BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Indonesia merupakan negara yang memiliki banyak daerah perbukitan dan lembah. Banyak perumahan penduduk yang terletak pada perbukitan, dan jalan-jalan raya juga banyak yang melintasi daerah perbukitan dan lembah. Ditambah curah hujan yang tinggi, menyebabkan potensi terjadinya tanah longsor di Indonesia menjadi sangat tinggi. Terjadinya tanah longsor ini menimbulkan banyak sekali kerugian diantaranya menimbulkan korban jiwa, mengganggu sarana transportasi, merusak lahan pertanian dan lainnya. Kerugian akibat tanah longsor bisa dikurangi jika ada peringatan dini dari sistem pendeteksi bencana tanah longsor. Dengan adanya sistem deteksi dini tanah longsor maka bencana tanah longsor dapat diantisipasi dan dicegah, dan jika tidak bisa dicegah setidaknya masyarakat dapat bersiap untuk menghadapi tanah longsor sehingga dapat meminimalisir kerugian yang terjadi [1].

Teknologi yang bisa digunakan uruntuk melakukan pendeteksian tanah adalah teknologi *wireless sensor network* (WSN). WSN merupakan teknologi yang dapat menghubungkan proses *sensing*, kontrol, dan komunikasi untuk *monitoring* lingkungan dengan pengukuran fisik. WSN terdiri dari beberapa perangkat *sensor node* dan sebuah perangkat *gateway node*. Komunikasi antar *sensor node* dan *gateway* menggunakan perangkat yang mendukung jaringan nirkabel [2]. Perangkat pada WSN yang mendukung jaringan nirkabel ada berbagai macam, salah satunya LoRa (*Long Range*) [3]. Selain LoRa ada teknologi lain seperti NB-IOT dan SigFox. Namun, pada penelitian ini dipilih LoRa karena dibandingkan teknologi yang lainnya kerentanan pada LoRa lebih mudah ditemukan dan dieksploitasi [4] sehingga memiliki prioritas untuk diamankan lebih tinggi dibanding teknologi lain.

LoRa adalah teknologi nirkabel berdaya rendah yang menggunakan spektrum radio untuk mengirimkan data. Salah satu kelebihan LoRa adalah bisa melakukan pengiriman sinyal hingga mencapai jarak 1 km jika menggunakan pengaturan yang tepat serta lingkungan sekitarnya memiliki sedikit gangguan. LoRa sangat sesuai untuk digunakan pada WSN yang membutuhkan teknologi untuk pengiriman data

yang tahan terhadap *noise*, konsumsi daya rendah serta dapat mengakomodasi jarak *sensor node* dan *gateway* yang jauh [5].

Pengiriman data pada jarak yang jauh terlebih pada jaringan bebas seperti *wireless* sangat rawan untuk dilakukan *sniffing, decode cature packet* dan *man-in-middle attack* [6]. Pengamanan terhadap jalur komunkasi dan data yang dikirimkan sangat perlu dilakukan dengan baik dan benar. Pengamanan yang bisa dilakukan adalah dengan melakukan enkripsi pada jalur komunikasi dan data yang akan dikirimkan. Salah satu contohnya adalah dengan penggunakan algoritma acorn [7].

Pengamanan yang baik harus memenuhi aspek *integrity*, *authentication* dan *non-repudation* karena merupakan aspek penting dalam memilih algoritma kriptografi. Pada penelitian ini algoritma kriptografi berbasis RSA digunakan untuk melakukan enkripsi karena dapat memenuhi ketiga aspek di atas [8]. Selain itu terdapat algoritma fungsi *hash* yang bisa digunakan sebagai *digital signature* pada data yang akan dikirim. Algoritma fungsi *hash* SHA-3 merupakan fungsi *hash* standar yang terbukti keamanannya karena tidak adanya *collision attack* seperti yang ada pada MD5, SHA-0 dan SHA-1[9]. Selain itu SHA-3 juga menggunakan *sponge function* yang membuatnya menjadi lebih tahan terhadap *collision attack* [10].

Penelitian ini melakukan penerapan keamanan pengiriman data pada WSN untuk menghindari terjadinya penyerangan atau pengubahan data oleh pihak yang tak bertanggungjawab. Dengan melakukan implementasi tersebut diharapkan dapat menciptakan sebuah jalur komunikasi yang aman untuk mengirimkan data *sensing* dari *sensor node* pada WSN.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah

1) Bagaimana cara menerapkan pengamanan pengiriman data menggunakan RSA 2048-bit dan SHA-3 pada WSN?
2) Bagaimana hasil *Quality of Service* dari pengujian program pengamanan yang telah dibuat?
3) Bagaimana bentuk data yang dikirimkan setelah dilakukan pengamanan menggunakan RSA 2048-bit dan SHA-3?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1) Penelitian ini hanya berfokus pada isu keamanan dalam kerahasiaan dan integrasi data.
2) Sistem operasi yang digunakan pada *sensor* dan *server node* adalah *Raspbian*.
3) Kunci *public* dan *private* yang digunakan RSA sepanjang 2048 bit.
4) Perangkat yang digunakan *Raspberry Pi, Modul Dragino LoRa/GPS HAT*.
5) Tidak membahas proses *sensing* pada *sensor node*.
6) Tidak membahas pendistribusian *public key* dan *private key*
7) Pengujian menggunakan data yang didapatkan dari sensor DHT11.

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1) Mendapatkan unjuk kerja sistem pengamanan pengiriman data menggunakan RSA 2048-bit dan SHA-3.
2) Menganalisis hasil *Quality of Service* yaitu *delay* pada pengujian program pengamanan menggunakan RSA 2048-bit dan SHA-3.
3) Menganalisis perubahan bentuk data sebelum dan sesudah diamankan menggunakan RSA 2048-bit dan SHA-3.

1.5 MANFAAT

Penelitian ini diharapkan dapat menghasilkan sebuah program pengiriman data menggunakan LoRa yang aman dan terpercaya datanya. Karena sistem komunikasi pengiriman data *sensing* dari *sensor node* pada WSN menggunakan algoritma kriptografi RSA 2048 bit dan SHA-3 yang aman.

1.6 SISTEMATIKA PENULISAN

Penelitian ini terbagi menjadi beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, manfaat dan tujuan penelitian, batasan masalah dan sistematika penulisan. Bab 2 membahas tentang kajian pustaka, dasar teori setiap komponen yang akan diteliti. Pada bab 3 membahas alat yang digunakan dalam

penelitian, alur penelitian, skenario penelitian, dan alur program yang akan diterapkan. Bab 4 membahas tentang hasil penerapan dan analisis sistem berdasarkan hasil penerapan. Bab 5 berisi kesimpulan dan saran pengembangan penelitian untuk kedepannya.