BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet of things (IoT) merupakan contoh kemajuan teknologi yang digunakan untuk berkomunikasi dengan mesin melalui jaringan internet, sebuah konsep pengendalian yang bersifat centralized, perangkat keras atau perangkat lunak dapat dioperasikan dari jarak jauh, kapan saja dan dimana saja. Selain IoT ada satu teknologi yang juga berkembang yang digunakan untuk berkomunikasi dengan mesin yaitu *Wireless Sensor Network (*WSN*),* ini merupakan jaringan pribadi atau *private network* yang sekarang banyak diintegrasikan juga ke dalam IoT (Begum & Nandury, 2023). IoT merupakan teknologi yang terus dikembangkan terutama dalam Interoperability, Security dan Scalability (Kumar, Tiwari, & Zymbler, 2019). Tantangan keamanan pada IoT meliputi *device security, network, data* dan *privacy*, Sedangkan teknologi WSN dikembangkan untuk daya konsumsi energi yang rendah untuk akuisisi data sensor (Jangra, 2010). WSN mempunyai jaringan *private network* yang difungsikan juga sebagai security (Keerthika & Shanmugapriya, 2021), tetapi WSN masih rentan terhadap keamanan terkait sentralisasi. Untuk mengatasi permasalahan teknologi tersebut terutama dalam security, teknologi blockchain dapat diterapkan dalam melindungi data sensor atau *node* sensor. Blockchain (BC) merupakan teknologi yang berbasis antar blok untuk menyimpan data, kemudian dalam blok tersebut memiliki enkripsi hash untuk tanda sebuah blok dan akan dihubungkan dengan blok yang lain (G.-T. Nguyen & Kim, 2018). Setiap blok di jaringan blockchain memiliki hash yang berbeda, jika ada informasi dari sebuah blok dimanipulasi, nilai hash blok tersebut akan langsung berubah, hal ini juga menyebabkan perubahan pada hash blok setelahnya (Tiwari, Dhanda, & Dev, 2023).

Blockchain merupakan buku besar digital yang terdistribusi, terstruktur dan banyak digunakan untuk teknologi manajemen transaksi. BC mengalami perkembangan dari segi konsep antara lain dari *peer to peer networks, distributed ledger, consensus mechanism, Smart Contract*, dan penggunaan aplikasi lain yang dianggap penting (Adere, 2022). Blockchain populer ketika konsepnya digunakan oleh Bitcoin dan Ethereum untuk transaksi mata uang kripto, keduanya mengembangkan teknologi algoritma keamanan yang berbeda yaitu Bitcoin's SHA-256 dan Ethereum's Ethash (Jaya, Rakkhitta, Sembiring, Edbert, & Suhartono, 2023). Teknologi blockchain sekarang ini sudah banyak diterapkan dalam banyak bidang, mulai dari keuangan, *supply chain*, pendidikan dan perawatan medis (M. Xu, Chen,

ian besar aplikasi blockchain reguler didasarkan pada transfer sian informasi ke seluruh jaringan berdasarkan kontrak pintar ng dianggap ideal untuk operasi bisnis dan sektor industri Koliousis, 2023). Blockchain telah mengalami perkembangan hain 3.0, Bockchain 1.0 mengembangkan *virtual currency*,

Blockchain 2.0 mengembangkan Bitcoin 2.0, *smart-contract, smart-property*, *decentralized applications (Dapps), decentralized autonomous organizations (DAOs),* dan *decentralized autonomous corporations (DACs),* Blockchain 3.0 diterapkan pada bidang selain mata uang dan keuangan, seperti di pemerintahan, kesehatan, sains, budaya, dan seni. Blockchain 3.0 bertujuan untuk mempopulerkan teknologi, dan berfokus pada regulasi dan tata kelola desentralisasi dimasyarakat (M. Xu et al., 2019). Blockchain banyak diintegrasikan dengan teknologi IoT dan WSN untuk meningkatkan keamanan (Alsaedy, Alraddadi, & Owais, 2020).

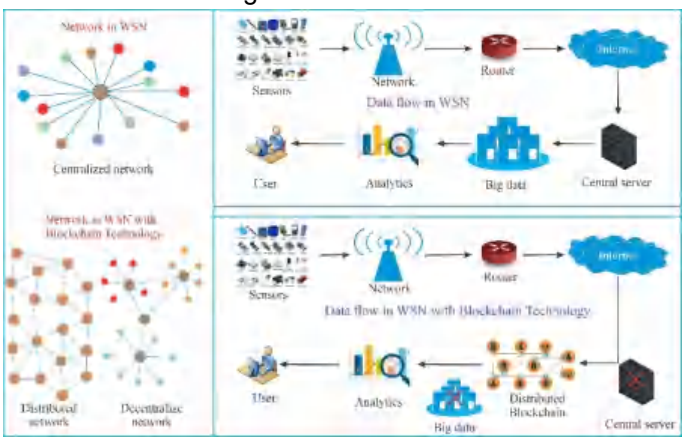
WSN merupakan sistem *embedded* yang terdiri dari beberapa titik sensor yang saling terhubung ke dalam sistem jaringan sensor nirkabel, jaringan ini dirancang dengan daya konsumsi rendah, berbentuk kecil yang berbasis pada standar komunikasi IEEE 802.15.4 (Patel, Kathiriya, & Bavarva, 2013). *Coordinator* berfungsi sebagai jembatan untuk menerima data dari berbagai sensor yang ada dalam jaringan dan disimpan ke dalam *database server* atau di pusat data (*centralized database*), data tersebut akan dikelola di dalam *database* pada satu tempat dan ditampilkan ke sistem informasi untuk mempermudah dalam memonitor data-data sensor. Keamanan WSN menjadi perhatian yang signifikan karena struktur yang kompleks dan kerentanan terhadap serangan internal dan eksternal, komunikasi nirkabel yang terbuka tanpa perlindungan keamanan membuat data dan *node* sensor rentan terhadap serangan aktif maupun pasif.

Jaringan WSN dipilih karena mempunyai beberapa keuntungan antara lain lebih mudah dalam pemeliharaan serta penggunaan daya yang rendah. WSN menggunakan topologi *Mesh* yang akan selalu terhubung satu sama lain di dalam jaringan *node* sensor melalui *node* sensor yang di atur sebagai router (Abed, Alkhatib, & Baicher, 2012). Pemodean arsitektur akan diuji terlebih dahulu dengan pemrograman python, kemudian untuk validasi melibatkan perangkat lunak dan perangkat keras, untuk perangkat keras terdiri dari mikrokontroler, *sensor dari Blockchain Sensor Monitoring (BSM) dan Blockchain Sensor Controlling (BSC)* dan modul *wireless* dengan protokol Zigbee sebagai pengirim dan penerima datanya. Perangkat berbentuk portable bisa berpindah-pindah dari satu tempat ke tempat lainnya tanpa instalasi power dan kabel data. Permasalahan lain dari kerentanan WSN berbasis Zigbee yang belum banyak diteliti antara lain perangkat lunak XCTU tanpa password untuk konfigurasi module Xbee, dan jalur komunikasi terbuka, hal ini akan sangat rentan ketika modul transmisi ini diambil atau dicuri kemudian akan dengan mudah melihat konfigurasinya, manipulasi data sensor, merubah konfigurasi settingan, dan menyambungkan dengan module yang lain, hal ini sangat berbahaya ketika akan diterapkan pada sistem pemantauan (monitoring) atau prediksi bencana,

n untuk kontrol atau transaksi.

SN dengan blockchain semakin berkembang, baik dari segi de untuk deteksi *node* yang berbahaya (anomali) dan juga 1. merupakan sentralisasi, desentralisasi, distribusi WSN dan ta *Body Wirelees Network* (BWSN), Untuk WSN sendiri ada

beberapa topologi salah satunya *Mesh Network*. Arsitektur ini memegang peranan penting dalam proses perlindungan data dan deteksi anomali pada *node* sensor. Konsep perkembangan integrasi diantara dua teknologi tersebut tidak selalu sama dalam penyelesaian suatu sistem, terutama jika akan melibatkan multisensor. Terkait perkembangan arsitektur integrasi WSN dan BC secara umum terdapat beberapa aspek yang perlu diperhatikan antara lain: pertama perlindungan *node* sensor dan data sensor dari *node* sensor yang tersebar sampai ke sentral (*coodinator node*), kedua yaitu teknologi BC, dalam BC ini ada aspek mekanisme konsensus seperti *Proof of Work* (PoW), *Proof of Information* (PoI), dan *Smart Contract* (SC), sedangkan algoritma untuk hash juga harus diperhatikan, tidak semua BC harus menggunakan SHA-256, ada beberapa hasing yang mungkin lebih unggul dalam kecepatan komputasi atau kapasitas penyimpanan seperti Bcrypt, Scrypt atau Argon2. Arsitektur untuk multisensor tentu akan berbeda dengan arsitektur Blockchain untuk transaksi keuangan atau bitcoin.



Gambar 1. 1. Sentralisasi, desentralisasi, distribusi WSN, serta aliran data WSN dan BWSN (C. V Nguyen, Nguyen, Le, Tran, & Nguyen, 2021)

Dalam penelitian ini akan diusulkan pengembangan model arsitektur WSN dan BC untuk deteksi anomali pada *node* dan data sensor. Anomali didefinisikan sebagai kondisi penyimpangan pada node sensor maupun data sensor yang tidak memenuhi kriteria validasi sistem Wireless Sensor Network berbasis blockchain. Anomali pada node sensor diidentifikasi melalui ketidaksesuaian identitas sensor yang meliputi MAC address, Personal Area Network (PAN) ID, dan *Key Hash* yang tidak terdaftar atau tidak dikenali oleh sistem, sehingga node tersebut dikategorikan sebagai node ilegal atau tidak sah. Sementara itu, anomali pada data sensor an mekanisme *Proof of Information* (PoI), di mana data sensor ambang batas nilai yang telah ditetapkan dianggap tidak valid itu, penelitian ini juga menerapkan mekanisme *Proof of Two-on* (Po2FA) sebagai verifikasi keamanan ganda, yang utentikasi dan masa berlaku token, data atau transaksi yang

gagal diverifikasi atau telah kedaluwarsa diklasifikasikan sebagai anomali. Dengan pendekatan ini, sistem hanya mengizinkan node dan data sensor yang tervalidasi untuk berpartisipasi dalam proses pencatatan dan pembentukan blok pada blockchain, sehingga integritas dan keandalan sistem WSN dapat terjaga. Dalam penelitian ini, jenis sensor atau multisensor akan dibagi menjadi dua jenis yaitu Blockchain *Sensor Monitoring* (*BSM*) dan Blockchain *Sensor Controlling*/Transaksi (*BSC*). Dua jenis arsitektur ini mempunya beberapa bagian yang berbeda, dikarenakan fungsinya juga berbeda. Langkah pertama untuk deteksi *node* sensor yaitu meregistrasi Mac Address, PAN ID, dan *Key Hash*. Kedua menetapkan batas *threshold* sensor yang digunakan untuk mencurigai pemalsuan data sensor. Kemudian jika langkah pertama dan kedua valid maka sistem akan membuat blok. Untuk *key hash* yang tertanam pada mikrokontroler, akan diuji menggunakan beberapa algoritma hash (SHA-256, Bcrypt, Scrypt dan Argon2) tujuannya untuk mencari model algoritma yang efisien, serta menerapkan mekanisme konsensus yang menjamin integritas data dan mendeteksi anomali pada *node* serta data sensor secara akurat berbasis *Smart Contract* (SC), *Proof of Information* (PoI) dan *Proof of Two Factor Authentification* (Po2FA). Pengujian dilakukan pada satu sampai tiga server terdistribusi (lokal dan online) guna menganalisis durasi eksekusi dan parameter jaringan, sehingga dapat diperoleh gambaran performa sistem secara menyeluruh.

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas maka dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana mengembangkan model arsitektur WSN BC untuk mendeteksi anomali pada *node* sensor dan data sensor, serta bagaimana implementasinya dengan dua model yaitu *Blockchain Sensor Monitoring* (BSM) dan *Blockchain Sensor Controlling* (BSC)?
2. Bagaimana perbandingan kecepatan dan efisiensi algoritma hash (SHA-256, Scrypt, Bcrypt, dan Argon2), serta algoritma mana yang paling sesuai untuk implementasi blockchain WSN?
3. Bagaimana mekanisme konsensus blockchain WSN dengan pendekatan metode SC, PoI, dan Po2FA dalam menentukan validitas data?
4. Bagaimana perbandingan kinerja arsitektur WSN BC pada tiga jenis server terdistribusi, ditinjau dari durasi waktu eksekusi dan parameter jaringan?

1.3 Tujuan Penelitian

enelitian ini adalah:

dan mengimplementasikan model arsitektur WSN BC yang
ksi anomali pada *node* sensor dan data sensor dengan dua
l dan BSC.

2. Melakukan evaluasi komprehensif terhadap waktu eksekusi dan efisiensi memori algoritma hash (SHA-256, Scrypt, Bcrypt, dan Argon2) guna mengidentifikasi algoritma yang paling optimal untuk mendukung implementasi blockchain pada lingkungan WSN
3. Menentukan model mekanisme konsensus blockchain WSN dengan *Smart Contract*, PoI, dan Po2FA.
4. Melakukan evaluasi empiris terhadap kinerja sistem WSN Blockchain pada tiga konfigurasi server terdistribusi berdasarkan durasi eksekusi dan metrik jaringan, sehingga memperoleh pemetaan performa yang objektif.

1.4 Batasan Masalah

Batasan masalah dari penelitian dapat diuraikan sebagai berikut:

1. Model arsitektur WSN Blockchain dikembangkan menggunakan protokol Zigbee dan hanya difokuskan pada dua model, yaitu BSM dan BSC.
2. Evaluasi algoritma hash dibatasi pada empat algoritma: SHA-256, Scrypt, Bcrypt, dan Argon2 dengan fokus pada efisiensi memori, kecepatan eksekusi, dan kesesuaiannya untuk blockchain WSN.
3. Mekanisme konsensus dibatasi pada tiga pendekatan: SC, PoI, dan Po2FA.
4. Uji performa hanya dilakukan pada tiga jenis server terdistribusi dengan analisis durasi waktu eksekusi dan parameter jaringan.

1.5 Manfaat Penelitian

Manfaat dari penelitian antara lain:

1. Pengembangan model arsitektur WSN dan BC dapat digunakan untuk mendeteksi anomali pada *node* sensor dan data sensor, arsitektur ini dapat diterapkan pada berbagai bidang seperti *Smart City, Smart Vehicle, Smart Health* dan sebagainya .
2. *WSN* dalam model arsitektur ini bersifat nirkabel atau portable tanpa kuota berbayar sehingga sangat memungkinkan untuk diterapkan diberbagai bidang, dan didukung dengan *BC* untuk menambah keamanan *node* dan data sensor.
3. Pertimbangan dalam memilih algoritma hash dan mekanisme konsensus yang diterapkan dalam *WSN* dan *BC* sesuai dengan kebutuhan.

1.6 Penelitian Terkait

WSN merupakan jaringan yang terdiri dari beberapa *node sensor* yang terintegrasi menjadi satu dan berhubungan satu sama lain melalui media nirkabel (W. Li, n.d.). WSN digunakan di berbagai bidang seperti militer, kebakaran hutan, mendeteksi pergerakan kendaraan, pemantauan lingkungan, industri, pertanian, ı, smart home, transportasi, smart city dan lain-lain. Contoh k memonitor terjadinya kebakaran pada lingkungan rumah dan modul Xbee (Fuzi, Ibrahim, Ismail, & Halim, 2014), han tanaman pada *greenhouse* melalui *Zigbee* yang dapat rnet dengan MySQL sebagai tempat menyimpan data (Song,

2010), WSN digunakan untuk memonitor dan pengendalian peralatan listrik pada bangunan gedung berkaca (Rahman & Kasrani, 2017), sedangkan dalam kesehatan contohnya penggunaan Wireless Sensor Network untuk memonitor detak jantung seseorang di saat melakukan aktivitas olahraga (Zulkifli, Che Harun, & Azahar, 2012).

Namun, Keamanan WSN menjadi perhatian yang signifikan karena struktur yang kompleks dan kerentanan terhadap serangan internal dan eksternal (Huanan, Suping, & Jiannan, 2021). Penggunaan saluran komunikasi nirkabel yang terbuka tanpa perlindungan keamanan membuat data rentan terhadap serangan. Salah satu contohnya masalah keamanan dibidang manajemen bencana yang terintegrasi ke WSN, sebagian besar sistem pengawasan tidak memiliki perlindungan data dan alat keamanan, jika penyerang berhasil mengubah data yang dikumpulkan oleh sensor *node* (misalnya aktivitas gunung berapi), hal ini menyebabkan pemalsuan parameter (Mostefa & Abdelkader, 2018). Serangan pada WSN bisa melalui *active* atau *pasif attacks.* Untuk mengatasi berbagai tipe serangan tersebut, banyak peneliti mengembangkan metode untuk keamanan data pada WSN. Data sensor pada WSN bersifat terpusat dan rentan terhadap penyerangan, untuk itu diperlukan metode yang bisa melindungi data dari *node* sensor dan kombinasi data terpusat dan terdistribusi. Salah satu konsep terdistrubusi yang berkembang adalah blockchain. Konsep ini dapat membantu dalam melindungi data dari sensor. Blockchain sudah banyak diintegrasikan dengan WSN terlebih untuk manfaat dan tantangan penerapan teknologi untuk keamanan WSN.

"*Blockchain Technology in Wireless Sensor Network: Benefits and Challenges*", penelitian membahas tentang teknologi blockchain terdesentralisasi yang dapat membantu proses komputasi dan manajemen serta keamanan di WSN, kemudian memberikan gambaran umum tentang integrasi Blockchain di WSN dengan berbagai manfaat dan tantangan penerapan teknologi ini ke WSN (C. V Nguyen et al., 2021).

"*Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission*", Sung-Jung hsiao dkk membahas tentang pemanfaatan blockchain untuk meningkatkan keamanan data dalam pengiriman data sensor. Dalam penelitian ini Teknologi blockchain memiliki beberapa keunggulan antara lain menggunakan desentralisasi dan mekanisme konsensus umum untuk memelihara database, terdistribusi, dan tahan terhadap gangguan dengan integritas. Basis data buku besar (*ledger*) ini dapat dianggap sebagai basis data untuk pengukuran WSN. Pada dasarnya, teknologi blockchain mengutamakan keamanan dan keandalan dibandingkan efisiensi (Hsiao & Sung, 2021b).

Trust Model for Malicious Node Detection in Wireless Sensor aan metode *Blockchain Trust Model (BTM)* untuk mendeteksi jaringan sensor nirkabel, mengevaluasi *node* berbahaya *ct*, kemudian memberikan metode lokasi WSN dalam kontrak

pintar (She et al., 2019a).

"*Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks*", Penerapan teknologi blockchain dalam jaringan sensor nirkabel (WSN) dan potensinya untuk meningkatkan keamanan dan keandalan data, Integrasi blockchain dengan WSN dapat menyediakan metode terdesentralisasi, Sistem ini menggunakan mikrokontroler tertanam seperti Raspberry Pi dan Arduino Yun untuk pengumpulan data dan menggunakan algoritma Merkeltree untuk perhitungan *hash* dan enkripsi. Merevisi buku besar transaksi berbasis blockchain menjadi catatan data sensor, memastikan keandalan data dalam struktur jaringan penginderaan nirkabel. Perbandingan antara metode tradisional dan metode berbasis blockchain yang diusulkan menunjukkan efektivitas pendekatan blockchain dalam meningkatkan keamanan data dalam jaringan sensor nirkabel (Hsiao & Sung, 2021a).

"*Secure and efficient blockchain-based consensus scheme for MWSNs with clustered architecture*", Skema konsensus diusulkan untuk mengamankan penyimpanan data di *Mobile Wireless Sensor Networks (MWSN)* menggunakan teknologi blockchain, Desain varian *Proof of Information (PoI)* untuk penambang yang adil berdasarkan jumlah data valid yang dihasilkan dari informasi. Penyesuaian dinamis batas volume data untuk mendeteksi *node* berbahaya dan mencegahnya dari kesalahan informasi. Skema konsensus yang diusulkan menggunakan algoritma konsensus PBFT dan menggunakan teknik pemfilteran multi level untuk mengisolasi *node* berbahaya dan memastikan efisiensi dalam jaringan skala besar (Qi et al., 2023a) . Tabel 1.1. merupakan perbandingan algoritma konsensus.

Tabel 1. 1. Perbandingan Algoritma Konsensus

Algorithm	Decentralized	Token	Evil number	Scalability	Security	Energy efficiency
PoW	Complete	Computing power	51%	Medium	High	Low
PoS	Semi	Wealth	51%	Medium	Medium	High
DAG	Complete	None	None	High	Medium	High
Raft	Complete	Vote	51%	Medium	Medium	High
PBFT	Semi	None	33%	Low	High	Medium
The proposed PoI	Complete	Effective data volume	51%	Medium	High	High

"*Toward Safety of Wireless Sensor Network Based on Blockchain*", Model baru yang disebut Secure Cluster-Header Decision (SCHD) untuk meningkatkan keamanan data WSN pada IoT. Model ini didasarkan pada teknologi blockchain dan memanfaatkan kontrak pintar Ethereum untuk validasi terdesentralisasi dan kerahasiaan setiap *node*. Implementasi model yang diusulkan pada lingkungan Ganache menggunakan soliditas sebagai bahasa pemrograman menunjukkan , pengurangan konsumsi energi, dan biaya yang lebih rendah. *'er Decision (SCHD)* untuk memastikan bahwa hanya *node* engakses dan memodifikasi data, kontrak pintar Ethereum erahasiaan setiap *node* dalam mekanisme terdesentralisasi. ɔakan program yang dieksekusi sendiri oleh blockchain dan

dapat mengotomatiskan pelaksanaan perjanjian antar pihak (Benaddi, Ibrahimi, & Dahri, 2021).

"*A Framework of Deploying Blockchain in Wireless Sensor Networks*", Penyusunan kerangka kerja dibuat untuk diterapkan pada teknologi blockchain dalam jaringan WSN untuk mengatasi kebutuhan keamanan, privasi, keandalan, dan otonomi jaringan. Kerangka ini mengacu pada kerentanan WSN yang terpusat dan potensi risiko yang terkait dengan berbagi data. Integrasi teknologi keamanan blockchain ke WSN dengan menyimpan identitas setiap *node* dalam blockchain dengan tipe *public blockchain* untuk mengotentikasi kepala *cluster* dan *private blockchain* untuk otentikasi *node* sensor. Metode tersebut untuk mengurangi serangan jaringan oleh *node* yang tidak terdaftar dan meningkatkan efisiensi dalam mendeteksi *node* berbahaya (Tran, Nguyen, & Nguyen, 2022). Tabel 1.2. berikut ini menampilkan *state of the art* yang lebih mengerucut selain yang dibahas sebelumnya.

Tabel 1. 2. *State of the art* penelitian

No	Judul/Tahun/Author	Fokus	Metode	GAP
1	*Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks* (2019), Wei She.	*Node* berbahaya di WSN	*Blockchain Trust Model (BTM)*	*Smart Contract* & ID belum menjamin keamanan penuh; BTM hanya fokus deteksi lokasi *node*.
2	*Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks* (2021), Shung Jung HSIAO dkk	Keamanan data & keandalan WSN.	Integrasi blockchain dengan Raspberry Pi & Arduino	Keterbatasan memori server Raspberry.
3	*Toward Safety of Wireless Sensor Network Based on Blockchain* (2021), Hafsa Benaddi dkk.	Ancaman keamanan data IoT/WSN.	Model SCHD dengan blockchain & *Smart Contract*.	Simulasi hanya berbasis Solidity; tidak bahas keamanan *node* sensor.
4	*A Framework of Deploying Blockchain inWireless Sensor*	Serangan internal/ekst ernal di WSN.	Blockchain dengan *hash* SHA-256.	Simulasi *Smart Contract* dan PoW tidak sesuai dengan penjelasan penelitian.
	lity	*Monitoring live fish*	Blockchain + multisensor, Kafka, Hyperledger	Kompleksitas arsitektur rumit, mengandalkan

No	Judul/Tahun/Author	Fokus	Metode	GAP
	monitoring based on wireless sensor and blockchain technology for live fish waterless transportation (2022), Huanhuan Feng dkk.	transportasi .		komponen eksternal (Apache ZooKeeper), menimbulkan titik kegagalan tambahan dan *overhead* pemeliharaan.
6	*Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability* (2023), Sanjeev Kumar dkk.	Audit & autentikasi data WSN	Blockchain on-chain & off-chain, Scyther & Ethereum.	Transmisi WSN, *node* registrasi dan validasi block tidak dijelaskan. Protokol diverifikasi dengan simulator Scyther dan platform Ethereum.
7	*Blockchain-empowered authentication scheme for worm detection in wireless sensor network* (2022) Q1, Yulian Chen dkk.	Deteksi worm atau serangan *node* WSN.	*Blockchain-empowered Authentication Scheme (BAS)*	Model Arsitektur tidak dijelaskan., penggunaan hash, mekanisme konsensus dengan *Smart Contract*, registrasi dengan PAN ID, masih rentan terhadap penyerangan.
8	*Secure and efficient blockchain-based consensus scheme for MWSNs with clustered architecture* (2023), Weiwei Qi dkk.	*Mobile WSN (MWSN)* dengan konsensus blockchain untuk mendeteksi *node* berbahaya dan mencegah informasi yang salah.	Skema konsensus menggabungkan PoI, DiT dengan PBFT, mekanisme konsensus ini digunakan untuk mendeteksi *node* berbahaya.	Hanya uji serangan replika/informasi palsu; otentikasi *node* & algoritma cerdas perlu diteliti lebih lanjut, simulasi dengan Zigbee.

Penelitian tentang model WSN dan BC banyak dikembangkan dengan berbagai metode dan mekanisme BC, Penelitian(She et al., 2019a), melakukan model deteksi *node* berbahaya dengan model kepercayaan dan *Smart Contract* untuk melacak id dan lokasi, model ini untuk *node* sensor dan belum dicoba dengan data. Penelitian (Hsiao & Sung, 2021a) dengan model perlindungan data dengan blockchain dengan memanfaatkan Respberry PI sebagai server, kelemahannya memori tidak akan cukup untuk data sensor. Penelitian (Benaddi et al., 2021) (Feng et al., 2022) membuat model dengan *Smart Contract* untuk memfilter *Cluster header* dan Monitoring serta memilih kualitas data yang bagus yang akan dibuatkan blok, kedua penelitian ini ada ketergantungan dengan komponen ekternal yaitu Solidity dan Zooke*peer*. Penelitian (Tran et al., 2022) (Dwivedi, Amin, & Vollala, 2023a) menggunakan PoW untuk keamanan data, PoW memakan sumber daya yang besar dan berpengaruh jika data sensor semakin banyak. Penelitian (Yuling Chen, Yang, Li, Ren, & Long, 2022a) menggunakan authentifikasi UID untuk melindungi *node* (mekanisme *tangle*), jika sesuai akan dibuat blok baru, kelemahannya tidak ada authetifikasi pada mekanisme blockchain. Penelitian (Qi et al., 2023a) dengan konsep PoI untuk membuat blok jika data valid terpenuhi, kelemahannya tidak ada perlindungan *node* sensor. Berdasarkan beberapa artikel yang telah diuraikan terdapat kelemahan dan kelebihan dalam memodelkan keamanan data sensor, untuk itu peneliti mengusulkan model arsitektur baru dengan penggabungan beberapa metode yang sudah ada dan penambahan metode baru seperti pada Tabel 1.3.

Tabel 1. 3. Parameter pada state of the art dan usulan model

WSN dan BC	WEI SHE dkk (2019)	SUNG-JUNG HSIAO (2021)	Hafsa Benaddi dkk(2021)	Hoang T. Tran dkk (2022)	Huanhuan Feng dkk (2022)Q1	Sanjeev Kumar Dwivedi dkk(2023)Q1	Yuling Chen dkk (2022) Q1	Weiwei Qi dkk (2023) Q1	Proposed New Model
Smart Contract									
PoI/PoW				PoW		PoW		PoI	PoI
Authentifikasi Mac/UID									
Authentifikasi ID									
Sensor Monitoring (BSM)									
Sensor Control (BSC)									
Hash256									
Scrypt, Bcrypt, Argon2									
Usulan Po2FA									
Other GAP	Pelacakan Lokasi	Raspberry Pi sebagai server (terbatas memori)	Solidity	Deskripsi Smart Contract, simulasi PoW	Ketergantungan Kafka dengan eksternal zookeeper	Audit data penyimpanan dengan BC	Fokus ke registrasi node dan mekanisme tangle	PoI untuk jumlah data yang valid	Authentifikasi identitas perangkat, Smart contract, PoI, Po2FA, Uji penggunaan beberapa algoritma dan membagi dua mode kelompok sensor.
Validasi	OPNET	Prototipe	Simulasi	Simulasi PoW tidak sesuai konsep	Simulasi	Simulasi Scyther dan platform Ethereum	Simulasi Matlab	Simulasi Matlab	Prototipe (Mikrokontroler, Zigbee, multisensor)

enunjukkan kolom *proposed new model* untuk Pengembangan
J dan BC untuk Deteksi *Node* dan Data Sensor yang berbahaya
state of the art, kebaruan dari penelitian yaitu memodelkan
mbagi dua model sensor atau multisensor akan dibagi menjadi

dua model yaitu *Blockchain Sensor Monitoring* (BSM) dan *Blockchain Sensor Controlling*/Transaksi (BSC). Dua model arsitektur ini mempunya beberapa bagian yang berbeda, dikarenakan fungsinya juga berbeda. Langkah pertama untuk deteksi *node* sensor yaitu meregistrasi Mac Address, PAN ID, dan *Key Hash*. Kedua menetapkan batas *threshold* sensor yang digunakan untuk mencurigai pemalsuan data sensor. Kemudian jika langkah pertama dan kedua valid maka sistem akan membuat blok. Untuk *key hash* yang tertanam pada Mikrokontroler, akan diuji dengan menggunakan beberapa algoritma hash *(SHA256, Bcrypt, Scrypt* dan *Argon2*) tujuannya untuk mencari model algoritma yang efisien, tidak menghabiskan memori. Kemudian diusulkan mekanisme konsensus yang cocok dengan dua model sensor tersebut dengan *Smart Contract* dan *Proof of Information (PoI)*. Untuk BSC akan diusulkan mekanisme baru untuk validasi kontrol atau transaksi yaitu Po2FA. Untuk hash dalam blockchain dilakukan pengujian model algoritma yang sesuai.

1.7 Ruang Lingkup Penelitian

Penelitian ini memiliki lingkup sebagai berikut:

1. Pengembangan arsitektur WSN BC
   - Fokus pada deteksi anomali pada *node* sensor dan data sensor.
   - Mengimplementasikan dua jenis sensor: *Blockchain Sensor Monitoring* (BSM) dan *Blockchain Sensor Controlling*/Transaksi (BSC).
   - Menggunakan protokol komunikasi nirkabel Zigbee.
2. Evaluasi algoritma hash
   - Menguji empat algoritma hash: SHA256, Bcrypt, Scrypt dan Argon2.
   - Analisis meliputi kecepatan eksekusi, efisiensi penggunaan memori, dan kesesuaian algoritma untuk blockchain berbasis PoI dan Po2FA.
3. Mekanisme konsensus blockchain
   - Menentukan validitas data menggunakan *Smart Contract*, PoI, dan Po2FA.
   - Fokus pada penerapan mekanisme konsensus pada blockchain sensor.
4. Pengujian kinerja pada server terdistribusi
   - Analisis dilakukan pada tiga jenis server terdistribusi.
   - Parameter yang dianalisis meliputi durasi waktu eksekusi dan parameter jaringan seperti latency, throughput, dan RSSI.
   - Membandingkan performa arsitektur WSN BC pada ketiga server tersebut

1.8 Kebaruan Penelitian (Novelti)

Kebaruan penelitian diuraikan sebagai berikut:

a) Pengembangan arsitektur WSN BC dengan dua jenis kategori sensor: *ensor Monitoring* (BSM) dan *Blockchain Sensor* aksi (BSC). Model ini digunakan untuk mendeteksi anomali or dan data sensor, serta mengintegrasikan autentikasi MAC), *Hash key*, dan penerapan *threshold* data sensor sebagai *art Contract* (SC), *Proof of Information* (PoI), dan usulan baru

Proof of Two Factor Authentication (Po2FA) untuk validasi data dan *node* sensor.

b) Evaluasi dan penerapan algoritma hash (SHA-256, Bcrypt, Scrypt, dan Argon2) dari sisi kecepatan eksekusi dan efisiensi memori, untuk autentikasi *node* sensor dan penambahan blok pada blockchain, serta analisis pengaruh pemilihan algoritma terhadap performa sistem WSN BC.

c) Pengujian arsitektur WSN BC pada tiga server terdistribusi, untuk menganalisis durasi waktu eksekusi, efisiensi algoritma hash, dan parameter jaringan, sehingga memberikan evaluasi performa sistem secara menyeluruh.

1.9 Hipotesis Penelitian

Hipotesis penelitian merupakan perkiraan keluaran yang akan dicapai dalam penelitian, berdasarkan kerangka konseptual yang telah dibuat, keluaran dari penelitian ini antara lain:

a) Arsitektur WSN BC dengan dua jenis sensor (BSM dan BSC), yang menerapkan mekanisme konsensus berbasis SC, PoI, dan Po2FA, mampu mendeteksi anomali pada *node* sensor dan data sensor sekaligus menentukan validitas data dengan lebih akurat.

b) Algoritma hash (SHA-256, Bcrypt, Scrypt, dan Argon2) akan menunjukkan kecepatan eksekusi dan efisiensi memori terbaik untuk implementasi blockchain WSN.

c) Pengujian pada tiga server terdistribusi akan menunjukkan perbedaan durasi waktu eksekusi dan performa jaringan.

BAB II
EVALUASI HASH BLOCKCHAIN TERDESENTRALISASI PADA *WIRELESS SENSOR NETWORK*

2.1 Abstrak

Blockchain merupakan teknologi yang sudah dikenal luas dan dapat digunakan untuk mengembangkan sistem terdistribusi, transparansi data, privasi, dan meningkatkan keamanan pada jaringan sensor nirkabel. Dalam studi ini, kami melakukan seleksi acak makalah penelitian dari periode antara tahun 2018 dan 2024, sehingga totalnya mencapai 70 makalah. Hampir semua artikel menggunakan sha256 dan desentralisasi, kami mengevaluasi dan membandingkannya dengan hash lainnya. Berdasarkan hasil pengujian hash blockchain dengan 3 desentralisasi *peer* (2 offline dan 1 online) yang terintegrasi ke dalam *Wireless Sensor Network* (WSN), didapatkan bahwa Scrypt dapat menyelesaikan 400 blockchain dalam waktu yang lebih cepat (1.193 detik) dibandingkan dengan Argon, SHA256 dan Bcrypt. Sementara itu, untuk menghemat memori, hash Bcrypt dapat menjadi pilihan (96 KB) dibandingkan dengan Argon2 (128 KB) dan Scrypt dan SHA256 (112 KB).

2.2 Pendahuluan

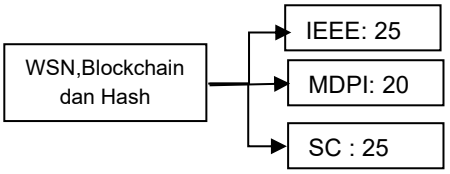
Revolusi industri 4.0 yang berkembang saat ini merupakan teknologi disrupsi, teknologi yang dipengaruhi oleh perkembangan sistem digital atau perkembangan dengan sistem lama akan ditransformasikan ke sistem masa depan atau sistem digital dalam bidang industri. Industri 4.0 sangat erat kaitannya dengan sistem cerdas dan otomatisasi industri, hal ini didukung dengan pengambilan keputusan secara otomatis melalui komputer yang saling terhubung dan berkomunikasi. Teknologi ini merupakan kombinasi dari infrastuktur jaringan komputer dan Internet of things (IoT). Tantangan penggunaan jaringan internet salah satunya yaitu keamanan data dan jaringan. WSN terdiri dari banyak *node* sensor yang saling terhubung dan dirancang untuk mengumpulkan data. Sama seperti IoT, WSN menghadapi masalah keamanan yang berasal dari sifatnya yang terpusat. Teknologi blockchain, sebagai sebuah inovasi yang terus berkembang dan bersifat disruptif, menawarkan metode yang layak untuk mengurangi risiko keamanan dalam WSN.

Teknologi ini memungkinkan distribusi data ke seluruh peserta jaringan. Sejak pengembangannya pada tahun 2008 dan penerapannya pada Bitcoin (Adam 2020), teknologi ini telah menjadi solusi untuk permasalahan ansaksi (Nuttah et al., 2023). Sistem transaksi Bitcoin menjadi lockchain pertama yang dikenal sebagai *Proof of Work* (PoW). meningkatkan privasi, transparansi data, dan keamanan baik cil maupun besar. Teknologi ini menawarkan keuntungan yang

signifikan di berbagai bidang, khususnya dalam membangun kepercayaan pada transaksi keuangan digital (Javaid et al., 2021). Selain itu, blockchain menyediakan infrastruktur teknis yang kuat untuk berbagai level platform dan mendukung penerapan aplikasi terdesentralisasi (DApps), yang dapat memenuhi beragam kebutuhan industri (Bao et al., 2023). Contoh Ethereum dengan Ethereum Blockchain (Sarkodie et al., 2022) dan Hyperledger dengan Hyperledger Fabric (W. Zheng et al., 2019). Dalam penelitian ini, kami melakukan pemilihan acak literatur terkait integrasi WSN dan blockchain dari tiga sumber pengindeks yang menghasilkan total 70 makalah. Makalah ini bertujuan untuk mengevaluasi kinerja dan penggunaan memori dari berbagai algoritma hash yang digunakan dalam teknologi blockchain untuk mengamankan data sensor dalam WSN.

2.3 Karya Terkait

Dalam penelitian ini, dilakukan pemilihan acak terhadap karya ilmiah yang terbit pada periode 2018 hingga 2024, dengan total sebanyak 70 makalah. Seluruh makalah tersebut berfokus pada keterkaitan antara WSN dan teknologi blockchain, serta penerapan algoritma hash dalam proses pembentukan blok, sebagaimana ditunjukkan pada Gambar 2. 1.



Gambar 2. 1. Data makalah terkait dari sumber indeksasi

Selanjutnya, pemilihan literatur diperluas dengan memfokuskan pada aspek desentralisasi, sehingga diperoleh 24 makalah dari IEEE, 16 makalah dari Science Direct (SC), dan 14 makalah dari MDPI. Tahap berikutnya, daftar tersebut dipersempit kembali berdasarkan relevansinya terhadap integrasi WSN, blockchain, dan desentralisasi, yang menghasilkan 18 makalah dari IEEE, 12 makalah dari SC, serta 9 makalah dari MDPI. Terakhir, diterapkan penyaringan tambahan untuk penggunaan fungsi hash yang banyak digunakan, yaitu SHA-256, sehingga tersisa 6 makalah dari IEEE, 6 makalah dari SC, dan 4 makalah dari MDPI. Hasil dari proses penyaringan akhir ini disajikan pada Tabel 2.1.

Tabel 2. 1. Data makalah dengan filter SHA-256

	Hash	Storage	Sensor	Consensus
	SHA-256	Desentralisasi	Sensor Monitoring	PoA
	SHA-256	Desentralisasi	*Node* Sensor Identification	Credit System
	SHA-256	Desentralisasi	Light Senor	Time windowing approach

Author	Hash	Storage	Sensor	Consensus
(Jagannadha Swamy et al., 2023)	SHA-256	Desentralisasi	Sensor Monitoring	Consensus of miner *node*s
(Kaschel et al., 2022)	SHA-256	Desentralisasi	*Node* Sensor Identification	NA
(Godawatte et al., 2022)	SHA-256	Desentralisasi	Soil and Temperature,etc.	NA
(Dwivedi et al., 2023a)	SHA-256	Desentralisasi	Health sensor	NA
(Zhu, 2023)	SHA-256	Desentralisasi	NA	PoW
(Abdussami et al., 2023)	SHA-256	Desentralisasi	Monitoring Sports sensor	NA
(Hasan et al., 2022)	SHA-256	Desentralisasi	Monitoring Sensor	NA
(Ebobissé Djéné et al., 2022)	SHA-256	Desentralisasi	Body Sensors	PoS
(J. Lee, 2018)	SHA-256	Desentralisasi	NA	PoAh
(Vinya et al., 2022)	SHA-256	Desentralisasi	NA	PoW
(Zhang et al.,2022)	SHA-256	Desentralisasi	*Node* Sensor	PoW, PoA
(Matusiewicz et al., 2005)	SHA-256	Desentralisasi	NA	PoW

Tabel 2.2. menunjukkan bahwa seluruh penelitian mengenai integrasi *Wireless Sensor Networks (WSN)* dengan blockchain menggunakan algoritma hash SHA-256, dengan variasi jenis konsensus dan sensor yang berbeda. Makalah ini akan membandingkan algoritma hash SHA-256 dengan Scrypt, Bcrypt, dan Argon2 yang diimplementasikan bersama *Smart Contract* serta jenis sensor dalam WSN. Hasil dari perbandingan ini akan menjadi dasar rekomendasi untuk menentukan fungsi hash yang paling efisien berdasarkan waktu eksekusi dan kebutuhan penyimpanan.

Penelitian ini akan mengevaluasi sistem terpusat dan terdesentralisasi dengan menggunakan tiga konfigurasi penyimpanan *peer*: *peer* A dan *peer* B (offline) serta *peer* C (online). SHA-256 umum digunakan untuk verifikasi tanda tangan digital, handshake SSL, keamanan kata sandi, dan berbagai fungsi keamanan lainnya (Matusiewicz et al., 2005). Bcrypt dikenal memiliki fase inisialisasi kunci yang mahal, namun tahan terhadap peningkatan kemampuan perangkat keras. Scrypt dirancang untuk menggunakan memori dalam jumlah besar, sehingga memberikan perlindungan yang kuat terhadap serangan brute force berbasis perangkat keras (Hatzivasilis et al., 2016). Sementara itu, Argon2 dirancang agar cepat sekaligus intensif dalam penggunaan memori, serta mampu mempertahankan keamanan terhadap serangan trade off (Callens, 2021).

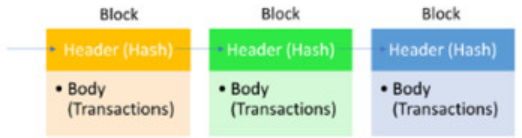
2.4 Evolusi dan Arsitektur Blockchain

Bagian ini menyajikan gambaran umum mengenai berbagai kategori dan klasifikasi dalam teknologi blockchain.

2.4.1 Blockchain 1.0 (Cryptocurrencies)

ı 1.0, perhatian utama tertuju pada pengembangan mata uang
ı sebagai contoh yang paling menonjol. Selain Bitcoin, terdapat
lain seperti Litecoin (Callens, 2021) dan Dogecoin, serta sekitar

700 jenis lainnya yang masih dalam tahap pengembangan (X. Li, Jiang et al., 2020). Teknologi mata uang kripto ini umumnya dibangun di atas dua lapisan utama, yaitu lapisan buku besar terdesentralisasi (*decentralized ledger layer*) dan lapisan protokol (*protocol layer*). Dalam jaringan Bitcoin, proses penambangan dan validasi transaksi umumnya memerlukan waktu sekitar 7–8 menit (Mohanta, Jena, Panda, & Sobhanayak, 2019). Para pengguna bekerja sama dalam jaringan *peer* to *peer* untuk memantau dan mengelola buku besar (*ledger*). Kerangka kerja blockchain terdiri dari dua komponen utama, yaitu Block Body dan Block Header, sebagaimana ditunjukkan pada Gambar 2.2. Block Header memuat elemen-elemen seperti versi blok, Merkle Tree Root Hash, nBits, cap waktu (timestamp), hash blok induk, dan nonce. Sementara itu, Block Body berisi data transaksi serta penghitung (*counter*). Kapasitas penyimpanan transaksi dalam sebuah blok ditentukan oleh ukuran total blok dan ukuran masing-masing transaksi di dalamnya (Nasir et al., 2021) (Y. Xu, 2020). *Proof of Work* (PoW) menjadi mekanisme konsensus awal yang diperkenalkan pada fase Blockchain 1.0.



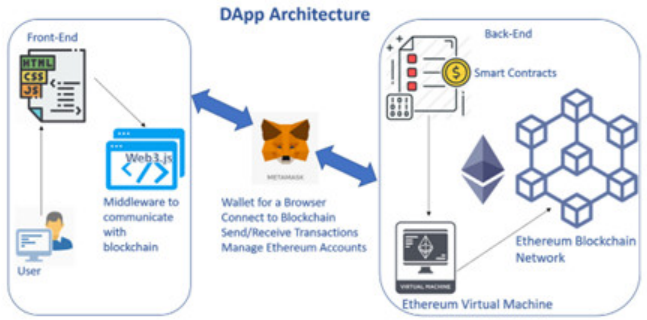
Gambar 2. 2. Blok dalam arsitektur *blockchain*

2.4.2. Blockchain 2.0 (*Smart Contract*)

Kontrak pintar (*Smart Contract*) telah ada sejak tahun 1994 dan didefinisikan sebagai protokol transaksi otomatis yang dirancang untuk menegakkan ketentuan dalam suatu kontrak. Kontrak ini bersifat deterministik, artinya dengan masukan (input) yang sama akan selalu menghasilkan keluaran (output) yang sama (Christidis & Devetsikiotis, 2016). Pada dasarnya, *Smart Contract* merupakan program perangkat lunak yang diintegrasikan ke dalam platform blockchain seperti Ethereum, Hyperledger Fabric, NEM, STELLAR, Waves, dan Corda (Hewa et al., 2021), yang memungkinkan perjanjian antara dua pihak atau lebih dapat dijalankan secara otomatis tanpa memerlukan perantara pihak ketiga yang dipercaya. Riwayat

i dalam blockchain mirip dengan mata uang digital, di mana :a dan aset ditentukan oleh urutan transaksi yang tercatat pada l., 2018). Ethereum merupakan salah satu kemajuan signifikan :chain yang sering disebut sebagai Blockchain 2.0. Setiap *node* reum menggunakan bahasa pemrograman yang dirancang

khusus untuk menjalankan *Smart Contract*. Demikian pula, berbagai sistem blockchain lainnya mengadopsi teknologi spesifik masing-masing: RSK menggunakan Solidity, Stellar memanfaatkan rantai transaksi (*transaction chains*), Monax bergantung pada bytecode EVM, sedangkan Lisk beroperasi dengan JavaScript (Bartoletti & Pompianu, 2017). *Smart Contract*, yang juga dikenal sebagai *Decentralized Applications* (DApps), merupakan bagian integral dari sistem Dapps yang memiliki beberapa fitur utama (Samreen & Alalfi, 2023): 1) Desentralisasi, transaksi dalam DApp dilakukan dijaringan publik untuk mengatasi keterbatasan aplikasi konvensional. 2) Insentif, penambang menerima hadiah berupa token kriptografi. 3) Protokol, melibatkan verifikasi nilai melalui persetujuan kriptografi dari para partisipan. 4) Transparansi, memungkinkan pengawasan dan analisis publik. Gambar 2.3. memperlihatkan arsitektur DApps.



Gambar 2. 3. Aplikasi arsitektur terdesentralisasi (DApp)
(Samreen & Alalfi, 2023)

2.4.3. Blockchain 3.0 (Blockchain *Application*)

Blockchain 3.0 telah muncul dan diterapkan di berbagai sektor industri, khususnya untuk aplikasi terdistribusi seperti permainan (game), jaringan pembuatan konten, *Internet of Things, smart hardware, supply chiain, source tracing, smart city, smart governance, smart mobility, smart environment (power, water),* dan *smart living* (Alnahari & Ariaratnam, 2022). Tahap ini, yang dikenal sebagai blockchain 3.0, berfokus pada peningkatan kinerja untuk aplikasi terdistribusi dengan menyediakan berbagai fitur, antara lain pengurangan latensi, peningkatan *throughput*, manajemen identitas yang lebih sederhana dan efisien, transaksi yang lebih optimal, serta pembaruan sistem yang fleksibel sehingga mempermudah perbaikan *bug* dan pemeliharaan (Cai et al., 2018) (M. S. Ali et al., 2019).

ıain

apat dikategorikan menjadi tiga jenis utama, yaitu Publik, Privat,
antung pada karakteristik serta tujuan penerapannya.

2.5.1. Blockchain Publik

Blockchain publik beroperasi dengan buku besar terbuka yang dapat diakses oleh siapa pun melalui internet, sehingga seluruh pengguna dapat melihat, memverifikasi, dan menambahkan blok transaksi ke dalam rantai (L. Xu et al., 2017). Pada jenis sistem ini, peserta tidak memerlukan izin khusus untuk bergabung dengan jaringan (Cai et al., 2018). Karena bersifat terdesentralisasi, pengguna dapat ikut serta dalam proses konsensus, membaca dan mengirimkan transaksi, serta secara kolektif mengelola dan memelihara buku besar tersebut (Ullah et al., 2023) (Godavarthi et al., 2023).

2.5.2. Blockchain Privat

Blockchain privat terbatas pada individu yang memiliki otorisasi di dalam suatu organisasi, sehingga hanya anggota tersebut yang dapat memverifikasi dan menambahkan blok transaksi, meskipun buku besarnya masih dapat terlihat secara publik melalui internet (Dinh et al., 2017) . Beroperasi dalam lingkungan yang terpusat dan terkendali (X. Xu et al., 2023), blockchain privat umumnya memiliki jumlah peserta yang lebih sedikit, sehingga pemrosesan transaksi menjadi lebih cepat dan konsensus di seluruh jaringan dapat dicapai dengan segera, memungkinkan penanganan jumlah transaksi yang lebih banyak per detik (R. Yang et al., 2020).

2.5.3. Konsorsium Blockchain

Mekanisme konsensus pada blockchain konsorsium beroperasi dengan kecepatan yang lebih lambat dibandingkan blockchain privat, namun lebih cepat daripada blockchain publik. Dari segi keamanan, blockchain konsorsium menawarkan perlindungan yang lebih baik selama proses pembaruan atau modifikasi, sehingga melampaui blockchain privat dalam hal ini. Contoh platform yang menggunakan struktur blockchain konsorsium antara lain Quorum, Corda, dan Sawtooth (Yaoliang Chen et al., 2020).

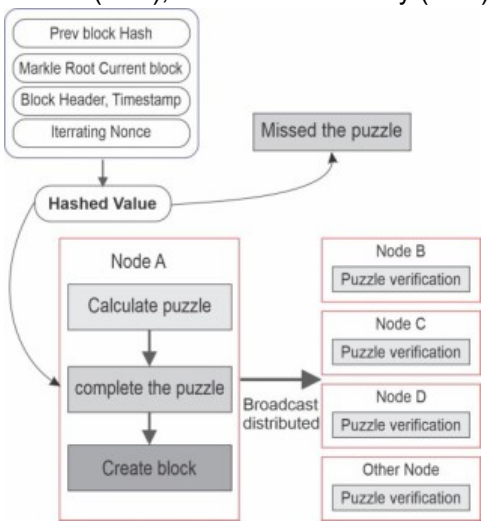
2.6. Mekanisme Konsensus

Dalam teknologi blockchain, mekanisme konsensus digunakan untuk memvalidasi transaksi dan memastikan kesepakatan mengenai bagaimana transaksi tersebut memengaruhi pembaruan pada buku besar. Berbagai model konsensus diterapkan pada berbagai *platform* blockchain, masing-masing dengan pendekatan yang berbeda. Berikut ini adalah uraian mengenai berbagai algoritma konsensus [illegible]n dalam teknologi blockchain.

r*k* (PoW)

akan metode konsensus yang digunakan dalam jaringan goritma ini memerlukan proses komputasi yang kompleks dan

sulit untuk diverifikasi. Setiap *node* dalam jaringan menghitung nilai hash dari *header* blok yang terus meningkat. Dalam sistem terdesentralisasi ini, seluruh peserta harus secara berulang menghitung nilai hash dengan variasi nilai *nonce* hingga berhasil memenuhi target yang telah ditentukan (Hasan et al., 2022). Fungsi hash berperan sebagai teka-teki kriptografi utama dalam algoritma konsensus PoW. Secara khusus, jaringan Bitcoin menggunakan fungsi hash kriptografi SHA-256. Gambar 2.4. menggambarkan mekanisme konsensus PoW. Namun, model PoW pada Bitcoin sangat boros energi, dengan konsumsi listrik sekitar 15,77 terawatt jam, yang mewakili sekitar 0,08% dari penggunaan energi global, serta menimbulkan kekhawatiran lingkungan melalui emisi gas rumah kaca (Tosh et al., 2017). Sistem blockchain tetap rentan terhadap pelanggaran integritas data dan ancaman keamanan. Kerentanan ini dapat disebabkan oleh permasalahan dalam konsensus PoW, seperti serangan mayoritas 51% yang memanipulasi kendali jaringan, atau keterlambatan dalam mencapai konsensus akibat serangan *distributed denial of service (DDoS)* (Göbel et al., 2016). PoW telah berkembang menjadi beberapa model alternatif, seperti *Proof of Reputation* (PoR), Proof of Space (PoS), Proof of Weight (PoW), Proof of Burn (PoB), dan Proof of History (PoH).

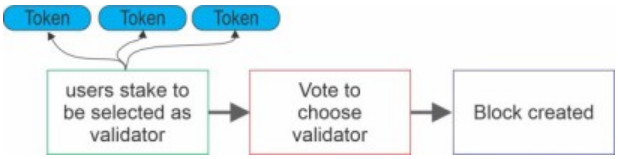


Gambar 2. 4. Mekanisme Konsensus PoW

2.6.2. *Proof of Stake* (PoS)

PoS menghilangkan kebutuhan bagi *node* untuk berinvestasi pada peralatan mahal. Sebagai gantinya, validasi atau penambangan blok ah mata uang kripto yang dimiliki oleh suatu *node* sebagai lockchain terbuka berbasis PoS, siapa pun dapat berpartisipasi tidak dibatasi. Protokol ini memilih sekelompok validator yang

bertugas mengusulkan dan memverifikasi batch transaksi berikutnya yang akan dicatat dalam buku besar (Garcia-Alfaro et al., 2017). Beberapa komunitas, seperti Novacoin, Cloakcoin, dan *Peer*coin, telah menciptakan versi alternatif dari mekanisme PoS. Salah satu variasi penting adalah *Delegated PoS*, yang menggabungkan proses pemungutan suara di mana para pemegang saham memilih *node* tertentu untuk mengambil tanggung jawab dalam menambahkan blok baru ke blockchain (Borse et al., 2022) Gambar 2.5. merupakan gambaran mekanisme konsensus PoS.



Gambar 2. 5. Mekanisme Konsensus PoS

2.6.3. *Proof of Importance* (PoI)

PoI adalah model cryptocurrency yang digunakan oleh *New Economy Movement (NEM)*, yang bekerja mirip dengan proses penambangan tetapi memberi peringkat pengguna berdasarkan jumlah koin yang mereka investasikan. PoI menilai pentingnya suatu *node* dalam jaringan dengan mempertimbangkan saldo koin harian pada akun *node* tersebut untuk menentukan pengaruhnya (Nasir et al., 2021).

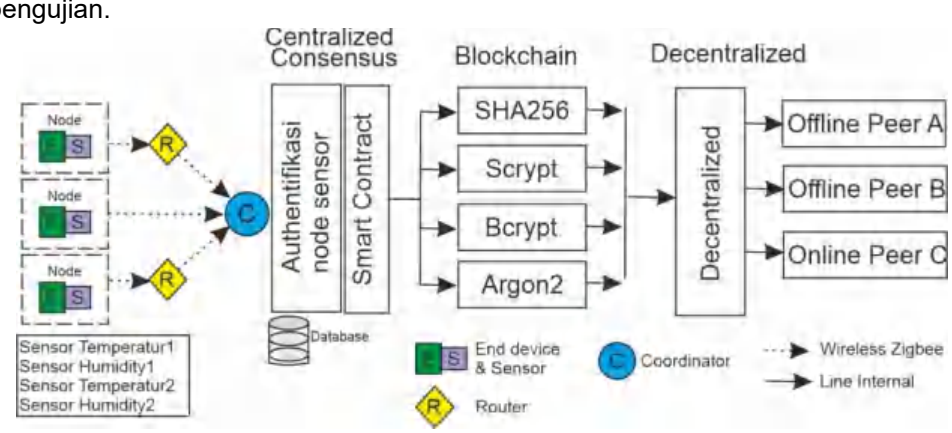
2.6.4. *Smart Contract*

Smart Contract adalah program komputer yang memiliki kemampuan untuk memverifikasi sendiri, menjalankan sendiri, dan tahan terhadap manipulasi. Kontrak ini dapat memuat variabel seperti nilai, alamat, fungsi, atau parameter lainnya. Sebagai bagian dari teknologi blockchain, *Smart Contract* beroperasi dalam sistem yang menggunakan protokol konsensus untuk mengeksekusi peristiwa secara berurutan. *Smart Contract* memiliki berbagai aplikasi di berbagai industri dengan tujuan menghilangkan kebutuhan akan pihak ketiga sebagai perantara dan mengotomatisasi proses (Mohanta et al., 2018).

2.7. Metode Penelitian

Penelitian ini akan menggunakan simulasi dengan pemrograman Python, yang berfokus pada sistem terpusat yang mengoordinasikan *Wireless Sensor Network* (WSN). Meskipun berbagai mekanisme konsensus biasanya digunakan
si data *node* sensor dalam sistem terpusat, studi ini secara
asi integrasi sistem terpusat dengan jaringan blockchain
ggunakan tiga *peer node*: *peer* A dan B (offline) serta *peer* C
kan difokuskan pada algoritma hash yang digunakan untuk
ain, dengan membandingkan SHA256, Scrypt, Bcrypt, dan

Argon2 pada masing-masing server *peer*. Hasil pengujian tersebut akan dievaluasi dan digunakan sebagai rekomendasi penerapan algoritma hash dalam jaringan WSN yang melibatkan ribuan *node* dan volume data sensor yang besar. Hal ini berkaitan dengan tantangan waktu eksekusi pada program WSN dan blockchain yang dipengaruhi oleh algoritma hash yang dipilih. Gambar 2.6. memperlihatkan skenario pengujian.



Gambar 2. 6. Skenario alur data WSN ke blockchain

Setiap dari keempat algoritma hash tersebut memiliki karakteristik unik, terutama dalam proses pembuatan hash. Tabel 2.2. menyajikan hasil penerapan algoritma-algoritma ini pada data "pan1234" yang di hash sebanyak empat kali. Panjang hash yang dihasilkan selalu tetap sesuai dengan pengaturan default algoritma, tanpa dipengaruhi oleh panjang data input. Dengan demikian, ukuran input tidak memengaruhi panjang hash yang dihasilkan.

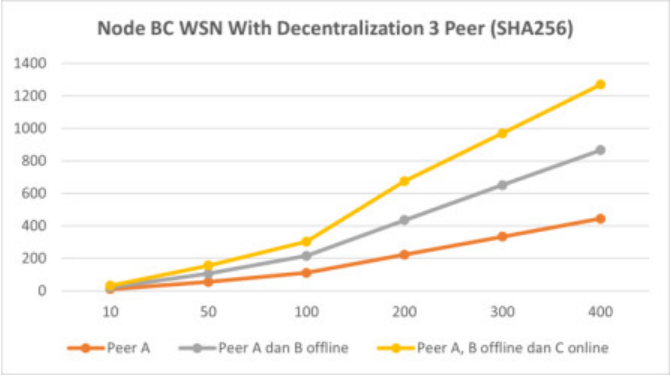
Tabel 2.2. menunjukkan bahwa algoritma hash SHA256 dan Scrypt secara konsisten menghasilkan output yang sama meskipun dihasilkan sebanyak empat kali, sedangkan Bcrypt dan Argon2 menghasilkan nilai yang berbeda pada setiap iterasi. Hasil ini mengindikasikan bahwa penggunaan Bcrypt dan Argon2 dapat meningkatkan keamanan data WSN pada blockchain karena kedua algoritma tersebut memberikan variabilitas yang lebih tinggi. Namun, dalam sistem blockchain, terutama saat membuat blok dalam jumlah besar, nilai hash yang unik diperlukan meskipun data inputnya sama. Untuk mencapai hal ini, parameter timestamp biasanya ditambahkan saat pembuatan blok, seperti yang diterapkan pada banyak implementasi blockchain yang menggunakan SHA256 (data + *timestamp*). Penelitian ini akan lebih menitikberatkan pada analisis waktu eksekusi dan penggunaan memori yang terlibat dalam pemrosesan jaringan WSN terpusat serta transisinya ke
alisasi dengan tiga server penyimpanan data *peer*. Selain itu,
n mengeksplorasi autentikasi *node* sensor melalui penggunaan

Tabel 2. 2. Data algoritma hash

No.	SHA256	Scrypt	Bcrypt	Argon2
1	199b4ef7175eec140453c8a53e30355ffd02046c720418fe79207d611519bf96	0eccd03663c76a963168e74d25a4a2f75a16761ffaa52eceeba8dea9796794ef	$2b$12$lQDhrMTuUoVLyR0R6GSl4uGKc.ER265goj16nk1qJ4EygNVFJHFTS	$argon2id$v=19$m=65536,t=3,p=4$tmbKL1orqdz0qa9BDU3pOA$XNrJUKgsbTm6l6JnneOi8MO6v1lWTkbM7wwT2nrRb58
2	199b4ef7175eec140453c8a53e30355ffd02046c720418fe79207d611519bf96	0eccd03663c76a963168e74d25a4a2f75a16761ffaa52eceeba8dea9796794ef	$2b$12$83HBKTh1Aihm3Uw../kDZuyiiYqlo43CSlAfm737mkMmJTzYJmzna	$argon2id$v=19$m=65536,t=3,p=4$gUiYV/wG8CKmx0DwelI0PIQ$2Kq6WaL3f3J51+qJaYXT03Rm415hd2Sk3yVjY9YeqqM
3	199b4ef7175eec140453c8a53e30355ffd02046c720418fe79207d611519bf96	0eccd03663c76a963168e74d25a4a2f75a16761ffaa52eceeba8dea9796794ef	$2b$12$N6yU3xJamuCfQCaW6c21VO3F3rjRWMO3VC0XwDAxRNZGr0lMMSn9K	$argon2id$v=19$m=65536,t=3,p=4$SJsZTtU7PJdcWSTLVyst1g$VyfPu0pJw9hpajPDlG87JTfKRVvWBuClRlig4d1iZKI
4	199b4ef7175eec140453c8a53e30355ffd02046c720418fe79207d611519bf96	0eccd03663c76a963168e74d25a4a2f75a16761ffaa52eceeba8dea9796794ef	$2b$12$n5Tqf.RIHolFn/Qb9vAgt.gPjy8pilLyxzIROWz0fK2BsYZhay.0m	$argon2id$v=19$m=65536,t=3,p=4$hlQ6OZhYsmgil4DRwWcf5g$khsK5M6iUt6fajQzlFiDjrqNRdLvedaxTkifoJCP94g

2.8. Hasil dan Diskusi

2.8.1. Pengujian *Node* WSN Blockchain dengan Desentralisasi 3 *Peer* (SHA-256)

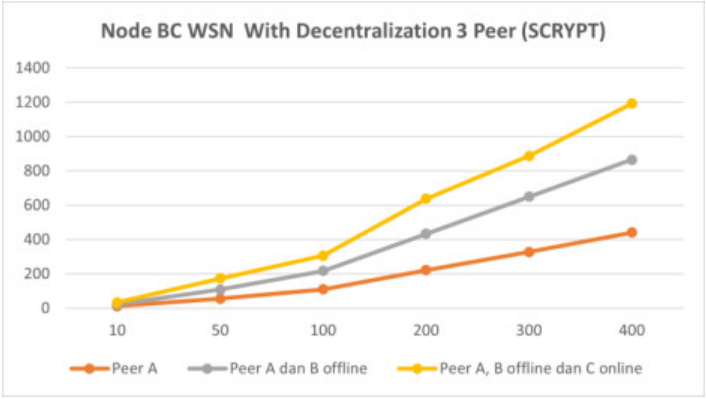


Gambar 2. 7. Grafik pengujian BC WSN dengan desentralisasi 3 *peer* (SHA-256)

Seperti yang ditunjukkan pada Gambar 2.7., pengujian algoritma SHA-256 dengan tiga skenario yaitu *peer* A (offline), *peer* A dan B (offline), serta *peer* A, B (offline), kan bahwa seiring dengan bertambahnya jumlah *node* sensor g masuk, waktu eksekusi pada skenario *peer* juga meningkat. ksekusi yang signifikan terjadi ketika data didistribusikan secara

terdesentralisasi dengan dua *peer* offline dan satu *peer* online. *Peer* C, yang selalu terhubung dengan internet, memberikan pengaruh paling besar karena berdampak pada kekuatan sinyal serta bandwidth jaringan.

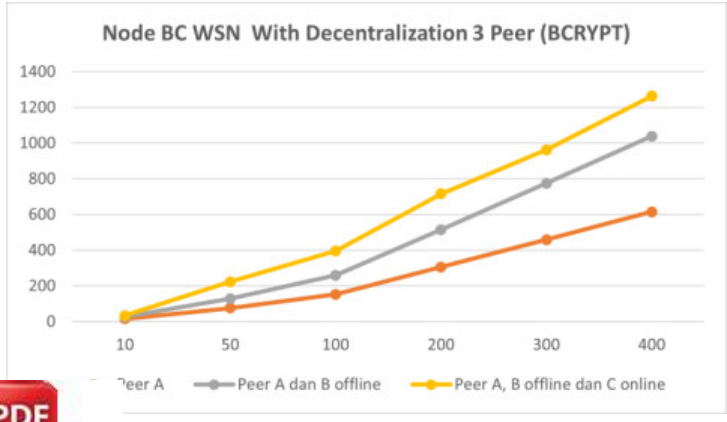
2.8.2. Pengujian *Node* WSN Blockchain dengan Desentralisasi 3 *Peer* (Scrypt)



Gambar 2. 8. Grafik pengujian BC WSN dengan desentralisasi 3 *peer* (Scrypt)

Hasil dari gambar 2.8 pengujian hash menggunakan Scrypt menunjukkan waktu eksekusi sekitar 1.193 detik ketika pengujian dilakukan pada *peer* A dan B (offline) serta *peer* C (online), dengan melibatkan 400 blok data dan pembuatan blockchain.

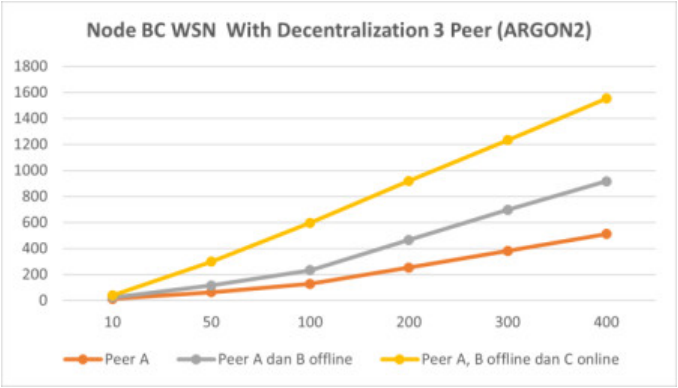
2.8.3. Pengujian *Node* WSN Blockchain dengan Desentralisasi 3 *Peer* (Bcrypt)



ik pengujian BC WSN dengan desentralisasi 3 *peer* (Bcrypt)

Gambar 2.9. merupakan hasil pengujian hash menggunakan Bcrypt menunjukkan waktu eksekusi sekitar 1.263 detik pada *Peer* A dan B (offline) serta *Peer* C (online), dengan melibatkan 400 blok.

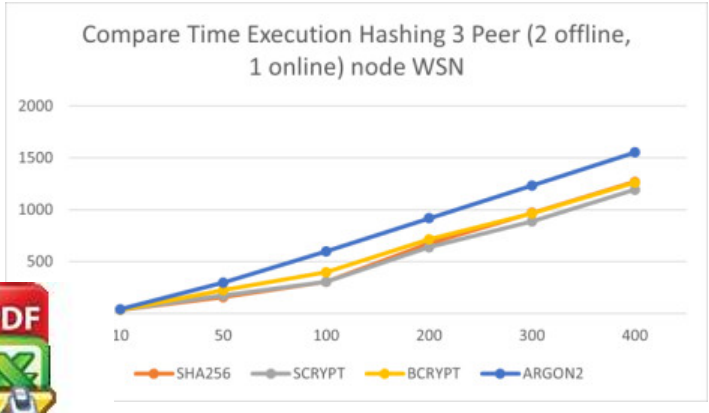
2.8.4. Pengujian *Node* WSN Blockchain dengan Desentralisasi 3 *Peer* (Argon2)



Gambar 2. 10. Grafik pengujian BC WSN dengan desentralisasi 3 *peer* (Argon2)

Gambar 2.10. menunjukkan hasil pengujian hash menggunakan Argon2 menunjukkan waktu eksekusi yang cukup lama, yaitu sekitar 1.553 detik pada *peer* A dan B (offline) serta *peer* C (online) dengan 400 blok data yang membentuk blockchain. Argon2 selalu menghasilkan hash kata sandi yang berbeda meskipun data yang diinput sama, dan hal ini menjadi salah satu keunggulannya dalam melindungi data.

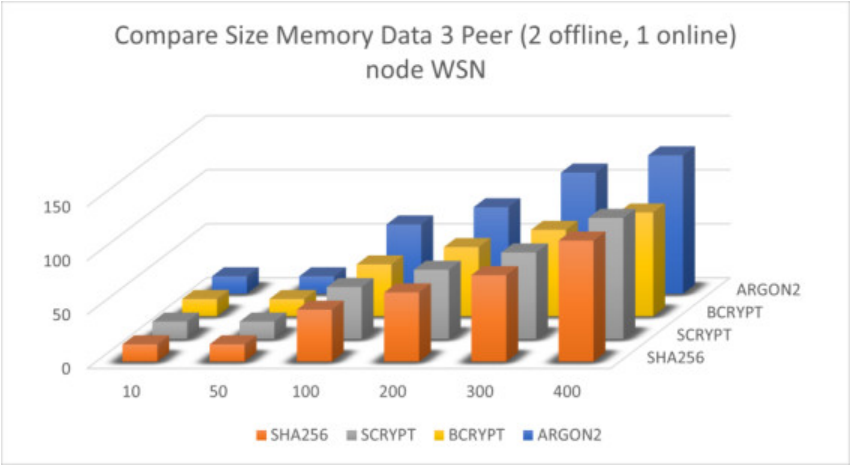
2.8.5. Perbandingan Pengujian Waktu Eksekusi Hash pada 3 *Peer* (2 Offline, 1 Online) *Node* WSN



k perbandingan waktu eksekusi hash pada 3 *peer* (2 offline, 1 online)

Pengujian pada Gambar 2.11. merupakan perbandingan empat algoritma hash yang diuji pada 3 *peer* (2 *peer* offline dan 1 *peer* online). Hasil pengujian menunjukkan bahwa Scrypt mampu menyelesaikan 400 blok dari *node* WSN dengan waktu eksekusi lebih cepat, yaitu 1.193 detik. Sementara itu, Argon2 mencatat waktu eksekusi terlama dibandingkan dengan Bcrypt dan SHA-256.

2.8.6. Perbandingan Pengujian Kapasitas Penyimpanan data dengan 3 *Peer* (2 Offline, 1 Online) *Node* WSN



Gambar 2. 12. Grafik perbandingan kapasitas memori dengan 3 *peer* (2 offline, 1 online)

Gambar 2.12. menyajikan perbandingan empat algoritma hash yang diuji pada tiga *peer* (dua offline dan satu online). Hasil pengujian menunjukkan bahwa Bcrypt memerlukan memori sebesar 96 KB untuk membuat 400 blok dari *node* WSN, sedangkan Argon2 128 KB. Sebaliknya, SHA-256 dan Scrypt menggunakan memori sekitar 112 KB. Pengujian dengan parameter yang sama dan konfigurasi algoritma standar menunjukkan bahwa Scrypt memberikan waktu eksekusi tercepat, sementara Bcrypt paling efisien dari segi penggunaan memori. Perlu dicatat bahwa WSN merupakan jaringan dengan kecepatan rendah, daya rendah, dan harus mampu mengirimkan data dari banyak sensor.

ıerupakan teknologi yang dikenal luas karena kemampuannya
istem terdistribusi, meningkatkan transparansi data, melindungi
baiki keamanan pada WSN. Berdasarkan pengujian hash peer
ıan tiga *peer* terdistribusi yang terintegrasi ke dalam WSN,

hasilnya menunjukkan bahwa Scrypt mampu menyelesaikan pembuatan 400 blok lebih cepat (1.193 detik) dibandingkan dengan Argon2, SHA-256, dan Bcrypt. Dari sisi efisiensi memori, Bcrypt terbukti menjadi pilihan paling optimal dengan konsumsi hanya 96 KB, sedangkan Argon2 memerlukan 128 KB, dan Scrypt maupun SHA-256 menggunakan memori sebesar 112 KB.

2.10. Ucapan Terima Kasih

Dalam artikel ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada Direktorat Riset, Teknologi, dan Pengabdian kepada Masyarakat (DRTPM) yang telah memberikan dukungan pendanaan melalui Hibah Penelitian Tahun 2024 dengan nomor kontrak 050/E5/PG.02.00.PL/2024, skema Penelitian Disertasi Doktor (PDD). Dukungan dana tersebut memiliki peran yang sangat penting dalam menunjang proses penelitian sehingga penelitian ini dapat diselesaikan dengan baik.

2.11. Daftar Pustaka

Abdussami, M., Amin, R., Saravanan, P., & Vollala, S. (2023). BSAPM: BlockChain based secured authentication protocol for large scale WSN with FPGA implementation. Computer Communications, 209(April), 63–77. https://doi.org/10.1016/j.comcom.2023.06.011

Adam, I. O., & Dzang Alhassan, M. (2020). Bitcoin: A *Peer*-to-*Peer* Electronic Cash System. Transforming Government: People, Process and Policy, 15(4), 580–596. https://doi.org/10.1108/TG-06-2020-0114

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 21(2), 1676–1717. https://doi.org/10.1109/COMST.2018.2886932

Alnahari, M. S., & Ariaratnam, S. T. (2022). The Application of Blockchain Technology to Smart City Infrastructure. Smart Cities, 5(3), 979–993. https://doi.org/10.3390/smartcities5030049

Atzei, N., Bartoletti, M., Cimoli, T., Lande, S., & Zunino, R. (2018). SoK: Unraveling bitcoin *Smart Contract*s. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10804 LNCS, 217–242. https://doi.org/10.1007/978-3-319-89722-6_9

Bao, Q., Li, B., Hu, T., & Sun, X. (2023). A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work. Journal of Systems and Software, 196. https://doi.org/10.1016/j.jss.2022.111555

Bartoletti, M., & Pompianu, L. (2017). An Empirical analysis of *Smart Contract*s: [illegible]cations, and design patterns. Lecture Notes in Computer [illegible]g Subseries Lecture Notes in Artificial Intelligence and Lecture [illegible]matics), 10323 LNCS, 494–509. https://doi.org/10.1007/978-3-

Borse, M., Shendkar, P., Undre, Y., Mahadik, A., & Patil, R. Y. (2022). A Review of Blockchain Consensus Algorithm. Lecture Notes in Networks and Systems, 444, 415–426. https://doi.org/10.1007/978-981-19-2500-9_31

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access, 6(September), 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Callens, E. (2021). Financial instruments entail liabilities: Ether, bitcoin, and litecoin do not. Computer Law and Security Review, 40(July 2020), 1–20. https://doi.org/10.1016/j.clsr.2020.105494

Chen, Y., Chen, S., Liang, J., Feagan, L. W., Han, W., Huang, S., & Wang, X. S. (2020). Decentralized data access control over consortium blockchains. Information Systems, 94, 101590. https://doi.org/10.1016/j.is.2020.101590

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and *Smart Contract*s for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Transactions on Services Computing, 13(2), 241–251. https://doi.org/10.1109/TSC.2020.2964537

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017). BLOCKBENCH: A framework for analyzing private blockchains. Proceedings of the ACM SIGMOD International Conference on Management of Data, Part F1277, 1085–1100. https://doi.org/10.1145/3035918.3064033

Dwivedi, S. K., Amin, R., & Vollala, S. (2023). Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability. Computer Communications, 197(January 2022), 124–140. https://doi.org/10.1016/j.comcom.2022.10.016

Ebobissé Djéné, Y. F., El Idrissi, M. S., Tardif, P. M., Jorio, A., El Bhiri, B., & Fakhri, Y. (2022). A Formal Energy Consumption Analysis to Secure Cluster-Based WSN: A Case Study of Multi-Hop Clustering Algorithm Based on Spectral Classification Using Lightweight Blockchain. Sensors, 22(20). https://doi.org/10.3390/s22207730

Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., & Herrera-Joancomartí, J. (2017). Securing Proof-of-Stake Blockchain Protocols Wenting. Proceedings, (September). https://doi.org/10.1007/978-3-319-67816-0

Göbel, J., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 104, 23–41. https://doi.org/10.1016/j.peva.2016.07.001

Godavarthi, B., Dhar, M., Devi, S. A., Raju, S. S., Balaram, A., & Srilakshmi, G. (2023). Blockchain integration with the internet of things for the employee
nagement. Journal of High Technology Management Research,
ttps://doi.org/10.1016/j.hitech.2023.100468
ch, P., & But, J. (2022). Use of blockchain in health sensor
ıre information integrity and accountability. Procedia Computer
, 124–132. https://doi.org/10.1016/j.procs.2022.10.128

Hasan, K., Chowdhury, M. J. M., Biswas, K., Ahmed, K., Islam, M. S., & Usman, M. (2022). A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks. Computer Networks, 211(April), 109004. https://doi.org/10.1016/j.comnet.2022.109004

Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2016). Password Hashing Competition - Survey and Benchmark. 1–30.

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based *Smart Contracts*: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177(November 2020). https://doi.org/10.1016/j.jnca.2020.102857

Jagannadha Swamy, T., Pallavi, B., Amaraveni, V., Sireesha, Y., & Siddarth, S. (2023). Secure Data Dissemination in Wireless Sensor Networks with the Help of Module Based Blockchain Technology. 2023 3rd International Conference on Intelligent Technologies, CONIT 2023, 1–6. https://doi.org/10.1109/CONIT59222.2023.10205841

Javaid, M., Haleem, A., Pratap Singh, R., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain: Research and Applications, 2(4). https://doi.org/10.1016/j.bcra.2021.100027

Kaschel, H., Cordero, S., Adasme, P., & Ahumada, C. (2022). Smart Agriculture 4.0: Technology Recommendations and Interoperability of Devices, Sensors and Data Management using Blockchain. 2022 IEEE International Conference on Automation/25th Congress of the Chilean Association of Automatic Control: For the Development of Sustainable Agricultural Systems, ICA-ACCA 2022, 1–7. https://doi.org/10.1109/ICA-ACCA56767.2022.10006132

Lee, J. (2018). Patch transporter: Incentivized, decentralized software patch system for WSN and IoT environments. Sensors (Switzerland), 18(2), 1–35. https://doi.org/10.3390/s18020574

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Matusiewicz, K., Pieprzyk, J., Pramstaller, N., Rechberger, C., & Rijmen, V. (2005). Analysis of simplified variants of SHA-256. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI), P-74(January), 123–134.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. Internet of Things (Netherlands), 8. https://doi.org/10.1016/j.iot.2019.100107

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of *Smart Contract* and Use Cases in Blockchain Technology. 2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018, (October), 1–4. https://doi.org/10.1109/ICCCNT.2018.8494045

Nasir, M., Bhutta, M., Khwaja, A. A., Nadeem, A., & Ahmad, H. F. (2021). A Survey [illegible] Technology : Evolution , Architecture and Security. 9. [illegible].1109/ACCESS.2021.3072849

[illegible]a, P., Lo Nigro, G., & Perrone, G. (2023). Understanding [illegible]ications in Industry 4.0: From information technology to [illegible]nd operations management. Journal of Industrial Information [illegible]larch). https://doi.org/10.1016/j.jii.2023.100456

Samreen, N. F., & Alalfi, M. H. (2023). An empirical study on the complexity, security and maintainability of Ethereum-based decentralized applications (DApps). Blockchain: Research and Applications, 4(2). https://doi.org/10.1016/j.bcra.2022.100120

Sarkodie, S. A., Ahmed, M. Y., & Owusu, P. A. (2022). COVID-19 pandemic improves market signals of cryptocurrencies–evidence from Bitcoin, Bitcoin Cash, Ethereum, and Litecoin. Finance Research Letters, 44(April 2021). https://doi.org/10.1016/j.frl.2021.102049

Sudheer, B. N., & Sujatha, K. (2023). A Brief Survey on Data Aggregation and Data Compression Models using Blockchain Model in Wireless Sensor Network. International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, 406–413. https://doi.org/10.1109/ICIDCA56705.2023.10100009

Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. (2017). Consensus protocols for blockchain-based data provenance: Challenges and opportunities. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 2018–Janua(October), 469–474. https://doi.org/10.1109/UEMCON.2017.8249088

Ullah, Z., Naeem, M., Coronato, A., Ribino, P., & De Pietro, G. (2023). Blockchain Applications in Sustainable Smart Cities. Sustainable Cities and Society, 97(September 2022), 104697. https://doi.org/10.1016/j.scs.2023.104697

Verma, S., Kaur, S., Manchanda, R., & Pant, D. (2020). Essence of Blockchain Technology in Wireless Sensor Network: A brief study. Proceedings - 2020 International Conference on Advances in Computing, Communication and Materials, ICACCM 2020, 394–398. https://doi.org/10.1109/ICACCM50413.2020.9212970

Vinya, V. L., Anuradha, Y., Karimi, H. R., Divakarachari, P. B., & Sunkari, V. (2022). A Novel Blockchain Approach for Improving the Security and Reliability of Wireless Sensor Networks Using Jellyfish Search Optimizer. Electronics (Switzerland), 11(21). https://doi.org/10.3390/electronics11213449

Xu, L., Shah, N., Chen, L., Diallo, N., Gao, Z., Lu, Y., & Shi, W. (2017). Enabling the Sharing Economy: Privacy Respecting Contract based on Public Blockchain. BCC 2017 - Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Co-Located with ASIA CCS 2017, (October), 15–21. https://doi.org/10.1145/3055518.3055527

Xu, X., Guo, Y., & Guo, Y. (2023). Fog-enabled private blockchain-based identity authentication scheme for smart home. Computer Communications, 205(February 2022), 58–68. https://doi.org/10.1016/j.comcom.2023.04.005

Xu, Y. (2020). Segment Blockchain : A Size Reduced Storage Mechanism for Blockchain. 8.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., … Chen, S. (2020). Public and private blockchain in construction business process and information

Automation in Construction, 118(May), 103276.
).1016/j.autcon.2020.103276

., Stacey, B., & Sampalli, S. (2022). A Novel Distributed Ledger
ıcture for Wireless Sensor Networks Based on IOTA Tangle.
(Switzerland), 11(15), 1–17.
).3390/electronics11152403

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A Blockchain-As-A-Service Platform. IEEE Access, 7, 134422–134433. https://doi.org/10.1109/ACCESS.2019.2941905

Zhu, J. (2023). Real-time monitoring for sport and mental health prevention of college student based on wireless sensor network. Preventive Medicine, 173(May), 107581. https://doi.org/10.1016/j.ypmed.2023.107581

BAB III
ARSITEKTUR WIRELESS SENSOR NETWORK DISTRIBUTED BLOCKCHAIN UNTUK DETEKSI ANOMALI PADA *NODE* DAN DATA SENSOR

3.1. Abstrak

Wireless Sensor Network (WSN) merupakan private network yang terdiri dari banyak sensor, WSN dikembangkan untuk daya konsumsi energi yang rendah untuk akuisisi data sensor. Private network jaringan ini masih rentan terhadap keamanan data, terutama terkait tantangan sentralisasi. Untuk mengatasi hal tersebut, teknologi *distruptive* blockchain yang mempunyai keamanan berbasis blok yang dihash dapat diterapkan. Penelitian ini mengusulkan model arsitektur yang sesuai untuk mengintegrasikan WSN dengan jaringan blockchain terdistribusi guna mendeteksi *node* sensor dan data yang mencurigakan. Model ini diimplementasikan menggunakan perangkat keras WSN dengan topologi Mesh serta komponen perangkat lunak terintegrasi, termasuk sistem blockchain. Hasil pengujian menunjukkan bahwa dengan iterasi 10 - 500 blok *node*, 3 *peer* server terdistribusi, hash Scrypt mempunyai waktu tercepat 469,49 detik dibandingkan hash lainnya. Kombinasi dua metode mekanisme konsensus antara *Smart Contract* (MAC dan SHA-256 pada mikrokontroler) dengan *Proof of Information* (PoI) 3 parameter sensor (*Temperature* atau Temp, *Humidity* atau Humd, dan *Gas Concentration* atau MQ2) menunjukkan bahwa metode ini mampu mendeteksi dan menjaga *node* sensor dan data sensor mencapai data valid 97,37%. Untuk *sensor controlling* yang terdiri dari dua *node Radio Frequency Identification* (RFID) dan satu *node Quick Response* (QR) code yang diterapkan pada 500 iterasi blok *node* menghasilkan waktu eksekusi 592,47 detik lebih lama dibandingkan dengan sensor monitoring. Hal ini menunjukkan bahwa pemisahan antara *sensor monitoring* dan *sensor controlling* merupakan pilihan terbaik untuk model arsitektur yang diusulkan. Alasan utama adalah sensor monitor memprioritaskan otomatisasi, kecepatan, dan akurasi data secara real time. Sementara itu, *sensor controlling* berfokus pada interaksi antara pengguna dan perangkat, khususnya ketika diintegrasikan ke dalam sistem transaksi.

3.2. Pendahuluan

WSN dan *Internet of Thing* (IoT) merupakan teknologi yang saling terhubung dan bekerjasama meskipun standar protokolnya berbeda. Kedua teknologi ini

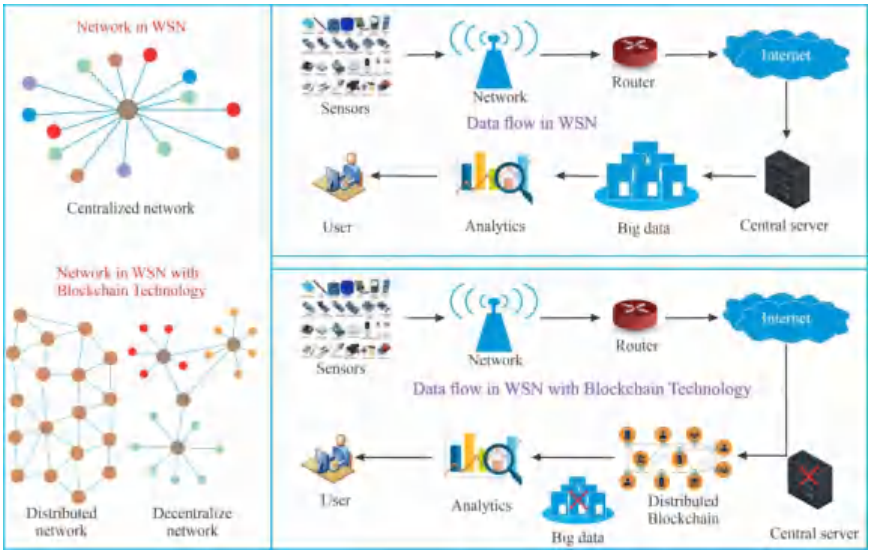
ep pengendalian sentralisasi. IoT merupakan teknologi
ma *dalam Interoperability, Security* dan *Scalability* (Kumar et
ı WSN merupakan *private network* yang dikembangkan untuk
si energi yang rendah untuk akuisisi data sensor (Begum &
gra, 2010). Kedua teknologi ini sering dikombinasikan untuk

mengakses dan memantau data dari luar WSN meskipun jaringan tersebut memiliki status privat (Keerthika & Shanmugapriya, 2021). Hal ini mendorong rekomendasi penggunaan teknologi blockchain yang bersifat disruptif, yang mampu menerapkan keamanan berbasis blok melalui mekanisme konsensus dan algoritma hash untuk mengatasi permasalahan tersebut. Blockchain (BC) adalah teknologi yang dikembangkan berdasarkan keterhubungan antar blok untuk menyimpan data dan memiliki enkripsi hash sebagai penanda blok yang penting untuk koneksi berikutnya (G.-T. Nguyen & Kim, 2018). Teknologi ini juga didefinisikan sebagai buku besar digital terdistribusi dan terstruktur yang banyak digunakan untuk pengelolaan transaksi. Beberapa konsep yang dikembangkan melalui blockchain meliputi jaringan *peer* to *peer*, buku besar terdistribusi, mekanisme konsensus, *Smart Contract*, serta penggunaan aplikasi lain yang dianggap diperlukan (Adere, 2022). Selain itu, Bitcoin dan Ethereum menggunakan blockchain untuk transaksi cryptocurrency melalui algoritma keamanan yang dikenal sebagai SHA-256 dan Ethash secara berturut-turut (Jaya et al., 2023). Penerapan ini memungkinkan pemindahan aset dan distribusi informasi melalui *Smart Contract* ke dalam jaringan (Onjewu et al., 2023). Sebagai contoh, blockchain versi 3.0 sering digunakan secara khusus untuk mendesentralisasi tata kelola dan regulasi (M. Xu et al., 2019). Teknologi ini juga telah banyak digunakan untuk meningkatkan keamanan WSN dan IoT (Alsaedy et al., 2020).

WSN merupakan sistem *embedded* yang menghubungkan banyak titik sensor yang saling terhubung ke dalam jaringan, dirancang dengan daya konsumsi rendah dengan standar komunikasi IEEE 802.15.4 (Patel et al., 2013). WSN diterapkan diberbagai bidang seperti militer, kebakaran hutan, mendeteksi pergerakan kendaraan, pemantauan lingkungan, industri, pertanian, perawatan kesehatan, smart home, transportasi, smart city dan lain-lain (Taieb, 2007). Keamanan WSN menjadi perhatian yang signifikan karena struktur yang kompleks dan kerentanan terhadap serangan internal dan eksternal (Huanan et al., 2021), komunikasi nirkabel yang terbuka membuat data dan *node* sensor rentan terhadap serangan aktif maupun pasif. Keamanan jaringan didefinisikan sebagai kebijakan, mekanisme, dan layanan yang mencegah akses tidak sah dan penggunaan ilegal ke jaringan. Saat membuat konsep mekanisme keamanan harus mempertimbangkan keterbatasan infrastruktur jaringan (Khah et al., 2023). Penggunaan blockchain dengan kemampuan hash yang saling terhubung akan dapat membantu mendeteksi jika terdapat gangguan atau manipulasi data sensor yang tersimpan, hal ini dapat diketahui melalui hash previous dan hash current setiap blok, misalkan ada 1000 blok

ipulasi maka data blok selanjutnya akan memberikan tanda
data diblok sebelumnya. Kemampuan ini yang akan digunakan
mendeteksi adanya manipulasi data sensor WSN. Selain hash,
ai kemampuan untuk memvalidasi data melalui mekanisme
bukti. Konsensus ini selalu berkembang mengikuti kebutuhan

teknologi, contoh konsensus yaitu *Proof of Work, Proof of Stake, Proof of Location, Smart Contract* dan lai-lainnya (Wen et al., 2023). Terkait penggunaan blockchain untuk menjaga keamanan data WSN, beberapa tahun terakhir ini banyak peneliti yang mengulas hal tersebut. Beberapa manfaat dan tantangan penggunaan blockchain untuk WSN telah dibahas, terutama sistem terdesentralisasi dengan hash sha256 (C. V Nguyen et al., 2021). Mekanisme konsensus dan terdesentralisasi untuk mengelola integritas data yang disimpan dalam buku besar merupakan salah satu keunggulannya, dan lebih mengutamakan keamanan dan keandalan daripada efisiensi (Hsiao & Sung, 2021). Gambar 3.1. Merupakan arsitektur sentralisasi, desentralisasi dan distribusi WSN serta aliran data Blockchain WSN.



Gambar 3. 1. Sentralisasi, desentralisasi, dan distribusi WSN dan aliran data WSN dan BWSN (C. V Nguyen et al., 2021).

Blockchain tidak hanya berfungsi sebagai mekanisme pencatatan data, tetapi juga sebagai sarana untuk memastikan integritas dan keamanan transmisi data sensor di berbagai titik dalam jaringan. Untuk meningkatkan efisiensi dan otomatisasi dalam proses validasi data sensor, diperkenalkan *Smart Contract*. *Smart Contract* merupakan skrip digital yang berjalan di atas blockchain dan secara otomatis mengeksekusi aturan yang telah ditentukan. *Smart Contract* juga telah diterapkan dalam mendeteksi *node* berbahaya (She et al., 2019a). Namun, karena sifat data sensor yang dinamis dan memiliki volume tinggi, tidak semua data perlu

ain. Oleh karena itu, kami mengusulkan pendekatan validasi *rmation* (PoI), yang berfungsi sebagai mekanisme seleksi untuk berdasarkan kualitas informasi dengan menggunakan ambang ntukan [19]. Integrasi antara blockchain, *Smart Contract*, dan rciptanya sistem yang lebih efisien, andal, serta tahan terhadap

manipulasi dalam lingkungan WSN terdistribusi. Beberapa artikel terkait menggunakan SHA-256 sebagai hash blockchain, dan penerapan algoritma ini terbilang sangat luas serta beragam. Namun, ketika diterapkan pada volume data sensor yang besar, SHA-256 dapat memberikan dampak signifikan terhadap waktu eksekusi dan kebutuhan penyimpanan dalam sistem terdistribusi. Oleh karena itu, penelitian ini mengkaji penggunaan algoritma hash alternatif untuk blockchain, dengan hasil yang digunakan untuk mengembangkan model arsitektur WSN-blockchain yang bertujuan mendeteksi data sensor dan serangan pada tingkat *node* dengan efisiensi yang lebih baik dalam hal kompleksitas waktu dan pemanfaatan penyimpanan.

Tujuan dari penelitian ini adalah mengintegrasikan mekanisme konsensus *Smart Contract* dengan PoI untuk melindungi baik *node* sensor maupun data sensor dari serangan yang tidak sah atau berbahaya dalam sistem terdistribusi. Kerangka kerja data sensor menggunakan dua lapisan fungsional utama. Lapisan pertama adalah *Blockchain Sensor Monitoring* (BSM), yang mengelola pemantauan data sensor secara real time, termasuk validasi keaslian dan integritas data sebelum dicatat pada blockchain. Lapisan ini bertanggung jawab untuk mendeteksi anomali atau manipulasi data pada tahap awal, serta memfilter informasi berdasarkan ambang batas yang telah ditentukan. Lapisan kedua, yaitu *Blockchain Sensor Controlling* (BSC), bertanggung jawab dalam mengelola kontrol akses, otorisasi *node*, serta penanganan transaksi antar sensor atau dengan sistem pusat. Pada lapisan ini, digunakan mekanisme seperti *Smart Contract*, verifikasi MAC address, dan autentikasi UID untuk memastikan hanya entitas yang berwenang yang diperbolehkan berinteraksi atau melakukan pembaruan pada sistem. *Smart Contract* dan PoI memegang peranan penting dalam memperkuat parameter identitas *node* sensor serta atribut data terkait, termasuk *Personal Area Network Identifiers* (PAN ID), alamat MAC address, nilai ambang batas (*threshold*), dan algoritma *key hash*.

3.3. Karya Terkait

Penelitian tentang model WSN dan BC banyak dikembangkan dengan berbagai metode dan mekanisme BC, Penelitian (She et al., 2019a), melakukan model deteksi *node* berbahaya dengan model kepercayaan dan *Smart Contract* untuk melacak ID dan lokasi, model ini untuk *node* sensor dan belum dicoba dengan data. Penelitian (Hsiao & Sung, 2021b) dengan model perlindungan data dengan blockchain dengan memanfaatkan Respberry PI sebagai server, kelemahannya memori tidak akan cukup untuk data sensor. Penelitian (Benaddi et al., 2021)(Feng

t model dengan *Smart Contract* untuk memfilter *Cluster header* memilih kualitas data yang bagus yang akan dibuatkan blok, ada ketergantungan dengan komponen ekternal yaitu Solidity nelitian (Tran et al., 2022)(Dwivedi et al., 2023) menggunakan an data, PoW memakan sumber daya yang besar dan

berpengaruh jika data sensor semakin banyak. Penelitian (Yuling Chen et al., 2022) menggunakan authentifikasi UID untuk melindungi *node* (mekanisme tangle), jika sesuai akan dibuat *block* baru, kelemahannya tidak ada authetifikasi pada mekanisme blockchain. Penelitian (Qi et al., 2023) dengan konsep PoI untuk membuat blok jika data valid terpenuhi, kelemahannya tidak ada perlindungan *node* sensor. Berdasarkan beberapa artikel yang telah diuraikan terdapat kelemahan dan kelebihan dalam memodelkan keamanan data sensor. Untuk itu peneliti mengusulkan model arsitektur baru dengan penggabungan beberapa metode untuk melindungi dan mendeteksi data *node* sensor itu sendiri dan data sensornya dari serangan yang berbahaya termasuk manipulasi data. Model yang diusulkan diuraikan dalam Tabel 3.1.

Tabel 3. 1. State of the art dan model yang diusulkan.

WSN dan Blockchain	Wei She (2019) (She et al., 2019)	Sung-Jung Hsiao (2021) (Hsiao & Sung, 2021)	Hafsa Benaddi (2021) (Benaddi et al., 2021)	Hoang T. Tran (2022) (Tran et al., 2022)	Huanhuan Feng (2022) (Feng et al., 2022)	Sanjeev Kumar Dwivedi (2023) (Dwivedi et al., 2023)	Yuling Chen (2022) (Yuling et al., 2022)	Weiwei Qi (2023) (Qi et al., 2023a)	*Proposed New Model*
Smart Contract	√		√	√	√				√
PoI/PoW				PoW		PoW		PoI	PoI
Authentifikasi Mac/UID							√		√
Authentifikasi ID	√					√	√		√
Sensor Monitoring (BSM)		√	√		√	√	√	√	√
Sensor Controlling (BSC)									√
SHA-256	√	√	√	√	√	√	√	√	√
Scrypt, Bcrypt, Argon2									√
Other GAP	Track lokasi	Raspberry Pi sebagai server (memroi terbatas).	Solidity	Simulasi *Smart Contract* dan PoW	Ketergantungan pada Kafka dan zookeeper	Audit penyimpanan data dengan blockchain	Simulasi fokus pada registrasi *node* sensor	PoI untuk data yang valid	Autentifikasi *node* sensor, *Smart Contract*, PoI dengan tiga sensor, pengujian beberapa hash algorithma, BSC dan BSM.
Test/ validation	OPNET	Prototipe	Simulasi	PoW simulasi tetapi tidak sesuai konsep	Simulasi	Simulasi dengan Scyther dan platform Ethereum	Simulasi Matlab	Simulasi Matlab	Prototipe (mikrokontroller, Zigbee, multisensor) dan system terdistribusi

enunjukkan kolom *proposed new model* untuk Arsitektur *WSN* ntuk Deteksi *Node* dan Data Sensor yang berbahaya atau data nelitian *state of the art.* Penelitian ini dilakukan karena belum

ada yang meneliti terkait perlindungan data *node* sensor dan data sensornya dengan dua metode konsensus *Smart Contract* untuk perlindungan dan deteksi data *node* sensor dan PoI multi sensor untuk melindungi data sensor. kebaruan dari penelitian yaitu diuraikan pada kolom *new proposed model* yang belum dilakukan oleh peneliti lain. *New proposed model* ini akan memodelkan arsitektur dengan membagi dua model sensor atau multisensor akan dibagi menjadi dua jenis yaitu *Blockchain Sensor Monitoring* (BSM) dan *Blockchain Sensor Controlling*/Transaksi (BSC). Dua jenis arsitektur ini mempunyai beberapa bagian yang berbeda, dikarenakan fungsinya juga berbeda. Langkah pertama untuk deteksi *node* sensor yaitu meregistrasi Mac Address, PAN ID, dan *Key Hash*. Kedua menetapkan batas *threshold* sensor yang digunakan untuk mencurigai pemalsuan data sensor. Kemudian jika langkah pertama dan kedua valid maka sistem akan membuat blok. Kemudian diusulkan mekanisme konsensus yang cocok dengan dua model sensor tersebut dengan *Smart Contract* dan PoI. Untuk BSC akan diusulkan mekanisme Smart Contract (Mac Address dan UID RFID, dan usulan baru yaitu validasi kontrol atau transaksi yaitu *Proof of Two Factor Authentification* (Po2FA), tetapi Po2FA tidak akan dibahas didalam artikel ini. Untuk hash dalam blockchain dilakukan pengujian model algoritma yang sesuai.

Tabel 3.1. membandingkan pendekatan terbaru dalam mengintegrasikan blockchain dengan WSN, dengan menyoroti beberapa keterbatasan seperti ketergantungan pada konsensus PoW (She et al., 2019) (Feng et al., 2022), penggunaan *Smart Contract* yang terbatas (Hsiao & Sung, 2021) (Benaddi et al., 2021), serta mekanisme autentifikasi identitas yang masih sederhana. Sebagian besar penelitian sebelumnya tidak menggabungkan kerangka kerja sensor pemantau atau sensor kontrol yang komprehensif, maupun memanfaatkan teknik validasi yang lebih maju. Sebaliknya, model yang diusulkan mengintegrasikan *Smart Contract* dengan mekanisme validasi berbasis PoI untuk berbagai input sensor, dilengkapi dengan autentifikasi yang lebih kuat, serta diimplementasikan dalam pengaturan terdistribusi di dunia nyata. Hal ini menawarkan solusi yang lebih baik dan skalabel dibandingkan simulasi dan prototipe pada penelitian sebelumnya.

Desentralisasi blockchain merupakan salah satu konsep yang sering digunakan untuk menduplikasi data. Ringkasan penelitian yang menggunakan desentralisasi dengan SHA-256 disajikan pada Tabel 3.2. Hasil pengamatan menunjukkan bahwa seluruh penelitian yang berfokus pada integrasi WSN ke dalam blockchain menggunakan algoritma hash SHA-256 dengan berbagai jenis

ɔr. Oleh karena itu, penelitian ini dilakukan untuk mengevaluasi
at maupun terdesentralisasi dengan menggunakan tiga
ɜnan *peer*, yaitu *peer* A offline (lokal) , *peer* B (online), dan *peer*
, beberapa algoritma hash juga diuji pada sistem terdistribusi

Tabel 3. 2. Data penelitian dengan SHA-256.

Ref.	Storage	Sensor	Consensus
(Sudheer & Sujatha, 2023)	Desentralisasi	*Sensor Monitoring*	*PoA*
(Cui et al., 2020)	Desentralisasi	*Node Sensor Identification*	*Credit System*
(Verma et al., 2020)	Desentralisasi	*Light Sensor*	*Time windowing method*
(Jagannadha Swamy et al., 2023)	Desentralisasi	*Sensor Monitoring*	*Consensus of miner nodes*
(Kaschel et al., 2022)	Desentralisasi	*Node Sensor Identification*	*NA*
(Godawatte, Branch, & But, 2022)	Desentralisasi	*Soil and Temperature, etc.*	*NA*
(Dwivedi et al., 2023)	Desentralisasi	*Health sensor*	*NA*
(Zhu, 2023)	Desentralisasi	*NA*	*PoW*
(Abdussami et al., 2023)	Desentralisasi	*Monitoring Sports sensor*	*NA*
(Hasan et al., 2022)	Desentralisasi	*Monitoring Sensor*	*NA*
(Ebobissé Djéné et al., 2022)	Desentralisasi	*Body Sensors*	*PoS*
(J. Lee, 2018)	Desentralisasi	*NA*	*PoAh*
(Vinya et al., 2022)	Desentralisasi	*NA*	*PoW*
(Zhang et al., 2022)	Desentralisasi	*Node Sensor*	*PoW, PoA*
(Matusiewicz et al., 2005)	Desentralisasi	*NA*	*PoW*

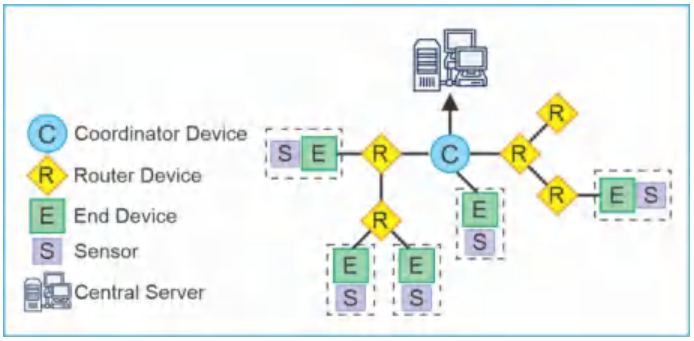
Seperti yang ditunjukkan pada Tabel 3.1. dan Tabel 3.2. berbagai pendekatan telah diusulkan untuk mengintegrasikan keamanan ke dalam WSN menggunakan teknologi blockchain. Namun, beberapa keterbatasan masih ditemukan dalam penelitian sebelumnya, antara lain keterbatasan memori dalam pemrosesan data sensor (Hsiao & Sung, 2021), kurangnya autentikasi identitas perangkat, ketergantungan pada komponen eksternal (Benaddi et al., 2021) (Feng et al., 2022), serta keterbatasan fleksibilitas mekanisme konsensus dalam menangani data dari multi sensor (Tran et al., 2022) (Dwivedi et al., 2023). Oleh karena itu, diperlukan model baru yang mampu mengatasi tantangan tersebut dengan efisiensi dan keamanan yang lebih tinggi. Model yang diusulkan dalam penelitian ini memperkenalkan arsitektur WSN berbasis blockchain terdistribusi dengan desain dua jenis sensor, yaitu BSM dan BSC. Kedua jenis ini dirancang untuk mengelola keamanan data *sensor monitoring* dan *controlling* / transaksi secara mandiri namun tetap terpadu. Sistem ini menggunakan mekanisme konsensus PoI untuk memvalidasi hanya data yang valid, sementara *Smart Contract* menjamin

lalui MAC address, PAN ID, UID dan Key hash. Selain itu, erti SHA-256, Bcrypt, Scrypt, dan Argon2 dievaluasi untuk nggunaan memori dan mengurangi waktu eksekusi pada mber daya terbatas, tanpa mengorbankan keandalan integritas *node*.

3.4. Landasan Teori

3.4.1. WSN

WSN sebuah jaringan *node* sensor yang menghubungkan perangkat seperti *end device*, *router*, *sink node* dan coordinator. WSN dapat berkomunikasi secara *hop to hop* atau *multi hop* (Zawawi et al., 2012). Gambar 3.2. merupakan contoh desain jaringan dengan protokol Zigbee dari sensor ke pusat server yang terdiri dari *coordinator, router* dan *end device.*



Gambar 3. 2. Desain jaringan dengan protokol Zigbee (Rahman, Mustika, & Kusumawardani, 2016).

Jaringan sensor terdiri dari beberapa *node* yang disebut sensor *node* dengan mikrokontroler serta transmisi, berukuran kecil dan portable. Sistem WSN merupakan kumpulan beberapa sensor *node* di beberapa tempat yang saling terhubung membentuk sebuah jaringan sensor *node*. Data sensor *node* tersebut dikumpulkan pada pusat melalui modul RF nirkabel. WSN merupakan sistem jaringan yang berfokus pada pemakaian daya rendah dengan harga yang rendah (Liu, 2015). Efisiensi energi, pengurangan ukuran dan biaya yang minimum merupakan perhatian utama untuk arsitektur sensor *node* (Huanan et al., 2021).

3.4.2. Keamanan WSN

Keamanan jaringan dapat didefinisikan sebagai seperangkat kebijakan, mekanisme, dan layanan yang mencegah akses tidak sah dan penggunaan ilegal ke dalam jaringan (Khah et al., 2023). keamanan WSN menjadi perhatian yang signifikan karena struktur yang kompleks dan kerentanan terhadap serangan internal dan eksternal (Huanan et al., 2021). Keamanan ini merupakan tantangan yang harus diatasi untuk memastikan keamanan informasi WSN. Metode serangan WSN antara

dropping, packet replays, packet changes or spoofing, node
cks such as Sybil, wormhole, sinkhole, DoS (denial-of-service),
injections of bogus messages (Ramadevi et al., 2023). WSN
enis serangan yang disebabkan oleh sifat media transmisi yaitu
serangan pasif (Butun et al., 2020). Dalam serangan aktif,

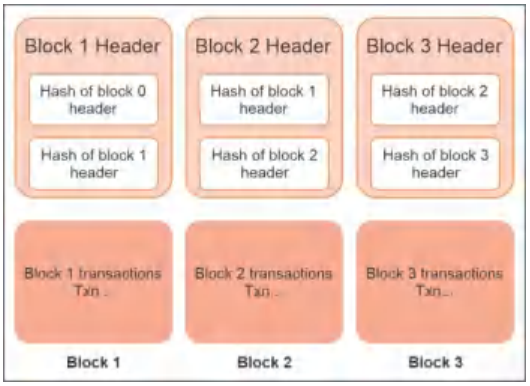
penyerang atau peretas mencari dan menghancurkan informasi, sedangkan serangan pasif penyerang biasanya mencuri informasi berharga seperti kata sandi atau data rahasia (Keerthika & Shanmugapriya, 2021).

Keamanan dalam WSN mencakup perlindungan terhadap kerentanan yang melekat, seperti keterbatasan daya komputasi, transmisi data yang terbuka, serta infrastruktur jaringan ad hoc yang sangat rentan terhadap serangan. Tantangan ini membuat WSN sangat rentan terhadap penyamaran *node*, manipulasi data, serta serangan fisik dan berbasis jaringan. Oleh karena itu, sistem keamanan WSN harus bersifat ringan namun efektif dalam menangani ancaman seperti pemalsuan data sensor, pemalsuan *node*, dan gangguan komunikasi. Tantangan utama dalam keamanan WSN meliputi autentikasi *node*, kerahasiaan data, integritas data, ketersediaan, keaslian data, serta konsistensi antar *node*. Karena kurangnya identitas yang permanen, *node* sensor rentan terhadap serangan penyamaran seperti serangan Sybil dan replikasi *node*. Keterbatasan kemampuan pemrosesan dan memori seringkali menghambat penggunaan enkripsi, sehingga data rentan terhadap penyadapan. Selain itu, data sensor dapat dimodifikasi selama transmisi, yang berpotensi menyebabkan serangan replay dan injeksi. Kondisi *node* sensor yang terbatas energi membuatnya rentan terhadap serangan DoS seperti flooding dan jamming (Ramadevi et al., 2023). Meskipun data terlihat valid, data tersebut bisa berasal dari *node* berbahaya, yang menyebabkan injeksi data palsu. Struktur terdistribusi pada WSN menimbulkan masalah sinkronisasi dan konsistensi, yang khususnya tampak pada masalah seperti fork pada buku besar terdistribusi.

3.4.3. Teknologi Blockchain

Blockchain merupakan teknologi disrupsi yang sedang berkembang terutama dalam dunia transaksi keuangan untuk keamanan. Pertama kali dikembangkan tahun 1991 oleh Stuart dan Harber, kemudian dilanjutkan oleh Satoshi Nakamoto tahun 2009 (Alsaedy et al., 2020). Pengembangan ini menghasilkan cryptocurrency yaitu bitcoin. Blockchain merupakan buku besar yang dibuat berdasakan block-block yang digunakan untuk menyimpan transaksi. Block tersebut dienkripsi menggunakan algoritma hash yang didalamnya berisi transaksi, timestamp dan hash sebelumnya (Nasraoui & Saidane, 2022). Blockchain sebagai sebuah *database* sekuensial atau *spreadsheet* raksasa yang melampaui buku besar keuangan klasik dengan mencatat informasi transaksional dengan keamanan menggunakan kriptografi, dan diatur oleh mekanisme konsensus. Teknologi ini merupakan kombinasi dari beberapa teknologi, yaitu jaringan P2P, kriptografi, dan buku besar terdistribusi (Han et al., 2023).

sebut memungkinkan transmisi data yang aman berdasarkan sangat kompleks. Hal ini dimungkinkan karena setiap blok berisi buatan yang terhubung dengan blok sebelumnya seperti yang mbar 3.3. Tren ini menunjukkan bahwa blockchain dirancang urangan dan perubahan data.



Gambar 3. 3. Struktur blok dalam blockchain (Nasraoui & Saidane, 2022).

Blockchain tidak terlepas dari *Smart Contract* dan mekanisme konsensus berbasis bukti (Proof Based). *Smart Contract* digunakan saat melakukan transaksi antara dua pihak dan transaksi tervalidasi yang dapat dimasukkan ke dalam blockchain. Untuk memvalidasi transaksi dikembangkan algoritma konsensus *Proof of Work* (PoW) ketika melakukan transaksi antar *node* blockchain (Pengguna), kemudian berkembang algoritma konsensus lainnya seperti *Proof of Stake* (PoS), *Proof of Location* (PoL), *Practical Byzantine Fault Tolerance* (PBFT)dan lain-lainnya. Konsep penerapan algoritma berbasis bukti adalah bahwa *node* dalam jaringan blockchain yang melakukan dan menunjukkan bukti yang cukup akan mendapatkan hak istimewa untuk menambahkan blok baru ke rantai utama (main chain) dan mengumpulkan *reward* (Wen et al., 2023).

Blockchain sangat cocok untuk WSN karena kemampuannya dalam menyediakan kepercayaan terdesentralisasi, immutability, dan integritas data tanpa bergantung pada otoritas terpusat. Mekanisme konsensus terdistribusi yang dimilikinya mampu mengurangi risiko *single point of failure*, sementara teknik kriptografi seperti hash *chaining* dan tanda tangan digital melindungi data sensor dari manipulasi, penyamaran, dan serangan replay. Selain itu, transparansi dan kemampuan audit bawaan pada blockchain meningkatkan kepercayaan serta akuntabilitas di antara *node* sensor yang terdistribusi. Karakteristik ini menjadikan blockchain sebagai fondasi yang kuat untuk memperkuat keamanan WSN, terutama ketika dikombinasikan dengan mekanisme konsensus ringan seperti PoI, yang disesuaikan dengan keterbatasan perangkat sensor yang memiliki sumber daya terbatas.

3.4.4 Enkripsi dan Hash

ısi dan hash merupakan konsep penting yang digunakan dalam
n utama dari keduanya adalah nilai masukkan dapat diambil
tidak. Enkripsi merupakan proses menyembunyikan pesan
lai form sehingga pihak yang tidak berkepentingan tidak dapat

membaca. Pesan yang tersembunyi disebut plaintext, dan hasil enkripsi adalah ciphertext. Pihak yang berwenang memiliki kunci rahasia untuk menyembunyikan dan membaca pesan. Enkripsi dapat ditulisan dengan rumus E(P)=C, sedangkan Dekripsi D(C)=P.

Hash merupakan Skema yang mengambil masukkan kata sandi teks biasa dan mengubah menjadi nilai hash dengan mempertimbangkan fungsi hash, iterasi dan salt. Parameter Iterasi bersifat opsional yang digunakan untuk menentukan jumlah eksekusi berturut-turut dari hash yang digunakan. Jumlah iterasi dapat disesuaikan sehingga perhitungan nilai hash membutuhkan waktu komputasi yang sangat besar (key *stretching*). Terdapat banyak fungsi yang digunakan untuk hash kata sandi antara lain: MD5, SHA1, SHA256-SHA512, PBKDF, Bcrypt, SCRYPT dan Argon2. Dalam penelitian ini kami mengambil 4 hash, SHA-256 yang merupakan default Hash Blockchain, kemudian Bcrypt, Scrypt dan Argon2.

3.4.5. Mikrokontroler

Mikrokontroler merupakan chip yang digunakan sebagai pengendali rangkaian elektronik yang mempunyai masukan dan keluaran serta program yang dapat ditulis dan dihapus. Salah satu perusahaan mikrokontroler Atmel dengan chipnya AVR telah mengembangkan perangkat komputasi fisik dengan ukuran kecil yang sekarang banyak digunakan pada papan board mikrokontroler, salah satunya Arduino. Perangkat ini berjalan pada 16 MHz dengan 8 bit core dan memiliki jumlah memori yang terbatas dengan 32 kilobyte penyimpanan dan 2 kilobyte memori RAM (Durfee, 2011). Arduino uno merupakan papan mikrokontroler berdasarkan Atmega328 yang mempunyai performa tinggi Atmel 8 bit AVR RISC (kode instruksi dan pengalamatan sedikit). Arduino Uno mempunyai 14 pin digital I/O, 6 pin analog, 16 MHz (kristal oscillator), 32 KB flash memori, 2 KB SRAM, power jack dan reset buton (Badamasi, 2014).

3.5. Metode Penelitian

3.5.1. Perancangan Sistem

Penelitian ini mengusulkan model arsitektur yang sesuai untuk mengintegrasikan WSN dan jaringan blockchain guna mendeteksi *node* sensor serta data yang mencurigakan. Model ini diimplementasikan menggunakan perangkat keras WSN dengan topologi mesh serta komponen perangkat lunak terintegrasi, termasuk sistem blockchain, tanpa bergantung pada alat simulasi konvensional. Perangkat lunak yang digunakan dalam penelitian ini meliputi Python untuk eksekusi Smart Contract, implementasi PoI, dan pembuatan blok; *database* SQL untuk gistrasi dan blok; serta antarmuka web untuk menampilkan data si. Pendekatan ini dicapai dengan membagi model sensor WSN C yang memiliki beberapa bagian berbeda karena perbedaan nggung jawab atas pemantauan data sensor secara real time,

validasi keaslian dan integritas data sebelum dicatat pada blockchain, deteksi anomali pada tahap awal, serta pemfilteran informasi berdasarkan nilai ambang batas yang telah ditentukan. Sebaliknya, BSC mengelola kontrol akses, otorisasi *node*, dan penanganan transaksi. Pada lapisan BSC, diterapkan mekanisme seperti *Smart Contract*, verifikasi MAC Address, dan autentikasi UID untuk memastikan hanya entitas yang berwenang yang dapat berinteraksi dengan sistem.

Langkah pertama dalam deteksi *node* sensor adalah melakukan registrasi MAC Address, PAN ID, dan Key Hash. Langkah kedua adalah menetapkan batas ambang sensor yang diperlukan untuk mendeteksi pemalsuan data sensor. Validasi pada langkah pertama dan kedua memungkinkan sistem untuk membentuk sebuah blok. Selain itu, key hash yang tertanam dalam mikrokontroler digunakan juga sebagai identitas tambahan pada *node* sensor. Mekanisme konsensus yang sesuai dengan dua jenis sensor, seperti *Smart Contract* dan PoI, juga diusulkan. Untuk model BSC, digunakan mekanisme konsensus *Smart Contract* yang melibatkan MAC, kunci SHA-256, dan UID. UID diregistrasi terlebih dahulu karena digunakan dalam proses kontrol atau transaksi yang diperlukan untuk memverifikasi data dan membentuk blok. Mekanisme ini banyak diterapkan pada proses kontrol, seperti akses ruangan atau transaksi keuangan, dengan tujuan melindungi pengguna. Mekanisme ini diterapkan pada sensor yang dirancang untuk kontrol atau transaksi, seperti fingerprint, RFID, dan QR code. Tren ini menunjukkan kemampuan model yang dikembangkan untuk melindungi integritas data melalui *Smart Contract*, PoI, atau mekanisme konsensus blockchain lainnya selain perlindungan pada *node* sensor. Selanjutnya, sistem blockchain terdistribusi diuji melalui penerapan tiga server *peer*. Salah satu server *peer* berfungsi sebagai master database untuk autentikasi dan pemfilteran *node* sensor atau data sensor. Sementara itu, dua server lainnya terintegrasi ke dalam *database* online untuk menyimpan data valid yang diduplikasi.

3.5.2. Langkah Prosedural untuk Keamanan dan Validasi Data Sensor

a) Inisialisasi sensor *node*

Setiap *node* sensor pertama-tama diregistrasikan ke dalam sistem melalui proses autentikasi awal. Informasi yang dikirimkan ke dalam *Smart Contract* mencakup:

- MAC address sebagai pengenal unik perangkat,
- PAN ID (Personal Area Network Identifier), sebagai identitas jaringan area pribadi,
- Key hash dari UID atau token unik perangkat, dienkripsi menggunakan
  h ringan.
  g dan akuisisi data (BSM)
  irimkan data secara real-time. Setiap paket data yang masuk

  slian menggunakan hash UID dan identitas *node*.

- Pemeriksaan integritas untuk memastikan format yang tepat dan rentang nilai yang dapat diterima.
- Pemfilteran berbasis ambang batas untuk menghilangkan data yang tidak memenuhi kriteria yang telah ditentukan.

c) Validasi konsensus dan pembentukan blok (PoI)
Jika data lolos validasi, algoritma konsensus PoI menentukan apakah informasi tersebut memiliki signifikansi dan integritas yang memadai (misalnya, berasal dari *node* tepercaya dan memenuhi semua kriteria ambang batas).
- Hanya data yang dianggap valid dan relevan yang memenuhi syarat untuk diproses.
- Data ini kemudian dibentuk menjadi blok baru dan ditambahkan ke blockchain.

d) Kontrol akses dan transaksi (BSC)
Semua aktivitas kontrol, transaksi antar-*node*, dan verifikasi data dikelola pada lapisan BSC. Mekanisme keamanan yang diterapkan pada tahap ini meliputi:
- *Smart Contract* yang memvalidasi hak akses berdasarkan peran dan izin *node*. Hanya *node* yang memenuhi aturan *Smart Contract* yang dapat memulai atau merespons transaksi.
- Verifikasi Identitas Multi-Faktor, yang mencakup:
  - Nomor RFID yang dipetakan ke *node* atau pengguna tertentu,
  - Kode QR unik yang terhubung dengan identitas sensor atau kumpulan data tertentu.

  Mekanisme ini memperkuat autentikasi entitas sebelum menerima atau mengeksekusi interaksi data.
- Audit Data Masuk.
  Semua data sensor harus melalui validasi visual atau digital melalui pemindaian QR code atau RFID sebelum dianggap sah untuk dimasukkan ke dalam blockchain. Lapisan kontrol tambahan ini mencegah injeksi data tidak sah dari *node* yang tidak terdaftar.

3.5.3. Skenario *Smart Contract* dan PoI dalam pengujian serangan

Variabel *Smart Contract* digunakan untuk melindungi data *node* sensor yang telah terdaftar dalam database, termasuk parameter seperti PAN ID, MAC address, dan kunci hash SHA-256. Sebaliknya, integritas data sensor dijaga menggunakan metode *Proof of Information* (PoI). PoI merupakan pendekatan konsensus dalam sistem terdistribusi yang dirancang untuk memverifikasi validitas informasi yang disetat pada blockchain. Dalam konteks ini, data sensor hanya akan dimasukkan ke [illegible]abila memenuhi kriteria validitas tertentu, yaitu: 1). Data berada [illegible]ang batas normal yang telah ditentukan. 2). Data tidak [illegible]ı anomali. 3). *Node* pengirim memiliki rekam jejak kepercayaan

yang baik. Secara formal, model PoI dapat diformulasikan sebagai integrasi dari ketiga aspek utama tersebut.

$$\text{PoI}_{\text{score}} = \alpha \times \text{Entropy}(\text{Data}) + \beta \times \text{Trust}(Node) + \gamma \times \text{Relevance} \quad (3.1)$$

Di sini, Entropy (Data) mengukur tingkat ketidakpastian atau keunikan pada data, Trust (*Node*) mengevaluasi kredibilitas *node* berdasarkan riwayatnya dalam mengirimkan data yang valid, sedangkan Relevance menilai relevansi data terhadap konteks atau kebutuhan sistem. Parameter α, β, dan γ merepresentasikan bobot yang diberikan pada masing-masing aspek, yang disesuaikan dengan desain sistem, dengan ketentuan bahwa α + β + γ = 1.

Dalam penelitian ini, pendekatan PoI disederhanakan menggunakan metode penyaringan berbasis ambang batas (*threshold based filtering*). Validitas data sensor ditentukan berdasarkan apakah data tersebut berada dalam rentang normal yang telah ditentukan. Untuk setiap sensor x_i, validasi dapat dinyatakan dengan fungsi indikator sebagai berikut:

$$\delta_i(x_i) = \begin{cases} 1 \text{ if } L_i < x_i < U_i \\ 0 \text{ if } x_i \leq L_i \text{ or } x_i \geq U_i \end{cases} \quad (3.2)$$

Di mana x_i adalah nilai dari sensor ke-i (misalnya suhu, kelembapan, MQ2), $L_i$dan U_i masing-masing merupakan batas bawah dan batas atas yang mendefinisikan rentang valid untuk nilai sensor tersebut, serta $\delta_i(x_i)$ adalah fungsi indikator untuk sensor ke-i.

Jika $$\sum_{i=1}^{n} \delta_i(x_i) = n \quad (3.3)$$

lalu buat blok baru karena semua pembacaan sensor valid.
Atau, dalam bentuk logika Boolean:

$$\text{Block\_Valid} \begin{cases} 1 \text{ if } \wedge_{i=1}^{n} \ \delta_i(x_i) = 1 \\ 0 \text{ otherwise} \end{cases} \quad (3.4)$$

Contoh untuk tiga sensor:

$$\delta_1(\text{temp}) \wedge \delta_2(\text{hum}) \wedge \delta_3(\text{MQ2}) = 1 \Rightarrow \text{Valid} \rightarrow \text{Store to Block} \quad (3.5)$$

Pseudocode metode PoI dapat dituliskan sebagai berikut:

eadings: temp, hum, MQ2
ds: temp_range (L1, U1), hum_range (L2, U2), MQ2_range (L3,

```
Function IsValid(x, L, U):
   Return 1 if (L < x < U) else 0

Begin:
   V_temp = IsValid(temp, L1, U1)
   V_hum  = IsValid(hum, L2, U2)
   V_MQ2  = IsValid(MQ2, L3, U3)

   If V_temp AND V_hum AND V_MQ2 == 1:
         CreateNewBlock(temp, hum, MQ2)
   Else:
         RejectDataOrMarkAsSuspicious()
```

Penelitian ini menerapkan metode penyaringan berbasis ambang batas (threshold-based filtering) untuk memastikan validitas data sensor sebelum dicatat ke dalam blockchain. Data dianggap valid apabila berada dalam rentang berikut: 20°C hingga 40°C untuk suhu, 40% hingga 70% RH untuk kelembapan, dan 50 hingga 600 untuk konsentrasi gas (MQ2). Ambang batas ini dipilih untuk merepresentasikan kondisi lingkungan normal serta mengecualikan pembacaan anomali dari sistem terdistribusi.

Rincian serangan dan strategi mitigasi yang digunakan untuk pengujian dijelaskan secara lengkap pada Tabel 3.3.

Tabel 3. 3. Ancaman keamanan dan strategi mitigasi dalam sistem WSN blockchain menggunakan *Smart Contract* dan PoI.

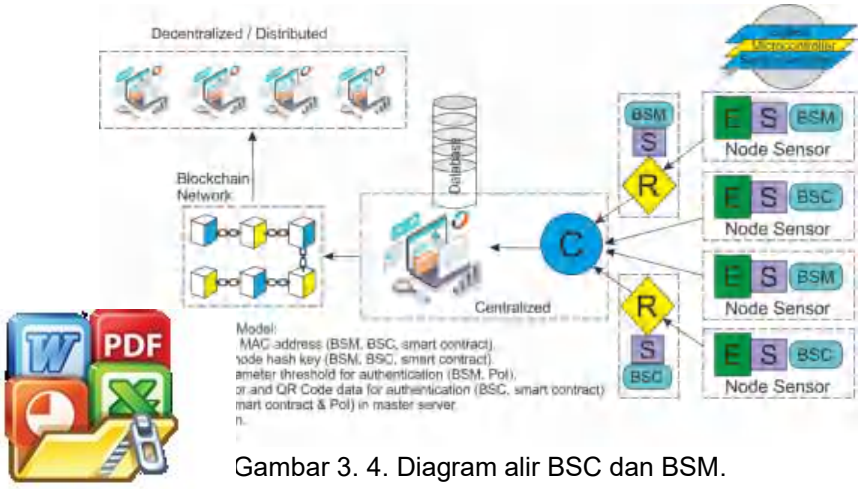
Ancaman	Strategi Mitigasi	Peran *Smart Contract*	Peran PoI
Sybil Attack	Verifikasi identitas *node* menggunakan kredensial unik dan validasi data sensor	Memverifikasi *node* secara otomatis sebelum menyetujui transaksi	Hanya menerima data terverifikasi dalam rentang ambang batas valid
Replay Attack	- Pencatatan waktu (timestamping) - Nonce unik pada setiap transaksi	Menolak transaksi yang sama atau duplikat	Hanya menerima data terverifikasi dalam rentang ambang batas valid
Sensor Data Manipulation	Validasi ambang batas	Menolak transaksi yang dianggap tidak valid oleh aturan kontrak	Fungsi indikator: hanya data dalam rentang valid yang disimpan
Malicious/ Untrustworthy *Node*	Daftar hitam otomatis	Mengunci atau menonaktifkan *node* dengan reputasi buruk	Hanya menerima data terverifikasi dalam rentang ambang batas valid
Data Tampering	Enkripsi dan hash data penyimpanan	Kontrak hanya menerima data dengan hash kunci *node* yang sesuai	Memeriksa integritas data sensor dan memvalidasi rentang ambang batas
	ujung ke ujung	Mengelola enkripsi dan autentikasi dalam *Smart Contract*	Terlibat secara tidak langsung dengan menjaga validitas data terverifikasi

Ancaman	Strategi Mitigasi	Peran *Smart Contract*	Peran PoI
Consensus Failure/ Blockchain Data Inconsistency	Sinkronisasi periodik antar *node*	Menjamin konsistensi urutan blok dan validasi hash	Data tidak valid dikecualikan dari blok, menjaga keseragaman

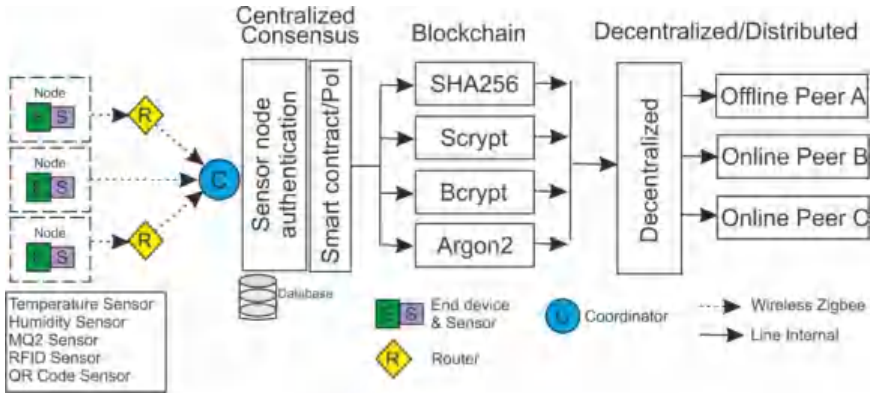
3.5.4. Perancangan Model

Sensor WSN dibagi menjadi dua jenis, yaitu BSM dan BSC seperti yang telah dibahas pada sub bagian sebelumnya. BSM menggunakan mekanisme konsensus *Smart Contract* berbasis MAC Address, PAN ID dan Key Hash serta PoI yang bebasis ambang batas, sedangkan BSC seperti fingerprint, RFID, dan QR Code memungkinkan model untuk melindungi integritas data melalui *Smart Contract* (MAC Address, PAN ID, UID dan *Key Hash*) dan keamanan tambahan multi faktor untuk memberikan perlindungan pada *node* sensor. Model arsitektur yang diusulkan ditunjukkan pada Gambar 3.4., di mana sensor BSM dan BSC terintegrasi ke dalam satu titik server atau sistem terpusat. Model ini tidak menghilangkan elemen sentralisasi, tetapi menambahkan desentralisasi melalui blockchain. Hal ini dicapai melalui penerapan jaringan WSN dengan topologi Mesh.

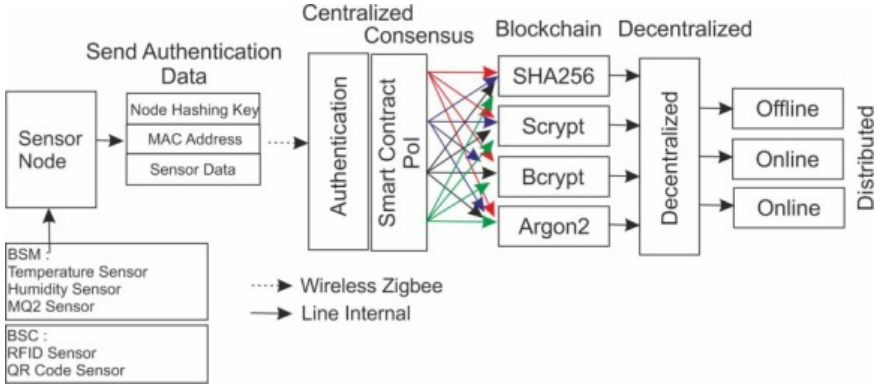
Skenario pengujian pertama dilakukan dengan menggunakan *Smart Contract* yang diintegrasikan ke dalam sistem terpusat dan terdesentralisasi dengan tiga *node peer* terdistribusi, yaitu *peer* A (*master*, lokal) dan *peer* B dan C (online). Pengujian ini juga diujicoba dengan beberapa algoritma hash yang digunakan untuk membentuk blockchain dengan (SHA-256, Scrypt, Bcrypt, dan Argon2) pada setiap skenario server. Hasil pengujian kemudian dievaluasi untuk memberikan rekomendasi terkait penerapan algoritma hash dalam jaringan WSN yang terdiri dari ribuan *node* dan sejumlah besar data sensor. Pengujian yang lain yang menjadi fokus yaitu waktu eksekusi dan kinerja program blockchain yang dipengaruhi oleh pemilihan algoritma hash. Skenario pengujian ini ditunjukkan pada Gambar 3.5. berikut.



Gambar 3. 4. Diagram alir BSC dan BSM.



Gambar 3. 5. Diagram alir skenario satu data WSN ke Blockchain.

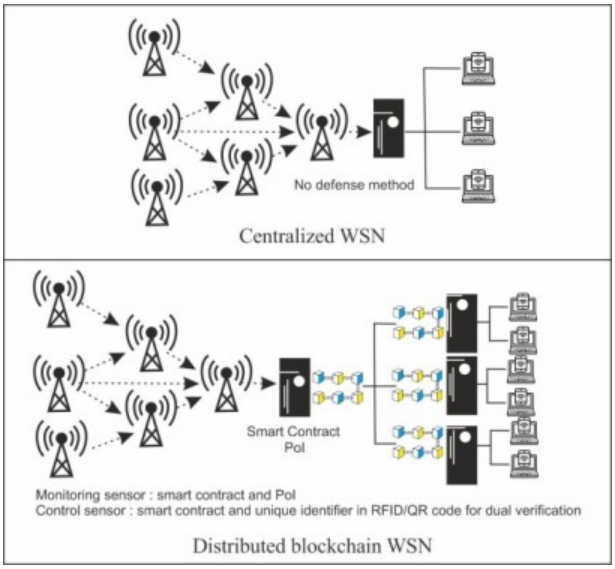


Gambar 3. 6. Diagram alir skenario pengujian kedua.

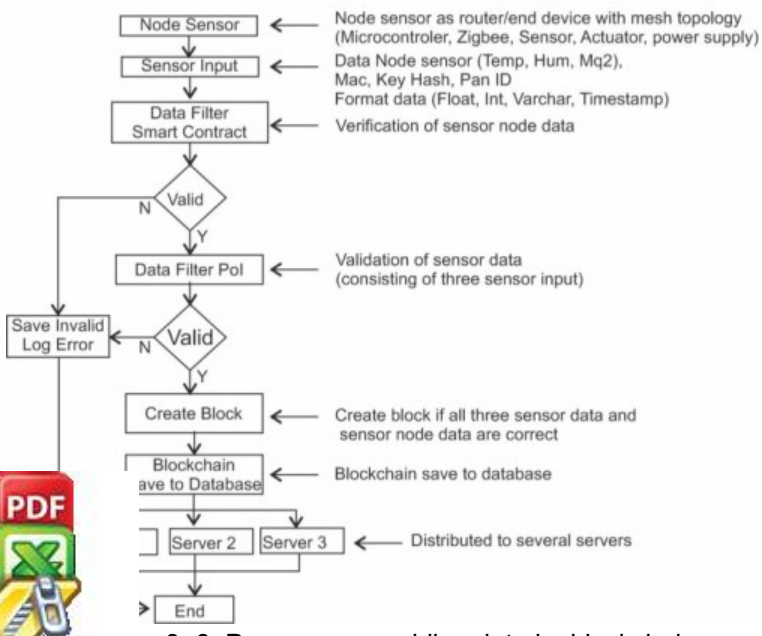
Masing-masing dari keempat algoritma hash menunjukkan karakteristik unik, khususnya dalam proses pembentukan hash. Selain itu, skenario pengujian kedua yang ditampilkan pada Gambar 3.6. menunjukkan efisiensi algoritma hash dan mekanisme konsensus untuk BSM dan BSC. Modul sensor dan transmisi nirkabel pada *node* yang terintegrasi ke dalam mikrokontroler diuji dengan algoritma hash sebagai identitas. Selanjutnya, dilakukan penilaian autentikasi melalui mekanisme konsensus pada WSN terpusat. Setelah proses validasi selesai, blockchain dengan algoritma tertentu dibentuk melalui sistem terdesentralisasi dengan akses yang dapat bersifat offline, online, atau hybrid. Algoritma *key hash* yang digunakan pada mikrokontroler dan blockchain dapat berbeda.

WSN terpusat dan WSN berbasis blockchain terdistribusi menunjukkan r dalam aliran data serta perlindungan keamanan baik untuk ı data sensor. Seperti yang digambarkan pada Gambar 3.7., sulkan mekanisme pertahanan keamanan yang ditingkatkan *monitoring* dan *controlling* sebelum pembentukan blok *ensor Monitoring*, digunakan pendekatan konsensus berbasis

Smart Contract dan mekanisme PoI. Sementara itu, untuk *sensor controlling*, *Smart Contract* diintegrasikan dengan pengidentifikasi unik yang tertanam pada RFID atau QR Code untuk memungkinkan verifikasi dua lapis (*dual-layer verification*). Proses pengambilan data untuk pembentukan blockchain terdistribusi ditunjukkan pada Gambar 3.8.



Gambar 3. 7. Diagram tinjauan perbandingan yang menggambarkan perbedaan antara WSN terpusat dan WSN terdistribusi.



ar 3. 8. Proses pengambilan data ke blockchain.

3.6. Pembahasan dan Diskusi

3.6.1. *Node* WSN dengan *Blockchain* Terdistribusi

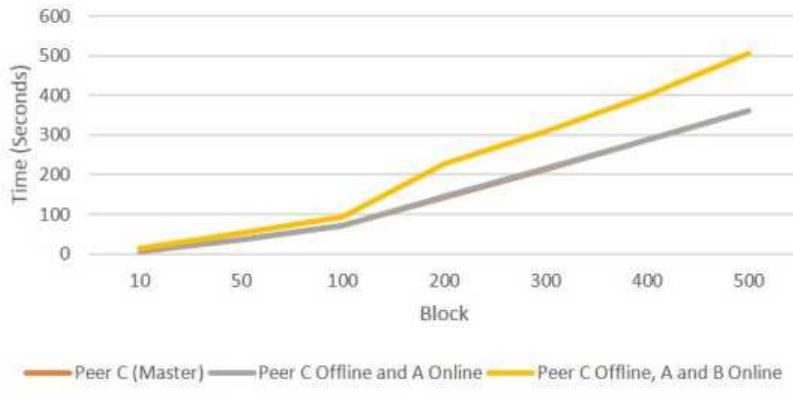
Node WSN dengan blockchain terdistribusi dalam bentuk SHA-256, Scrypt, Bcrypt, dan Argon2 diuji untuk menentukan waktu eksekusi tercepat dan kapasitas memori untuk menyimpan data. Hal ini dicapai menggunakan prototipe WSN dengan 3-5 *node* Zigbee xbee dan tiga sensor pemantauan. Selain itu, 10-500 iterasi blockchain dilakukan menggunakan tiga server *peer* terdistribusi, termasuk satu luring dan dua daring.

1) ***Node* WSN dengan SHA-256**
   Gambar 3.9. menunjukkan bahwa waktu yang dibutuhkan untuk mengirim data ke tiga server *peer* menggunakan SHA-256 adalah sekitar 506,62 detik.

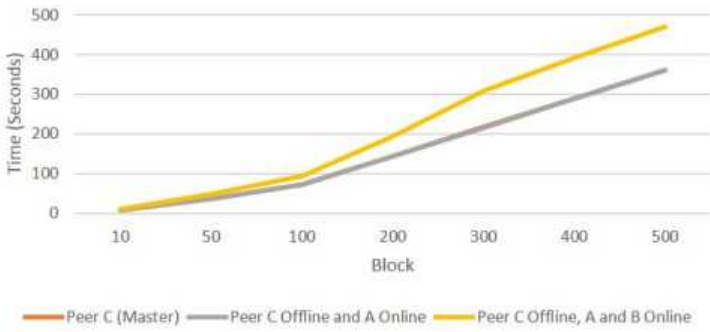
2) ***Node* WSN dengan Scrypt**
   Gambar 3.10. menunjukkan bahwa waktu yang dibutuhkan Scrypt untuk mengiterasi 500 blok dari tiga server *peer* adalah 469,49 detik.

3) ***Node* WSN dengan Bcrypt**
   Gambar 3.11. menunjukkan bahwa waktu yang dibutuhkan Bcrypt untuk mengiterasi 500 blok dari tiga server *peer* adalah 705,87 detik.

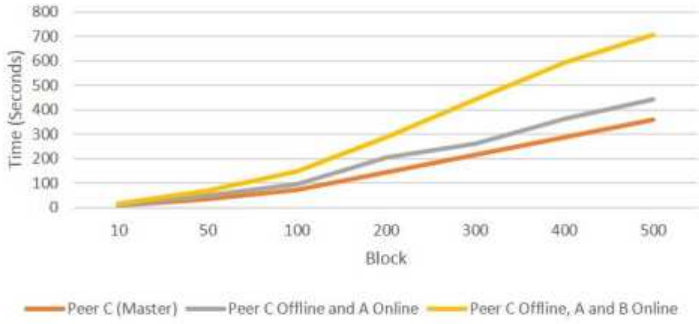
4) ***Node* WSN dengan Argon2**
   Argon2 menyelesaikan 500 blok dari tiga server *peer* dalam 602,84 detik seperti yang ditunjukkan pada Gambar 3.12.



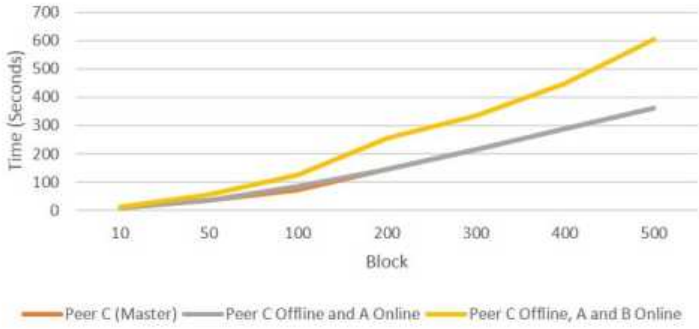
Gambar 3. 9. *Node* WSN menggunakan SHA-256.



Gambar 3. 10. *Node* WSN menggunakan Scrypt.



Gambar 3. 11. *Node* WSN menggunakan Bcrypt.

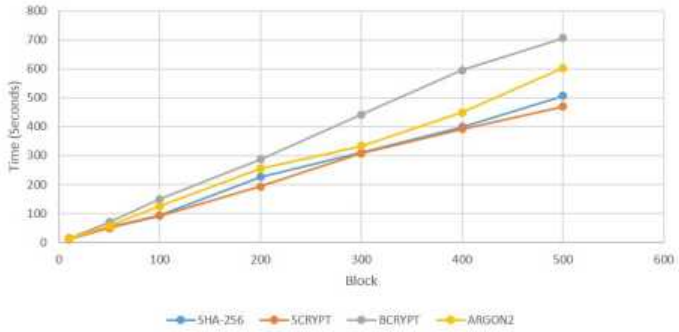


Gambar 3. 12. *Node* WSN menggunakan Argon2.

5) Perbandingan waktu eksekusi

Gambar 3.13. membandingkan waktu eksekusi untuk keempat algoritma hash pada tiga server *peer*. Hasil menunjukkan bahwa Scrypt oses untuk 500 blok dengan waktu 469,49 detik lebih cepat 3, Bcrypt, dan Argon2. Hal ini mendorong penerapan Scrypt lanjutnya terhadap model yang diusulkan. Argon2 diamati

memiliki kapasitas penyimpanan terbesar, sementara Bcrypt memiliki kapasitas terkecil.



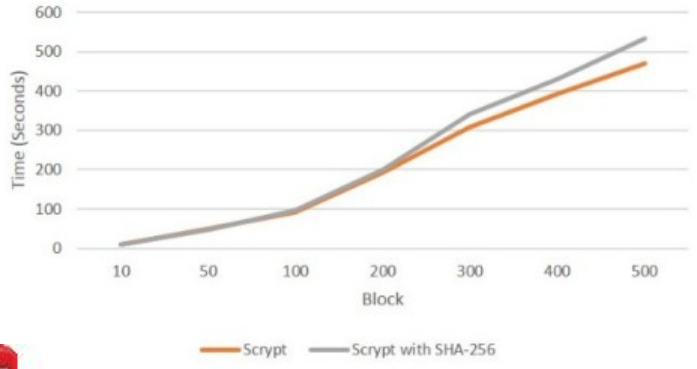
Gambar 3. 13. Perbandingan waktu eksekusi.

3.6.2. Perbandingan WSN Blockchain ((Scrypt vs Scrypt with SHA-256)

Penelitian ini membandingkan blockchain WSN yang hanya menggunakan Scrypt dengan SHA-256 yang tertanam dalam mikrokontroler sebagai autentikasi ganda pada *node* sensor. Hal ini dijelaskan lebih lanjut di subbagian berikut.

1) **Perbandingan Waktu Eksekusi WSN Blockchain (Scrypt vs Scrypt menggunakan SHA-256 in *Node* Sensor)**

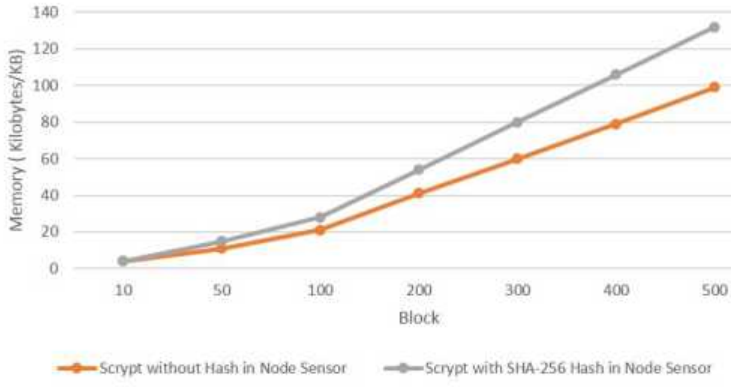
   Hasil penelitian menunjukkan bahwa penambahan autentikasi keamanan atau *Smart Contract* pada *node* sensor atau mikrokontroler menyebabkan waktu eksekusi menjadi lebih lama, sebagaimana ditunjukkan pada Gambar 3.14. Perbedaannya diperkirakan mencapai 63,54 detik. Keuntungan dari penambahan dari SHA-256 pada *node* sensor untuk authentifikasi keamanan ganda. SHA-256 yang ada dimikrokontroler akan digunakan untuk pengujian selanjutnya dan diterapkan pada arsitektur untuk penambahan parameter *Smart Contract*.



ɔandingan waktu eksekusi WSN Blockchain (Scrypt vs Scrypt menggunakan SHA-256).

2) Perbandingan Kapasitas Penyimpanan WSN Blockchain (Scrypt vs Scrypt menggunakan SHA-256 in *Node* Sensor)

Gambar 3.15. menunjukkan bahwa penambahan autentikasi keamanan atau *Smart Contract* pada *node* sensor atau mikrokontroler meningkatkan ukuran memori menjadi 132 KB. Hal ini disebabkan karena data hash yang dikirim disimpan pada setiap blok dalam blockchain.



Gambar 3. 15. Perbandingan kapasitas memori WSN Blockchain (Scrypt vs Scrypt menggunakan SHA-256).

3.6.3. Kapasitas Deteksi WSN dengan Blockchain

Prototipe WSN diuji menggunakan 3-5 *node* Xbee Zigbee dengan tiga sensor monitoring. Skenario ini berfokus pada penerapan algoritma hash Scrypt dengan 10 hingga 500 iterasi pada tiga server *peer* yang terdistribusi yang terdiri dari satu server master dan dua server online. Tujuan utama eksperimen ini adalah untuk mendeteksi *node* sensor dan data yang valid dan tidak valid (termasuk yang berbahaya atau anomali), yang mungkin diakibatkan oleh manipulasi atau kesalahan perangkat keras. Berikut penjelasan tentang apa yang dimaksud dengan data valid dan tidak valid:

- **Data Valid**: Data sensor yang berasal dari *node* yang identitasnya telah diautentikasi melalui *Smart Contract*, menggunakan MAC address, PAN ID, dan key hash. Data ini selanjutnya divalidasi menggunakan mekanisme PoI, berdasarkan kriteria ambang batas untuk suhu, kelembapan, dan gas MQ2.
- **Data Tidak Valid**: Data yang berasal dari *node* yang tidak terdaftar, pembacaan sensor yang dimanipulasi atau dipalsukan, nilai yang berada di luar ambang batas yang telah ditentukan, atau data yang terpengaruh oleh serangan Sybil, rta jenis intrusi berbahaya lainnya.

gistrasi *Node*

jukkan hasil pengujian deteksi yang dilakukan menggunakan , tiga server *peer* terdistribusi, dan iterasi blockchain *node* . Diketahui bahwa *node* eksternal dengan PAN ID yang sama

tetapi tidak terdaftar berhasil masuk ke server terdistribusi. Sebagai contoh, dari 400 *node* blok yang diiterasikan dalam server, hanya 304 yang ditemukan valid setelah pemeriksaan dan analisis, sedangkan 96 sisanya berasal dari luar.

2) Deteksi menggunakan registrasi alamat MAC

Pengujian deteksi yang dilakukan dengan menggunakan tiga *node* sensor, tiga server *peer* terdistribusi, dan iterasi blockchain *node* sebanyak 10–500 menunjukkan bahwa data yang dieksekusi dan didistribusikan hanya berasal dari *node* MAC yang terdaftar. *Node* ilegal disimpan dalam log data yang telah ditentukan. Namun, metode ini memiliki kelemahan, yaitu terdeteksinya penyimpanan data sensor yang dimanipulasi (termasuk temp, humd, dan MQ2) di server, meskipun *node* tersebut terdaftar. Tabel 3.5. menunjukkan hasil pengujian deteksi yang dilakukan dengan alamat MAC terdaftar. Dari hasil tersebut, contoh untuk 300 blok, terdeteksi 264 *node* terdaftar dan 36 *node* tidak terdaftar. Selain itu, dari 264 *node* terdaftar tersebut, terdapat 84 data yang dimanipulasi atau tidak valid, sehingga total data yang dianggap valid hanya 201.

Tabel 3. 4. Deteksi data tanpa registrasi.

No	Blok	Outer Nodes	Number Sent to Server
1	10	2	10
2	50	12	50
3	100	22	100
4	200	45	200
5	300	67	300
6	400	96	400
7	500	138	500

Tabel 3. 5. Deteksi data menggunakan registrasi.

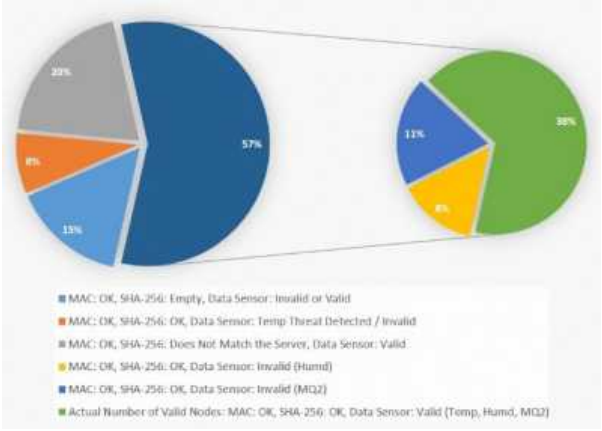
Blok	Registered MAC Address *Nodes*	Unregistered MAC Address *Nodes*	Registered MAC Address *Nodes* with Manipulated Data	Actual Number of Valid *Nodes*
10	8	2	3	5
50	41	9	14	27
100	81	19	23	58
200	158	42	36	122
300	264	36	63	201
400	358	42	84	274
500	460	40	106	354

Tabel 3. 6. Deteksi data menggunakan *Smart Contract* (MAC dan SHA-256).

	MAC: OK, SHA-256: empty, data sensor: invalid or valid	MAC: OK, SHA-256: available but not registered, data sensor: valid	MAC: OK, SHA-256: OK, data sensor: invalid (Temp, Humd, MQ2)	Actual valid *node*s, MAC: OK, SHA-256: OK, data sensor: valid (Temp, Humd, MQ2)
	27	13	7	53

3) **Deteksi data menggunakan *Smart Contract* (MAC dan SHA-256)**
Tabel 3.6. menunjukkan hasil pengujian deteksi untuk *node* yang menggunakan registrasi MAC serta penyertaan algoritma hash SHA-256 pada mikrokontroler. Hasil dari 100 iterasi yang dilakukan pada *node* blok menunjukkan bahwa 60 *node* valid berdasarkan identitas registrasi, 27 terdeteksi tanpa hash SHA-256, dan 13 teridentifikasi menggunakan algoritma hash yang berbeda. Setelah dilakukan pemeriksaan ulang, ditemukan 7 *node* blok memiliki data sensor yang tidak valid atau telah dimanipulasi, sehingga hanya 53 *node* blok yang tervalidasi. Tren ini menunjukkan perlunya metode yang lebih akurat dalam bentuk mekanisme konsensus PoI.

4) **Deteksi data menggunakan *Smart Contract* (MAC dan Hash SHA-256) dan PoI (Temp)**
Gambar 3.16. menunjukkan penerapan *Smart Contract* dan PoI Temp pada 100 iterasi *node* blok. Hasil pengujian menunjukkan bahwa 57% data berhasil masuk ke server terdistribusi atau dianggap valid, sedangkan sisanya terdeteksi sebagai tidak valid berdasarkan informasi yang diperoleh. Hasil analisis ulang mengungkapkan bahwa dari 57% data yang dianggap valid tersebut, terdapat 8% yang merupakan data sensor 2 (kelembapan) tidak valid dan 11% yang merupakan data sensor 3 (MQ2) tidak valid. Metode ini juga memiliki kelemahan, yaitu ketidakmampuannya dalam mendeteksi sensor lainnya.

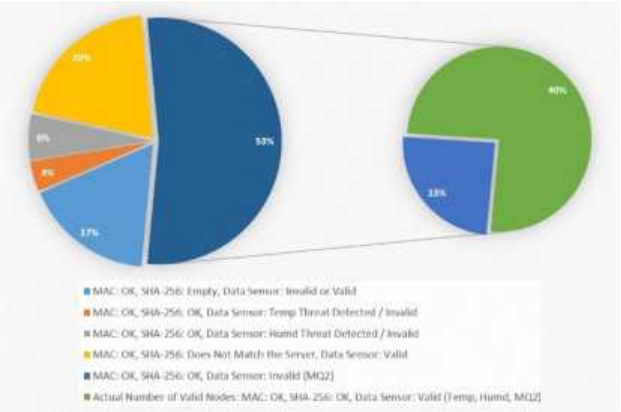


Gambar 3. 16. Deteksi data menggunakan *Smart Contract* (MAC dan hash SHA-256).

5) **Deteksi data menggunakan *Smart Contract* (MAC dan Hash SHA-256) dan**
l)

nunjukkan penerapan *Smart Contract* dan PoI (Temp, Humd) *node* sensor dan data. Hasil pengujian menunjukkan bahwa 0 iterasi *node* blok pada server terdistribusi dianggap valid, ya terdeteksi tidak valid. Hasil analisis ulang menunjukkan data yang valid tersebut, terdapat 13% yang merupakan data

MQ2 tidak valid, sehingga hanya sekitar 40% data yang benar-benar valid. Metode ini juga memiliki kelemahan, yaitu ketidakmampuannya dalam mendeteksi sensor ketiga akibat adanya data yang dimanipulasi atau rusak.



Gambar 3. 17. Deteksi data menggunakan *Smart Contract* (MAC dan hash SHA-256).

6) Deteksi data menggunakan *Smart Contract* (MAC dan Hash SHA-256) dan PoI (Temp, Humd, MQ2)

Gambar 3.18. menunjukkan penerapan *Smart Contract* dan PoI (Temp, Humd, MQ2) pada 100 iterasi *node* blok. Hasil pengujian menunjukkan bahwa 38% data berhasil masuk ke server terdistribusi atau dianggap valid, sedangkan sisanya terdeteksi sebagai tidak valid. Berdasarkan informasi dari PoI, terdapat 1% dari 38% data valid yang mengalami kesalahan akibat pengaruh jaringan. Metode gabungan ini mampu mendeteksi *node* yang valid dan tidak valid sekaligus mengidentifikasi jenis sensor yang bermasalah. Persentase yang ditampilkan menunjukkan jumlah blok yang tervalidasi dari total 100 *node* yang diuji.

- Nilai 38% pada bagian "Jumlah aktual *node* yang valid..." menunjukkan bahwa terdapat 38 blok yang berhasil diverifikasi sebagai valid (yaitu MAC dan SHA-256 sesuai, serta nilai sensor berada dalam batas ambang yang dapat diterima).
- Demikian pula, nilai lain seperti 15%, 8%, 4%, dan seterusnya masing-masing merepresentasikan jumlah blok dari total 100 blok yang diuji.

Secara keseluruhan, dari 100 blok yang dianalisis, sebanyak 38 blok dikonfirmasi sepenuhnya valid dan layak untuk dimasukkan ke dalam blockchain. Informasi yang disajikan dalam Tabel 3.7. menunjukkan bahwa penerapan dua mekanisme *Smart Contract* dan PoI, meningkatkan persentase data valid di si menjadi 97,37%, Sedangkan 2,63% terkait dengan jaringan dalam mendistribusikan data ke semua server. angka relatif kecil, kesalahan residual ini memiliki dampak kritis an sistem WSN. Dalam aplikasi yang sensitif terhadap

keamanan, bahkan persentase kecil data yang tidak terkirim atau tidak tervalidasi dapat menyebabkan inkonsistensi sistem, keterlambatan pengambilan keputusan, atau membuka celah terhadap serangan replay maupun injection.

Kategori A, ini merupakan kategori awal yang hanya menggunakan registrasi Mac dan hanya mampu mendeteksi *node* invalid sebesar 17 blok, sedangkan *node* invalid yang tidak terdeteksi masih tergabung dengan data valid, jumlah keduanya 83 blok (*T*), setelah dilakukan audit data ternyata ada 45 data invalid (*I*) dan 38 data valid (*V*). Rumus untuk menghitung persentase data valid dan tidak valid adalah sebagai berikut:

$$\text{Valid (\%)} = \left(\frac{\text{V}}{\text{T}}\right) \times 100 \ , \ \text{Invalid (\%)} = \left(\frac{\text{I}}{\text{T}}\right) \times 100 \qquad (3.6)$$

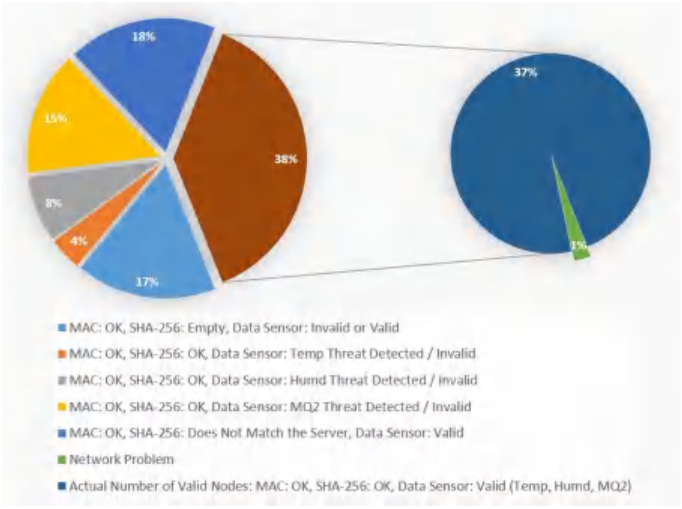
Dengan demikian, Kategori A memiliki persentase data tidak valid yang tidak terdeteksi sebesar 54,22%. Rumus ini digunakan juga untuk Kategori B dan C.

Kategori B, sistem berhasil mendeteksi 29 blok data yang tidak valid. Analisis dan verifikasi lebih lanjut menunjukkan bahwa 71 blok (*T*) awalnya dianggap valid, setelah dianalisis Kembali ternyata ada 33 blok tidak valid yang tidak terdeteksi (*I*) dan 38 blok valid (*V*). Hasil menunjukkan bahwa 53,52% data valid, sementara 46,48% tidak valid.

Pada Kategori C, sistem berhasil mendeteksi 44 blok tidak valid dengan 15 blok berasal dari data sensor MQ2 yang tidak valid. Namun, analisis selanjutnya mengungkapkan bahwa terdapat 18 data tidak valid masuk ke dalam blok terverifikasi (total 56 blok). Hal ini terjadi karena verifikasi identitas SHA-256 tidak sesuai dikarenakan pengujiannya untuk autentifikasi SHA-256 di non aktifkan dan hanya PoI tiga sensor yang digunakan, sehingga persentase data valid (*V*) dan tidak valid (*I*) dihitung ulang dan didapatkan *V* = 38 dan *I* = 18, sehingga total menjadi 56 blok (*T*).

Pada Kategori D, sistem awalnya mendeteksi 38 blok data valid (100%) dengan mengaktifkan semua *Smart Contract* dan PoI. Namun, setelah validasi ulang atau audit data, ditemukan bahwa 1 blok bermasalah (satu blok hilang di server atau jumlah total blok tidak sinkron). Data valid pertama (V_a) dan data tidak valid baru (I_b) dihitung ulang untuk menentukan nilai data valid baru (V_b), dengan: $V_b = V_a - I_b$. Oleh karena itu, total blok (T) = $V_b + I_b$. Validasi kemudian diperbarui sebagai berikut: V_a: 38, I_b:1. Dengan demikian, persentase data valid dan tidak valid (setelah audit) dapat dihitung sebagai berikut:

$$\text{Valid (\%)} = \left(\frac{V_b}{T}\right) \times 100 \ , \ \text{Invalid (\%)} = \left(\frac{I_b}{T}\right) \times 100 \qquad (3.7)$$



Gambar 3. 18. Deteksi data menggunakan *Smart Contract* (MAC dan hash SHA-256).

Tabel 3. 7. Data valid *node* menggunakan *Smart Contract* dan PoI.

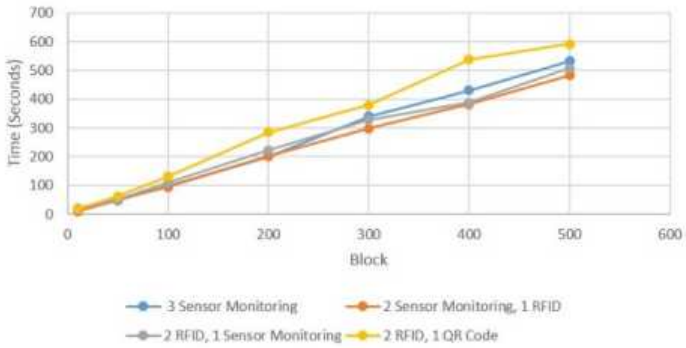
Cat.	Category A MAC: OK, SHA-256: empty, data sensor: invalid or valid	Category B MAC: OK, SHA-256: OK, data sensor: Humd threat detected/ invalid	Category C MAC: OK, SHA-256: OK, data sensor: MQ2 threat detected/ invalid	Category D MAC: OK, SHA-256: OK, data sensor: valid (Temp, Humd, MQ2), 1 Block lost/Network Problem
Valid	45,78%	53,52%	67,86%	97,37%
Invalid	54,22%	46,49%	32,14%	2,63%

3.6.4. Perbandingan Waktu Eksekusi WSN Blockchain (*Sensor Monitoring* dan *Controlling*)

Pengujian dilakukan untuk membandingkan waktu eksekusi sensor pemantauan, pengontrol, dan hibrida. Sensor pemantauan terdiri dari suhu, kelembapan, dan MQ2 dalam satu *node*. Sementara itu, sensor pengontrol adalah *node* RFID dan kode QR. Skenario difokuskan pada perbandingan tiga *node* sensor pemantauan, dua sensor pemantauan dan satu *node* RFID, dua RFID dan satu *node* sensor pemantauan, serta dua RFID dan satu *node* Kode QR. Hal ini dicapai dengan menggunakan 10-500 iterasi *node* blok dengan tiga server *peer* terdistribusi.

Hasil yang disajikan pada Gambar 3.19. menunjukkan bahwa waktu eksekusi sekitar 592,47 detik ketika *node* WSN digunakan untuk sensor pengontrol. ıa dibandingkan dengan penerapan hanya sensor pemantauan 33,03 detik. Sensor pengontrol membutuhkan waktu yang lebih kontrol manual antara pengguna dan perangkat dibandingkan sor pemantauan yang sepenuhnya otomatis. Sementara itu, menyebabkan waktu eksekusi yang tidak stabil. Hal ini ɔkan oleh masalah jaringan yang diidentifikasi sebagai bagian

dari faktor-faktor yang memengaruhi proses pengiriman atau transaksi dalam jaringan terdistribusi.



Gambar 3. 19. Perbandingan waktu eksekusi WSN blockchain.

3.6.5. Diskusi

Skalabilitas sistem pada jaringan *peer* dengan topologi mesh menghadirkan tantangan terkait latensi dan konsumsi bandwidth, yang dapat memengaruhi kinerja sinkronisasi. Arsitektur yang diusulkan menunjukkan kinerja yang andal di bawah beban kerja yang meningkat, dengan mempertahankan tingkat kesalahan yang minimal bahkan hingga 1.000 blok. Untuk memastikan ketahanan dan efisiensi yang berkelanjutan dalam skala besar, disarankan untuk meningkatkan komunikasi antar *node*, mengoptimalkan penggunaan bandwidth, dan menerapkan segmentasi berbasis wilayah.

Penelitian ini secara khusus berfokus pada efisiensi memori, kecepatan eksekusi, keamanan data, dan validasi sensor dalam arsitektur WSN berbasis blockchain terdistribusi, dengan penekanan khusus pada verifikasi identitas *node* dan penyaringan data melalui mekanisme konsensus *Smart Contract* dan PoI. Oleh karena itu, parameter evaluasi seperti distribusi latensi, konsumsi energi, overhead jaringan, dan tingkat kesalahan tidak menjadi prioritas pada fase eksperimen saat ini. Meskipun demikian, parameter-parameter tersebut diakui sebagai faktor penting dalam menilai kinerja keseluruhan sistem WSN, terutama dalam konteks penerapan skala besar dan jangka panjang. Evaluasi aspek-aspek ini direncanakan untuk penelitian selanjutnya, sehingga solusi yang diusulkan dapat dinilai tidak hanya dari segi keamanan dan validitas data, tetapi juga dari efisiensi jaringan serta pemanfaatan sumber daya.

menyajikan pendekatan baru melalui arsitektur BSM dan BSC
ıgsi *monitoring* dan *controlling* dalam WSN berbasis blockchain.
sikan mekanisme konsensus *Smart Contract* dan PoI, serta

evaluasi algoritma hash, model ini meningkatkan validitas data, keamanan *node*, dan efisiensi pemrosesan pada perangkat dengan sumber daya terbatas. Hasil penelitian menunjukkan bahwa algoritma *blockchain* tercepat untuk arsitektur WSN dan blockchain terdistribusi dalam mendeteksi *node* berbahaya atau anomali dan data sensor adalah Scrypt dengan waktu eksekusi 469,49 detik. Penambahan algoritma SHA-256 sebagai *Smart Contract* pada *node* sensor atau mikrokontroler menyebabkan waktu eksekusi menjadi lebih lama dibandingkan tanpa hash, dengan selisih sekitar 63,54 detik. Namun, penambahan ini memberikan tingkat keamanan yang lebih tinggi bagi *node* sensor. Kombinasi dua mekanisme konsensus, yaitu *Smart Contract* (MAC dan SHA-256) serta PoI dengan tiga parameter sensor (Temp, Humd, MQ2), berhasil mendeteksi dan mempertahankan 97,37% *node* sensor dan data yang valid. Selain itu, implementasi sensor pengendali yang terdiri dari dua *node* RFID dan satu *node* QR code pada 500 iterasi *node* blok di tiga server *peer* terdistribusi menghasilkan total waktu eksekusi 592,47 detik, yang lebih lama dibandingkan dengan waktu eksekusi *sensor monitoring* sebesar 533,03 detik. Hal ini disebabkan oleh proses penggunaan manual antara pengguna dan perangkat. Kombinasi antara sensor *monitoring* dan *controlling* menunjukkan waktu eksekusi yang tidak stabil. Oleh karena itu, arsitektur model seperti ini dipelukan pemisahan antara *sensor monitoring* dan *controlling*. Hal ini diperlukan karena *sensor monitoring* memprioritaskan operasi otomatis, kecepatan, dan akurasi data secara *real time.* Pekerjaan di masa depan dapat difokuskan pada optimalisasi algoritma PoI untuk penerapan real-time pada jaringan sensor skala besar dengan mengatasi tantangan seperti latensi jaringan dan efisiensi energi.

3.8. Daftar Pustaka

Abdussami, M., Amin, R., Saravanan, P., & Vollala, S. (2023). BSAPM: BlockChain based secured authentication protocol for large scale WSN with FPGA implementation. Computer Communications, 209(April), 63–77. https://doi.org/10.1016/j.comcom.2023.06.011

Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. Array, 14(October 2021). https://doi.org/10.1016/j.array.2022.100139

Alsaedy, S., Alraddadi, S., & Owais, A. (2020). A review on using blockchain in wireless sensor networks. Journal of Theoretical and Applied Information Technology, 98(23), 3879–3886.

Badamasi, Y. A. (2014). The Working Principle Of An Arduino .

Begum, B. A., & Nandury, S. V. (2023). Data aggregation protocols for WSN and IoT applications – A comprehensive survey. Journal of King Saud University - Computer and Information Sciences, 35(2), 651–681. https://doi.org/10.1016/j.jksuci.2023.01.008

i, K., & Dahri, H. (2021). Toward Safety of Wireless Sensor on Blockchain. Advances in Dynamical Systems and 2), 1705–1723.

Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys and Tutorials, 22(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Chen, Y., Yang, X., Li, T., Ren, Y., & Long, Y. (2022). A blockchain-empowered authentication scheme for worm detection in wireless sensor network. Digital Communications and Networks, 141291. https://doi.org/10.1016/j.dcan.2022.04.007

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Transactions on Services Computing, 13(2), 241–251. https://doi.org/10.1109/TSC.2020.2964537

Durfee, W. (2011). Arduino Microcontroller Guide. www.me.umn.edu/courses/me2011/arduino/, pp. 1–27.

Dwivedi, S. K., Amin, R., & Vollala, S. (2023a). Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability. Computer Communications, 197(January 2022), 124–140. https://doi.org/10.1016/j.comcom.2022.10.016

Dwivedi, S. K., Amin, R., & Vollala, S. (2023b). Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability. Computer Communications, 197(January 2022), 124–140. https://doi.org/10.1016/j.comcom.2022.10.016

Ebobissé Djéné, Y. F., El Idrissi, M. S., Tardif, P. M., Jorio, A., El Bhiri, B., & Fakhri, Y. (2022). A Formal Energy Consumption Analysis to Secure Cluster-Based WSN: A Case Study of Multi-Hop Clustering Algorithm Based on Spectral Classification Using Lightweight Blockchain. Sensors, 22(20). https://doi.org/10.3390/s22207730

Feng, H., Zhang, M., Gecevska, V., Chen, B., Saeed, R., & Zhang, X. (2022a). Modeling and evaluation of quality monitoring based on wireless sensor and blockchain technology for live fish waterless transportation. Computers and Electronics in Agriculture, 193(December 2020), 1–14. https://doi.org/10.1016/j.compag.2021.106642

Feng, H., Zhang, M., Gecevska, V., Chen, B., Saeed, R., & Zhang, X. (2022b). Modeling and evaluation of quality monitoring based on wireless sensor and blockchain technology for live fish waterless transportation. Computers and Electronics in Agriculture, 193(December 2020), 106642. https://doi.org/10.1016/j.compag.2021.106642

Godawatte, K., Branch, P., & But, J. (2022). Use of blockchain in health sensor networks to secure information integrity and accountability. Procedia Computer Science, 210(C), 124–132. https://doi.org/10.1016/j.procs.2022.10.128

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). International Journal of Accounting Accounting and auditing with blockchain technology and artificial Intelligence : A literature review. International Journal of Accounting
ems, 48(November 2022), 1–16.

y, M. J. M., Biswas, K., Ahmed, K., Islam, M. S., & Usman, M.
chain-based secure data-sharing framework for Software
s Body Area Networks. Computer Networks, 211(April), 109004.
.1016/j.comnet.2022.109004

Hsiao, S. J., & Sung, W. T. (2021). Utilizing blockchain technology to improve WSN security for sensor data transmission. Computers, Materials and Continua, 68(2), 1899–1918. https://doi.org/10.32604/cmc.2021.015762

Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486–492. https://doi.org/10.1016/j.procs.2021.02.088

Jagannadha Swamy, T., Pallavi, B., Amaraveni, V., Sireesha, Y., & Siddarth, S. (2023). Secure Data Dissemination in Wireless Sensor Networks with the Help of Module Based Blockchain Technology. 2023 3rd International Conference on Intelligent Technologies, CONIT 2023, 1–6. https://doi.org/10.1109/CONIT59222.2023.10205841

Jangra, A. (2010). Wireless Sensor Network (WSN): Architectural Design issues and Challenges. International Journal on Computer Science and Engineering, 2(9), 3089–3094.

Jaya, R. M., Rakkhitta, V. D., Sembiring, P., Edbert, I. S., & Suhartono, D. (2023). Blockchain applications in drug data records. Procedia Computer Science, 216, 739–748. https://doi.org/10.1016/j.procs.2022.12.191

Kaschel, H., Cordero, S., Adasme, P., & Ahumada, C. (2022). Smart Agriculture 4.0: Technology Recommendations and Interoperability of Devices, Sensors and Data Management using Blockchain. 2022 IEEE International Conference on Automation/25th Congress of the Chilean Association of Automatic Control: For the Development of Sustainable Agricultural Systems, ICA-ACCA 2022, 1–7. https://doi.org/10.1109/ICA-ACCA56767.2022.10006132

Keerthika, M., & Shanmugapriya, D. (2021). Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures. Global Transitions Proceedings, 2(2), 362–367. https://doi.org/10.1016/j.gltp.2021.08.045

Khah, S. A., Barati, A., & Barati, H. (2023). A dynamic and multi-level key management method in wireless sensor networks (WSNs). Computer Networks, 236(June), 109997. https://doi.org/10.1016/j.comnet.2023.109997

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0268-2

Lee, J. (2018). Patch transporter: Incentivized, decentralized software patch system for WSN and IoT environments. Sensors (Switzerland), 18(2), 1–35. https://doi.org/10.3390/s18020574

Liu, X. (2015). Atypical Hierarchical Routing Protocols for Wireless Sensor Networks : A Review. IEEE SENSORS JOURNAL, 15(10), 5372–5383.

Matusiewicz, K., Pieprzyk, J., Pramstaller, N., Rechberger, C., & Rijmen, V. (2005). Analysis of simplified variants of SHA-256. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI), P-74(January), 123–134.

Nasraoui, L., & Saidane, L. A. (2022). Blockchain for WSN and IoT Applications. 2022 tional Conference on Sciences of Electronics, Technologies of Telecommunications (SETIT), (September), 1–6.

n, K. (2018). A survey about Consensus Algorithms Used in nal of Information Processing System, 14(1), 101–128.

Nguyen, C. V, Nguyen, M. T., Le, T. T. H., Tran, T. A., & Nguyen, D. T. (2021). Blockchain Technology in Wireless Sensor Network : Benefits. Transactions on Computer Networks and Communications, X(Y), 1–4.

Onjewu, A. E., Walton, N., & Koliousis, I. (2023). Technological Forecasting & Social Change Blockchain agency theory. Technological Forecasting & Social Change, 191(April 2022), 1–10.

Patel, N., Kathiriya, H., & Bavarva, A. (2013). WIRELESS SENSOR NETWORK USING ZIGBEE. International Journal of Research in Engineering and Technology ISSN: 2319-1163 WIRELESS, 2(6), 1038–1042.

Qi, W., Xia, Y., Zhu, P., Zhang, S., Zhu, L., & Zhang, S. (2023). Secure and efficient blockchain-based consensus scheme for MWSNs with clustered architecture. Pervasive and Mobile Computing, 94, 1–17. https://doi.org/10.1016/j.pmcj.2023.101830

Rahman, A. F. S., Mustika, I. W., & Kusumawardani, S. S. (2016). Pengelolaan Sistem Informasi Data Presensi dengan Media Transmisi Menggunakan Sistem Wireless Sensor Network. SENIATI Proceeding, 1–7.

Ramadevi, P., Ayyasamy, S., Suryaprakash, Y., Anilkumar, C., Vijayakumar, S., & Sudha, R. (2023). Security for wireless sensor networks using cryptography. Measurement: Sensors, 29(August). https://doi.org/10.1016/j.measen.2023.100874

She, W., Liu, Q., Tian, Z., Chen, J. Sen, Wang, B., & Liu, W. (2019). Blockchain trust model for malicious *node* detection in wireless sensor networks. IEEE Access, 7, 38947–38956. https://doi.org/10.1109/ACCESS.2019.2902811

Sudheer, B. N., & Sujatha, K. (2023). A Brief Survey on Data Aggregation and Data Compression Models using Blockchain Model in Wireless Sensor Network. International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, 406–413. https://doi.org/10.1109/ICIDCA56705.2023.10100009

Taieb, F. (2007). Wireless Sensor Networks : Technology, Protocols, and Applications.

Tran, H. T., Nguyen, C. V., & Nguyen, M. T. (2022). A Framework of Deploying Blockchain inWireless Sensor Networks. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 9(32), 1–8. https://doi.org/10.4108/eetinis.v9i32.1125

Verma, S., Kaur, S., Manchanda, R., & Pant, D. (2020). Essence of Blockchain Technology in Wireless Sensor Network: A brief study. Proceedings - 2020 International Conference on Advances in Computing, Communication and Materials, ICACCM 2020, 394–398. https://doi.org/10.1109/ICACCM50413.2020.9212970

Vinya, V. L., Anuradha, Y., Karimi, H. R., Divakarachari, P. B., & Sunkari, V. (2022). A Novel Blockchain Approach for Improving the Security and Reliability of Wireless Sensor Networks Using Jellyfish Search Optimizer. Electronics (Switzerland), 11(21). https://doi.org/10.3390/electronics11213449

Qing, Y., Zheng, H., Qin, B., & Yang, C. (2023). Security and n technologies in securing blockchain applications. Information uly 2022), 119322. https://doi.org/10.1016/j.ins.2023.119322

Kou, G. (2019). A systematic review of blockchain. Financial https://doi.org/10.1186/s40854-019-0147-z

Zawawi, A. El, Ieee, M., & Ibrahim, A. (2012). Using ZigBee to Build a Web-Based DCS System. 2012 IEEE Power and Energy Society General Meeting, 1–8.

Zhang, H., Zaman, M., Stacey, B., & Sampalli, S. (2022). A Novel Distributed Ledger Technology Structure for Wireless Sensor Networks Based on IOTA Tangle. Electronics (Switzerland), 11(15), 1–17. https://doi.org/10.3390/electronics11152403

Zhu, J. (2023). Real-time monitoring for sport and mental health prevention of college student based on wireless sensor network. Preventive Medicine, 173(May), 107581. https://doi.org/10.1016/j.ypmed.2023.107581

BAB IV
IMPLEMENTASI SMART CONTRACT DAN PROOF OF TWO FACTOR AUTHENTICATION UNTUK KEAMANAN SISTEM WSN BLOCKCHAIN TERDISTRIBUSI

4.1. Abstrak

Integrasi *Wireless Sensor Network* (WSN) dengan Blockchain (BC) menghadirkan potensi besar dalam meningkatkan keamanan dan keandalan data sensor pada sistem terdistribusi. Penelitian ini tidak dilakukan melalui simulasi, melainkan menggunakan prototipe nyata berbasis perangkat keras, mencakup *sensor controlling* fisik, mikrokontroler, serta modul komunikasi XBee ZigBee sebagai media transmisi. Sistem diuji pada tiga konfigurasi server blockchain yang berbeda (1 lokal sebagai master, 1 lokal dan 1 online, serta 1 lokal dan dua online) dengan 500 blok data dari *node* sensor acak. Dua mekanisme diuji: *Smart Contract* (SC) dan *Smart Contract* dengan *Proof of Two Factor Authentication* (SC+Po2FA). Hasil menunjukkan bahwa penambahan jumlah server online meningkatkan overhead sinkronisasi, sehingga memperbesar kompleksitas waktu secara linier terhadap jumlah blok dan menambah kompleksitas ruang akibat replikasi data. Pengujian pada tiga server terdistribusi (1 lokal, 2 online) dengan 500 blok SC+Po2FA membutuhkan 2.792,54 detik, sedangkan SC hanya 760,94 detik. Perbandingan SC dan SC+Po2FA menunjukkan trade off yang jelas antara efisiensi dan keamanan. SC unggul dalam kecepatan dan efisiensi dengan kompleksitas O(n), namun proteksi yang diberikan terbatas. Sebaliknya, SC+Po2FA memberikan lapisan autentikasi ganda yang terbukti meningkatkan keamanan dengan akurasi 93% dan F1 Score 95,17%, meskipun membutuhkan waktu eksekusi dan ruang penyimpanan yang lebih besar. Sedangkan SC mempunyai nilai akurasi 91% dengan F1 Score 93,5%. Dari sisi jaringan, performa *node* menunjukkan latency tinggi dengan deviasi signifikan, throughput rendah namun fluktuatif, serta kualitas sinyal RSSI yang tidak konsisten.

4.2. Pendahuluan

WSN telah menjadi salah satu teknologi utama dalam sistem monitoring dan kontrol modern. WSN banyak diterapkan dalam berbagai bidang, mulai dari pertanian pintar, pemantauan lingkungan, hingga sistem keamanan dan industri (Q. Yang et al., 2015)(Sen, 2009). Namun, keterbatasan dari sisi komputasi, penyimpanan, dan sumber daya energi menjadikan WSN sangat rentan terhadap berbagai jenis ıyusupan *node* palsu (Sybil attack), data injection, replay attack, ɔr (Arshad et al., 2021) (Anwar et al., 2015) (Karlof & Wagner,

Sistem WSN tradisional yang terpusat (centralized) tidak memiliki mekanisme validasi ganda dan rentan terhadap *single point of failure* (Stajano & Anderson, 2000). Salah satu tantangan terbesar dalam WSN adalah mengamankan sensor kontrol (seperti RFID dan QR Code), yang sangat penting karena digunakan untuk mengatur akses, transaksi, atau perintah kepada sistem (Finkenzeller, 2003). Ketika sensor kontrol berhasil disusupi, maka konsekuensinya lebih serius dibandingkan dengan *sensor monitoring* biasa. Penelitian sebelumnya telah mengusulkan beberapa pendekatan keamanan untuk kontrol sensor, salah satunya adalah dengan menggunakan mekanisme autentikasi berbasis blockchain (Zheng et al., 2018)(Satoshi, 2022). Contohnya, She et al. (Moinet et al., 2017) mengembangkan model berbasis blockchain untuk mendeteksi *node* berbahaya melalui reputasi dan *trust score*. Model ini cukup efektif dalam mengenali *node* yang mencurigakan, namun memiliki kekurangan yaitu membutuhkan komputasi tinggi dan tidak fokus pada sensor kontrol. Di sisi lain, Tian et al. (Tian et al., 2020) menerapkan sistem manajemen kunci berbasis blockchain untuk memperkuat otentikasi *node*, tetapi tidak menyediakan mekanisme otorisasi dua arah antara pengguna dan sensor. Beberapa penelitian lain juga mencoba mengintegrasikan *Smart Contract* untuk autentikasi dan validasi data, seperti yang dilakukan (Paulraj et al., 2023) dengan menggabungkan pemilihan cluster head dan blockchain. Namun, pendekatan ini lebih cocok untuk monitoring massal, bukan untuk transaksi atau pengendalian. Sementara itu, Nouman et al. (Nouman et al., 2023) menggunakan pendekatan pembelajaran mesin dan blockchain untuk mendeteksi *node* jahat, namun metode ini kurang fleksibel dalam autentikasi *real time* pada sensor kontrol. Penelitian terbaru (Kebande et al., 2021) juga menegaskan bahwa kombinasi blockchain dengan multi-factor authentication memberikan potensi besar dalam meningkatkan keamanan WSN, tetapi belum diterapkan pada skema sensor kontrol yang terdistribusi.

Kelebihan pendekatan sebelumnya adalah peningkatan keamanan dari sisi jaringan dan *node*, mendeteksi *node* jahat dan memperkuat integritas data, namun sebagian besar belum menggabungkan dua lapisan autentikasi (*user & device*) secara langsung. Selain itu, umumnya penelitian tersebut hanya mengandalkan hash sederhana (seperti SHA-256) tanpa verifikasi pengguna akhir. Dua lapisan autentifikasi disebut juga sebagai *Multi Factor Authentification* (MFA), metode otentikasi yang menggabungkan dua atau lebih faktor dari kategori berbeda untuk memastikan keaslian pengguna atau perangkat sebelum memberikan akses ke sistem (Q. Yang et al., 2015). Oleh karena itu, penelitian ini mengusulkan pendekatan

me konsensus blockchain *Smart Contract* (MAC address, PAN dan *Proof of Two Factor Authentication* (Po2FA), yang fikasi UID dari *sensor controlling* (RFID atau QR Code) dengan melalui tautan unik (*One Time Verification Link*) yang dikirim ke l. Hanya data yang telah diverifikasi dan divalidasi yang akan

dimasukkan ke dalam blockchain. Po2FA merupakan implementasi spesifik MFA yang dikembangkan pada WSN berbasis blockchain. Selain itu metode ini diintegrasikan ke dalam arsitektur blockchain terdistribusi dengan tiga *peer* server (1 Master lokal server, 2 online server) untuk memperkuat replikasi data dan mengurangi resiko manipulasi.

Kontribusi dari usulan ini yaitu menambahkan lapisan keamanan kedua yang melibatkan pengguna secara langsung, mengatasi serangan *node* palsu dan manipulasi data *sensor controlling*, mengintegrasikan otentikasi real time antara pengguna dan perangkat sebelum pembentukan block, memastikan hanya data terverifikasi yang masuk ke blockchain, sehingga memperkuat integritas data WSN terdistribusi. Penelitian ini mempunyai manfaat antara lain menyediakan pendekatan baru (Po2FA) yang menggabungkan multi faktor autentifikasi dalam WSN berbasis blockchain, memberikan solusi pengamanan lebih kuat untuk sistem *controlling* berbasis RFID dan QR Code, serta mendukung penerapan keamanan IoT, *smart acces control* atau transaksi di lingkungan yang rawan serangan. Dengan demikian, sistem yang diusulkan mampu mengatasi kelemahan pada penelitian sebelumnya sekaligus menjawab kerentanan mendasar pada data WSN, yaitu lemahnya autentikasi ganda antara pengguna dan sensor, serta ketidakmampuan sistem dalam menyaring data yang berasal dari *node* berbahaya atau manipulatif sebelum direkam secara permanen di blockchain.

4.3. Karya Terkait

Penelitian mengenai keamanan WSN telah berkembang pesat dalam satu dekade terakhir, terutama dalam konteks deteksi *node* berbahaya dan perlindungan data sensor. Berbagai pendekatan telah diusulkan, mulai dari manajemen kunci, mekanisme trust, hingga penerapan teknologi blockchain untuk mengatasi kerentanan pada arsitektur WSN (Xia, Wei, & Zhang, 2022) (Ramasamy et al., 2021). Blockchain menawarkan fitur desentralisasi, integritas data, dan immutability yang mampu meningkatkan keamanan jaringan sensor, sehingga banyak peneliti mengadopsinya sebagai solusi untuk mencegah serangan seperti sybil attack, replay attack, dan manipulasi data sensor (Hsiao & Sung, 2021a) (And & Darwish, 2021) (Singh & Hosen, 2021). Sejumlah penelitian mengkaji penerapan blockchain dalam autentikasi *node*. Moinet et al. (Moinet et al., 2017) mengembangkan skema autentikasi berbasis *peer* trust untuk mendeteksi *node* yang tidak sah, namun menghadapi keterbatasan pada konsumsi energi. She et al. (She et al., 2019a) mengusulkan model trust blockchain untuk mendeteksi *node* berbahaya, yang efektif

asi serangan sybil tetapi membutuhkan overhead komputasi erbasis *Smart Contract* juga telah dikaji, seperti oleh Amjad et), yang menggabungkan pemilihan cluster head (DDR-LEACH) nun, pendekatan ini tidak secara khusus membahas *sensor*) dan tidak melibatkan autentikasi dua faktor.

Selain itu, beberapa studi terbaru memanfaatkan kombinasi blockchain dengan pembelajaran mesin untuk meningkatkan deteksi serangan (Nouman et al., 2023b). Meskipun efektif dalam menganalisis pola serangan, metode ini cenderung kompleks dan sulit diterapkan pada perangkat sensor yang memiliki keterbatasan sumber daya. Sebagian besar penelitian yang ada hanya fokus pada autentikasi *node* atau *filtering* data berbasis *threshold*, tanpa menggabungkan faktor autentikasi pengguna secara real time. Studi tinjauan sistematis oleh Almadani et al. (Almadani, Alotaibi, Alsobhi, Hussain, & Hussain, 2023) menunjukkan bahwa penerapan autentikasi multi faktor berbasis blockchain mampu memperkuat keamanan identitas dan mencegah penyalahgunaan kredensial, namun sebagian besar penelitian masih berfokus pada aplikasi umum IoT dan belum menyasar secara spesifik skenario WSN dengan keterbatasan sumber daya.

Berdasarkan tinjauan tersebut, terlihat adanya celah penelitian pada autentikasi *sensor controlling* yang melibatkan interaksi langsung dengan pengguna. Oleh karena itu, penelitian ini mengusulkan Po2FA, yaitu mekanisme konsensus yang menggabungkan autentikasi UID sensor (RFID/QR Code) dengan verifikasi pengguna melalui tautan eksternal (whatsApp/email atau yang lainnya). Data yang disimpan ke blockchain merupakan data yang diverifikasi melalui dua lapisan keamanan untuk menjamin keabsahan data sensor. Pendekatan ini memberikan perlindungan tambahan terhadap manipulasi data, *node* palsu, dan serangan berbasis pengguna yang belum terakomodasi secara memadai pada penelitian sebelumnya.

Tinjauan terhadap penelitian terdahulu pada keamanan WSN berbasis blockchain menunjukkan bahwa solusi yang ada terbagi menjadi beberapa kategori. Pendekatan awal seperti yang dilakukan (Moinet et al., 2017) memanfaatkan blockchain sebagai mekanisme trust dan reputasi *node* dalam autentikasi *peer to peer*, memberikan keuntungan desentralisasi namun belum optimal untuk perangkat dengan keterbatasan sumber daya. Model trust berbasis blockchain yang diajukan (She et al., 2019) memperkuat deteksi *node* berbahaya termasuk serangan sybil, meski dihadapkan pada beban komputasi dan komunikasi yang tinggi. (Tian et al., 2020) mengarahkan fokus pada manajemen kunci terdistribusi pada jaringan dinamis (DWSN) dengan integrasi algoritma pembentukan klaster, meningkatkan keandalan namun bergantung pada operasi kriptografi yang relatif berat. Di sisi lain, inovasi seperti PoAh oleh (Puthal et al., 2020) memperkenalkan protokol konsensus yang lebih ringan untuk perangkat *resource constrained*, walau belum mengakomodasi [illegible]. Pendekatan berbasis *Smart Contract* seperti pada (Amjad et [illegible]ngkan registrasi *node* dan pemilihan *cluster head* (DDR-LEACH) [illegible]rtisipasi *node* palsu, namun fokusnya masih pada pengelolaan [illegible]*r controlling* RFID/QR. Upaya menghemat energi juga terlihat [illegible]., 2024) dengan *Energy Aware* PoA yang memperpanjang umur

jaringan, meskipun kompleksitas desain dan sinkronisasi menjadi tantangan. Integrasi pembelajaran mesin untuk deteksi otomatis *node* jahat, seperti pada (Nouman et al., 2023), berhasil meningkatkan tingkat deteksi tetapi membutuhkan training data dan sumber daya yang besar. Sementara itu, (Goyat et al., 2022) menekankan privasi dan autentikasi pada penyimpanan data berbasis blockchain, namun belum diarahkan khusus pada *sensor controlling*. Kajian komprehensif oleh (Ismail et al., 2023) memperlihatkan tren integrasi blockchain dan pembelajaran mesin, tetapi masih minim pada aspek implementasi autentikasi pengguna secara langsung.

Dari analisis ini terlihat bahwa mayoritas studi fokus pada autentikasi perangkat, manajemen kunci, atau deteksi *node* berbahaya, sedangkan autentikasi pengguna secara real time dan validasi ganda perangkat dan pengguna belum banyak dibahas. Penelitian ini menawarkan Po2FA sebagai solusi yang menggabungkan autentikasi UID sensor (RFID/QR) atau Smarct Contract dan verifikasi pengguna dengan tautan eksternal. Pendekatan ini mengisi celah yang belum terakomodasi oleh penelitian sebelumnya, yaitu pengamanan ganda terhadap manipulasi data dan penyusupan *node* palsu dengan melibatkan faktor manusia dalam proses autentikasi..

Tabel 4. 1. State of the art dan model yang diusulkan.

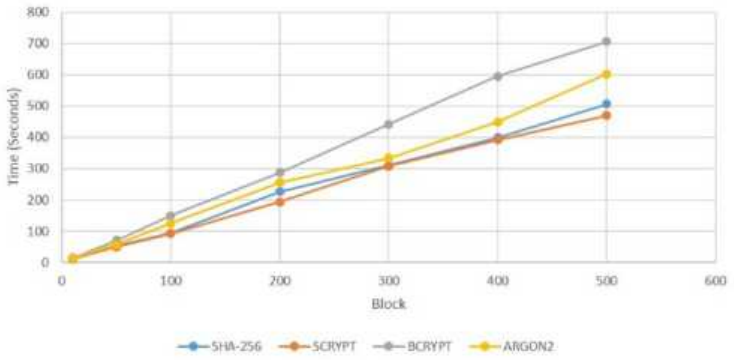
No	Peneliti, Tahun	Tujuan penelitian	Mekanisme Konsensus / Teknologi	Kelebihan	Kekurangan
1	Moinet, Darties, Baril (2017) — *Blockchain based trust & authentication for decentralized sensor networks* (Moinet et al., 2017).	Menyajikan model trust & authentication berbasis blockchain untuk jaringan sensor terdesentralisasi.	Blockchain untuk menyimpan kriteria autentikasi & skor trust *peer-to-peer*.	Konsep desentralisasi trust, cocok untuk jaringan tanpa otoritas pusat.	Studi konseptual, implementasi pada *node* terbatas/energi rendah belum lengkap.
2	She et al. (2019) — *Blockchain Trust Model for Malicious Node Detection in WSNs* (She et al., 2019b).	Mendeteksi *node* berbahaya (mis. Sybil) dengan model reputasi yang dicatat di blockchain.	Model trust + pencatatan insiden pada blockchain; penggunaan reputasi untuk filtering.	Audit trail dan kemampuan deteksi berbasis reputasi.	Overhead komputasi & komunikasi relatif tinggi untuk *node resource-constrained*.
3	Tian et al. (2020) — *A Blockchain-*	Menyediakan manajemen kunci terdistribusi & mekanisme trust untuk Dynamic WSN (DWSN).	Blockchain sebagai trust machine untuk key management & cluster formation.	Meningkatkan key management terdistribusi, cocok untuk DWSN/IIoT.	Menggunakan kriptografi berat, beban pada sensor lemah, tidak membahas verifikasi user.

No	Peneliti, Tahun	Tujuan penelitian	Mekanisme Konsensus / Teknologi	Kelebihan	Kekurangan
4	Puthal et al. (2020) — *PoAh: Proof-of-Authentication for large-scale IoT (PoAh)* (Puthal et al., 2020).	Mengusulkan konsensus ringan (PoAh) untuk perangkat *resource constrained* IoT/WSN.	Proof of Authentication: menggantikan PoW dengan mekanisme autentikasi yang lebih ringan.	Latensi rendah dibanding PoW, lebih cocok untuk perangkat kecil.	Pengujian real world terbatas, tidak mengcover *user driven* 2FA.
5	Amjad et al. (2022) — *Blockchain Based Authentication & Cluster Head Selection (DDR-LEACH)* (Amjad et al., 2022).	Integrasi *Smart Contract* untuk autentikasi *node* + pengelolaan pemilihan cluster head.	*Smart Contract* + DDR-LEACH + off-chain storage (mis. IPFS).	Mengurangi *node* palsu, efisiensi clustering, memanfaatkan off-chain storage.	Fokus pada monitoring/cluster, belum pada *sensor controlling* (RFID/QR) & MFA.
6	Murat Dener et al. (2023) — *BBAP-WSN: A New Blockchain-Based Authentication Protocol for WSNs* (Dener & Orman, 2023).	Mendesain protokol autentikasi blockchain untuk WSN (protokol BBAP-WSN).	Private blockchain, *node* registration, cluster *nodes* & base station model.	Protokol terstruktur untuk autentikasi *node*, open access implementasi.	Tidak memasukkan verifikasi real time user (2FA) untuk sensor controlling.
7	Nouman et al. (2023) — *Malicious Node Detection Using ML + Distributed Storage Using Blockchain in WSNs* (Nouman et al., 2023b).	Gabungan ML (deteksi anomali) dan blockchain (penyimpanan/traceability) untuk mendeteksi *node* jahat.	Machine Learning untuk deteksi + blockchain untuk pencatatan dan penyimpanan terdistribusi.	Akurasi deteksi tinggi berkat ML, audit trail via blockchain.	Kompleks, butuh data latih & sumber daya komputasi, kurang cocok sepenuhnya di *node* lemah.
8	Hsiao & Sung (2021) — *Employing Blockchain Technology to Strengthen Security of WSNs* (Hsiao & Sung, 2021a).	Menyajikan kerangka kerja penerapan blockchain untuk memperkuat keamanan data WSN.	Penyimpanan hash data sensor di blockchain, mobile database (Raspberry Pi) sebagai relay.	Implementasi praktis dengan perangkat *single board*, mudah diadaptasi.	Masih bergantung pada *node* gateway, tidak menambahkan MFA berbasis pengguna.
9	Hanggoro et al. (2024) — *Energy-aware Proof-of-Authority:*	Mendesain PoA yang sadar energi untuk blockchain dalam arsitektur clustered WSN.	EA PoA (*Proof of Authority* yang mempertimbangkan energi) untuk klasterisasi.	Memperpanjang umur jaringan dan efisiensi energi untuk cluster WSN.	Perlu sinkronisasi kompleks & validasi skala produksi lebih lanjut.
		Menggabungkan Smart	*Smart Contract* + Po2FA	Menutup gap autentikasi	Memerlukan koneksi user

No	Peneliti, Tahun	Tujuan penelitian	Mekanisme Konsensus / Teknologi	Kelebihan	Kekurangan
	Authentication), sensor controlling (RFID/QR) pada distributed WSN	Contact dan Po2FA untuk meningkatkan keamanan ganda pada *sensor controling*		user+device real time, keamanan ganda.	(latensi/verifikasi), perlu studi reliabilitas & UX.

Analisis Tabel 4.1. state of the art menunjukkan bahwa penelitian keamanan WSN berbasis blockchain telah berkembang dari pendekatan autentikasi sederhana hingga integrasi teknologi lanjutan seperti machine learning dan konsensus hemat energi. Beberapa studi awal berfokus pada mekanisme trust berbasis blockchain untuk mendeteksi *node* berbahaya, seperti yang dilakukan oleh Moinet et al. (Moinet et al., 2017) dan She et al. (She et al., 2019) yang menawarkan pendekatan terdesentralisasi dengan pencatatan reputasi *node* namun masih menghadapi kendala overhead komputasi dan efisiensi energi. Pendekatan lain mengarah pada manajemen kunci dan keandalan sistem di jaringan sensor dinamis, seperti penelitian Tian et al. (Tian et al., 2020), yang memanfaatkan blockchain untuk key management terdistribusi tetapi masih mengandalkan operasi kriptografi berat.

Selain itu, terdapat upaya mengembangkan konsensus yang lebih ringan, seperti *Proof of Authentication* (PoAh) (Puthal et al., 2020) dan *Energy Aware Proof of Authority* (EA-PoA) (Hanggoro et al., 2024), yang dirancang untuk perangkat dengan sumber daya terbatas. Meskipun efektif mengurangi latensi dan memperpanjang umur jaringan, pendekatan ini belum secara eksplisit mengintegrasikan autentikasi dua faktor berbasis interaksi pengguna. Penelitian Amjad et al. (Amjad et al., 2022) memperkenalkan pemilihan *cluster head* berbasis DDR-LEACH dengan *Smart Contract*. sedangkan (Dener & Orman, 2023), mengusulkan protokol autentikasi berbasis blockchain yang menggabungkan efisiensi kriptografi dengan optimisasi konsumsi energi di WSN, menunjukkan potensi signifikan dalam mengatasi tantangan autentikasi multi-*node* dengan beban komputasi rendah. sedangkan Nouman et al. (Nouman et al., 2023b) dan Ismail et al. (Ismail et al., 2023) mengombinasikan *machine learning* dengan blockchain untuk meningkatkan deteksi serangan, namun metode ini memerlukan data pelatihan dan sumber daya komputasi yang signifikan. Sebagian besar penelitian terdahulu menggunakan SHA-256 dalam membuat blockchain, tetapi untuk menyimpan sensor dalam jumlah yang banyak dan tingkat pemrosesan data yang cepat dibutuhkan lebih cepat, penelitin tentang penggunaan berbagai jenis hash tribusi blockchain dan WSN pada sensor monitoring juga an, Scrypt hash mempunyai waktu lebih cepat dari SHA-256, Rahman, Achmad, & Wardi, 2025). Gambar 4.1. merupakan eksekusi pada sistem terdistribusi dengan 3 *peer* server.



Gambar 4. 1. Perbandingan waktu eksekusi (Rahman et al., 2025).

Kesenjangan penelitian (research gap) yang terlihat adalah belum adanya mekanisme autentikasi yang secara bersamaan memverifikasi identitas perangkat sensor (RFID/QR) atau samrt contract dan identitas pengguna secara real-time pada WSN dan Blockchain. Penelitian ini menawarkan Po2FA yang menggabungkan verifikasi Mac address, *hash key*, UID sensor (*Smart Contract*) dengan autentikasi pengguna melalui link OTP, serta pembuatan blockchain menggunakan hash Scrypt dikarenakan data sensor yang masuk akan lebih banyak dan membutuhkan waktu akuisisi data lebih cepat. Pendekatan ini memberikan lapisan keamanan tambahan yang belum banyak diadopsi oleh studi sebelumnya.

4.4. Tinjauan Pustaka

4.4.1. Wireless Sensor Network (WSN)

WSN merupakan jaringan terdistribusi yang terdiri dari banyak *node* sensor berdaya rendah yang memiliki kemampuan penginderaan, pemrosesan lokal, dan komunikasi nirkabel untuk mengumpulkan data lingkungan dan meneruskannya ke sink/gateway untuk pemrosesan lebih lanjut; arsitektur tipikal meliputi *node* sensor, sink/gateway, dan server/cloud, dengan topologi star/tree/mesh dan protokol komunikasi berdaya rendah seperti IEEE 802.15.4 (Mostafaei & Menth, 2018). Tantangan utama yang terus menjadi fokus riset meliputi manajemen energi guna memperpanjang umur jaringan, mekanisme toleransi kesalahan untuk mempertahankan layanan meskipun terjadi kegagalan *node*, keamanan terhadap beragam serangan lapisan jaringan, serta isu skalabilitas dan pemenuhan *Quality of Service* (QoS) pada jaringan berskala besar (Survey & Directions, 2022)(Faris et al., 2023). Perkembangan penting mencakup adopsi paradigma *software defined* (SD-
emisahkan *controlling*/data plane dan memudahkan orkestrasi
SN dengan ekosistem IoT dan platform cloud/edge untuk analitik
erta penggunaan *machine learning* untuk optimasi energi dan
kasi nyata WSN meliputi pemantauan lingkungan (termasuk
n, industri, pertanian presisi, dan smart cities (Pule et al., 2018).

WSN berperan penting dalam pengumpulan data lingkungan secara real time untuk berbagai aplikasi, mulai dari pemantauan lingkungan hingga otomasi industri (Alobaidy et al., 2020). Kinerja dan keandalan WSN sangat bergantung pada teknologi transmisi data yang digunakan, khususnya terkait dengan konsumsi daya, jangkauan komunikasi, throughput, dan topologi jaringan (A. I. Ali & Zorlu Partal, 2022)(Inthasuth et al., 2025). Berbagai teknologi transmisi seperti ZigBee Mesh, LoRa, Wi-Fi, NB-IoT, Bluetooth Low Energy (BLE), dan Ultra-Wideband (UWB) memiliki karakteristik berbeda yang memengaruhi penggunaannya pada WSN (Haxhibeqiri et al., 2018)(Rawat et al., 2014)(Che et al., 2023). ZigBee Mesh, misalnya, dikenal dengan efisiensi energi dan kemampuan jaringan mesh yang meningkatkan keandalan data serta keamanan dengan enkripsi AES-128, sehingga cocok untuk aplikasi WSN yang terintegrasi dengan blockchain (Healy et al., 2009). Tabel 4.2. perbandingan teknologi transmisi berikut ini menyajikan kelebihan, kekurangan, dan contoh aplikasi dari masing-masing teknologi, yang dapat digunakan sebagai referensi dalam pemilihan solusi transmisi terbaik untuk kebutuhan WSN yang kompleks dan terdesentralisasi (Roman, Zhou, & Lopez, 2013).

Tabel 4. 2. Perbandingan teknologi transmisi WSN.

Teknologi	Kelebihan	Kekurangan	Contoh Penggunaan WSN	Contoh Produk/Modul
ZigBee Mesh	- Konsumsi daya rendah, cocok baterai tahan lama. - Jaringan mesh meningkatkan keandalan & jangkauan. - Enkripsi AES-128 bawaan (Inthasuth et al., 2025)	- Jarak per-hop pendek (puluhan meter). - Throughput rendah (~250 kbps).	Smart home, smart building, integrasi sensor.	XBee Series, Digi XBee ZigBee
LoRa (LPWAN)	- Jarak sangat jauh (km), hemat daya. - Tidak perlu infrastruktur seluler (Haxhibeqiri et al., 2018).	- Throughput sangat rendah (0.3–50 kbps). - Latensi tinggi.	Pemantauan lingkungan outdoor, pertanian.	Semtech SX1276, RFM95W
Wi-Fi	- Throughput tinggi (Mbps). - Infrastruktur luas dan mudah akses (M. D. Nguyen et al., 2025).	- Konsumsi daya tinggi. - Rentan interferensi. - Kurang cocok untuk baterai.	Aplikasi data besar real-time, video streaming.	ESP8266, ESP32
NB-IoT	- Jangkauan luas via jaringan seluler. - Hemat daya, penetrasi indoor baik (Inthasuth et al., 2025)(Martinez, Adelantado,	- Memerlukan langganan operator. - Throughput rendah. - Latensi variabel.	Smart metering, pemantauan udara jarak jauh.	Quectel BC95, SIM7000
	osana, 2019)			
	aya sangat as di bile. (Hughes, Yan,	- Jarak terbatas (~10-50 m). - Throughput terbatas (~1 Mbps).	Wearable, health monitoring, smart home.	Nordic nRF52, TI CC2640

Teknologi	Kelebihan	Kekurangan	Contoh Penggunaan WSN	Contoh Produk/Modul
	& Soga, 2015)(Gomez, Oller, & Paradells, 2012).			
Ultra-Wideband (UWB)	- Akurasi posisi sangat tinggi (sentimeter). - Kecepatan data tinggi. - Resistensi interferensi tinggi (Elechi & Obi-Ijeoma, 2022).	- Jangkauan pendek (<100 m). - Konsumsi daya lebih tinggi dari BLE/ZigBee.	Indoor positioning, pelacakan aset, robotika.	Decawave DWM1000, Qorvo DW3000

Penggunaan XBee ZigBee Mesh sangat cocok untuk aplikasi WSN yang membutuhkan:

- Efisiensi energi yang tinggi, karena perangkat sensor bisa bertahan lama dengan baterai kecil (Alobaidy et al., 2020).
- Reliabilitas jaringan, mesh topology memungkinkan rute alternatif saat terjadi kegagalan *node*, sehingga mendukung kesinambungan data (Rodenas-Herraiz et al., 2013).
- Keamanan bawaan AES-128, yang memperkuat autentikasi dan integritas data untuk blockchain (Healy et al., 2009).
- Latency rendah dan modularitas, memungkinkan *gateway* melakukan transaksi blockchain segera saat menerima data (Piyare & Lee, 2013), Karena itu, XBee ZigBee Mesh sangat mendukung integrasi WSN dan blockchain, terutama untuk aplikasi yang mengutamakan efisiensi energi, keandalan data, dan keamanan.

4.4.2. Security WSN

WSN memiliki karakteristik khas sensor berdaya rendah, komputasi terbatas, penyebaran skala besar, dan kemungkinan kompromi fisik *node* yang membuat kebutuhan keamanan berbeda dari jaringan umum. Persyaratan keamanan yang biasa ditekankan meliputi confidentiality, integrity, availability, autentikasi, serta *freshness* (proteksi replay); namun penerapan kontrol keamanan harus meminimalkan *overhead* energi dan komunikasi agar tidak mengurangi lifetime jaringan (Farooq et al., 2019) (Ahmad & Wazirali, 2022). Ancaman terhadap WSN dapat diklasifikasikan per-lapisan: pada lapisan fisik muncul serangan jamming dan *node* capture; pada MAC/link ada collision dan exhaustion; pada lapisan jaringan terdapat sinkhole, wormhole, Sybil, selective forwarding, dan pengalihan rute berbahaya; serta pada lapisan aplikasi/aggregasi muncul *false data injection* dan kompromi *aggregator*. Karena vektor serangan sangat beragam, solusi keamanan

an beberapa mekanisme (kriptografi ringan, manajemen kunci outing, dan deteksi intrusi) agar saling melengkapi (Faris et al., afi, pendekatan praktis mengutamakan algoritma simetris (*AES-ryption Standard Counter with CBC MAC*) untuk enkripsi data : *Curve Cryptography* (ECC) untuk operasi kunci publik yang

hemat ukuran kunci, serta skema manajemen kunci yang mendukung pembaruan/revocation bila *node* terdeteksi terkompromi. Arsitektur hierarkis (clustered) dan penggunaan gateway/edge yang lebih kuat untuk menangani tugas kriptografi berat merupakan praktik umum guna menjaga efisiensi energi pada *node* end-sensor (Zhou et al., 2022).

Deteksi intrusi menjadi area riset aktif di WSN modern: teknik anomaly based dan signature-based digabungkan dengan metode kecerdasan komputasi machine learning (ML) untuk meningkatkan akurasi deteksi serangan adaptif. Namun penerapan ML pada WSN menghadapi trade off antara akurasi dan overhead (komputasi/komunikasi), oleh karena itu pendekatan gabungan seperti menempatkan model inference di gateway, menggunakan model ringan, atau pelatihan terdistribusi/*federated learning* lebih banyak direkomendasikan (Ahmad & Wazirali, 2022). Selain itu, paradigma baru seperti *Software Defined WSN* (SD-WSN) memungkinkan pengelolaan kebijakan keamanan terpusat dan respons dinamis terhadap ancaman yang mempermudah orkestrasi mekanisme mitigasi di skala jaringan (Zhou et al., 2022). Secara ringkas, desain keamanan efektif untuk WSN menuntut keseimbangan teknis antara toleransi terhadap serangan, efisiensi energi, dan kemampuan pemulihan (resilience). Rangka kerja penelitian saat ini cenderung menggabungkan: (a) kriptografi ringan + manajemen kunci skalabel, (b) routing aman dan sistem reputasi untuk mitigasi perilaku berbahaya, (c) IDS berbasis ML dengan eksekusi di edge/gateway, dan (d) penggunaan arsitektur SDN/SD-WSN untuk kontrol kebijakan keamanan yang adaptif. Penerapan nyata harus diuji melalui simulasi/skenario serangan dan metrik seperti *lifetime* jaringan, throughput, latency, serta rate false-positive/negative IDS (Farooq et al., 2019).

4.4.3. Teknologi Blockchain

Blockchain adalah teknologi buku besar (*ledger*) terdistribusi yang menyimpan serangkaian transaksi atau catatan dalam struktur berantai (blok), di mana setiap blok berisi sekumpulan transaksi, cap waktu (timestamp), dan *hash* dari blok sebelumnya sehingga rantai menjadi tahan terhadap perubahan retroaktif (M. S. Ali et al., 2019). Arsitektur blockchain pada dasarnya menggabungkan empat komponen inti: (1) jaringan *peer to peer* (P2P) yang menyebarkan data dan menyimpan salinan ledger; (2) struktur blok dan fungsi hash kriptografis yang menjamin integritas data; (3) protokol konsensus untuk menyetujui urutan blok baru; dan (4) mekanisme aplikasi (mis. *Smart Contracts*) untuk menjalankan logika otomatis di dalam jaringan (Fernández-Caramés & Fraga-Lamas, 2018). Sifat-sifat fundamental blockchain desentralisasi, imutabilitas, transparansi, dan auditabilitas

ik untuk aplikasi yang membutuhkan bukti integritas dan *aceability*), seperti rantai pasokan, keuangan, dan Internet of Namun, karakteristik ini datang dengan trade off misalnya, usi dapat menimbulkan overhead komunikasi dan latensi, konsensus (Proof of Work) mengonsumsi energi besar dan

catatan publik dapat menimbulkan masalah privasi bila tidak diatur dengan baik (M. S. Ali et al., 2019)(Reyna et al., 2018).

Klasifikasi konsensus yang umum diterapkan meliputi *Proof of Work* (PoW), *Proof of Stake* (PoS), *Proof of Authority* (PoA) dan variasi lain yang dirancang untuk lingkungan *resource constrained* seperti perangkat IoT/WSN (*Proof of Authentication, Energy Aware PoA*). Riset menunjukkan pergeseran penelitian dari PoW yang berat menuju mekanisme yang lebih ringan (*low overhead*) untuk mendukung perangkat terbatasnya sumber daya dengan mempertahankan keamanan yang memadai. Pemilihan konsensus menjadi titik desain penting, penggantian PoW pada jaringan kecil/terkontrol biasanya dengan PoA/PoS/PoAh atau mekanisme voting yang lebih efisien secara energi (Ferrag et al., 2019).

Smart Contract adalah skrip/kontrak yang berjalan otomatis di lingkungan blockchain (*virtual machine*) untuk menegakkan aturan atau logika bisnis: memungkinkan verifikasi, eksekusi dan pencatatan otomatis tanpa intervensi pihak ketiga, sehingga cocok untuk otomasi validasi data atau otorisasi tindakan pada sistem terdistribusi. Dalam konteks WSN atau *sensor controlling* (RFID/QR), *Smart Contract* dapat berfungsi sebagai *gatekeeper* seperti menolak data yang tidak terverifikasi atau menegakkan kebijakan akses, namun penerapan *Smart Contract* pada skenario ini harus mempertimbangkan keterbatasan latensi dan sumber daya (Fernández-Caramés & Fraga-Lamas, 2018).

Tantangan dan isu terbuka yang sering dibahas dalam literatur modern meliputi: (i) skalabilitas (throughput vs. latency), (ii) efisiensi *energi* dan kecocokan untuk perangkat *resource constrained*, (iii) privasi data pada ledger publik, (iv) interoperabilitas antar chain, dan (v) model keamanan terhadap serangan khusus seperti 51% attack, replay attack, atau manipulasi data sensor sebelum masuk ke chain. Riset-riset ulasan dan survey merekomendasikan arsitektur hibrida (*off chain storage, gateway/edge node, privat -permissioned chains*) dan adopsi konsensus ringan serta teknik proteksi privasi (enkripsi, *off chain commitment*) untuk mengatasi masalah ini. Singkatnya, blockchain menawarkan fondasi kuat untuk meningkatkan integritas, auditabilitas, dan desentralisasi pada sistem terdistribusi termasuk WSN tetapi implementasi praktis memerlukan penyesuaian arsitektur (konsensus, off chain, gateway) dan desain kebijakan (*Smart Contract*, MFA, filtering) agar sesuai dengan keterbatasan perangkat dan persyaratan latensi serta privasi (Reyna et al., 2018).

4.4.4. Sistem Terdistribusi

Sistem terdistribusi merupakan jaringan komputer otonom yang bekerja
entitas dari perspektif pengguna, dengan replikasi data di
meningkatkan toleransi kesalahan, ketersediaan tinggi, dan
ın utamanya adalah menjaga konsistensi data, yang dapat
ı strong consistency atau eventual consistency, namun sering
tara konsistensi, ketersediaan, dan toleransi partisi sesuai CAP

theorem (Hussein et al., 2023). Untuk mencapai koordinasi dan kesesuaian data antar-*node*, protokol konsensus seperti Paxos digunakan dalam sistem seperti Spinnaker yang menyeimbangkan konsistensi dan ketersediaan (Bano et al., 2017), sedangkan Raft menawarkan pendekatan sederhana dan kuat dengan desain intuitif untuk pemilihan pemimpin dan replikasi log (Deshwal, 2025). Sebagai contoh unggulan dalam sistem terdistribusi, blockchain menggunakan distributed ledger yang disalin secara kriptografis ke semua *node* dan memperkuat keamanan serta immutabilitas data melalui konsensus berbasis Proof of Work, Proof of Stake, dan varian lainnya, sebagaimana dibahas secara mendalam dalam literatur kontemporer (Wang et al., 2019) (Bano et al., 2017).

4.4.5. *Multi Factor Authentication* (MFA)

Otentikasi faktor tunggal (*Single Factor Authentication*, SFA) seperti kata sandi atau PIN telah menjadi metode dominan selama beberapa dekade. Namun, seiring meningkatnya ancaman seperti phishing, credential stuffing, dan kebocoran basis data, kelemahan SFA semakin jelas. Hal ini mendorong munculnya *Multi Factor Authentication* (MFA) yang mengharuskan pengguna membuktikan identitas melalui dua atau lebih faktor yang saling independen, sehingga kompromi pada satu faktor tidak langsung memberi akses penuh kepada penyerang (Ometov et al., 2018). MFA diperkenalkan untuk meningkatkan tingkat keamanan secara signifikan dan menyediakan perlindungan berkelanjutan terhadap perangkat komputer serta layanan penting lainnya agar terhindar dari akses yang tidak sah, dengan memanfaatkan lebih dari dua jenis kredensial (Ometov et al., 2018). Survei terbaru menggarisbawahi bahwa MFA tidak hanya meningkatkan keamanan, tetapi juga menjadi standar regulasi di berbagai sektor, meskipun masih menghadapi tantangan adopsi dan usability (Syahreen et al., 2024) (Otta et al., 2023). Faktor autentikasi dikategorikan menjadi tiga kelompok utama:

- *Knowledge Factor* (Sesuatu yang kita tahu): kata sandi, PIN, atau jawaban pertanyaan rahasia.
- *Possession Factor* (Sesuatu yang kita miliki): smartphone untuk menerima OTP, token keamanan, atau kartu pintar.
- *Inherence Factor* (Sesuatu yang melekat pada diri kita): karakteristik biometrik seperti sidik jari, wajah, atau suara.

Kombinasi minimal dua kategori dianggap valid sebagai MFA. Studi usability terhadap lima metode MFA menunjukkan bahwa kombinasi faktor yang tepat dapat menjaga keseimbangan antara keamanan dan kemudahan penggunaan (Reese et al., 2019). Dalam penelitian (Otta et al., 2023) model fungsi autentikasi gabungan diperikut:

$$\text{...}_1) \cup f_2(x_2) \begin{cases} 1, & if\ f_1(x_1) \cup f_2(x_2) = TRUE \\ 0, & otherwise \end{cases} \quad (4.1)$$

Di mana:

- $F(x)$ adalah fungsi autentikasi sistem MFA untuk pengguna x,
- $f_1(x_1)$ adalah fungsi faktor autentikasi pertama dengan input x_1 (misalnya password),
- $f_2(x_2)$ adalah fungsi faktor autentikasi kedua dengan input x_2 (misalnya biometrik atau OTP).

Model ini menyiratkan bahwa keduanya (atau lebih) harus berhasil untuk menghasilkan nilai 1 (granted).

Salah satu implementasi MFA paling umum adalah One Time Password (OTP), yang banyak digunakan untuk faktor possession. Berikut ini Algoritma dan Rumus Matematis OTP (HOTP & TOTP):

1. HOTP (*HMAC-based One-Time Password*)

Digunakan sebagai algoritma OTP berbasis counter/event (El-Booz et al., 2016), HOTP menggunakan *hash function* + *counter event*. Rumusnya secara matematis:

$$\text{HOTP}\,(K, C) = \text{Truncate}\left(\text{HMAC} - \text{SHA1}(K, C)\right) \bmod 10^d \tag{4.2}$$

- K: kunci rahasia (shared secret)
- C: nilai counter (biasanya 64-bit)
- Truncate: mengambil sebagian output HMAC untuk menghasilkan kode numerik sepanjang *d* digit (umumnya 6–8 digit)

2. TOTP (*Time-based One-Time Password*)

Merupakan varian HOTP yang menggantikan counter dengan waktu sebagai variabel bergerak (Lumburovska et al., 2021), TOTP menambahkan komponen waktu di atas hash, menjadikan token hanya valid dalam jangka pendek:

$$T = \left[\frac{CurrentUnixTime - T_0}{X}\right] \tag{4.3}$$

$$\text{TOTP}\,(K, T) = \text{HOTP}\,(K, T) \tag{4.4}$$

ɔch (biasanya 0, 1 Jan 1970).
lidasi kode (contoh: 30 detik).
ı setiap interval; meningkatkan keamanan terhadap serangan

Meski OTP berbasis SMS populer, riset empiris menunjukkan kelemahan signifikan seperti SIM-swap, interception, dan malware pada perangkat. Studi lanjutan menemukan bahwa prosedur autentikasi operator seluler sering gagal mencegah pengambilalihan nomor telepon (K. Lee et al., 2020). Oleh karena itu, riset terbaru merekomendasikan penggunaan metode berbasis aplikasi TOTP atau teknologi FIDO2/U2F yang lebih tahan terhadap phishing (Barbosa et al., 2021). FIDO2 dan U2F menawarkan autentikasi tanpa kata sandi berbasis public key cryptography. Analisis formal membuktikan bahwa protokol ini aman terhadap serangan phishing dan replay, meskipun masih terdapat tantangan implementasi di tingkat browser dan perangkat (Barbosa et al., 2021). Penelitian lain menyoroti bahwa MFA berbasis hardware key memiliki tingkat adopsi rendah pada infrastruktur cloud karena faktor biaya dan kompatibilitas (Otta et al., 2023).

4.4.6. Mikrokontroler

Mikrokontroler didefinisikan sebagai sebuah sistem *on-chip* yang mengintegrasikan unit pemrosesan pusat (CPU), memori (RAM dan memori program), serta berbagai periferal I/O pada satu sirkuit terintegrasi (IC) tunggal (Barrett, 2010). Mikrokontroler dirancang secara spesifik untuk menjalankan fungsi-fungsi kontrol dalam sistem terbenam (*embedded system*). Arsitekturnya yang ringkas dan efisien membuatnya ideal untuk aplikasi dengan sumber daya terbatas, seperti pada perangkat Internet of Things (IoT), robotika, dan otomasi industri (El-Abd, 2017). Seiring dengan kemajuan teknologi, kompleksitas pemrograman mikrokontroler tradisional menjadi hambatan bagi non-spesialis. Prosesnya membutuhkan pemahaman mendalam tentang register perangkat keras, bahasa pemrograman C tingkat rendah, dan penggunaan alat-alat khusus. Di sinilah Arduino muncul sebagai solusi inovatif. Arduino adalah platform *open-source* yang tidak hanya menyediakan perangkat keras yang mudah digunakan, tetapi juga lingkungan pemrograman yang sangat ramah pengguna. Platform ini, yang sebagian besar menggunakan mikrokontroler Atmel AVR, bertujuan untuk menjembatani kesenjangan antara teori elektronika dan implementasi praktisnya (García-Tudela & Marín-Marín, 2023).

Kehadiran Arduino telah merevolusi cara belajar dan berinovasi di bidang elektronika dan komputasi. Menurut beberapa penelitian, penggunaan Arduino di lingkungan akademik terbukti meningkatkan pemahaman konseptual dan keterampilan praktis di kalangan mahasiswa, terutama di bidang teknik dan sains (Durfee, 2011) . Beberapa alasan utama kepopulerannya adalah:

- Sederhana dan Aksesibel: Arduino menghilangkan banyak rintangan teknis, engguna untuk fokus pada logika program dan desain proyek, urasi perangkat keras yang rumit.
- an Arduino dan komponen pendukungnya memiliki harga yang u, menjadikannya alat yang ideal untuk prototyping dan

eksperimen berskala kecil di berbagai sektor, termasuk pendidikan, hobi, dan startup.

- Komunitas dan Sumber Daya Luas: Sifatnya yang *open source* telah menciptakan ekosistem global yang masif. Ribuan proyek, tutorial, dan pustaka kode telah dikembangkan oleh komunitas, memberikan sumber belajar tak terbatas bagi pengguna baru maupun berpengalaman.
- Fleksibilitas dan Skalabilitas: Kemampuan Arduino untuk terintegrasi dengan beragam sensor, aktuator, dan modul komunikasi (seperti Wi-Fi dan Bluetooth) memungkinkan pengembang untuk membangun berbagai proyek, mulai dari sistem pemantauan lingkungan hingga robot *otonom*.

Singkatnya, Arduino telah mengubah mikrokontroler dari alat yang eksklusif menjadi platform yang demokratis dan memberdayakan siapa pun untuk berinovasi dan mewujudkan ide-ide elektronik mereka.

4.5. Metode Penelitian

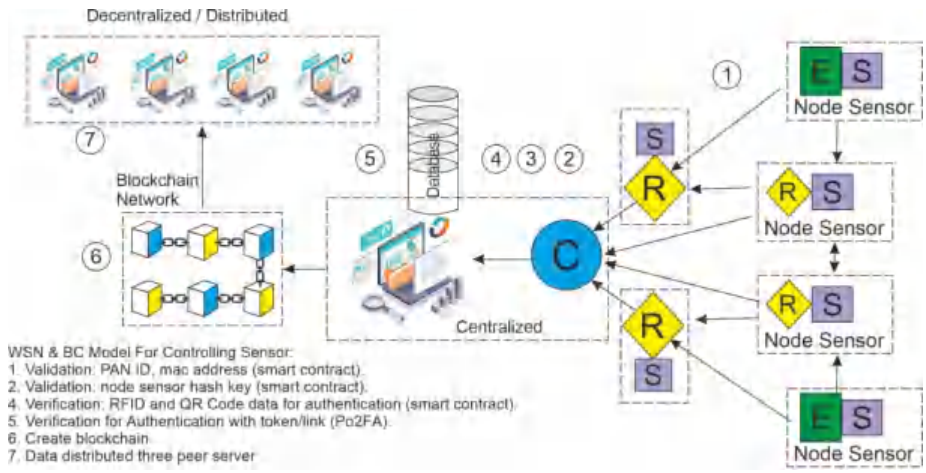
Penelitian ini menggunakan pendekatan yang terbagi menjadi dua tahap utama, yaitu perancangan model dan perancangan sistem. Tahap perancangan model difokuskan pada pengembangan representasi konseptual dan algoritma yang akan digunakan untuk mendeteksi serangan serta mengukur keakuratannya melalui metrik evaluasi seperti True Positive, False Positive, Recall, dan Precision. Selanjutnya, tahap perancangan sistem mengimplementasikan model tersebut ke dalam sistem nyata yang terdiri dari perangkat keras, perangkat lunak, serta arsitektur jaringan dan blockchain terdistribusi untuk memastikan sistem dapat berjalan secara efektif dan aman. Dengan membagi metode penelitian ke dalam dua tahap ini, diharapkan dapat menjelaskan secara sistematis dari konsep hingga implementasi solusi yang diusulkan.

4.5.1. Perancangan Model

Pada tahap ini membuat representasi abstrak dari mekanisme autentikasi ganda dan konsensus blockchain terdistribusi agar dapat dianalisis validitas dan efisiensinya. Beberapa komponen dalam tahap ini dijelaskan pada Tabel 4.3. Sedangkan Gambar 4.2. merupakan alur dari model.

Tabel 4. 3. Komponen perancangan model.

Komponen	Deskripsi
Sensor controlling	*Node* sensor yang menghasilkan UID (RFID/QR Code) sebagai input data.
Mekanisme konsensus 1 (*Smart Contract*)	*Smart Contract* yang memvalidasi atribut *node* (MAC Address, PAN ID, hash *node*) sebelum blok dibuat.
Mekanisme konsensus 2	Proses verifikasi dua faktor: validasi UID sensor dan otentikasi pengguna via tautan unik (One Time Link) melalui WhatsApp/Email.
	Tiga *peer* server (1 Master, 2 Online) yang mereplikasi data dan melakukan verifikasi blok.
	Filter data agar hanya data terverifikasi ganda yang diterima dan dimasukkan ke blockchain.



Gambar 4. 2. Alur diagram model.

Model yang dikembangkan dalam mendeteksi dan mencegah serangan pada WSN dan blockchain akan dievaluasi menggunakan metrik-metrik standar klasifikasi untuk mengukur performa dan keakuratannya. Metrik-metrik tersebut meliputi:

- True Positive (TP), Serangan terdeteksi dengan benar (valid diterima).
- False Positive (FP), Data normal salah terdeteksi sebagai serangan (tidak valid tapi diterima).
- True Negative (TN), Data normal diidentifikasi dengan benar (tidak valid dan ditolak).
- False Negative (FN): Serangan yang tidak terdeteksi (valid ditolak).

Berdasarkan nilai-nilai tersebut, dihitung metrik evaluasi sebagai berikut:

1. Recall (Sensitivitas)
   Mengukur kemampuan model untuk mendeteksi semua kasus serangan yang sebenarnya:

$$\text{Recall} = \frac{TP}{TP+FN} \tag{4.5}$$

2. Precision (Presisi)
   Mengukur ketepatan model dalam mengklasifikasikan serangan yang terdeteksi:

$$\text{Precision} = \frac{TP}{TP+FP} \tag{4.6}$$

urasi)
rediksi yang benar dari seluruh data:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (4.7)$$

4. F1-Score
   Harmonis rata-rata dari Precision dan Recall, memberikan keseimbangan antara keduanya:

$$F1 = 2\,x\,\frac{\text{Precision x Recall}}{\text{Precision} + \text{Recall}} \quad (4.8)$$

Metrik-metrik ini digunakan untuk mengukur performa model deteksi serangan pada data uji dan menentukan efektivitasnya dalam membedakan antara serangan dan aktivitas normal. Nilai Recall yang tinggi menandakan model mampu menangkap hampir semua serangan, sementara Precision yang tinggi mengindikasikan sedikit kesalahan positif (false alarms). Model dioptimasi agar nilai False Positive (FP) dan False Negative (FN) dapat diminimalisasi, sehingga sistem deteksi yang dihasilkan dapat diandalkan dan efektif dalam pengamanan jaringan. Analisis performa jaringan terdistribusi pada sistem menggunakan arsitektur jaringan terdistribusi dengan 3 server (1 server lokal, 2 online). Pengukuran dilakukan pada kedua konfigurasi (*Smart Contract* vs *Smart Contract* + Po2FA) dengan parameter antara lain throughput: jumlah data yang berhasil dikirim per detik, RSSI: kekuatan sinyal dari *node* sensor ke server, latency: waktu tunda antara pengiriman dan penerimaan data, dan waktu eksekusi: total waktu pemrosesan transaksi di tiap server. Hasil akhir menampilkan perbandingan langsung antara *Smart Contract* vs *Smart Contract* + Po2FA, baik dari segi keamanan maupun kinerja.

4.5.2. Perancangan Sistem

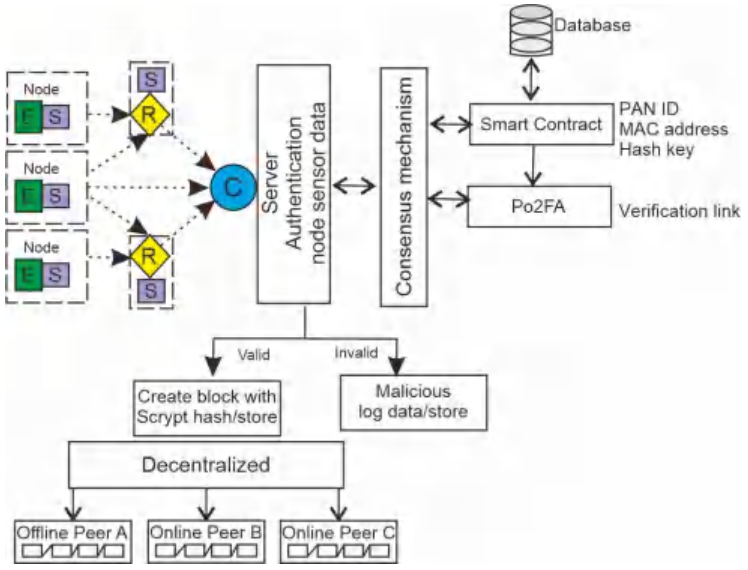
Penelitian ini mengusulkan sebuah pendekatan inovatif yang mengintegrasikan mekanisme konsensus berbasis blockchain dengan model autentikasi multi-faktor khusus pada WSN. Pendekatan ini terdiri dari dua komponen utama, yaitu mekanisme konsensus *Smart Contract* yang memanfaatkan parameter jaringan seperti MAC Address, PAN ID, dan *key hash*, serta metode autentikasi Po2FA. Mekanisme konsensus *Smart Contract* dirancang untuk memastikan bahwa setiap data sensor yang masuk ke dalam blockchain telah melalui proses verifikasi awal berdasarkan identitas fisik *node*, yaitu MAC Address dan PAN ID, serta validasi keaslian data melalui verifikasi hash. Selanjutnya, Po2FA mengimplementasikan autentikasi ganda dengan memadukan verifikasi UID dari *sensor controlling* berupa RFID atau QR Code dan otentikasi pengguna akhir melalui tautan verifikasi sekali

rification Link) yang dikirim secara langsung melalui platform
il. Hanya data yang berhasil melewati verifikasi kedua faktor
dimasukkan ke dalam blockchain, sehingga meningkatkan
ɲ keabsahan data yang tersimpan.

Po2FA merupakan pengembangan spesifik dari konsep *Multi Factor Authentication* (MFA) yang diadaptasi untuk kebutuhan sistem WSN berbasis blockchain, di mana otentikasi tidak hanya melibatkan identitas perangkat sensor, tetapi juga keikutsertaan pengguna dalam proses verifikasi data secara real-time. Integrasi metode ini dalam arsitektur blockchain terdistribusi dilakukan melalui tiga *peer* server, yaitu satu Master server dan dua server online, yang berfungsi memperkuat replikasi data secara simultan dan mengurangi risiko manipulasi data atau serangan pada satu titik. Dengan kombinasi mekanisme konsensus *Smart Contract* dan Po2FA, sistem yang diusulkan diharapkan mampu menghadirkan keamanan dan validasi data yang robust pada jaringan sensor terdistribusi, sekaligus mendukung transparansi dan ketahanan data melalui teknologi blockchain. Pendekatan ini memberikan kontribusi baru dalam pengembangan WSN yang aman, efisien, dan terintegrasi dengan teknologi *ledger* terdistribusi. Komponen perancangan sistem seperti pada Tabel 4.4. Sedangkan Gambar 4.3 merupakan alur diagram sistem.

Tabel 4. 4. Komponen perancangan sistem.

Komponen	Fungsi
Sensor controlling	Menghasilkan UID sensor dan data sensor yang akan diverifikasi.
Gateway WSN	Mengelola verifikasi MAC Address dan PAN ID, menghasilkan dan mengirim One Time Verification Link.
Sistem verifikasi OTP	Mengirim tautan verifikasi ke WhatsApp/email, menerima konfirmasi klik link dari pengguna.
Smart Contract Blockchain	Mengeksekusi logika konsensus, cek validitas *node* berdasarkan MAC, PAN ID, hash, dan status OTP.
Peer server (master & online)	Melakukan penyimpanan, replikasi, dan sinkronisasi blockchain untuk data yang tervalidasi.
Database	Menyimpan data sementara seperti status verifikasi dan metadata transaksi.



Gambar 4. 3. Alur diagram sistem.

Parameter yang dianalisis pada sistem terdistribusi blockchain tiga server meliputi throughput (Kbps), RSSI (dBm), latency (ms), dan waktu eksekusi. pengujian replikasi blockchain juga dilakukan untuk memastikan data yang tersimpan pada ketiga server identik (*data consistency check*).

4.5.3. *Proof of Two Factor Authentication* (Po2FA)

Penelitian ini mengusung konsep Po2FA sebagai pengembangan dari model *Multi Factor Authentication* (MFA) yang umum digunakan. Po2FA memodifikasi MFA dengan menggabungkan dua mekanisme autentikasi yang terintegrasi ke dalam sistem blockchain. Mekanisme pertama adalah *Smart Contract*, yang berfungsi sebagai authentication 1, sementara mekanisme kedua adalah OTP link yang memuat kode token sebagai authentication 2. Sebuah blok baru hanya akan terbentuk jika kedua autentikasi ini bernilai benar, sehingga meningkatkan keamanan transaksi pada jaringan. Secara konseptual, MFA tradisional dapat direpresentasikan sebagai:

$$\mathrm{MFA} = f(\mathrm{Auth}_1, \mathrm{Auth}_2, \ldots, \mathrm{Auth}_n) \tag{4.9}$$

Dalam Po2FA, jumlah faktor autentikasi dibatasi menjadi dua dengan spesifikasi:

$$\begin{cases} \text{rue} & if\ (\mathrm{Auth}_{SC} = true) \wedge (\mathrm{Auth}_{OTP} = true) \\ \text{alse} & otherwise \end{cases} \tag{4.10}$$

ntikasi melalui *Smart Contract*

- Auth_{OTP} = autentikasi melalui OTP link

Dengan kondisi block baru terbentuk jika:

$$\text{Create\_block} \Leftrightarrow (\text{Auth}_{SC} = \text{True}) \wedge (\text{Auth}_{OTP} = \text{True}) \quad (4.11)$$

Atau

$$\begin{cases} \text{Create\_block} = \text{true} & if\ \text{Po2FA} = \text{true} \\ \text{Log\_attack} = \text{true} & if\ \text{Po2FA} = \text{false} \end{cases} \quad (4.12)$$

Dengan pendekatan ini, Po2FA tidak hanya mempertahankan prinsip keamanan MFA, tetapi juga mengoptimalkan proses verifikasi transaksi pada sistem blockchain, sehingga meminimalkan risiko manipulasi dan meningkatkan kepercayaan jaringan.

4.5.4. Mitigasi Ancaman Menggunakan SC dan SC+Po2FA

Untuk memahami kontribusi mekanisme keamanan yang digunakan, penelitian ini menyajikan perbandingan mitigasi serangan antara *Smart Contract* (SC) dan *Smart Contract* dengan *Proof of Two Factor Authentication* (SC+Po2FA). Tabel 4.5. menggambarkan sejauh mana masing-masing pendekatan mampu menghadapi berbagai potensi ancaman pada WSN Blockchain terdistribusi, mulai dari serangan sederhana seperti data injection hingga serangan kompleks yang melibatkan kompromi identitas *node*. SC murni pada dasarnya efektif dalam validasi dasar, seperti integritas data dan pencegahan replay attack, namun masih memiliki kelemahan dalam menanggulangi serangan berbasis identitas. Sementara itu, SC+Po2FA memberikan lapisan autentikasi tambahan berbasis token/OTP yang lebih ketat, sehingga mampu menutup celah keamanan yang tidak tercakup oleh SC. Dengan demikian, tabel mitigasi ini memperlihatkan perbedaan fundamental antara efisiensi SC murni dan proteksi komprehensif SC+Po2FA, serta menegaskan adanya trade-off antara kinerja sistem dan tingkat keamanan.

Tabel 4. 5. Mitigasi Serangan pada WSN Blockchain dengan SC vs SC+Po2FA.

Jenis Serangan / Ancaman	Dampak pada WSN Blockchain	Mitigasi dengan SC	Mitigasi dengan SC+Po2FA
Data Injection Attack (penyisipan data palsu dari *node*)	Validitas blok terganggu karena data sensor dipalsukan	SC memverifikasi format dan hash data sebelum blok terbentuk	SC+Po2FA menambahkan verifikasi ganda melalui OTP/token sehingga data palsu sulit lolos meskipun hash dimanipulasi
Sybil Attack (*node* palsu menyamar sebagai banyak identitas)	Penyerang mendominasi jaringan sensor dan blockchain	SC mengenali identitas *node* berdasarkan hash & MAC address	SC+Po2FA menambahkan autentikasi faktor kedua (link/token unik), sehingga *node* palsu sulit diverifikasi
	ata lama anggap data aru dan embentuk blok alah	SC memeriksa timestamp dan nonce untuk mendeteksi data ganda	SC+Po2FA memastikan setiap transaksi hanya valid jika diverifikasi ulang melalui faktor kedua
	ata sensor ensitif terekspos	SC tidak mencegah penyadapan	SC+Po2FA menambah lapisan autentikasi, sehingga

Jenis Serangan / Ancaman	Dampak pada WSN Blockchain	Mitigasi dengan SC	Mitigasi dengan SC+Po2FA
(penyadapan data sensor)		langsung, hanya memastikan integritas saat blok terbentuk	data hasil sadapan tidak dapat divalidasi tanpa token
Node Compromise (*node* sah diretas)	*Node* sah mengirim data berbahaya ke blockchain	SC tetap menganggap *node* sah valid selama hash cocok	SC+Po2FA mewajibkan autentikasi faktor kedua eksternal, sehingga meskipun *node* diretas, blok tidak terbentuk tanpa verifikasi tambahan
Denial of Service (DoS)	Sistem melambat akibat serangan trafik berlebihan	SC hanya menangani transaksi sah, tetapi tidak bisa menyaring volume serangan	SC+Po2FA menambah overhead validasi sehingga mempersempit peluang DoS berbasis transaksi palsu, meskipun tidak menghilangkan sepenuhnya

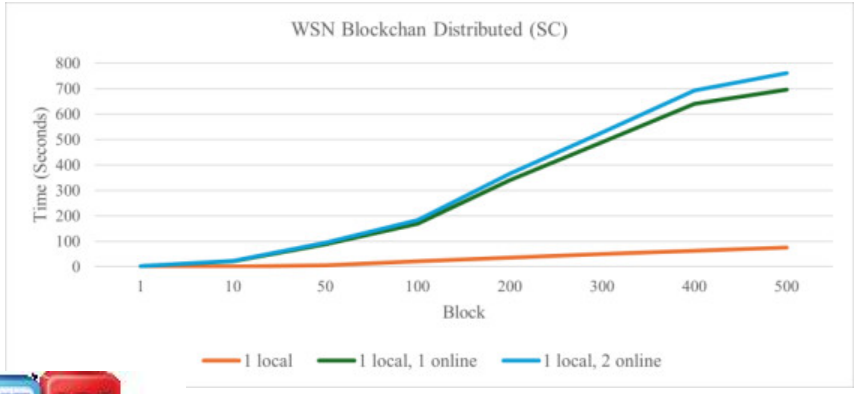
4.6. Pembahasan Hasil dan Diskusi

4.6.1. Perbandingan waktu eksekusi WSN BC Terdistribusi

Pada tahap ini dilakukan pengujian untuk membandingkan waktu eksekusi dari tiga sistem terdistrubusi yaitu 1) satu server master, 2) satu server master, satu online, dan 3) satu server master, dua server online. Pengujian menggunakan hardware serta transmisi dari protokel Zigbee dengan topologi mesh, iterasi dilakukan 500 kali dengan 3 *node sensor controlling* yang diacak dan satu sebagai server. Pengujian dilakukan di sistem SC dan SC+Po2FA.

a) WSN blockchain terdistribusi menggunakan SC

Gambar 4.4. Menunjukkan bahwa pengujian dengan tiga *peer* server terdistribudi (1 local, 2 online) dengan iterasi 500 block membutuhkan waktu 760,943 detik, sedangkan untuk 1 server 75,96 detik. Tiga server terdistribusi dipengaruh oleh kualitas jaringan internet.



nbar 4. 4. WSN blockchain terdistribusi (SC).

ui sebaran data waktu eksekusi pada masing-masing pengujian igunakan statistik deskriptif yang hasilnya seperti pada Tabel

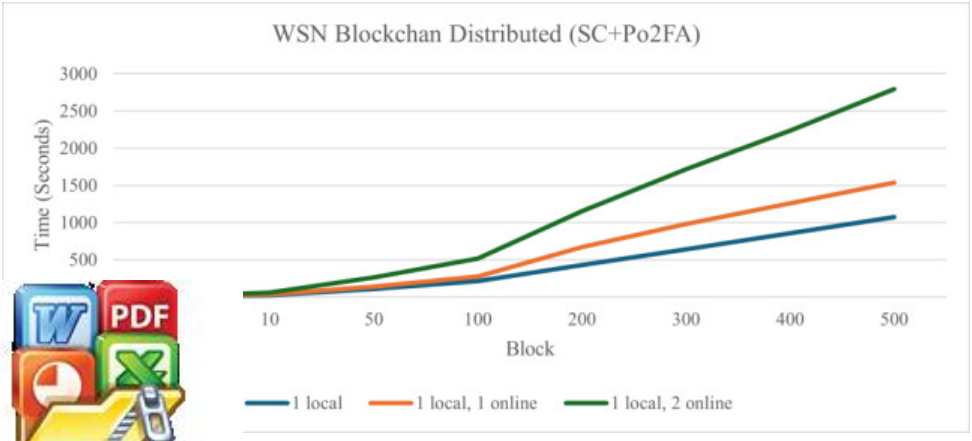
Tabel 4. 6. Statistik deskriptif waktu eksekusi WSN blockchain menggunakan SC

Method	1 local (detik)	1 local, 1 online (detik)	1 local, 2 online (detik)
Mean	0,152	1,394	1,522
Median	0,122	0,607	0,735
Min	0,054	0,255	0,372
Max	2,035	15,622	15,778
Std. Deviasi	0,18	1,843	1,844

Berdasarkan hasil pengukuran pada Tabel 4.6 terlihat bahwa metode dengan 1 local memiliki kinerja paling efisien dengan nilai rata-rata (mean) 0,152 detik, median 0,122 detik, serta standar deviasi yang relatif rendah (0,18), menunjukkan konsistensi waktu eksekusi yang stabil. Ketika ditambahkan 1 local, 1 online, rata-rata waktu meningkat signifikan menjadi 1,394 detik dengan median 0,607 detik, disertai standar deviasi 1,843 yang mengindikasikan variasi eksekusi lebih tinggi akibat adanya proses komunikasi jaringan. Penambahan lebih lanjut menjadi 1 local, 2 online menghasilkan rata-rata 1,522 detik dan median 0,735 detik, dengan standar deviasi hampir sama (1,844), yang menunjukkan bahwa peningkatan jumlah *node* online memperbesar overhead waktu meskipun tidak sebanding dengan lonjakan dari konfigurasi satu *node* online sebelumnya. Secara keseluruhan, semakin banyak *node* online yang terlibat, waktu eksekusi cenderung meningkat dengan fluktuasi yang lebih besar, menandakan trade-off antara skalabilitas sistem dan stabilitas kinerja.

b) WSN blockchain terdistribusi menggunakan SC+Po2FA

Gambar 4.5. Menunjukkan bahwa pengujian dengan tiga *peer* server terdistribudi (1 local, 2 online) dengan iterasi 500 block membutuhkan waktu 2.792,542 detik, sedangkan untuk 1 server 1.073, 794 detik. Tiga server terdistribusi dipengaruh oleh kualitas jaringan internet.



r 4. 5. WSN blockchain terdistribusi (SC+Po2FA).

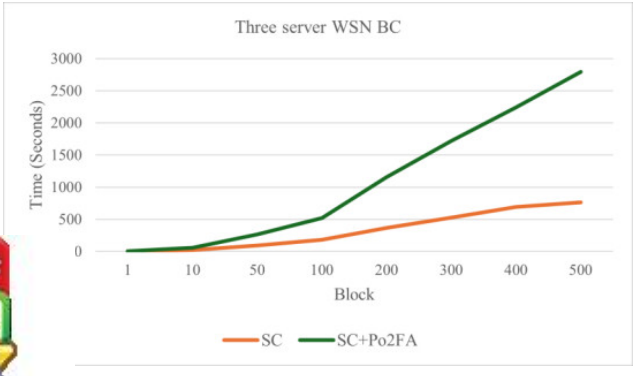
Untuk mengetahui sebaran data waktu eksekusi pada masing-masing pengujian sistem terdistribusi digunakan statistik deskriptif yang hasilnya seperti pada Tabel 4.7.

Tabel 4. 7. Statistik deskriptif waktu eksekusi WSN blockchain menggunakan SC+Po2FA

Method	1 local (detik)	1 local, 1 online (detik)	1 local, 2 online (detik)
Mean	2,148	3,082	5,585
Median	2,143	2,605	5,187
Min	2,094	2,339	4,713
Max	2,386	13,865	16,357
Std. Deviasi	0,029	1,407	1,409

Tabel 4.7. menggambarkan performa waktu eksekusi ketiga konfigurasi server yang berbeda, konfigurasi 1 local memberikan performa paling stabil dengan rata-rata waktu 2,148 detik, median 2,143 detik, serta standar deviasi yang sangat rendah (0,029), sehingga variasi eksekusi hampir tidak signifikan. Ketika ditambahkan 1 local, 1 online, rata-rata waktu meningkat menjadi 3,082 detik dengan median 2,605 detik, disertai lonjakan standar deviasi menjadi 1,407 yang menunjukkan adanya fluktuasi besar akibat keterlibatan komunikasi jaringan. Penambahan lebih lanjut menjadi 1 local, 2 online menghasilkan kenaikan rata-rata waktu lebih tinggi lagi menjadi 5,585 detik dengan median 5,187 detik dan standar deviasi 1,409, yang menunjukkan pola waktu eksekusi lebih lambat sekaligus tidak stabil. Secara keseluruhan, data ini memperlihatkan bahwa semakin banyak *node* online yang terlibat, sistem mengalami peningkatan waktu eksekusi dan variabilitas performa, menandakan adanya overhead signifikan dari sisi sinkronisasi dan komunikasi jaringan yang memengaruhi konsistensi kinerja.

c) Perbandingan pada tiga server terdistribusi (1 local, 2 online)



Perbandingan waktu eksekusi antara SC vs SC+Po2FA.

Berdasarkan hasil pengukuran waktu eksekusi Gambar 4.6. menunjukkan perbedaan signifikan antara mekanisme SC+Po2FA dan SC murni. Pada blok 100, durasi SC+Po2FA tercatat 517,77 detik, hampir tiga kali lebih lama dibandingkan SC yang hanya 182,88 detik. Tren ini konsisten hingga blok 500, di mana SC+Po2FA membutuhkan 2.792,54 detik, sementara SC hanya 760,94 detik. Kenaikan waktu pada kedua metode relatif linier terhadap pertambahan blok, namun gradien pada SC+Po2FA jauh lebih curam. Hal ini mengindikasikan bahwa penambahan lapisan autentikasi ganda (Po2FA) meningkatkan kompleksitas dan overhead komputasi, sehingga berdampak pada efisiensi waktu eksekusi. Meskipun SC lebih efisien dalam hal durasi, SC+Po2FA menawarkan lapisan keamanan tambahan yang signifikan, sehingga terdapat trade off antara performa dan keamanan dalam implementasi sistem ini.

Dari sisi *time complexity* menunjukkan bahwa baik SC maupun SC+Po2FA memiliki pola pertumbuhan waktu yang linier terhadap jumlah blok, dengan kompleksitas waktu sebesar O(n). Namun, garis pertumbuhan SC+Po2FA memiliki kemiringan (slope) yang lebih curam, sehingga setiap penambahan blok menimbulkan kenaikan waktu eksekusi yang jauh lebih besar dibandingkan hanya dengan SC. Dari perspektif ruang, SC memiliki kompleksitas O(n) karena hanya menyimpan data transaksi dasar, sedangkan SC+Po2FA meningkat menjadi O(n + k) akibat adanya overhead tambahan berupa log autentikasi, hash, dan metadata. Visualisasi ini menegaskan bahwa meskipun SC+Po2FA memberikan lapisan keamanan tambahan, mekanisme tersebut menimbulkan peningkatan computational overhead baik dari sisi waktu maupun ruang. Dengan demikian, terdapat trade off yang jelas antara efisiensi dan keamanan, yang perlu diperhatikan dalam perancangan sistem blockchain berbasis autentikasi ganda. Berikut Tabel 4.8. ringkasan perbandingan time complexity dan space complexity antara SC dan SC+Po2FA.

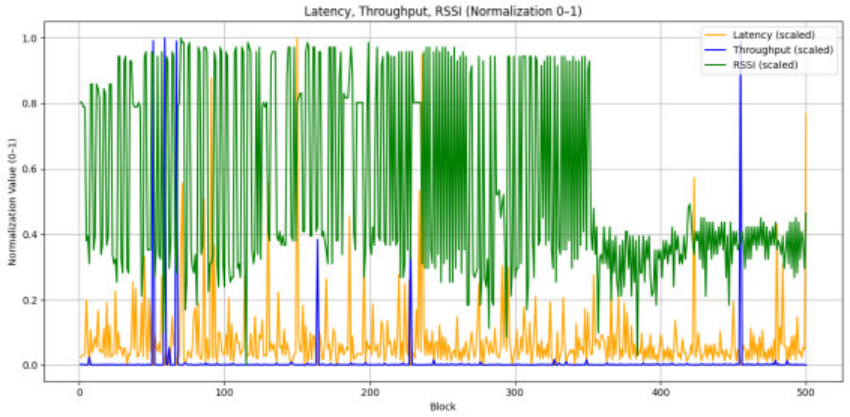
Tabel 4. 8. Perbandingan time dan space complexity

Metode	Time Complexity	Space Complexity	Karakteristik
SC	O(n)	O(n)	Peningkatan waktu hampir linier; penyimpanan hanya untuk data transaksi dasar.
SC+Po2FA	O(n) dengan slope lebih besar	O(n + k)	Peningkatan waktu linier dengan overhead signifikan; membutuhkan ruang tambahan untuk hash, metadata, dan log autentikasi.

Tabel 4.8 menunjukkan bahwa kedua metode memiliki kompleksitas asimtotik
SC+Po2FA menambahkan konstanta overhead (k) pada ruang
oefisien pertumbuhan pada waktu. Artinya, semakin besar
ensi antara SC dan SC+Po2FA akan semakin lebar, meskipun
awarkan keamanan tambahan.

4.6.2. Analisis Performa WSN Blockchain Terdistribusi

a) WSN Blockchain Terdistribusi SC



Gambar 4. 7. Latency, throughput dan RSSI pada WSN blockchain terdistribusi SC.

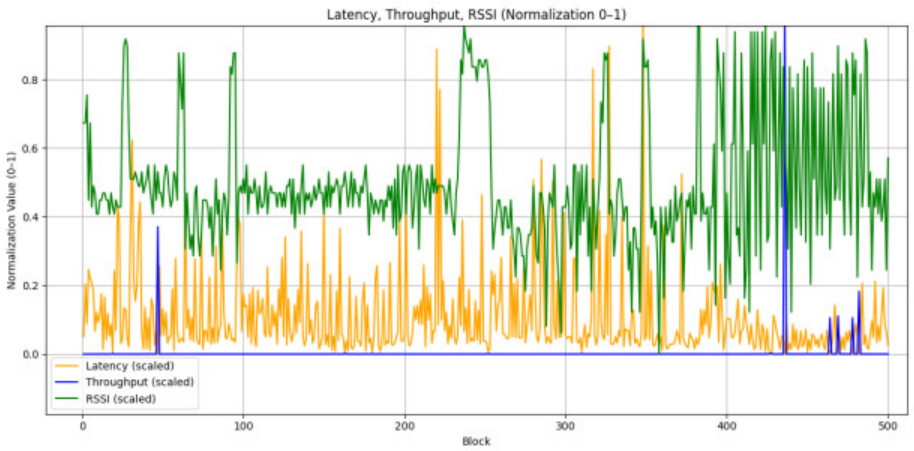
Tabel 4. 9. Statistik deskriptif pada WSN blockchain terdistribusi SC

Metode	Latency (ms)	Throughput (kbps)	RSSI (dBm)
Mean	9072,081	1,053	-44,848
Median	5231,012	0,102	-55
Min	0	0	-83
Max	119095,028	94,067	-12
Std. Deviasi	13205,57	8,605	20,106

Berdasarkan hasil pengujian pada Gambar 4.7. dan Tabel 4.9. sistem menunjukkan karakteristik performa jaringan yang cukup berfluktuasi. Nilai latency memiliki rata-rata 9.072,081 ms dengan median 5.231,012 ms serta standar deviasi yang tinggi (13.205,57), menandakan adanya variasi waktu tunda yang besar mulai dari 0 hingga maksimum 119.095,028 ms. Dari sisi throughput, rata-rata tercatat 1,053 kbps dengan median sangat rendah (0,102 kbps), sementara nilai maksimum mencapai 94,067 kbps dan standar deviasi 8,605, yang menunjukkan kapasitas transfer data cenderung rendah namun sesekali mampu mencapai puncak yang jauh lebih tinggi. Sementara itu, kualitas sinyal yang direpresentasikan oleh RSSI memiliki
m dengan median -55 dBm, bergerak dari -83 dBm (lemah)
ngat kuat), serta standar deviasi 20,106 yang menunjukkan
lam kestabilan sinyal. Secara keseluruhan, data ini
wa meskipun sistem mampu mencapai performa tinggi dalam

kondisi tertentu, konsistensi masih menjadi kendala utama akibat tingginya variasi pada latency, throughput, dan kekuatan sinyal.

b) WSN Blockchain Terdistribusi SC+Po2FA



Gambar 4. 8. Latency, throughput dan RSSI pada WSN blockchain terdistribusi SC+Po2FA.

Tabel 4. 10. Statistik deskriptif pada WSN blockchain terdistribusi SC+Po2FA.

Metode	Latency (ms)	Throughput (kbps)	RSSI (dBm)
Mean	11891,61971	2,975630835	-60,646
Median	6209,835291	0,090582495	-62
Min	0,74005127	0,005075525	-85
Max	110825,9659	760,0824742	-36
Std. Deviasi	14459,12365	37,21188083	9,0058139

Berdasarkan Gambar 4.8. dan Tabel 4.10. hasil analisis data menunjukkan bahwa nilai RSSI menunjukkan rata-rata sebesar –60,646 dBm dengan penyebaran relatif kecil (standar deviasi 9,006), menandakan kualitas sinyal cukup stabil meskipun bervariasi antara –85 dBm hingga –36 dBm. Pada sisi lain, throughput memiliki rata-rata rendah (2,976 kbps) dan median sangat kecil (0,091 kbps), namun lebar hingga 760,082 kbps dengan standar deviasi tinggi ın adanya fluktuasi ekstrem antara kondisi jaringan yang sangat t cepat, beberapa titik mengalami outlier yang bisa disebabkan rkirim sangat cepat atau pengukuran anomali dari noise atau dak selalu berarti error tetapi diperlukan pemeriksaan apakah

dari kondisi jaringan yang tidak normal atau bug perhitungan. Sementara itu, latency memperlihatkan nilai rata-rata sangat tinggi (11.891,62 ms) dengan sebaran luas (standar deviasi 14.459,124), meskipun median 6.209,835 ms lebih rendah, menandakan distribusi latency cenderung skewed akibat beberapa nilai ekstrem yang sangat besar. Secara umum, hasil ini mengindikasikan bahwa meskipun kualitas sinyal relatif stabil, performa jaringan cenderung tidak konsisten dengan throughput dan latency yang sangat fluktuatif, yang berimplikasi pada reliabilitas komunikasi dalam sistem yang diuji.

4.6.3. Hasil Evaluasi Keamanan dan Akurasi

Pada pengujian ini, digunakan tiga *node* sensor yang terdiri dari dua RFID dan satu QR Code yang dilakukan iterasi sebanyak 100 kali pada sistem WSN terintegrasi menggunakan blockchain terdistribusi dengan tiga server (satu offline sebagai master, dua online server). Pengujian membandingkan dua sistem yaitu 1). sistem WSN blockchain menggunakan *Smart Contract* (SC), dan 2). Sistem WSN blockchain menggunakan SC dan SC+Po2FA. Pengukuran performa dan keakuratan deteksi anomali terhadap data dan *node* sensor menggunakan Confusion Matrix.

Tabel 4. 11. Data deteksi WSN blockchain SC+Po2FA.

Matrix	SC + Po2FA	SC
TP (valid diterima)	69	64
FN (valid ditolak)	7	0
FP (invalid tapi diterima)	0	9
TN (invalid dan ditolak)	24	27

Pada Tabel 4.11. terdapat empat matrix yaitu TP (serangan terdeteksi dengan benar, registrasi SC dan Po2FA), FN (data terdeteksi benar tetapi ditolak oleh sistem seperti kode token atau link expired), FP (data invalid tapi masuk ke sistem seperti kartu RFID atau QR Code dipakai oleh orang lain), dan TN (data yang invalid dan berhasil ditolak). Pada sistem SC+Po2FA nilai FN tercatat tinggi dikarenakan token atau link expired, sedangkan pada sistem SC nilai FP terdeteksi 9 dikarenakan kartu atau akses dipakai oleh orang lain atau bukan pemilik asli kartu.

Tabel 4. 12. Sistem SC.

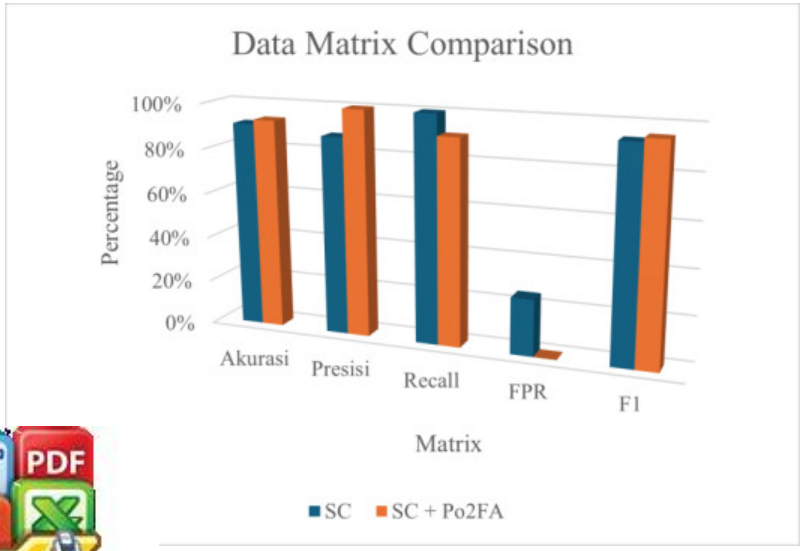
Matrix	Nilai	Analisa
Akurasi	91%	Sistem memproses 91 dari 100 transaksi dengan benar. Nilai ini sedikit di bawah SC + Po2FA, yang menunjukkan Po2FA memberikan kontribusi positif pada akurasi.
Presisi	87,67%	Dari semua data yang diterima, hanya sekitar 88% yang benar-benar valid. Artinya ada false positive yang cukup signifikan (sekitar 12%).
		Semua data valid berhasil diterima tanpa ada yang terlewat, namun hal ini dicapai dengan mengorbankan presisi karena data tidak valid ikut lolos.

FPR	25%	Seperempat data tidak valid ikut diterima. Ini menunjukkan kelemahan dalam mekanisme verifikasi SC tanpa Po2FA.
F1 Score	93.5%	Meskipun recall sempurna, penurunan presisi menyebabkan F1 Score lebih rendah dibanding SC + Po2FA.

Tabel 4. 13. Sistem SC+Po2FA.

Matrix	Nilai	Analisa
Akurasi	93%	Sistem berhasil memproses 93 dari 100 transaksi secara benar. Nilai ini menunjukkan bahwa integrasi Po2FA membantu mempertahankan tingkat akurasi yang tinggi.
Presisi	100%	Semua data yang diterima benar-benar valid. Tidak ada satupun data palsu yang lolos (false positive = 0%). Po2FA efektif dalam menyaring data yang tidak memenuhi kriteria.
Recall	90.79%	Sekitar 91% dari semua data valid berhasil diterima. Ada sedikit kehilangan data valid (~9%) karena faktor seperti kegagalan verifikasi pengguna.
FPR	0%	Tidak ada penerimaan data yang salah (tidak valid). Menunjukkan tingkat keamanan dan ketepatan verifikasi yang sempurna.
F1 Score	95.2%	Gabungan presisi sempurna dan recall yang tinggi menghasilkan kinerja keseluruhan yang sangat baik.

Tabel 4.12. dan 4.13. merupakan analisa hasil dari evaluasi matrix, tabel tersebut menjelaskan perbandingan antara penggunaan sistem SC dengan SC+Po2FA pada sistem terdistribusi tiga jenis server dalam mencegah dan mendeteksi serangan. Data yang dianggap mencurigakan atau ancaman tidak akan disimpan didalam block tetapi akan disimpan pada log data ancaman, data ini dapat digunakan untuk menganalisis history ancaman.



Gambar 4. 9. Perbandingan data matrix.

Berdasarkan gambar 4.9 menunjukkan bahwa nilai akurasi keduanya tinggi tetapi SC + Po2FA sedikit lebih akurat yaitu 93%, nilai presisi untuk SC+Po2FA dapat mengeliminasi semua False Positive sedangkan SC 87,67%, nilai recall SC+Po2FA 90,79% dikarenakan lebih ketat pada verifikasi, sehingga beberapa serangan mungkin tidak lolos tahap verifikasi ganda yang mengakibatkan FN bertambah. Aspek F1 Score merupakan nilai keseimbangan antara recall dan precision, SC+Po2FA memiliki F1 Score lebih tinggi (95,17%) yang berarti model ini memberikan hasil deteksi yang optimal. Nilai FPR pada SC 25%, ini menunjukkan cukup tinggi tingkat false alarm.

4.6.4. Diskusi

Hasil uji sistem terdistribusi menunjukkan adanya *trade off* antara skalabilitas dan efisiensi kinerja. Penambahan jumlah server online meningkatkan reliabilitas distribusi data, tetapi juga menambah overhead sinkronisasi sehingga waktu eksekusi bertambah signifikan. Hal ini mengindikasikan bahwa sistem perlu mempertimbangkan jumlah server optimal agar tidak terjadi degradasi kinerja. Dari sisi performa jaringan, variasi tinggi pada latency, throughput, dan RSSI memperlihatkan tantangan mendasar pada real deployment WSN, yaitu kestabilan komunikasi antar *node*. Fluktuasi RSSI dan throughput rendah menunjukkan bahwa faktor lingkungan serta kualitas sinyal sangat berpengaruh terhadap performa blockchain berbasis sensor.

Perbandingan SC vs SC+Po2FA menegaskan adanya trade-off antara performa dan keamanan. SC lebih efisien dengan kompleksitas waktu dan ruang O(n), namun hanya memberikan proteksi dasar. Sebaliknya, SC+Po2FA menambah lapisan autentikasi kedua yang meningkatkan proteksi terhadap serangan berbasis identitas seperti Sybil attack, meskipun dengan overhead waktu (O(n) dengan slope lebih curam) dan ruang tambahan (O(n+k)). Hasil evaluasi akurasi mendukung temuan ini: SC+Po2FA menghasilkan F1 Score lebih tinggi (95,17%) dan mengeliminasi False Positive, sehingga lebih andal dalam deteksi serangan. Namun, recall sedikit menurun karena verifikasi ganda menyebabkan peningkatan False Negative. Dengan demikian, SC+Po2FA memberikan keamanan optimal dengan biaya waktu dan ruang yang lebih besar, sementara SC lebih cocok untuk aplikasi ringan dengan kebutuhan komputasi cepat.

Secara keseluruhan, penelitian ini menekankan pentingnya menjaga keseimbangan antara performa, keamanan, dan akurasi dalam desain WSN Blockchain. Untuk aplikasi dengan *node* terbatas, SC cukup memadai, sedangkan untuk skenario dengan ancaman tinggi, SC+Po2FA lebih relevan. Penelitian lanjutan

ada optimasi Po2FA agar lebih ringan, pengujian dengan ta integrasi algoritma konsensus alternatif untuk mencapai ien sekaligus aman.

4.7. Kesimpulan

Penelitian ini berhasil mengintegrasikan Wireless Sensor Network dengan Blockchain dalam skema sistem terdistribusi menggunakan konfigurasi multi server (1 local, 1 local + 1 online, dan 1 local + 2 online) serta membandingkan mekanisme SC dan SC+Po2FA**.** Hasil pengujian menunjukkan bahwa jumlah server online berbanding lurus dengan peningkatan overhead sinkronisasi, sehingga waktu eksekusi sistem meningkat signifikan meskipun reliabilitas distribusi juga lebih terjamin. Dari sisi performa jaringan, pengukuran latency, throughput, dan RSSI memperlihatkan variabilitas yang tinggi, menegaskan tantangan mendasar pada penerapan WSN nyata, yaitu kestabilan komunikasi antar *node*. Pengujian pada tiga server terdistribusi dengan 500 blok SC+Po2FA membutuhkan 2.792,54 detik, sementara SC hanya 760,94 detik. Kenaikan waktu pada kedua metode relatif linier terhadap pertambahan blok. Sementara itu, perbandingan SC dan SC+Po2FA menunjukkan trade off yang jelas antara efisiensi dan keamanan. SC unggul dalam kecepatan dan efisiensi dengan kompleksitas O(n), namun proteksi yang diberikan terbatas. Sebaliknya, SC+Po2FA memberikan lapisan autentikasi ganda yang terbukti meningkatkan keamanan dengan akurasi 93% dan F1 Score 95,17%, meskipun membutuhkan waktu eksekusi dan ruang penyimpanan yang lebih besar. Sedangkan SC mempunyai nilai akurasi 91% dengan F1 Score 93,5%.

Secara keseluruhan, penelitian ini menyimpulkan bahwa SC cocok digunakan pada aplikasi dengan jumlah *node* terbatas dan kebutuhan komputasi ringan**,** sementara SC+Po2FA lebih relevan untuk aplikasi berskala besar atau dengan tingkat ancaman tinggi**.** Penelitian lanjutan perlu diarahkan pada pengembangan mekanisme Po2FA yang lebih efisien**,** pengujian dengan skenario serangan nyata**,** serta integrasi algoritma konsensus alternatif guna mencapai keseimbangan optimal antara performa, keamanan, dan akurasi dalam WSN Blockchain terdistribusi.

4.8. Daftar Pustaka

Ahmad, R., & Wazirali, R. (2022). Machine Learning for Wireless Sensor Networks Security : An Overview of Challenges and Issues.

Ali, A. I., & Zorlu Partal, S. (2022). Development and performance analysis of a ZigBee and LoRa-based smart building sensor network. Frontiers in Energy Research, 10(August), 1–13. https://doi.org/10.3389/fenrg.2022.933743

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of Blockchains in the Internet of Things: A Comprehensive

Communications Surveys and Tutorials, 21(2), 1676–1717. .1109/COMST.2018.2886932

taibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). d multi-factor authentication: A systematic literature review. of Things (Netherlands), Vol. 23. .1016/j.iot.2023.100844

Alobaidy, H. A. H., Mandeep, J. S., Nordin, R., & Abdullah, N. F. (2020). A review on zigbee based WSNs: Concepts, infrastructure, applications, and challenges. International Journal of Electrical and Electronic Engineering and Telecommunications, 9(3), 189–198. https://doi.org/10.18178/ijeetc.9.3.189-198

Amjad, S., Abbas, S., Abubaker, Z., Alsharif, M. H., Jahid, A., & Javaid, N. (2022). Blockchain Based Authentication and Cluster Head Selection Using DDR-LEACH in Internet of Sensor Things. Sensors, 22(5), 1–20. https://doi.org/10.3390/s22051972

And, I. A. A. E. M., & Darwish, S. M. (2021). Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach. IEEE Access, 9(1), 103822–103834. https://doi.org/10.1109/ACCESS.2021.3098933

Anwar, R. W., Bakhtiari, M., Zainal, A., & Qureshi, K. N. (2015). A survey of wireless sensor network security and routing techniques. Research Journal of Applied Sciences, Engineering and Technology, 9(11), 1016–1026. https://doi.org/10.19026/rjaset.9.2595

Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. *PeerJ* Computer Science, 7(September), 1–33. https://doi.org/10.7717/*peer*j-cs.673

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the Age of Blockchains. Retrieved from http://arxiv.org/abs/1711.03936

Barbosa, M., Boldyreva, A., Chen, S., & Warinschi, B. (2021). Provable Security Analysis of FIDO2. In Lecture Notes in Computer Science. Springer International Publishing. https://doi.org/10.1007/978-3-030-84252-9_5

Barrett, S. F. (2010). Arduino Microcontroller Processing for Everyone! Part I. In Synthesis Lectures on Digital Circuits and Systems (Vol. 5). https://doi.org/10.2200/S00280ED1V01Y201005DCS028

Che, F., Ahmed, Q. Z., Lazaridis, P. I., Sureephong, P., & Alade, T. (2023). Indoor Positioning System (IPS) Using Ultra-Wide Bandwidth (UWB)—For Industrial Internet of Things (IIoT). Sensors, 23(12), 1–28. https://doi.org/10.3390/s23125710

Dener, M., & Orman, A. (2023). BBAP-WSN: A New Blockchain-Based Authentication Protocol for Wireless Sensor Networks. Applied Sciences (Switzerland), 13(3). https://doi.org/10.3390/app13031526

Deshwal, K. (2025). Raft Consensus Algorithm: Simplicity and Robustness in Distributed Systems. European Journal of Computer Science and Information Technology, 13(14), 184–197. https://doi.org/10.37745/ejcsit.2013/vol13n14184197

Durfee, W. (2011). Arduino Microcontroller Guide. www.me.umn.edu/courses/me2011/arduino/, pp. 1–27.

El-Abd, M. (2017). A Review of Embedded Systems Education in the Arduino Age: d and Future Directions. International Journal of Engineering), 7(2), 79. https://doi.org/10.3991/ijep.v7i2.6845

, G., & El-Fishawy, N. (2016). A secure cloud storage system based one-time password and automatic blocker protocol. urnal on Information Security, 2016(1).).1186/s13635-016-0037-0

Elechi, P., & Obi-Ijeoma, C. P. (2022). Performance Analysis of an Ultra-Wide Band (UWB) Antenna for Communication System. Trends Journal of Sciences Research, 2(1), 1–12. https://doi.org/10.31586/ojes.2022.359

Faris, M., Mahmud, M. N., Fadzli, M., Salleh, M., & Alnoor, A. (2023). Wireless sensor network security : A recent review based on state-of-the-art works. 15, 1–29. https://doi.org/10.1177/18479790231157220

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6(June), 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188–2204. https://doi.org/10.1109/JIOT.2018.2882794

Finkenzeller, K. (2003). RFID Handbook. In RFID Handbook. https://doi.org/10.1002/0470868023

García-Tudela, P. A., & Marín-Marín, J. A. (2023). Use of Arduino in Primary Education: A Systematic Review. Education Sciences, 13(2). https://doi.org/10.3390/educsci13020134

Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors (Switzerland), 12(9), 11734–11753. https://doi.org/10.3390/s120911734

Hanggoro, D., Windiatmaja, J. H., Muis, A., Sari, R. F., & Pournaras, E. (2024). Energy-aware proof-of-authority: Blockchain consensus for clustered wireless sensor network. Blockchain: Research and Applications, 5(3), 100211. https://doi.org/10.1016/j.bcra.2024.100211

Haxhibeqiri, J., De Poorter, E., Moerman, I., & Hoebeke, J. (2018). A survey of LoRaWAN for IoT: From technology to application. Sensors (Switzerland), 18(11). https://doi.org/10.3390/s18113995

Healy, M., Newe, T., & Lewis, E. (2009). Security for wireless sensor networks: A review. SAS 2009 - IEEE Sensors Applications Symposium Proceedings, (March 2009), 80–85. https://doi.org/10.1109/SAS.2009.4801782

Hsiao, S. J., & Sung, W. T. (2021). Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks. IEEE Access, 9, 72326–72341. https://doi.org/10.1109/ACCESS.2021.3079708

Hughes, J., Yan, J., & Soga, K. (2015). Development of wireless sensor network using bluetooth low energy (BLE) for construction noise monitoring. International Journal on Smart Sensing and Intelligent Systems, 8(2), 1379–1405. https://doi.org/10.21307/ijssis-2017-811

Hussein, Z., Salama, M. A., & El-Rahman, S. A. (2023). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. Cybersecurity, 6(1). https://doi.org/10.1186/s42400-023-00163-y

[illegible] mras, Y., Somwong, S., & Boonsong, W. (2025). Comparative Bee, LoRa, and NB-IoT in a smart building: advantages, ntegration possibilities. International Journal of Reconfigurable edded Systems (IJRES), 14(1), 165.).11591/ijres.v14.i1.pp165-175

Intrusion Detection System in Wireless Sensor Networks - A Comprehensive Survey. (n.d.).

Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. Future Internet, 15(6), 1–45. https://doi.org/10.3390/fi15060200

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, SNPA 2003, 113–127. https://doi.org/10.1109/SNPA.2003.1203362

Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M. D. (2021). A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. Sensors, 21(18), 1–20. https://doi.org/10.3390/s21186018

Lee, K., Kaiser, B., Mayer, J., & Narayanan, A. (2020). An empirical study of wireless carrier authentication for SIM swaps. Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020, 2020(January), 61–80.

Lumburovska, L., Dobreva, J., Andonov, S., Trpcheska, H. M., & Dimitrova, V. (2021). A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose? International Scientific journal “Security & Future,” 5(4), 131–138.

Martinez, B., Adelantado, F., Bartoli, A., & Vilajosana, X. (2019). Exploring the performance boundaries of NB-IoT. IEEE Internet of Things Journal, 6(3), 5702–5712. https://doi.org/10.1109/JIOT.2019.2904799

Moinet, A., Darties, B., & Baril, J.-L. (2017a). Blockchain based trust & authentication for decentralized sensor networks. 1–6. Retrieved from http://arxiv.org/abs/1706.01730

Moinet, A., Darties, B., & Baril, J.-L. (2017b). Blockchain based trust & authentication for decentralized sensor networks. (June). https://doi.org/10.48550/arXiv.1706.01730

Mostafaei, H., & Menth, M. (2018). Software-Defined Wireless Sensor Networks : A Survey. (July). https://doi.org/10.1016/j.jnca.2018.06.016

Nguyen, M. D., Tizon, L. D. A., Le, N. T., Nguyen, D. T., Vu, T. C., Nguyen, T. V., … Nguyen, M. T. (2025). A Comparative Study of Wi-Fi Technologies in Wireless Sensor Networks. Computer Networks and Communications, 3(1), 75–87. https://doi.org/10.37256/cnc.3120256070

Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., & Javaid, N. (2023a). Malicious *Node* Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs. IEEE Access, Vol. 11, pp. 6106–6121. https://doi.org/10.1109/ACCESS.2023.3236983

Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., & Javaid, N. (2023b). Malicious *Node* Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs. IEEE Access, 11, 6106–6121. https://doi.org/10.1109/ACCESS.2023.3236983

ev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, i-factor authentication: A survey. Cryptography, 2(1), 1–31. .3390/cryptography2010001

Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. Future Internet, 15(4), 1–20. https://doi.org/10.3390/fi15040146

Paulraj, D., Lavanya, R., Jayasudha, T., Ishwarya Niranjana, M., Daniya, T., & Daniel Shadrach, F. (2023). Blockchain-based Wireless Sensor Network Security Through Authentication and Cluster Head Selection. 2023 IEEE International Conference on Integrated Circuits and Communication Systems, ICICACS 2023. https://doi.org/10.1109/ICICACS57338.2023.10099593

Piyare, R., & Lee, S. (2013). Performance Analysis of XBee ZB Module Based Wireless Sensor Networks. 4(4), 1615–1621.

Pule, M., Yahya, A., & Chuma, J. (2018). Wireless sensor networks : A survey on monitoring water quality. Revista Mexicana de Trastornos Alimentarios, 15(6), 562–570. https://doi.org/10.1016/j.jart.2017.07.004

Puthal, D., Mohanty, S. P., Yanambaka, V. P., & Kougianos, E. (2020). PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks. 1–26. Retrieved from http://arxiv.org/abs/2001.07297

Rahman, A. F. S., Achmad, A., & Wardi. (2025). Distributed Blockchain Wireless Sensor Network Architecture for Malicious *Node* and Sensor Data Detection. International Journal of Electrical and Electronic Engineering and Telecommunications, 14(4), 219–232. https://doi.org/10.18178/ijeetc.14.4.219-232

Ramasamy, L. K., Khan K. P., F., Imoize, A. L., Ogbebor, J. O., Kadry, S., & Rho, S. (2021). Blockchain-Based Wireless Sensor Networks for Malicious *Node* Detection: A Survey. IEEE Access, 9, 128765–128785. https://doi.org/10.1109/ACCESS.2021.3111923

Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: A survey on recent developments and potential synergies. Journal of Supercomputing, 68(1), 1–48. https://doi.org/10.1007/s11227-013-1021-9

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., Seamons, K., & Brigham Young University. (2019). “A Usability Study of Five Two-Factor Authentication Methods”, Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS ’19), Santa Clara, CA, USA, August 12 - 13, 2019,. Retrieved from https://www.usenix.org/conference/soups2019/presentation/reese

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88(2018), 173–190. https://doi.org/10.1016/j.future.2018.05.046

Rodenas-Herraiz, D., Garcia-Sanchez, A. J., Garcia-Sanchez, F., & Garcia-Haro, J. (2013). Current trends in wireless mesh sensor networks: A review of competing approaches. Sensors (Switzerland), 13(5), 5958–5995. https://doi.org/10.3390/s130505958

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security
istributed internet of things. Computer Networks, Vol. 57, pp.
s://doi.org/10.1016/j.comnet.2012.12.018
tcoin: A *Peer*-to-*Peer* Electronic Cash System. SSRN Electronic
ps://doi.org/10.2139/ssrn.3977007
vey on Wireless Sensor Network Security. Wireless Networks,
s://doi.org/10.1007/s11276-019-02070-y

She, W., Liu, Q., Tian, Z., Chen, J. Sen, Wang, B., & Liu, W. (2019a). Blockchain trust model for malicious *node* detection in wireless sensor networks. IEEE Access, 7, 38947–38956. https://doi.org/10.1109/ACCESS.2019.2902811

She, W., Liu, Q., Tian, Z., Chen, J. Sen, Wang, B., & Liu, W. (2019b). Blockchain trust model for malicious *node* detection in wireless sensor networks. IEEE Access, 7(c), 38947–38956. https://doi.org/10.1109/ACCESS.2019.2902811

Singh, S., & Hosen, A. S. M. S. (2021). Blockchain Security Attacks , Challenges , and Solutions for the Future Distributed IoT Network. 9. https://doi.org/10.1109/ACCESS.2021.3051602

Stajano, F., & Anderson, R. (2000). The resurrecting duckling: Security issues for ad-hoc wireless networks. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1796, 172–182. https://doi.org/10.1007/10720107_24

Survey, W., & Directions, F. (2022). Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions.

Syahreen, M., Hafizah, N., Maarop, N., & Maslinan, M. (2024). A Systematic Review on Multi-Factor Authentication Framework. International Journal of Advanced Computer Science and Applications, 15(5), 1043–1050. https://doi.org/10.14569/IJACSA.2024.01505105

Tian, Y., Wang, Z., Xiong, J., & Ma, J. (2020). A Blockchain-Based Secure Key Management Scheme with Trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics, Vol. 16, pp. 6193–6202. https://doi.org/10.1109/TII.2020.2965975

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., … Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access, 7(January), 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

Xia, Z., Wei, Z., & Zhang, H. (2022). Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks. Computational Intelligence and Neuroscience, 2022. https://doi.org/10.1155/2022/3449428

Yang, Q., Zhu, X., Fu, H., & Che, X. (2015). Survey of Security Technologies on Wireless Sensor Networks. Journal of Sensors, 2015. https://doi.org/10.1155/2015/842392

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647

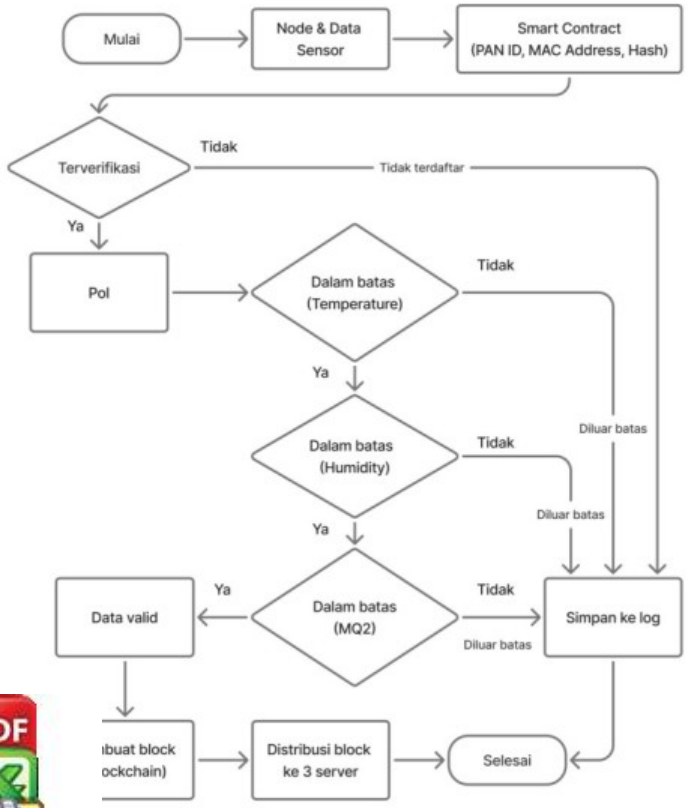
Zhou, L., Kang, M., & Chen, W. (2022). Lightweight Security Transmission in Wireless Sensor.

BAB V
PEMBAHASAN UMUM

5.1. Alur Kerja Sistem WSN Blockchain

5.1.1. Mekanisme konsensus *Smart Contract* dan PoI

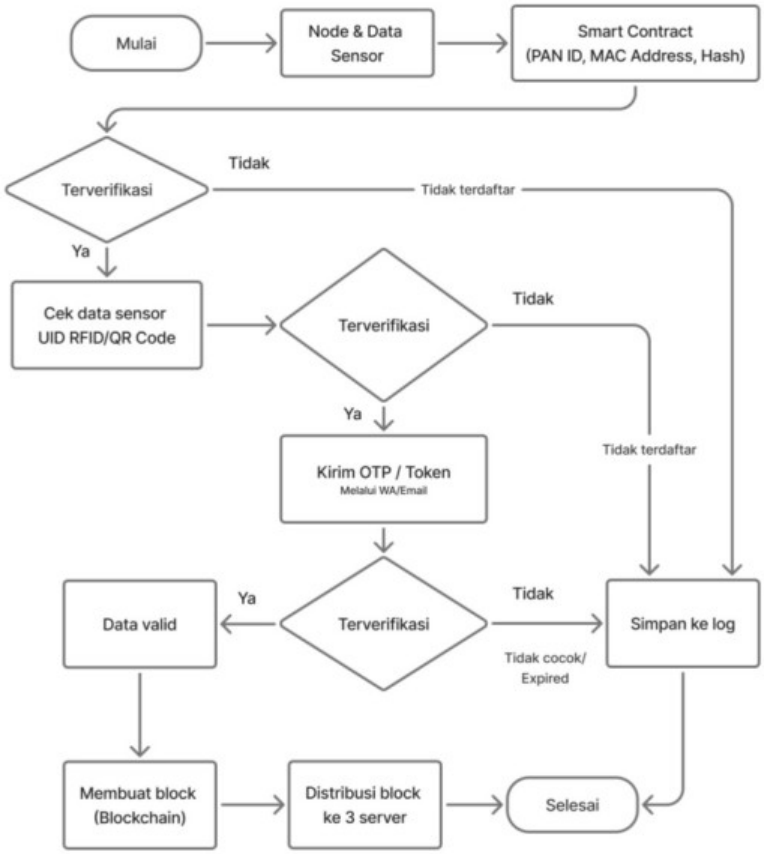
Mekanisme *Smart Contract* dan PoI pada Gambar 5.1 menunjukkan proses penerimaan data node dan sensor melalui jaringan WSN, kemudian identitas node diverifikasi oleh smart contract berdasarkan PAN ID, MAC address, dan hash. Node yang tidak terdaftar akan diklasifikasikan sebagai anomali dan dicatat dalam log. Apabila node terverifikasi, sistem melanjutkan ke tahap PoI untuk melakukan validasi data sensor. Tiga parameter sensor (Temperatur, Humidity, dan gas MQ2) diperiksa secara berurutan untuk memastikan bahwa nilai sensor berada dalam ambang batas. Data yang tidak memenuhi salah satu kriteria akan ditandai sebagai anomali dari sensor, sementara data yang tervalidasi akan diijinkan untuk membuat block dan membentuk blockchain, kemudian didistribusikan ke tiga server.



Gambar 5. 1. Alur Smart Contract dan PoI.

5.1.2. Mekanisme konsensus *Smart Contract* dan Po2FA

Mekanisme ini menggabungkan teknologi *smart contract* dengan otentikasi ganda *Proof of Two Factor Authentication* (Po2AF) untuk meningkatkan keamanan dan validitas transaksi dalam jaringan seperti pada Gambar 5.2 proses dimulai dari verifikasi identitas node oleh smart contract berdasarkan PAN ID, MAC address, dan hash, kemudian verifikasi data RFID/QR Code, jika semua terverifikasi akan dilanjutkan ke tahap Po2FA yaitu mengirimkan OTP ke pengguna. Data sensor yang terverifikasi akan membuat blok transaksi baru membentuk blockchain, kemudian didistribusikan ke tiga server.

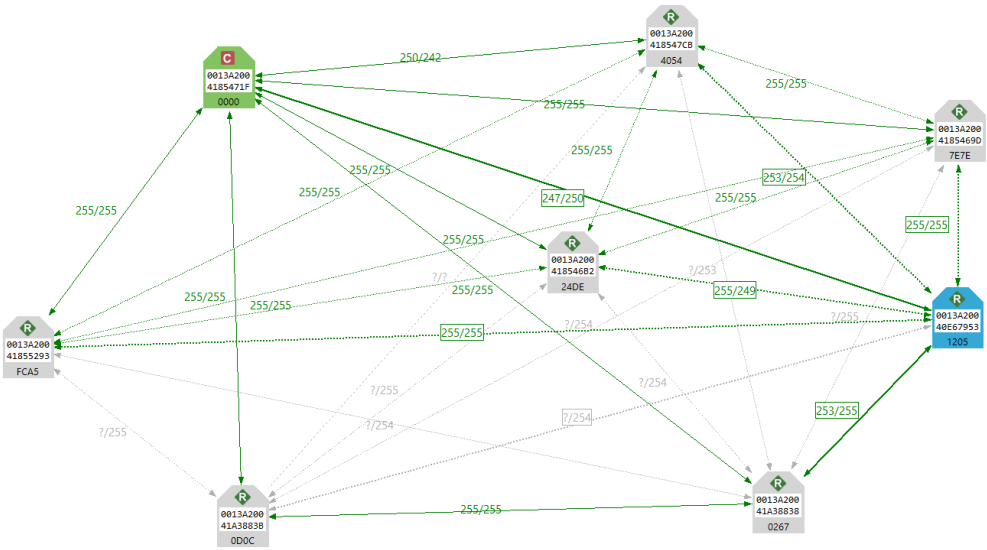


Gambar 5. 2. Alur *Smart Contract* dan Po2FA.

5.2. Desain Jaringan WSN

5.2.1. Topologi Jaringan

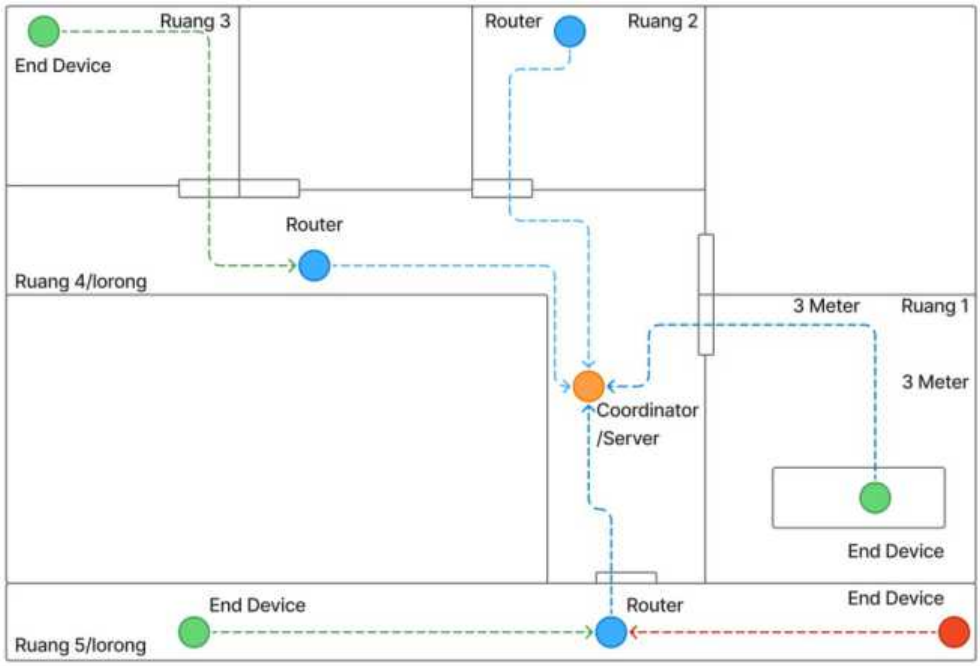
Pengujian dalam penelitian ini menggunakan jaringan WSN topologi mesh dengan transmisi protocol zigbee, *node* transmisi yang digunakan berjumlah 8 *node* sensor yang terdiri dari *node monitoring*, *controlling*, *coordinator* dan *node* tidak terdaftar. Gambar 5.3 merupakan tampilan topologi yang digunakan.



Gambar 5. 3. Topologi WSN.

5.2.2. Area pengujian

Area pengujian yang ditunjukkan pada Gambar 5.4 digunakan untuk memetakan alur komunikasi dalam jaringan WSN. Perangkat koordinator/server ditandai dengan warna coklat, berfungsi sebagai pusat pengolahan dan penerimaan data. Perangkat router berwarna biru ditempatkan dibeberapa titik untuk memperluas jangkauan dan meneruskan paket data antar node. Sementara itu, perangkat end device berwarna hijau berfungsi sebagai pengirim data sensor ke router terdekat atau bisa secara langsung jika terjangkau. End device warna merah merupakan node yang tidak terdaftar dan digunakan untuk pengujian. Jalur komunikasi digambarkan dengan garis putus-putus, menunjukkan rute pengiriman data dari end device menuju server melalui beberapa router sesuai posisi fisik dalam ruangan.



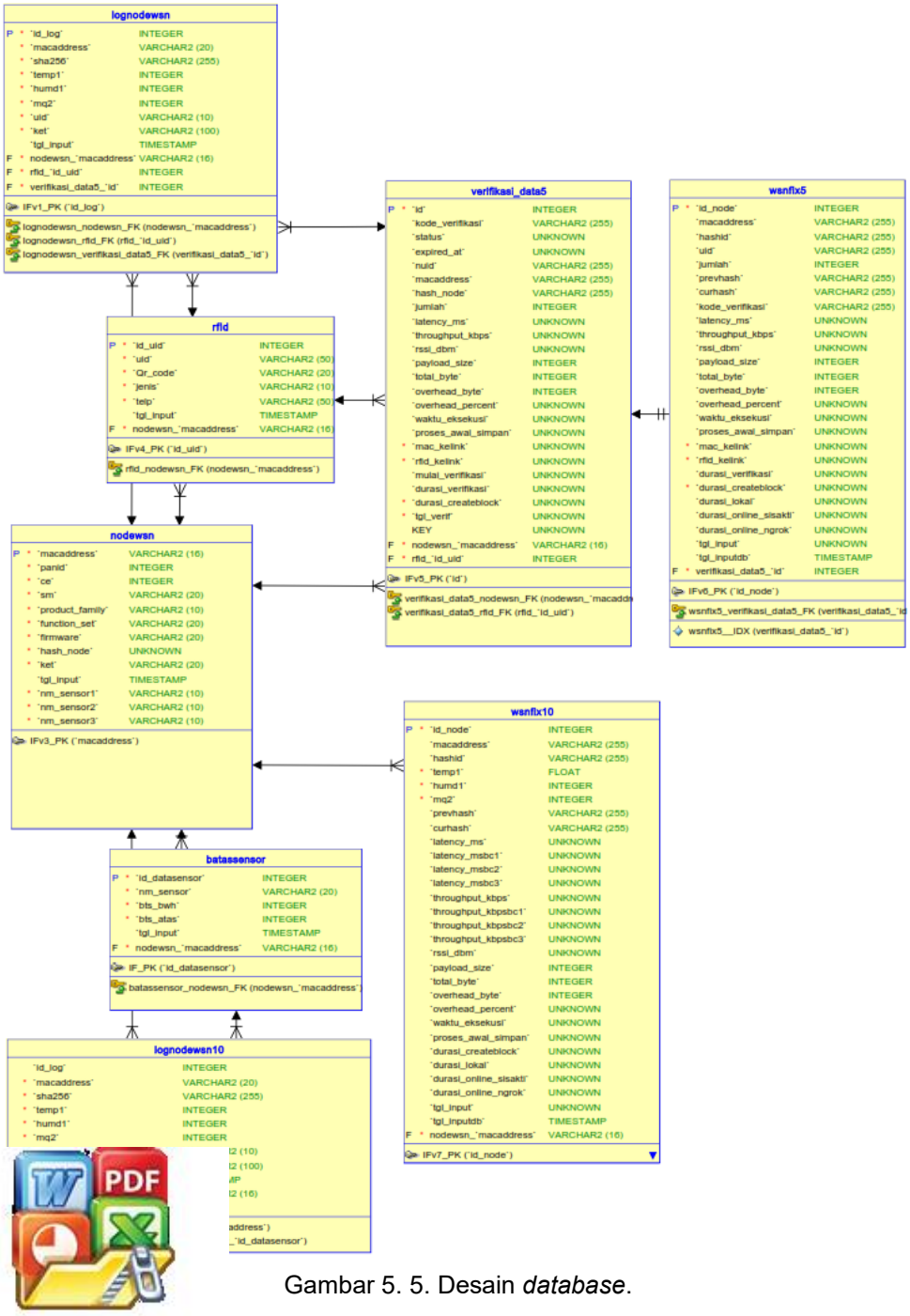
Gambar 5. 4. Area pengujian

5.3. Desain Database

Data sensor dalam penelitian merupakan data utama yang harus disimpan dalam database secara terstruktur, salah satu *Database Management System* yang digunakan dalam penelitian yaitu MySQL. Gambar 5.5 merupakan desain database yang digunakan dalam sistem pada penelitian ini. Desain database terdiri dari 1 database dan 8 tabel, berikut uraian dari tabel tersebut:

- nodewsn : digunakan untuk menyimpan data master identitas *node* sensor.
- batassensor: data tabel digunakan untuk membuat margin *sensor monitoring* yang digunakan untuk metode *Proof of Information* (PoI)
- wsnfix10 : tabel untuk menyimpan data blockchain sensor monitoring dan parameter pendukung lainnya seperti latency, throughput, durasi create blockchain dan sebagainya.
- lognodewsn10 : untuk menyimpan data log dari sensor monitoring yang dianggap sebagai data tidak sah atau tidak terdaftar.
- rfid : untuk menyimpan data master *sensor controlling* (RFID dan QR Code).
- untuk menyimpan data verifikasi sementara yang dikirim dari , pada tabel ini verifikasi menggunakan OTP atau link kode onsensus tambahan yaitu Po2FA.
- menyimpan data blockchain *sensor controlling* yang sudah rverifikasi serta parameter jaringan WSN.

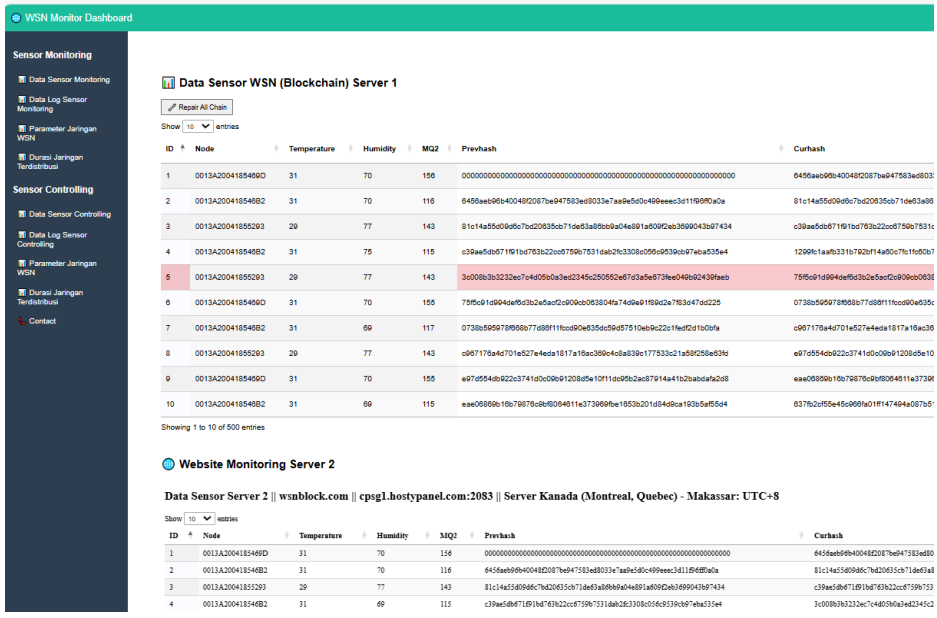
- Lognodewsn5 : untuk menyimpan data log dari sensor controlling yang dianggap sebagai data tidak sah atau tidak terdaftar



Gambar 5. 5. Desain *database*.

5.4. Desain Interface Blockchain

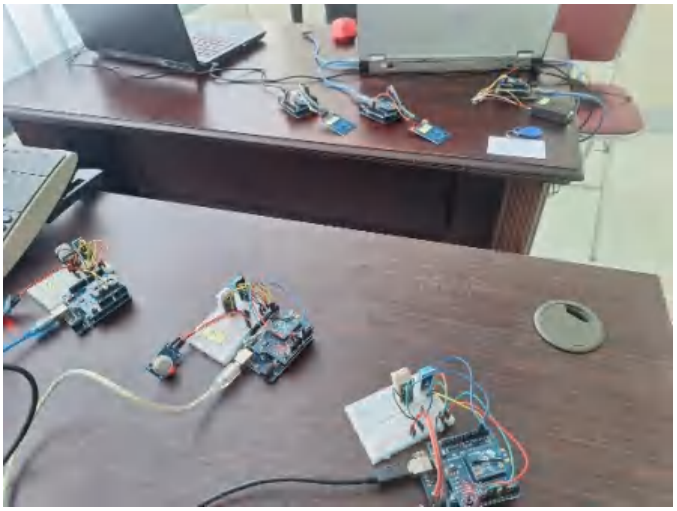
Gambar 5.6 merupakan tampilan berbasis web yang digunakan untuk memonitor proses akuisisi data sensor WSN dengan Blockchain. Sistem informasi untuk memonitor data terdiri dari 3 server yaitu 1 server lokal sebagai master dan 2 server online yang letak servernya masing-masing berbeda. Setiap sistem informasi akan menampilkan data terdistribusi dari ketiga server dalam bentuk tabel, dalam gambar 5.6. terlihat pada tabel 1 (server 1) terdapat warna merah pada salah satu block, warna tersebut menunjukkan kalau ada 1 block diatas warna tersebut diubah atau dimanipulasi, data server 1 bisa dibandingkan dengan data server 2 atau 3 untuk mengecek integritas data dari ketiga server.



Gambar 5. 6. Blockchain WSN.

5.5. Prototipe Pengujian

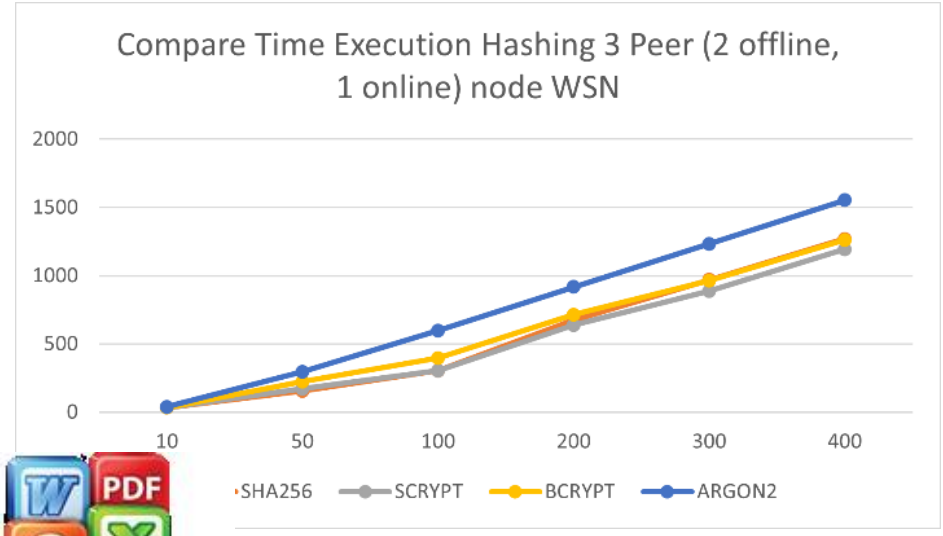
Gambar 5.7 merupakan prototipe yang digunakan untuk pengujian penelitian ini, perangkat keras WSN yang digunakan sebanyak 8 WSN yang terdiri dari 1 coordinator, 3 *node sensor controlling* (QR Code, RFID), 3 sensor monitoring (Temperature, Humadity dan MQ2), dan 1 *node* yang tidak terdaftar.



Gambar 5. 7. Pengujian sistem.

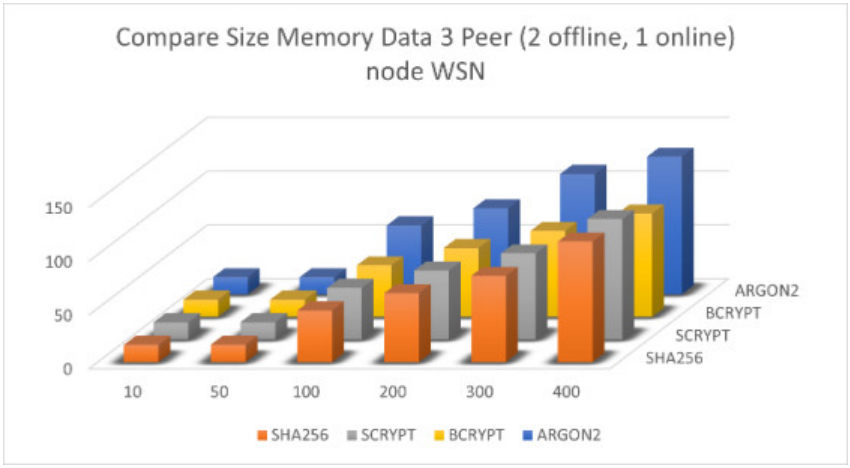
5.6. Pengujian Waktu Eksekusi Hash dengan Simulasi (2 Offline, 1 Online)

Gambar 5.8 merupakan perbandingan empat algoritma hash yang diuji pada 3 *peer* (2 *peer* offline dan 1 *peer* online). Pengujian tahap ini dilakuakn dengan simulasi *node* sensor dengan 3 server real. Hasil pengujian menunjukkan bahwa Scrypt mampu menyelesaikan 400 blockchain dari *node* WSN dengan waktu eksekusi lebih cepat, yaitu 1.193 detik. Sementara itu, Argon2 mencatat waktu eksekusi terlama dibandingkan dengan Bcrypt dan SHA256.



r 5. 8. Grafik perbandingan waktu eksekusi hash.

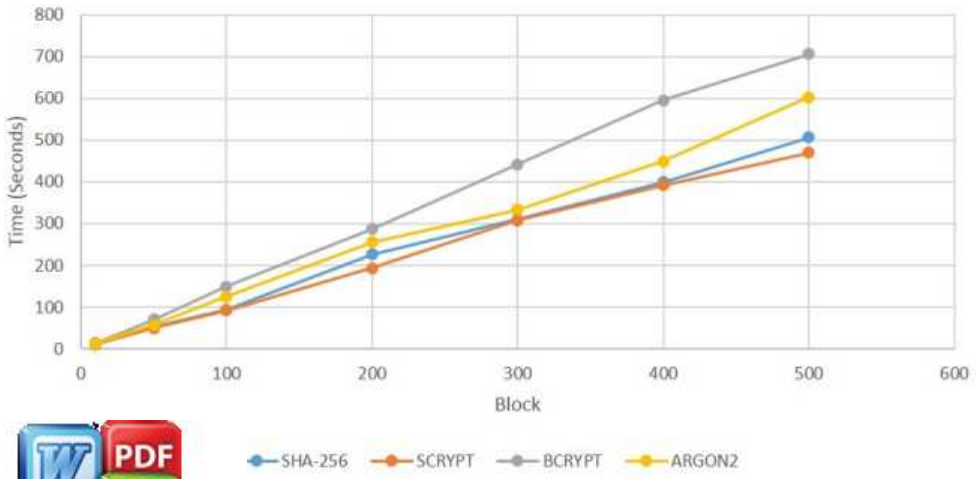
5.7. Perbandingan Pengujian Kapasitas Penyimpanan Data



Gambar 5. 9. Grafik perbandingan kapasitas memori.

Gambar 5.9 menyajikan perbandingan empat algoritma hash yang diuji pada tiga *peer* (dua offline dan satu online). Hasil pengujian menunjukkan bahwa Bcrypt memerlukan memori sebesar 96 KB untuk membuat 400 blockchain dari *node* WSN, sedangkan Argon2 mengonsumsi 128 KB. Sebaliknya, SHA256 dan Scrypt menggunakan memori sekitar 112 KB.

5.8. Pengujian Waktu Eksekusi Hash dengan Prototipe (1 Offline, 2 Online)

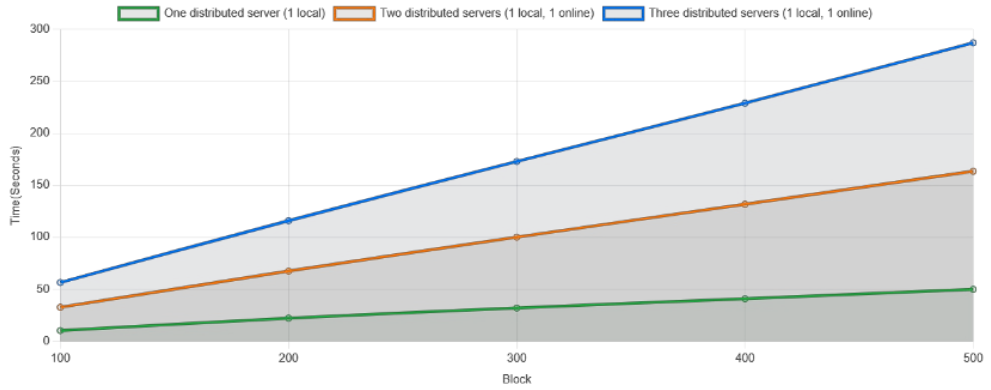


ambar 5. 10. Perbandingan waktu eksekusi.

) membandingkan waktu eksekusi untuk keempat algoritma
n pada tiga server *peer*. Hasil menunjukkan bahwa Scrypt

menyelesaikan proses untuk 500 blok dengan waktu 469,49 detik lebih cepat daripada SHA-256, Bcrypt, dan Argon2.

5.9. Perbandingan waktu eksekusi sensor monitoring (3 server, Scrypt+SHA-256)



Gambar 5. 11. Pengujian waktu eksekusi sensor monitoring (3 server, Scrypt+SHA-256).

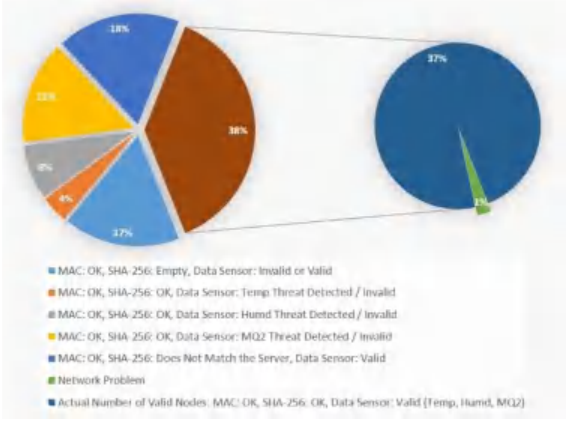
Tabel 5. 1. Statistik deskriptif waktu eksekusi sensor monitoring

Metode	1 local (s)	1 local, 1 online (s)	1 local, 2 online (s)
Mean	0,1	0,327	0,574
Median	0,093	0,319	0,56
Min	0,067	0,238	0,463
Max	0,199	0,487	2,935
Std. Deviasi	0,025	0,03	0,113

Data hasil pada Gambar 5.11 dan Tabel 5.1 menunjukkan bahwa durasi eksekusi sistem blockchain meningkat seiring jumlah block dan jumlah server yang dilibatkan. Pada grafik per 100 blok, konfigurasi 1 local server memperlihatkan pertumbuhan waktu yang relatif rendah dan stabil. Namun, ketika ditambah 1 local + 1 online server, waktu eksekusi meningkat sekitar tiga kali lipat (32,551 detik hingga 163,477 detik). Kondisi ini semakin signifikan pada 1 local + 2 online server, dengan durasi mencapai 287,17 detik pada 500 block, menandakan bahwa overhead distribusi dan sinkronisasi antarserver sangat berpengaruh. Temuan ini selaras

riptif, di mana rata-rata durasi per blok naik dari 0,1 (1 local) al + 1 online) dan 0,574 (1 local + 2 online). Stabilitas sistem n: standar deviasi sangat kecil pada 1 local (0,025) tetapi ıfigurasi multi-server (0,03 dan 0,113), bahkan dengan nilai hingga 2,935.

5.10. Deteksi Data Menggunakan *Smart Contract* (MAC dan Hash SHA-256) dan PoI (Temp, Humd, MQ2)



Gambar 5. 12. Deteksi data menggunakan *Smart Contract* dan PoI.

Tabel 5. 2. Data valid *node* menggunakan *Smart Contract* dan PoI.

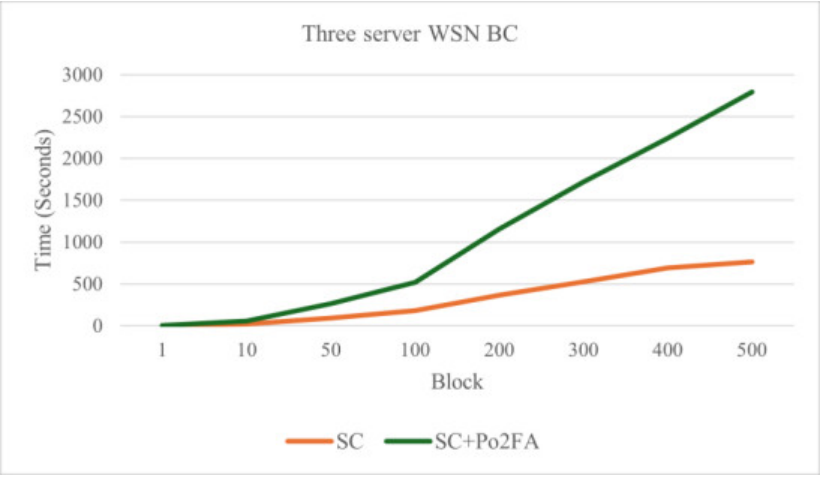
Cat.	Category A MAC: OK, SHA-256: empty, data sensor: invalid or valid	Category B MAC: OK, SHA-256: OK, data sensor: Humd threat detected/ invalid	Category C MAC: OK, SHA-256: OK, data sensor: MQ2 threat detected/ invalid	Category D MAC: OK, SHA-256: OK, data sensor: valid (Temp, Humd, MQ2), 1 Block lost/Network Problem
Valid	45,78%	53,52%	67,86%	97,37%
Invalid	54,22%	46,49%	32,14%	2,63%

Gambar 5.12 menunjukkan penerapan *Smart Contract* dan PoI (Temp, Humd, MQ2) pada 100 iterasi *node* blok. Hasil pengujian menunjukkan bahwa 38% data berhasil masuk ke server terdistribusi atau dianggap valid, sedangkan sisanya terdeteksi sebagai tidak valid. Berdasarkan hasil analisa, terdapat 1% dari 38% data valid yang mengalami kesalahan akibat pengaruh jaringan. Tabel 5.2. menunjukkan bahwa penerapan dua mekanisme konsensus, yaitu *Smart Contract* dan PoI, meningkatkan persentase data valid di server terdistribusi menjadi 97,37%, Sedangkan 2,63% terkait dengan ketidakmampuan jaringan dalam mendistribusikan data ke semua server

ın Waktu Eksekusi *Sensor Controlling* (SC dan

hasil pengukuran waktu eksekusi pada 1 server lokal dan 2
ır 5.13 menunjukkan perbedaan signifikan antara mekanisme

SC+Po2FA dan SC murni. Pada blok 100, durasi SC+Po2FA tercatat 517,77 detik, hampir tiga kali lebih lama dibandingkan SC yang hanya 182,88 detik. Tren ini konsisten hingga blok 500, di mana SC+Po2FA membutuhkan 2.792,54 detik, sementara SC hanya 760,94 detik. Kenaikan waktu pada kedua metode relatif linier terhadap pertambahan blok, namun gradien pada SC+Po2FA jauh lebih curam. Hal ini mengindikasikan bahwa penambahan lapisan autentikasi ganda (Po2FA) meningkatkan kompleksitas dan overhead komputasi, sehingga berdampak pada efisiensi waktu eksekusi



Gambar 5. 13. Hasil pengujian (SC+Po2FA).

Tabel 5. 3. Perbandingan time dan space complexity.

Metode	Time Complexity	Space Complexity	Karakteristik
SC	O(n)	O(n)	Peningkatan waktu hampir linier; penyimpanan hanya untuk data transaksi dasar.
SC+Po2FA	O(n) dengan slope lebih besar	O(n + k)	Peningkatan waktu linier dengan overhead signifikan; membutuhkan ruang tambahan untuk hash, metadata, dan log autentikasi.

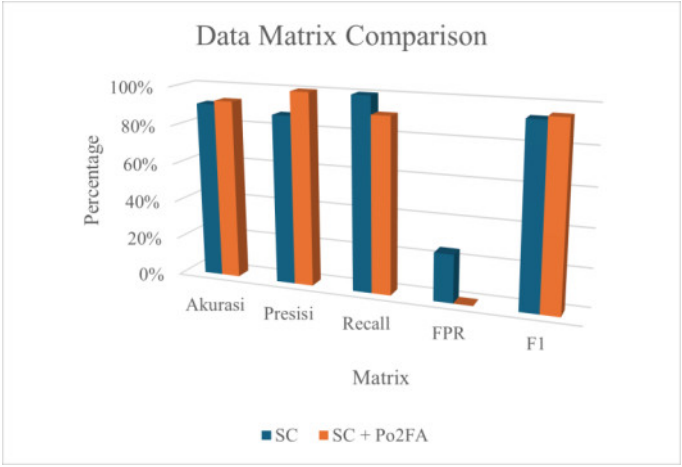
Tabel 5.3 menunjukkan bahwa kedua metode memiliki kompleksitas asimtotik linier (O(n)), namun SC+Po2FA menambahkan konstanta overhead (k) pada ruang dan meningkatkan koefisien pertumbuhan pada waktu. Artinya, semakin ap efisiensi antara SC dan SC+Po2FA akan semakin lebar, tetap menawarkan keamanan tambahan.

5.12. Hasil Evaluasi Keamanan dan Akurasi *Sensor Controlling* (SC+Po2FA)

Tabel 5. 4. Data deteksi WSN blockchain SC+Po2FA.

Matrix	SC + Po2FA	SC
TP (valid diterima)	69	64
FN (valid ditolak)	7	0
FP (invalid tapi diterima)	0	9
TN (invalid dan ditolak)	24	27

Tabel 5.4. menunjukkan data pengujian dengan empat matrix yaitu TP (serangan terdeteksi dengan benar, registrasi SC dan Po2FA), FN (data terdeteksi benar tetapi ditolak oleh sistem seperti kode token atau link expired), FP (data invalid tapi masuk ke sistem seperti kartu RFID atau QR Code dipakai oleh orang lain), dan TN (data yang invalid dan berhasil ditolak). Pada sistem SC+Po2FA nilai FN tercatat tinggi dikarenakan token atau link expired, sedangkan pada sistem SC nilai FP terdeteksi 9 dikarenakan kartu atau akses dipakai oleh orang lain atau bukan pemilik asli kartu.

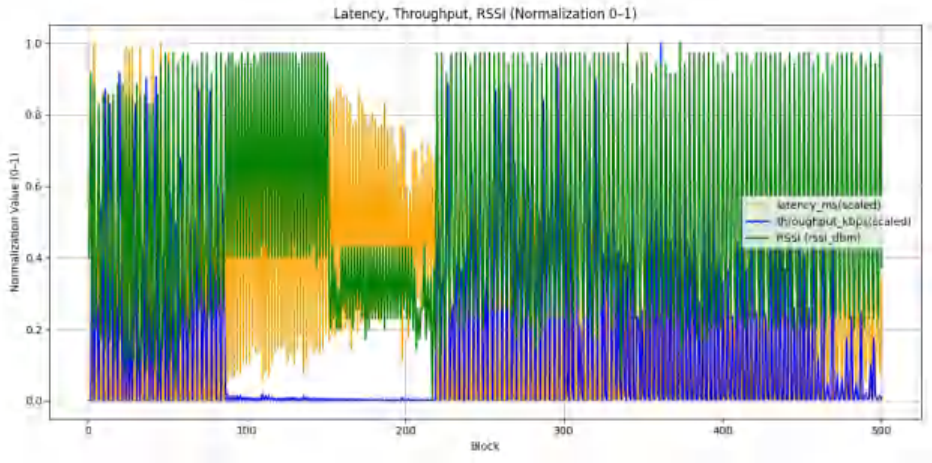


Gambar 5. 14. Perbandingan data matrix.

Gambar 5.14 menunjukkan bahwa nilai akurasi keduanya tinggi tetapi SC + Po2FA sedikit lebih akurat yaitu 93%, nilai presisi untuk SC+Po2FA dapat mengeliminasi semua False Positive sedangkan SC 87,67%, nilai recall SC+Po2FA 90,79% dikarenakan lebih ketat pada verifikasi, sehingga beberapa serangan mungkin tidak lolos tahap verifikasi ganda yang mengakibatkan FN bertambah. Aspek F1 Score merupakan nilai keseimbangan antara recall dan precision, F1 Score lebih tinggi (95,17%) yang berarti model ini teksi yang optimal. Nilai FPR pada SC 25%, ini menunjukkan alse alarm.

5.13. Analisis Performa WSN Blockchain Terdistribusi

5.13.1. WSN Blockchain Terdistribusi (Sensor Monitoring : *Smart Contract* + PoI)



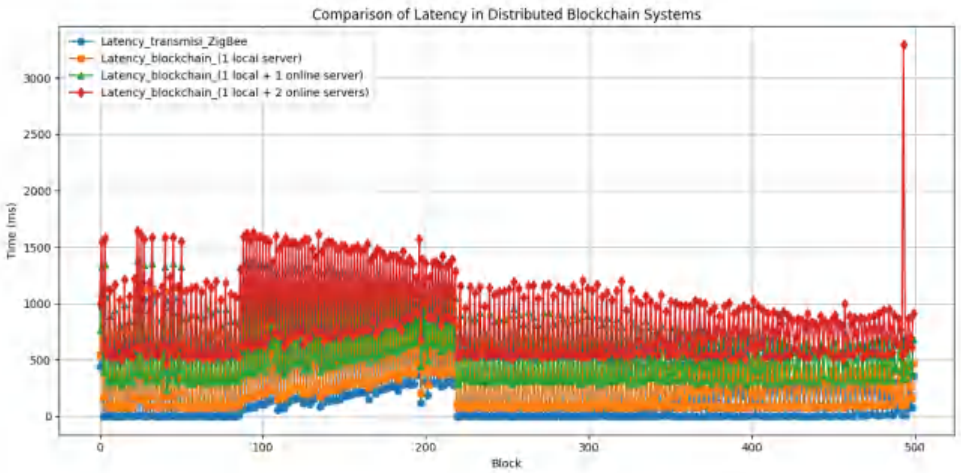
Gambar 5. 15. Kualitas jaringan (latency, throughtput dan RSSI).

Tabel 5. 5. Statistik deskriptif kualitas jaringan WSN blockchain sensor monitoring

Metrik	Mean	Median	Min	Max	Std Deviasi
RSSI (dBm)	-49,302	-53	-67	-32	11,029
Throughput (Kbps)	87,534	2,953	0,551	477,335	131,641
Latency (ms)	285,607	195,078	1,207	1045,167	310,289
Overhead (byte)	83,333	83,333	83,333	83,333	0

Berdasarkan hasil pengukuran pada Gambar 5.15 dan Tabel 5.5 nilai RSSI menunjukkan rata-rata –49,302 dBm dengan median –53 dBm, minimum –67 dBm, dan maksimum –32 dBm serta standar deviasi 11,029. Hal ini mengindikasikan bahwa kualitas sinyal berada pada kategori cukup baik hingga sangat baik, dengan variasi kekuatan sinyal yang masih stabil. Pada sisi throughput, nilai rata-rata tercatat 87,534 kbps, tetapi median hanya 2,953 kbps. Perbedaan yang jauh ini, ditambah standar deviasi yang tinggi (131,641), menunjukkan adanya fluktuasi signifikan dan kemungkinan keberadaan beberapa nilai ekstrim (outlier). Sementara itu, latency memiliki rata-rata 285,607 ms dengan median 195,078 ms, minimum 1,207 ms, dan maksimum 1045,167 ms dengan standar deviasi 310,289. Nilai ini memperlihatkan bahwa latensi umumnya rendah hingga sedang, namun kadang terjadi lonjakan besar yang menambah variabilitas sistem. Secara keseluruhan, metrik ini kualitas sinyal relatif stabil, tetapi throughput dan latency ca yang perlu diperhatikan untuk optimasi kinerja jaringan.

5.13.2. Latency WSN Blockchain Terdistribusi (Sensor Monitoring : *Smart Contract* + PoI)



Gambar 5. 16. Perbandingan latency dari empat titik WSN BC.

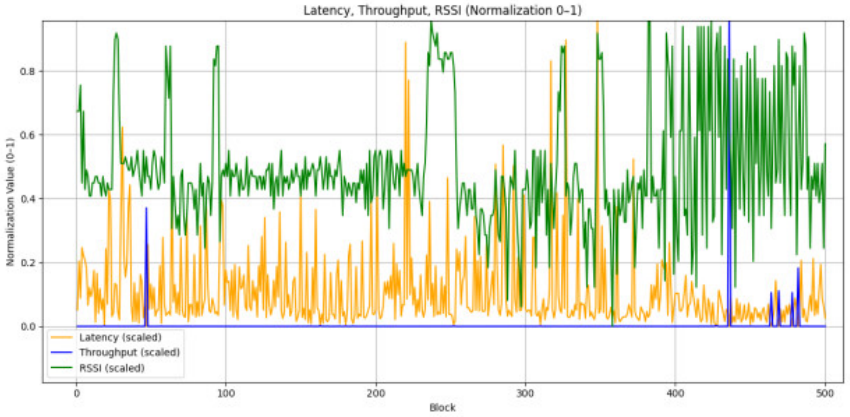
Tabel 5. 6. Data statistik latency dari empat titik WSN BC sensor monitoring

Metode	Original transmission (ms)	1 Local (ms)	1 local, 1 online (ms)	1 local, 2 online (ms)
Mean	285,607	385,282	612,564	859,949
Median	195,078	289,308	514,445	755,933
Min	1,207	69,652	240,057	465,769
Max	1045,167	1144,378	1401,371	3294,324
Std. Deviasi	310,289	327,173	328,021	347,35

Gambar 5.16 dan Tabel 5.6 menunjukkan bahwa latensi ZigBee tanpa blockchain relatif rendah dengan rata-rata 285,607 ms, median 195,078 ms, dan standar deviasi 310,289. Setelah integrasi blockchain, latensi meningkat bertahap sesuai jumlah server: 385,282 ms (1 local server), 612,564 ms (1 local + 1 online), dan 859,949 ms (1 local + 2 online). Kenaikan ini mencerminkan pertumbuhan time complexity yang hampir linier, karena setiap tambahan server menambah overhead validasi dan distribusi blok sehingga memperpanjang eksekusi. Dari sisi space complexity, replikasi blok pada beberapa server menuntut kapasitas penyimpanan lebih besar serta pengelolaan buffer dan antrian data yang lebih kompleks. Meski demikian, standar deviasi tetap relatif stabil (310,289 - 347,35), yang menandakan

dikendalikan. Dengan demikian, integrasi blockchain pada
an pola terukur: semakin kompleks konfigurasi server, semakin
ktu (time complexity) dan ruang (space complexity) dengan
mbuhan linier.

5.13.3. WSN Blockchain Terdistribusi (*Sensor Controlling* : *Smart Contract* + Po2FA)



Gambar 5. 17. Kualitas jaringan (latency, throughtput dan RSSI).

Tabel 5. 7. Statistik deskriptif kualitas jaringan WSN blockchain sensor controlling

Metrik	Mean	Median	Min	Max	Std Deviasi
RSSI (dBm)	-60,646	-62	-85	-36	9,006
Throughput (Kbps)	2,976	0,091	0,005	760,082	37,212
Latency (ms)	11.891,62	6.209,835	0,74	11.0825,966	14.459,124
Overhead (byte)	86,456	88,889	83,333	88,889	2,756

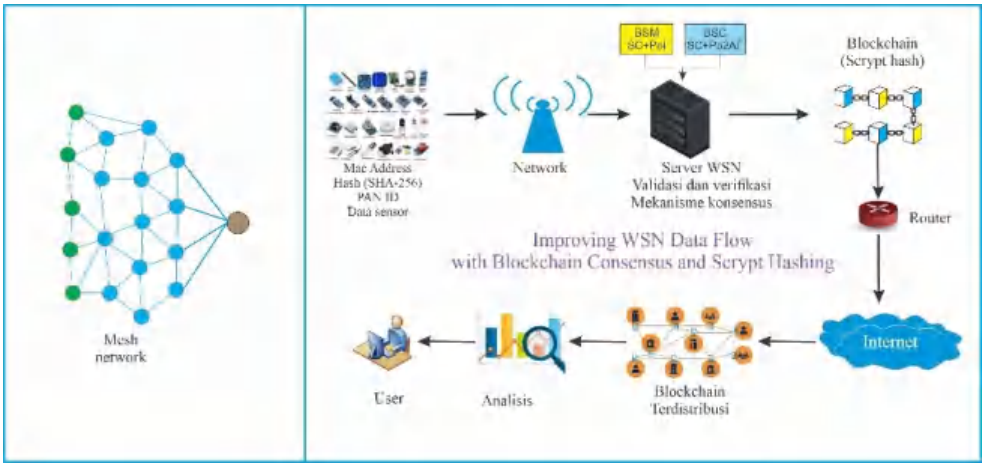
Berdasarkan hasil analisis data, nilai RSSI menunjukkan rata-rata sebesar -60,646 dBm dengan penyebaran relatif kecil (standar deviasi 9,006), menandakan kualitas sinyal cukup stabil meskipun bervariasi antara -85 dBm hingga -36 dBm. Pada sisi lain, throughput memiliki rata-rata rendah (2,976 kbps) dan median sangat kecil (0,091 kbps), namun rentangnya sangat lebar hingga 760,082 kbps dengan standar deviasi tinggi (37,212), menunjukkan adanya fluktuasi ekstrem antara kondisi jaringan yang sangat lambat hingga sangat cepat. Sementara itu, latency memperlihatkan nilai rata-rata sangat tinggi (11.891,62 ms) dengan sebaran luas (standar deviasi 14.459,124 ms), meskipun median 6.209,835 ms lebih rendah, menandakan distribusi latency cenderung skewed/miring akibat beberapa nilai ekstrem yang sangat besar. Secara umum, hasil ini mengindikasikan bahwa meskipun kualitas sinyal relatif stabil, performa jaringan cenderung tidak konsisten dengan throughput dan latency yang sangat fluktuatif, yang berimplikasi pada

i dalam sistem yang diuji

SN dan Blockchain

perancangan yang sudah dikonsep diawal dan hasil an, maka didapatkan hasil gambaran *data flow* WSN dan

Blockchain dengan peningkatan mekanisme konsensus pada BSM dan BSC, serta hash Scrypt pada blockchain, Gambar 5. 18 merupakan *data flow* WSN dan blockchain dengan peningkatan mekanisme konsensus dan hash.



Gambar 5. 18. *Data flow* WSN dan BC dengan peningkatan consensus dan hash.