JINTECH: Journal of Information Technology Vol. 3, No. 1
Februari 2022, Halaman : 10 - 21
E-ISSN : 2746-2331
P-ISSN : 2746-234X

IDENTIFIKASI KEBUTUHAN DAN PENANGANAN KEAMANAN DATA PADA *WIRELESS SENSOR NETWORK*

Sri Wahyuni [1], Satrio Danuasmo[2]
[1]Prodi Teknologi Informasi Universitas Islam Negeri Ar-Raniry
[2]Prodi Ilmu Komputer Universitas Bina Bangsa Getsempena
[1]sri.wahyuni@ar-raniry.ac.id, [2]danuasmo.satrio@gmail.com
Email korespondensi: sri.wahyuni@ar-raniry.ac.id,

Abstract: Wireless Sensor Networks (WSN) is becoming a trend of technology along with the development of data transmission and the human need for the Internet of Things (IoT). IoT is a technology term created to connect one object to be able to send data through a transmission medium (internet) without the help of computers and humans. WSN is one of the technological elements in IoT that helps create connectivity. Currently WSN is widely used to assist tasks related to monitoring, evaluating, tracking, controlling things, and others. WSN consists of a collection of small sensors that will collect data and then transmit it. WSN with wireless system is very vulnerable to security holes. Here we will focus on examining the security vulnerabilities of WSN, how to avoid, and protect the WSN network.
Keywords : wireless sensor network, security and threats, internet of things

Abstrak: *Wireless Sensor Networks* (WSN) merupakan suatu teknologi yang menjadi trend seiring dengan perkembangan teknologi transmisi data dan kebutuhan manusia akan *Internet* of *Things* (IoT). IoT adalah suatu istilah teknologi yang dibuat untuk menghubungkan satu objek untuk dapat berkirim data melalui sebuah media transmisi (internet) tanpa bantuan komputer dan manusia. WSN merupakan salah satu unsur teknologi di dalam IoT yang membantu terciptanya konektivitas.. Saat ini WSN banyak digunakan untuk membantu tugas yang terkait dalam melakukan pengawasan, pemantauan, pelacakan, mengendalikan sesuatu, dan lain-lain. WSN terdiri dari kumpulan sensor kecil yang akan mengumpulkan data dan kemudian mentransmisikannya. WSN dengan sistem *wireless* sangat rentan terhadap celah keamanan. Disini akan focus dalam mengkaji celah-celah keamanan dari WSN, bagaimana cara menghindari, dan melindungi jaringan WSN.
Kata kunci : WSN, Keamanan, Ancaman, *internet of things*

1. PENDAHULUAN

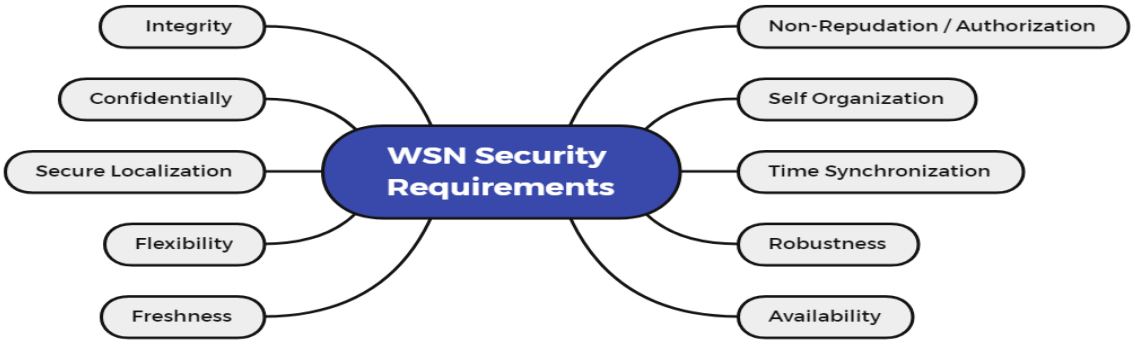
Wireless Sensor Networks (WSN) adalah sekumpulan perangkat kecil yang dikenal dengan *node*. Node berfungsi untuk merasakan, mengawasi, dan mendapatkaan informasi mengenai keadaan di sekitar lingkungan. Informasi tersebut akan diteruskan ke *base station* terdekat melalui WSN dan dilanjutkan untuk pengambilan keputusan. (Al-Ani et al., 2019). Setiap node-node tersebut dapat mengumpulkan informasi secara mandiri dari lingkungan sekitarnya melalui penggunaan sensor. (Sohraby et al., 2007). WSN menjadi cepat populer karena berdasarkan kemampuan penyelesaian masalah yang terjadi pada berbagai bidang. Solusi ini sering dipakai dalam tugas-tugas sipil dan militer. (Akyildiz et al., 2002). WSN mulai dilirik untuk digunakan dalam pengembangan aplikasi *Internet of Things* (IoT) karena biaya pengembangan juga merupakan isu penting yang perlu

E-ISSN : 2746-2331
P-ISSN : 2746-234X

dioptimalkan. WSN terdiri dari perangkat sensor berbiaya rendah yang memiliki kemampuan sumber daya komunikasi dan komputasi yang terbatas dengan kendala sumber daya yang ketat. Tugas utama dari WSN adalah melakukan konfigurasi jaringan disertai dengan pengumpulan data yang menyebabkan keriskanan di dalam sistem keamanannya. Hal ini menjadikan perhatian mendalam untuk menghindari isu keamanan pada transformasi teknologi ini, sehingga menjadi suatu teknologi yang solutif dan aman untuk digunakan.(Gudymenko et al., 2012)

2. KEBUTUHAN KEAMANAN WIRELESS SENSOR NETWORKS (WSN)

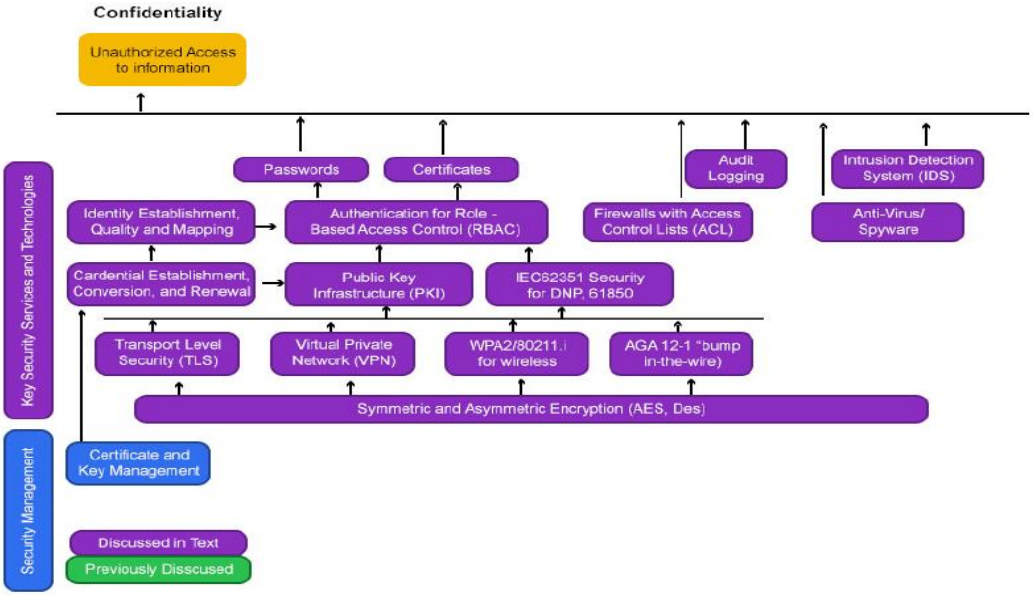
Besarnya peranan wireless sensor network dalam membangun suatu sistem terintegrasi menjadikan bagian keamanan data dan informasi pada setiap tahapannya adalah suatu hal yang sangat krusial, Adapun sektor kebutuhan pengamanan dalam jaringan sensor nirkabel tersebut dapat diuraikan sebagai berikut :



Gambar 1. Kebutuhan Keamanan WSN (*Security Requirements in Wireless Sensor Networks*, n.d.)

2.1 Konfidensial (*Confidentiallity*)

Pada sektor konfidensial kebutuhan keamanan akan kepastian informasi yang sensitif terlindungi dengan baik dari pihak ketiga yang tidak berwenang. Tujuan kerahasiaan ini membantu melindungi informasi yang berjalan di antara node jaringan. Karena dengan perangkat yang sesuai *hacker* dapat melakukan penyadapan informasi dari komunikasi yang sedang berlangsung. Hal ini menjadi celah untuk mendapatkan informasi data penting. Dari data tersebut memungkinkan pengguna yang berniat jahat untuk dapat menyebabkan kerusakan atau kerugian dengan berbagai tujuan illegal seperti sabotase, pemerasan, dan lain-lain.



Gambar 2. Keamanan dan Pencegahan Sektor Konfidensial (Shahzad et al., 2017)

2.2 Integritas (Integrity)

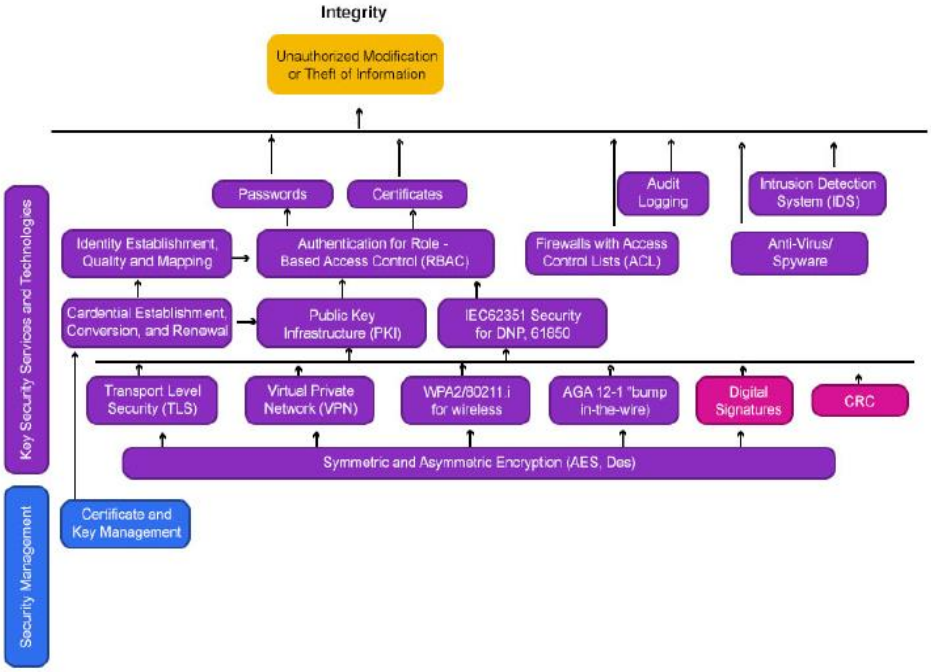
Sector integritas bertujuan memastikan pesan tidak dimodifikasi oleh pengguna node perantara yang berbahaya selama pesan dikirim ke yang node lain dalam jaringan. Kurangnya integritas dapat mengakibatkan banyak masalah karena konsekuensi dari penggunaan informasi yang tidak akurat, misalnya penyalahgunaan data sensor dalam jaringan pada sektor kesehatan dimana kesalahan ini dapat berdampak fatal yang berkaitan langsung dengan keselamatan pasien.

Kontrol Integritas harus diterapkan untuk memastikan bahwa tidak ada informasi yang diubah dengan cara yang tidak terduga. Seperti halnya pada aplikasi sensor pemantauan polusi dan kesiagaan bencana yang mengandalkan integritas informasi agar berfungsi dengan hasil yang akurat.

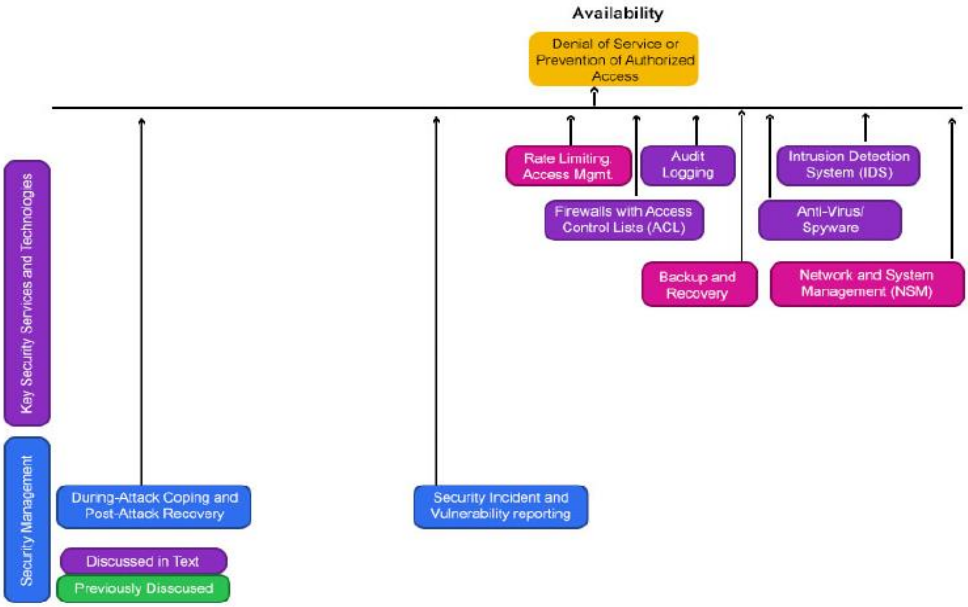
2.3 Ketersediaan (*Availability*)

Sektor ketersediaan adalah jaminan terhadap ketersediaan layanan jaringan meskipun terdapat ancaman serangan seperti *Denial of Services* (DoS). Di dalam sensor nirkabel, adanya banyak risiko yang dapat mengakibatkan hilangnya ketersediaan layanan seperti penangkapan node sensor dan serangan penolakan layanan. Hal tersebut dapat memengaruhi pengoperasian banyak aplikasi *real-time* terkait lainnya.

E-ISSN : 2746-2331
P-ISSN : 2746-234X



Gambar 3. Keamanan dan Pencegahan Sektor Integritas



Gambar 4. Keamanan dan Pencegahan Sektor Ketersediaan (*Availability*)

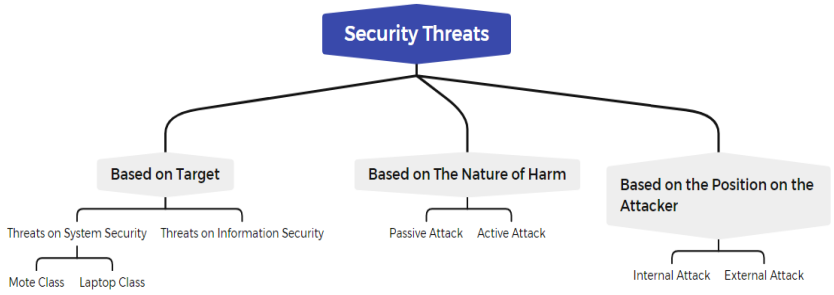
2.4 *Non-Repudiation / Authentication*

Tujuan utama pada sector otentikasi adalah mempersiapkan fasilitas untuk menjamin keamanan data dengan memastikan seseorang tidak dapat menduplikasi keaslian data seperti tanda tangan. Pada banyak kasus dalam jaringan sensor nirkabel, node sensor dan *base station* harus memiliki kemampuan memverifikasi bahwasanya data yang diterima telah sesuai dengan

yang dikirimkan oleh pengirim yang terpercaya dan bukan dari pihak lain dengan maksud memanipulasi node yang sah untuk menerima data palsu. Jika kasus seperti itu terjadi dan data palsu berhasil dimasukkan ke dalam jaringan, maka perilaku jaringan tidak dapat diprediksi, selain itu juga memakan sebagian waktu dengan hasil yang tidak sesuai harapan.

Perlunya otentikasi dilakukan untuk pengelompokan node. Pengelompokan node akan membentuk sebuah klaster berdasarkan beberapa atribut seperti lokasi, data penginderaan dan lainnya. Masing-masing klister akan memiliki head(kepala) sebagai inti konektifitas dalam sebuah klister. Dalam hal ini terdapat dua situasi otentikasi, yang pertama adalah otentikasi antar node dalam satu klister. Kedua adalah situasi otentikasi dalam komunikasi yang terjalin antara sesame head klister. Komunikasi harus terjalin hanya dengan kepala Indepen yang dapat membuktikan identitasnya. Tidak ada node jahat yang dapat menyamar sebagai kepala klister dan berkomunikasi dengan kepala klaster yang sah lainnya, sehingga dapat mengirimkan data palsu atau membahayakan data yang dipertukarkan.

Selain keempat sektor yang telah diuraikan sebelumnya, pada wireless sensor network juga harus memastikan detail lainnya seperti kebaharuan (freshness) data yang dikirimkan, tidak adanya data lama yang berulang. Fleksibilitas (flexibility) dimana jaringan harus siap digunakan dalam segala kondisi. Setiap node dalam WSN bersifat independent sehingga dikaitkan dengan struktur jaringan ad-hoc WSN, maka tidak hanya fleksibilitas namun halnya self organization(mampu mengatur sendiri) dan robustness juga menjadi perhatian dalam menghadapi berbagi bentuk penyerangan. Bentuk lainnya adalah secure localization dan time synchronization, dimana waktu dan lokasi yang digunakan dalam komunikasi harus mampu tervalidasi dengan baik, terpercaya dan sesuai dengan aslinya.(Paharia & Bhushan, 2019)



Gambar 5. Ancaman Keamanan WSN

E-ISSN : 2746-2331
P-ISSN : 2746-234X

3. BENTUK PENCEGAHAN DAN SERANGAN PADA WSN

Serangan yang terjadi pada jaringan WSN adalah suatu upaya mendapatkan akses secara tidak sah untuk mendapatkan informasi sensitif atau mengorbankan sector kerahasiaan, otentikasi, integritas, atau ketersediaan jaringan. Berikut adalah jenis-jenis serangan yang terbagi dalam tiga persyaratan keamanan yang dapat terjadi pada jaringan WSN.

3.1 Konfidensial dan Autentikasi

- Replikasi Node (*Node Replication*)
  Jenis serangan yang melakukan duplikasi terhadap pengidentifikasi *node* atau simpul yang sah dan menambah salinan *node* te(Ashraf & Latif, 2014)rsebut ke dalam WSN, ini akan mempengaruhi pada proses kemampuan dalam mengkomunikasikan seluruh jaringan dari *node* yang direplikasi (Chan & Perrig, 2003)
- *Eavesdropping* dan serangan pemantauan pasif (*passive monitoring attack*)
  Serangan ini terjadi ketika pengguna terhubung ke dalam jaringan dimana trafiknya belum diamankan atau belum terenkripsi dan mengirimkan data bisnis yang sensitif pada rekannya. Data dikirimkan melalui jaringan yang terbuka, yang memberikan kesempatan pada penyerang untuk mengeksploitasi kelemahan dan mencegat dengan beberapa metode. (*What Are Eavesdropping Attacks? | Fortinet*, n.d.)
- Serangan analisis trafik (*traffic analysis attack*)
  Pada metode ini penyerang dapat mendeteksi beberapa node dengan peran atau aktivitas khusus yang dapat memberikan informasi penting tentang cara komunikasi WSN(Solanki & Kohli, 2016)
- Serangan kamuflase (*Camouflage attack*)
  Penyerang berusaha menambahkan node perantara berbahaya ke WSN [11]. Kemudian, simpul-simpul ini dapat digunakan untuk menyamar sebagai simpul biasa untuk mengiklankan informasi perutean palsu dan menarik paket komunikasi ke penerusan lebih lanjut di WSN yang dimaksud.

3.2 Integritas Layanan

- *Jamming*
  Mengganggu frekuensi radio resmi dari node WSN. (Mukherjee et al., 2014)
- *Tampering*
  Mengakses node WSN secara fisik dan mengekstrak datanya seperti password kunci kriptografik dan informasi sensitif lainnya
- *Collision* (Tabrakan)

Collision muncul ketika transmisi node yang berbeda berjalan secara bersamaan dengan rentang frekuensi yang sama.

- *Exhaustion*
  Terjadinya proses serangan dengan cara munculnya *collision* yang berulang sehingga mengkonsumsi semua sumber daya energi dari node WSN sampai node ini menjadi mati yang mengakibatkan tidak dapat memberikan layanan.
- *Spoofed*
  Mengganggu lalu lintas WSN dengan memalsukan, mengubah, atau memutar ulang informasi perutean saat dipertukarkan di antara node sensor.
- *Selective Forwarding*
  Serangan *Selective Forwarding* bekerja dengan cara membuat node jahat atau membahayakan node jaringan. Serangan dapat diadopsi dengan menggunakan node ini untuk secara selektif meneruskan paket tertentu dan menjatuhkan yang lain(Kumar et al., 2008)

3.3 Ketersedian

- *Black Hole*
  Bentuk spesifik dari serangan *Selective Forwarding* di mana node jahat atau yang dikompromikan menjatuhkan semua paket yang diterima.(Burhanuddin et al., 2018)
- *Sinkhole*
  Suatu teknik serangan yang mempersiapkan node yang dikompromikan agar terlihat lebih menarik bagi node tetangganya dengan memberikan informasi routing yang salah.
- *Sybil*
  Metode serangan dengan cara satu node akan mengirimkan beberapa identitas ke WSN. Pada dasarnya, serangan ini dengan mudah mempengaruhi algoritma dan protokol seperti penyimpanan terdistribusi, dan skema toleransi kesalahan.
- *Wormholes*
  Penyerang akan memberikan tautan di antara dua bagian WSN yang dicirikan oleh latensi rendah dan memberikan kemampuan bagi penyerang untuk memutar ulang pesan jaringan
- *Hello Flood*
  Teknik ini musuh dapat menggunakan serangan *Hello Flood* melalui node pemancar bertenaga tinggi untuk menipu banyak node untuk percaya bahwa mereka adalah tetangga dan dalam jangkauannya.
- *Acknowledgement Spoofing*
  Acknowledgement Spoofing yang terdengar antara node yang menyerang dan tetangganya untuk menyebarkan informasi palsu seperti status node yang salah di antara WSN. Pesan kesalahan palsu

E-ISSN : 2746-2331
P-ISSN : 2746-234X

dihasilkan oleh penyerang. Loop perutean dibuat. Akibatnya, latensi ujung ke ujung meningkat dan jaringan dibagi

Jenis Serangan	Layer	Klasifikasi	Persyaratan Keamanan	Pencegahan
Jamming	Physical	Aktif	Ketersediaan	Penggunaan perangkat lunak dan perangkat keras yang reaktif, DEEJAM, JAID (Mpitziopoulos et al., 2009)
Man in The Middle	Physical & Network	Aktif	Ketersediaan	Menggunakan *Intrusion Detection System* (IDS) (Mohapatra et al., 2020)
Eaves Dropping	Physical & Network	Pasif	Konfidensial dan Autentifikasi	Menggunakan mekanisme penjadwalan sensor atau skema konvensional *round robin* (Intercept Behavior Analysis of Industrial WSN in the presence of eavesdropping attack)
Sybil	Data Link	Aktif	Ketersediaan	Sertifikasi yang menjamin untuk identifikasi tiap node (Douceur, 2002)
Traffic Analysis	Data Link & Network	Pasif	Konfidensial dan Autentifikasi	
Blackhole, Sinkhole	Network	Aktif	Ketersediaan	Routing protokol yang berbasis pada lokasi geografis(Karlof & Wagner, 2003)
Spoofing	Network	Aktif	Ketersediaan	autentikasi melalui *base station* (Perrig et al., 2002), Mengkonfirmasi lokasi oleh *node* pengirim, Kunci berbasis orientasi lokasi (Zhang et al., 2006)
Wormhole	Data Link & Network	Aktif	Ketersediaan	Pocket leashes(Y. C. Hu et al., 2003), antena terarah(L. Hu & Evans, 2004), pengecekan

				topologi dari pusat server(Wang & Bhargava, 2004), DAWWSEN active routing protocols(Sharma & Ghose, 2010), mendeteksi node yang mencurigakan melalui sinyal (Sharma & Ghose, 2010)
Denial of Service (DOS)	Network	Aktif	Ketersediaan	Pesan prioritas, pemantauan, otorisasi, redundansi, enkripsi(Raymond & Midkiff, 2008). melarang jaringan untuk dilakukan *broadcast* dari node sensor(Deng et al., 2003)
Hello Flood	Network	Aktif	Ketersediaan	Mendeteksi node yang mencurigakan dengan menguatkan sinyal (Sharma & Ghose, 2010)

.

4. Kesimpulan Dan Saran

Artikel ini menjelaskan tentang celah keamanan impelementasi *Wireless Sensor Network* (WSN), dampak serangan terhadap layanan WSN, dan alternatif bentuk pencegahan dan penanggulangan ancaman keamanan tersebut. Dengan ini akan memberikan wawasan dan kehatian-hatian dalam merancang desain WSN. Banyak celah yang dapat dimanfaatkan oleh penyerang untuk meretas dan mengambil data penting. Untuk Penelitian selanjutnya dapat mengacu kepada detail-detail dan solusi baru untuk menangani celah keamanan pada WSN.

Daftar Kepustakaan

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, *40*(8), 102–105. https://doi.org/10.1109/MCOM.2002.1024422

Al-Ani, K. W., Abdalkafor, A. S., & Nassar, A. M. (2019). An overview of

wireless sensor network and its applications. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(3), 1480–1486. https://doi.org/10.11591/ijeecs.v17.i3.pp1480-1486

Ashraf, J., & Latif, S. (2014). Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques. *National Software Engineering Conference, NSEC 2014*, 55–60. https://doi.org/10.1109/NSEC.2014.6998241

Burhanuddin, M. A., Mohammed, A. A. J., Ismail, R., Hameed, M. E., Kareem, A. N., & Basiron, H. (2018). A review on security challenges and features in wireless sensor networks: IoT perspective. *Journal of Telecommunication, Electronic and Computer Engineering*, *10*(1–7), 17–21.

Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *Computer*, *36*(10), 103–105. https://doi.org/10.1109/MC.2003.1236475

Deng, J., Han, R., & Mishra, S. (2003). *A Performance Evaluation of Intrusion-Tolerant*. 349–364.

Douceur, J. R. (2002). The sybil attack. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2429*, 251–260. https://doi.org/10.1007/3-540-45748-8_24

Gudymenko, I., Borcea-pfitzmann, K., & Tietze, K. (2012). *Privacy Implications of the Internet of Things Introduction Privacy Implications of IoT Possible solutions*. 280–286.

Hu, L., & Evans, D. (2004). Using Directional Antennas to Prevent Wormhole Attacks. *Network and Distributed Systems Symposium, NDSS*, *February*, 1–11. http://www.isoc.org/isoc/conferences/ndss/04/proceedings/Papers/Hu.pdf

Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. *Proceedings - IEEE INFOCOM*, *3*(C), 1976–1986. https://doi.org/10.1109/infcom.2003.1209219

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, *1*(2–3), 293–315. https://doi.org/10.1016/S1570-8705(03)00008-8

Kumar, H., Sarma, D., & Kar, A. (2008). Security threats in wireless sensor networks. *IEEE Aerospace and Electronic Systems Magazine*, *23*(6), 39–45. https://doi.org/10.1109/MAES.2008.4558008

Mohapatra, H., Rath, S., Panda, S., & Kumar, R. (2020). Handling of man-in-the-middle attack in WSN through intrusion detection system. *International*

Journal of Emerging Trends in Engineering Research, *8*(5), 1503–1510. https://doi.org/10.30534/ijeter/2020/05852020

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys and Tutorials*, *11*(4), 42–56. https://doi.org/10.1109/SURV.2009.090404

Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys and Tutorials*, *16*(3), 1550–1573. https://doi.org/10.1109/SURV.2014.012314.00178

Paharia, B., & Bhushan, K. (2019). A comprehensive review of distributed denial of service (DDoS) attacks in fog computing environment. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. https://doi.org/10.1007/978-3-030-22277-2_20

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, *8*(5), 521–534. https://doi.org/10.1023/A:1016598314198

Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, *7*(1), 74–81. https://doi.org/10.1109/MPRV.2008.6

Security Requirements in Wireless Sensor Networks. (n.d.). Retrieved January 31, 2022, from https://krazytech.com/technical-papers/security-requirements-in-wireless-sensor-networks

Shahzad, F., Pasha, M., & Ahmad, A. (2017). *A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures*. *14*(12), 54–65. http://arxiv.org/abs/1702.07136

Sharma, K., & Ghose, M. (2010). Wireless sensor networks: An overview on its security threats. *International Journal of Computers and Their Applications*, 42–45. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.3550&rep=rep1&type=pdf

Sohraby, K., Minoli, D., & Znati, T. (2007). Basic Wireless Sensor Technology. In *Wireless Sensor Networks*. https://doi.org/10.1002/9780470112762.ch3

Solanki, S., & Kohli, J. (2016). Wireless sensor network: A survey. *Far East Journal of Electronics and Communications*, *SpecialVol*, 767–776. https://doi.org/10.17654/ECSV3PII16767

E-ISSN : 2746-2331
P-ISSN : 2746-234X

Wang, W., & Bhargava, B. (2004). Visualization of wormholes in sensor networks. *Proceedings of the 2004 ACM Workshop on Wireless Security, WiSe*, 51–60. https://doi.org/10.1145/1023646.1023657

What Are Eavesdropping Attacks? | Fortinet. (n.d.). Retrieved January 31, 2022, from https://www.fortinet.com/resources/cyberglossary/eavesdropping

Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 247–260. https://doi.org/10.1109/JSAC.2005.861382