Pada data asli akan dilakukan proses *hashing* dan menghasilkan *message digest* yang dihasilkan oleh *gateway.* Hasil *message digest node* dan hasil *message digest gateway* akan dilakukan pengecekan jika hasil dari kedua *message digest* maka dapat dinyatakan valid, namun sebalikanya jika hasil dari kedua *message digest* tidak sama maka dapat dinyatakan tidak valid.

3.2 Perancangan Pengujian

Pada perancangan pengujian akan dilakukan serangkaian uji terhadap implementasi sistem maupun implementasi algoritme.

Perancangan pengujian kinerja keamanan integritas data akan dilakukan dengan cara menyerang secara aktif terhadap sistem ketika dijalankan. Penyerangan yang akan digunakan yaitu melakukan uji serangan *Man In The Middle Attack.* Penyerangan ini bertujuan untuk memastikan integritas data yang dikirimkan tidak diubah oleh pihak yang tidak berwenang. Skenario uji akan menggunakan *node* tambahan sebagai penyerang, dimana *node* penyerang akan melakukan serangan dengan cara mengirimkan data palsu berupa suhu dan kelembaban pada saat *node* dan *gateway* asli sedang berkomunikasi. Ketika serangan dimulai, *gateway* akan menerima data dari *node* asli dan data palsu dari *attacker. Gateway* kemudian menyeleksi dengan memastikan data yang dikirimkan oleh *node* asli dan *gateway* sama, jika tidak sama maka dapat dipastikan data mengalami perubahan oleh pihak yang tidak berwenang. Berikut adalah gambar skenario rancangan serangan *Man In The Middle Attack.*



Gambar 4. Rancangan Skenario Serangan

4. IMPLEMENTASI

Pada bab implementasi akan menjelaskan proses implementasi secara jelas berdasarkan perancangan yang telah dibuat pada bab sebelumnya. Proses implementasi dibagi menjadi implementasi pengembangan sistem *node* dan *gateway* serta implement tasi algoritme BLAKE2S.

4.1 Implementasi Pengembangan Sistem Node dan Gateway

Implementasi sistem dengan modul komunikasi LoRa dilakukan dengan menambahkan keamanan dengan menggunakan algoritme BLAKE2S. Pada bagian sistem node, tahapan awal dimulai yaitu dengan mengaktifkan *library* RF95. Jika sudah aktif, selanjutnya fungsi *sensor_Nodes* melakukan *looping* untuk melakukan pengambilan data sensor suhu dan kelembaban. Setelah itu melakukan pengamanan data dengan memanggil fungsi BLAKE2S dengan parameter data dan *key*. Dalam proses pengaman data dilakukan dengan fungsi *hash.* Setelah fungsi *hash* selesai maka didapatkan hasil final yaitu *message digest.* Hasil *message digest* diubah kedalam bentuk heksadesimal. Setelah data sudah berhasil diamankan maka dimasukkan kedalam *struct* yang berisi suhu, kelembaban, *message digest* suhu, dan *message digest* kelembaban. Setelah itu data *struct* dikirimkan ke *gateway* dalam bentuk *bytearray.* Selanjutnya data yang sudah diamankan dan sebelum diamankan ditampilkan oleh *node.*

Pada bagian sistem *gateway* saat dijalankan, melalui proses yang sama dengan *node* yaitu mengaktifkan terlebih sahulu RF95. Setelah aktif, *gateway* menerima data dari *node* dalam bentuk *struct.* Kemudian *gateway* melakukan *unpack* terhadap data *struct* yang berisi data sebelum dan sesudah diamankan. Data yang belum diamankan kemudian dilakukan *hashing* oleh *gateway* dengan menggunkan BLAKE2S dengan parameter inputan data dan *key.* Dalam proses pengamanan data akan dilakukan dengan fungsi *hash*. Selanjutnya didapatkan hasil *message digest* suhu dan kelembaban oleh *gateway.* Setelah didapatkan hasil *message digest* suhu dan kelembaban oleh *node* dan *gateway.* Selanjutnya dilakukan pengecekan antara *message digest* suhu dan kelembaban *node* dan *gateway*, jika sama maka data valid dan tidak mengalami perubahan namun sebaliknya jika data tidak sama maka data tidak valid dan kemungkinan telah mengalami perubahan oleh pihak yang tidak berwenang.

4.2 Implementasi Algoritme BLAKE2S

Dalam implementasi algoritme BLAKE2S dibagi menjadi 2 fungsi yaitu *Class* BLAKE2S dan fungsi *compress*. Setiap fungsi memiliki proses dalam mengolah data yang akan di *hash.*

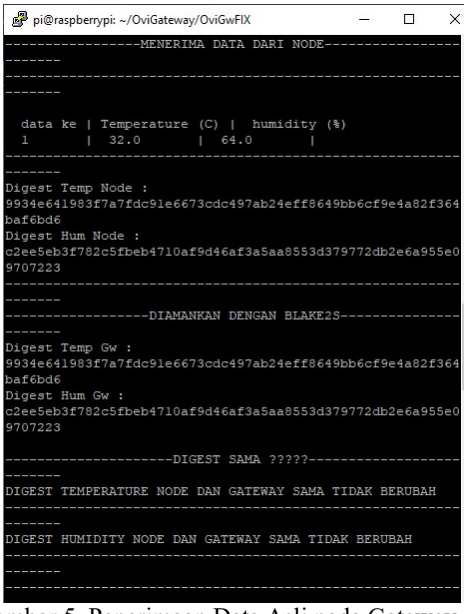
Tahapan pertama pada *Class* BLAKE2S dilakukan proses menginisialisasi kebutuhan *constant* yang dibutuhkan algoritme yaitu inisialisasi IV, sigma permutasi, dan inisialisasi nilai dari rotasi yang akan digunakan.

Tahapan kedua pada fungsi *compress* dilakukan proses untuk melakukan komputasi yang disebut proses *hashing*. Dalam fungsi *compress* berisi inisialisasi nilai V awal dimana nilai V terdiri dari V_0 hingga $V_{15.}$ Kemudian V_0 hingga V_7 akan diisi dengan nilai *h* awal dimana *h* awal didapatkan dari nilai *h* yang terdapat pada SHA256. Sedangkan V_8 hingga V_{15} akan diisi dengan nilai IV dari IV_0 hingga $IV_{7.}$ Terdapat fungsi G yang merupakan fungsi dasar bagi algoritme BLAKE2S untuk melakukan komputasi dimana didalamnya terdapat operasi rotasi, penjumlahan, dan XOR. Pada fungsi G akan melakukan komputasi pada variabel V guna untuk menghasilkan nilai V yang baru dengan parameter fungsi G berupa *message permutation* (sigma) dan masukan berupa a, b, c, dan d yang merepresentasikan nilai dari V.

5. PENGUJIAN DAN ANALISIS

5.1 Pengujian Keamanan

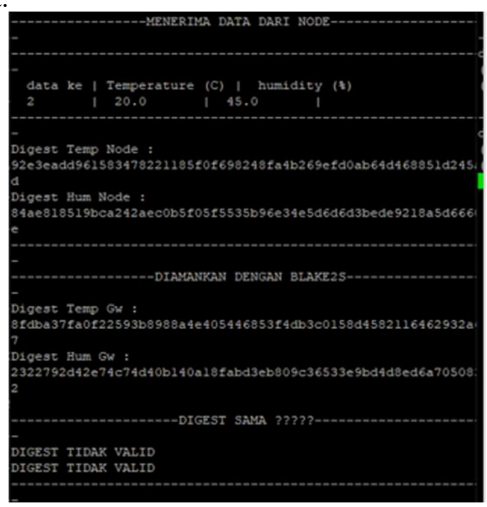
Pengujian keamanan akan dilakukan dengan melakukan serangan aktif menggunakan teknik *Man In The Middle Attack* dimana *node* penyerang atau *attacker* akan menyisipkan data palsu saat *node* dan *gateway* asli sedang melakukan proses pertukaran data.



Gambar 5. Penerimaan Data Asli pada Gateway

Pada Gambar diatas dapat dilihat bahwa *gateway* menerima data dari *node* sebelum serangan dilakukan. Dimana data yang diterima menyatakan suhu dan kelembaban bernilai 32.0 C dan 64.0. Dari hasil pengecekan menyatakan bahwa hasil *message digest* yang dihasilkan *node* dan *gateway* bernilai valid yaitu sama dan tidak berubah.

Attacker memulai serangan dengan mengirimkan data palsu kepada *gateway* dengan berpura-pura menjadi *node* asli. Serangan yang telah dilakukan oleh *attacker* mengakibatka *gateway* menerima data yang berbeda. Dapat dilihat pada Gambar 5.12 dibawah ini yang memperlihatkan bahwa data yang dikirimkan oleh *node* asli ke *gateway* bernilai suhu 32.0 C dan kelembaban 64.0 serta hasil *message digest* yang dihasilkan oleh keduanya. Hasilnya data sama dan tidak berubah, namun ketika *attacker* melakukan serangan dengan mengirimkan data palsu dengan nilai suhu 20.0 C dan kelembaban 45.0 mengakibatkan ketika *gateway* mengecek menghasilkan data yang tidak valid karen a terdapat perbedaan hasil *message digest* dari *node* dan *gateway* akibat dari data palsu yang dikirimkan oleh *attacker.* Sehingga kinerja keamanan yang dilakukan terhadap data dengan menggunakan BLAKE2S dapat disimpulkan telah berhasil melakukan pengecekan integritas data.



Gambar 6. Pengubahan Data oleh *Attacker*

6. PENUTUP

Berdasarkan masalah yang telah dirumuskan serta hasil yang diperoleh dari pengujian pada penelitian yang berjudul Implementasi Algoritme BLAKE2S sebagai algoritme *hashing* untuk integritas data pada modul komunikasi LoRa yang telah dibuat oleh penulis, dapat disimpulkan bahwa implementasi algoritme BLAKE2S untuk mengamankan integritas data pada modul komunikasi LoRa berhasil diimplementasikan. Algoritme BLAKE2S yang diimplementasikan terbukti dapat memberi keamanan terhadap data yang dibuktikan melalui pengujian keamanan dengan melakukan serangan dimana sistem berhasil melakukan pengecekan integritas data terhadap serangan pihak yang tidak berwenang.

7. DAFTAR PUSTAKA

Arijuddin, H., Bhawiyuga, A. and Amron, K., 2019. Pengembangan Sistem Perantara Pengiriman Data Menggunakan Modul Komunikasi LoRa dan Protokol MQTT Pada Wireless Sensor Network. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 3(2), pp.1655–1659.

Aumasson, J.P., Neves, S., Wilcox-O'Hearn, Z. and Winnerlein, C., 2013. BLAKE2: Simpler, smaller, fast as MD5. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7954 LNCS, pp.119–135.

Farooq, M.O. and Pesch, D., 2018. Analyzing LoRa: A use case perspective. *IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings*, 2018-Janua, pp.355–360.

Khovratovich, D., Rechberger, C. and Savelieva, A., 2012. Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7549 LNCS, pp.244–263.

Semiconductors, N.X.P., 2018. IoT Device Secure Connection with LoRa.