

1. Latar Belakang

Dengan luasnya komunikasi IoT, WSN sebagai fasilitator dari komunikasi tersebut juga terus dikembangkan sehingga sesuai dengan laju perkembangan IoT. *Wireless Sensor Network* adalah sekumpulan *nodes* yang terorganisir menjadi jaringan yang saling bekerja sama. Setiap *node* terdiri dari *processing capacity*, penyimpan memori, RF *transceiver*, sumber tenaga dan mengakomodasi berbagai jenis sensor dan aktuator. *Nodes* tersebut berkomunikasi secara *wireless* dan biasanya tertanam 1.000 bahkan 10.000 *nodes* didalam sistem yang besar seperti *smart city*. Sekarang WSN sedang gencarnya dikembangkan, sehingga 10-15 tahun lagi dunia ini akan penuh dengan WSN yang bisa kita akses melalui Internet. Teknologi baru ini dapat berkembang dengan potensi yang tak terhingga di berbagai bidang seperti kesehatan, militer, transportasi dan lain lain. Dikarenakan WSN adalah sistem *real time*, maka banyak sekali celah keamanan yang dapat di *exploit* oleh oknum yang tidak bertanggung jawab, salah satu metode yang sering digunakan adalah *Sybil Attack*[1].

Untuk pencegahan metode penyerangan tersebut, penggunaan *Blockchain* adalah solusi yang tepat untuk hal tersebut. Dengan metode tersebut, *centralized database* akan terhapus dan menjadikannya *decentralized database*. Dimana data tidak bisa dirubah ataupun diganti, dan yang lebih pentingnya data tersebar di berbagai tempat sehingga penyerangan hampir mustahil untuk dilakukan. *Blockchain* mempunyai sifat transparan, dimana aktivitas bisa dianalisis oleh siapapun yang mempunyai akses ke jaringan tersebut. Sehingga jika ada sesuatu yang rusak ataupun kebocoran data, maka titik kelemahan dapat dengan mudah diidentifikasi dan diperbaiki langsung. Penggunaan enkripsi dan penyimpanan distributif membuat keseluruhan yang terkait dapat mempercayai data yang masuk. Sehingga *Blockchain* adalah metode yang tepat untuk melindungi WSN dan meningkatkan keamanannya[2].

1.1 Topik dan Batasannya

Berdasarkan latar belakang, masalah yang ada didalam tugas akhir adalah bagaimana *database* berbasis sistem *Blockchain* menghentikan penyerangan pada *Wireless Sensor Network* dengan yang telah dibuat.

- Batasan masalah yang ada didalam tugas akhir ini adalah pembuatan *Wireless Sensor Network* menggunakan *NodeMCU*, hanya 5 buah *node* didalam *Wireless Sensor Network*, *Wireless Sensor Network* yang dibuat telah terhubung dengan *Wi-Fi* yang telah ditentukan, dan topologi yang digunakan untuk *Wireless Sensor Network* adalah topologi *Mesh*. Serangan yang digunakan hanya serangan yang diuji pada skenario pengujian

1.2 Tujuan

Tujuan dari tugas akhir ini adalah membuat *database* yang bersistemkan *Blockchain* untuk mencegah penyerangan pada *Wireless Sensor Network* dan menganalisis hasil dari pengujian tugas akhir tersebut. Tujuan dari tugas akhir ini dapat dilihat pada Tabel 1 yaitu :

Tabel 1. Keterkaitan antara tujuan, pengujian dan kesimpulan

No	Tujuan	Pengujian	Kesimpulan
1	Mengimplementasi <i>Blockchain</i> pada <i>Wireless Sensor Network</i> untuk pencegahan penyerangan	Membuat algoritma yang mengimplementasikan tata cara kerja <i>Blockchain</i> dan membuat keamanannya	Sistem berjalan dengan baik dalam mencegah penyerangan
2	Menganalisis performansi <i>Blockchain</i> dalam meningkatkan keamanan <i>Wireless Sensor Network</i> terhadap serangan	Membuat dan mengeksekusi skema penyerangan untuk mengetahui kekuatan keamanan	Metode berhasil meningkatkan keamanan <i>Wireless Sensor Network</i> terhadap serangan

1.3 Organisasi Tulisan

Pada bab pertama menjelaskan masalah, batasan serta tujuan dari tugas akhir ini. Penulisan bab dua dijelaskan studi literatur yang digunakan untuk informasi dan referensi pada perancangan *database* bersistem *Blockchain*. Bab tiga membahas rancangan sistem dan *resource* yang dibutuhkan oleh sistem. Untuk bab empat dibahas hasil pengujian dan analisis sistem. Pada bab lima menjelaskan kesimpulan dan saran untuk tugas akhir ini.