

**PENERAPAN *BLOCKCHAIN* UNTUK MENGAMANKAN
DATA PADA SISTEM *SMART HOME***

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



OLEH :

**AGUSTINUS YULIUS BAGUS
09011281924078**

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2023**

HALAMAN PENGESAHAN

Penerapan *Blockchain* untuk Mengamankan Data pada Sistem *Smart Home*

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh :

**AGUSTINUS YULIUS BAGUS
09011281924078**

Indralaya, 15 Mei 2023

Mengetahui,

Ketua Jurusan Sistem Komputer,



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

Pembimbing Tugas Akhir,

Ahmad Fali Oklilas, M.T.

NIP. 197210151999031001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 21 Maret 2023

Tim Penguji :

1. Ketua : Sutarno, M. T (.....)
2. Sekretaris : Abdurahman, S. Kom., M. Han. (.....)
3. Pembimbing I : Ahmad Fali Oklilas, M. T (.....)
4. Penguji : Huda Ubaya, M. T (.....)

Mengetahui, 17/5/23

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Agustinus Yulius Bagus

NIM : 09011281924078

Judul : Penerapan *Blockchain* untuk Mengamankan Data pada Sistem *Smart Home*

Hasil pengecekan *Software Turnitin* : 6%

Menyatakan bahwa Laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, 15 Mei 2023



AGUSTINUS YULIUS BAGUS
NIM.09011281924078

HALAMAN PERSEMBAHAN

“Failure is enriching. It’s also important to accept that you’ll make mistakes, it’s how you build your expertise. The trick is to learn a positive lesson from all of life’s negative moments.” — Alain Ducasse

SKRIPSI ini kupersembahkan kepada:

- **Bapak dan ibuku tercinta.**
- **Saudara-saudaraku dan seluruh keluarga besarku.**
- **Teman-teman seperjuangan Sistem Komputer 2019.**
- **Almamater Universitas Sriwijaya**

KATA PENGANTAR

Puji dan syukur Penulis panjatkan kepada Tuhan yang maha pengasih yang telah melimpahkan karunia yang sangat besar dan tidak pernah berhenti kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini yang berjudul **“Penerapan Blockchain Untuk Mengamankan Data Pada Sistem Smart Home”**.

Pada kesempatan ini, dengan segala kerendahan hati Penulis mengucapkan terima kasih kepada semua pihak atas bantuan, bimbingan, dan saran yang telah diberikan dalam menyelesaikan Tugas Akhir ini, antara lain:

1. Kedua orang tua saya, serta keluarga yang telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat baik, menyertai dengan doa, semangatnya dan dukungan baik secara moril, materiil maupun spiritual kepada Penulis hingga dapat menyelesaikan laporan Tugas Akhir.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan di Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Julian Supardi, S.Pd., M.T., selaku Dekan Bidang Akademik di Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi., M.T., selaku Ketua Jurusan Sistem Komputer di Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Rendyansyah, S.Kom., M.T., selaku Dosen Pembimbing Akademik saya selama 6 semester di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Abdurahman, S. Kom., M. Han., selaku Dosen Pembimbing Akademik saya selama 2 semester di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Bapak Ahmad Fali Oklilas., M.T., selaku Pembimbing Tugas Akhir saya di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah berkenan meluangkan waktunya untuk membimbing, memberikan saran dan motivasi kepada saya untuk menyelesaikan Tugas Akhir.
8. Ibu Renny Virgasari selaku Admin di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu Penulis dalam hal-hal administrasi.
9. Sahabat saya Onkky Alexander dari sekolah dasar sampai dengan sekarang masih memberikan motivasi.
10. Teman-teman seperjuangan semasa kuliah di luar jurusan Sistem Komputer Universitas Sriwijaya, Sherli Septina, Kevin Natalino, Charles, dan Nicholas Yavin yang sudah menjadi rekan diskusi demi kelancaran perkuliahan.
11. Teman-teman seperjuangan Jurusan Sistem Komputer Universitas Sriwijaya Angkatan 2019, terutama rekan bimbingan saya Anggita Putri Anti, Jumiati, Sri Nadhila dan Rizki Amalia yang sudah menjadi *Support System* saya.
12. Teman-teman seperjuangan Fasilkom Science Community (FASCO) dan Network Administrator Club (NAC) Fakultas Ilmu Komputer Universitas Sriwijaya.
13. Seluruh Dosen dan Karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
14. Seluruh *Platform* belajar seperti *Google, Youtube, Scopus, kaggle, IEEE, Mendelej* dan lain sebagainya serta semua pihak yang tidak dapat saya sebutkan satu per-satu yang telah memberikan semangat serta doa.
15. Almamater

Penulis menyadari bahwa Tugas Akhir ini masih sangat jauh dari kata sempurna. Untuk itu Penulis sangat terbuka jika ada kritik dan saran yang bersifat membangun agar lebih baik di kemudian hari.

Akhir kata dengan segala keterbatasan, Penulis berharap semoga laporan Tugas Akhir ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbang pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Palembang, Mei 2023

Penulis,

AGUSTINUS YULIUS BAGUS

NIM. 09011281924078

PENERAPAN *BLOCKCHAIN* UNTUK MENGAMANKAN DATA PADA SISTEM *SMART HOME*

AGUSTINUS YULIUS BAGUS (09011281924078)

*Computer Engineering Department, Computer Science Faculty,
Sriwijaya University*

Email : yulius.bagus28@gmail.com

Abstrak

Teknologi *Internet of Things* (IoT) telah menjadi bagian penting dalam kehidupan modern saat ini, dan aplikasinya dalam berbagai industri, termasuk *smart home*, semakin meningkat pesat. Namun, keamanan *smart home* menjadi perhatian utama karena rentan terhadap pencurian informasi, pemantauan aktivitas, perubahan data, dan penyerangan informasi. Dalam penelitian ini, penulis mengusulkan sistem keamanan berbasis *blockchain* untuk *smart home* dengan menggunakan algoritma konsensus *Proof of Authority* (PoA) yang hanya memungkinkan pengguna yang memiliki reputasi dan terpercaya untuk mengakses informasi pada platform *web3*. *Web3* dibangun dengan menggunakan berbagai bahasa pemrograman, termasuk *Solidity* sebagai *smart contract*, *JavaScript* dan *Python* untuk pengolahan data, dan *HTML*, *CSS*, dan *React.js* sebagai pembangun website dengan transaksi yang dilakukan oleh pengguna menggunakan *Metamask*. Untuk menguji akurasi data, penulis melakukan validasi value terhadap 100 kali transaksi. Sedangkan untuk menguji keamanan data, penulis melakukan simulasi serangan yang ingin memantau dan mengubah informasi data menggunakan alat seperti *Burp Suite*, serta eksploitasi yang memanfaatkan jalur *client site* untuk memproses informasi menggunakan alat *XSppear*. Hasil penelitian ini menunjukkan bahwa sistem yang diusulkan dapat memantau aktivitas di rumah dan mencegah akses informasi yang tidak diizinkan, sehingga hanya pengguna yang memiliki reputasi dan terpercaya yang dapat mengakses sistem tersebut.

Kata kunci : Blockchain, Konsensus, Internet of Things

IMPLEMENTATION OF BLOCKCHAIN FOR DATA SECURITY IN SMART HOMES SYSTEM

AGUSTINUS YULIUS BAGUS (09011281924078)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : yulius.bagus28@gmail.com

Abstract

The technology of the Internet of Things (IoT) has become an essential part of modern life, and its applications in various industries, including smart homes, are rapidly increasing. However, the security of smart homes has become a major concern due to their vulnerability to information theft, activity monitoring, data tampering, and information attacks. In this study, the author proposes a blockchain-based security system for smart homes using the Proof of Authority (PoA) consensus algorithm, which only allows trusted and reputable users to access information on the web3 platform. Web3 is built using various programming languages, including JavaScript, Solidity for smart contracts, Python for data processing, and HTML, CSS, and React.js for website development, with transactions carried out by users using Metamask. To test data accuracy, the author validated the value against 100 transactions. To test the security of the system, the author simulated attacks that attempted to monitor and modify information using tools like Burp Suite, as well as exploits that leveraged the client site path to process information using XSSpear. The results of this study demonstrate that the proposed system can monitor activities in the home and prevent unauthorized information access, allowing only trusted and reputable users to access the system.

Keywords : *Blockchain, Consensus, Internet of Things*

DAFTAR ISI

	Halaman
HALAMAN PENGESAHAN	i
HALAMAN PERSETUJUAN.....	ii
/HALAMAN PERNYATAAN.....	iii
HALAMAN PERSEMBAHAN.....	iv
KATA PENGANTAR.....	v
<i>Abstract</i>	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL.....	xv
DAFTAR LAMPIRAN	xvi
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	3
1.3 Batasan Masalah	4
1.4 Tujuan	4
1.5 Manfaat	4
1.6 Metodologi Penelitian	5
1.6.1 Metode Studi Pustaka dan Literatur.....	5
1.6.2 Metode Konsultasi.....	5
1.6.3 Metode Pembuatan Model.....	5
1.6.4 Metode Pengujian.....	5
1.6.5 Metode Analisa dan Kesimpulan	5
BAB II	6
STUDI PUSTAKA	6
2.1 Penelitian Terkait.....	6
2.2 Smart Home.....	10
2.3 Blockchain.....	13
2.3.1 Tipe-tipe <i>blockchain</i>	14
2.3.2 Struktur Data <i>Blockchain</i>	15
2.3.3 Distribusi Data pada <i>Blockchain</i>	16

2.3.4	Validasi Blok	18
2.3.5	Ethereum	19
2.3.6	Smart Contract	20
2.3.7	Kegunaan Blockchain	20
2.4	Keamanan Data	22
2.5	Fungsi Hash	24
2.6	Akurasi Data	24
BAB III	25
METODOLOGI PENELITIAN	25
3.1	Waktu dan Tempat Penelitian	25
3.2	Lingkungan hardware dan Software	25
3.2.1	Kebutuhan <i>Hardware</i>	25
3.2.2	Kebutuhan <i>Software</i>	25
3.3	Struktur Penelitian.....	26
3.3.1	Studi Literatur	28
3.3.2	Perumusan Masalah.....	28
3.3.3	Menentukan Tujuan dan Manfaat	28
3.3.4	Menentukan Metodologi Penelitian.....	28
3.3.5	Menentukan Dataset	29
3.3.6	Pencarian Dataset.....	29
3.3.7	<i>Clean Dataset</i>	31
3.3.8	Menentukan Algoritma Blockchain.....	32
3.3.9	Arsitektur <i>Blockchain</i>	32
3.3.10	Model Blockchain	33
3.3.11	Pengujian Model.....	34
3.3.12	Validasi Akurasi Data	34
3.3.13	Pengujian Keamanan	34
3.3.14	Analisa	34
BAB IV	36
HASIL DAN PEMBAHASAN	36
4.1	Implementasi <i>Blockchain</i>	36
4.2	Rancangan Private Blockchain.....	37
4.3	Deploy Contract	38
4.4	Simulasi Model	41
4.5	Uji Akurasi Data	51
4.6	Analisa Keamanan	52

4.7	Analisa	59
BAB V	61
KESIMPULAN DAN SARAN	61
5.1	Kesimpulan	61
DAFTAR PUSTAKA	62

DAFTAR GAMBAR

	Halaman
Gambar 1. 1 Struktur Blockchain	2
Gambar 2. 1 Blockchain [16]	15
Gambar 2. 2 Topologi [16]	17
Gambar 2. 3 Saluran informasi klasik [19]	23
Gambar 3. 1 Struktur Penelitian	27
Gambar 3. 2 Dataset yang digunakan	30
Gambar 3. 3. 1 Alur Blockchain [10]	33
Gambar 3. 3. 2 Kerangka kerja	33
Gambar 4. 1 Setelah dataset dibersihkan	36
Gambar 4. 2 Halaman utama	37
Gambar 4. 3 Import akun	39
Gambar 4. 4 Memasukkan private key	39
Gambar 4. 5 Setelah dilakukan import akun	40
Gambar 4. 6 Deploy kontrak berhasil	40
Gambar 4. 7 Gas fee rendah	42
Gambar 4. 8 Gas fee sedang	42
Gambar 4. 9 Gas fee tinggi	43
Gambar 4. 10 Simulasi transaksi pada mozilla firefox	45
Gambar 4. 11 Console log mozilla firefox	45
Gambar 4. 12 Output pada mozilla firefox	45
Gambar 4. 13 Detail transaksi 1	46
Gambar 4. 14 Simulasi transaksi pada microsoft edge	47
Gambar 4. 15 Console log microsoft edge	47
Gambar 4. 16 Output pada microsoft edge	48
Gambar 4. 17 Detail transaksi 2	48

Gambar 4. 18	Simulasi transaksi pada google chrome.....	49
Gambar 4. 19	Console log google chrome	49
Gambar 4. 20	Output pada website 3	50
Gambar 4. 21	Detail transaksi 3	50
Gambar 4. 22	Pengujian akurasi data	52
Gambar 4. 23	Skema spoofing attack.....	53
Gambar 4. 24	Bentuk response pada burp suite	54
Gambar 4. 25	Xspear dengan menggunakan Kali Linux.....	58
Gambar 4. 26	Public key akun mom	59
Gambar 4. 27	Private key akun mom	59

DAFTAR TABEL

	Halaman
Tabel 1. Literatur mengenai Blockchain dan Smart Home	6
Tabel 2. Perbandingan Hash.....	16
Tabel 3. Kode program 1	29
Tabel 4. Kode program 2.....	31
Tabel 5. Public address yang digunakan	38

DAFTAR LAMPIRAN

	Halaman
Lampiran 1. Dataset smart home hasil cleaning dan uji akurasi data	1
Lampiran 2. Hasil Turnitin.....	6
Lampiran 3. Form perbaikan ujian skripsi	11
Lampiran 4. Listing program.....	13

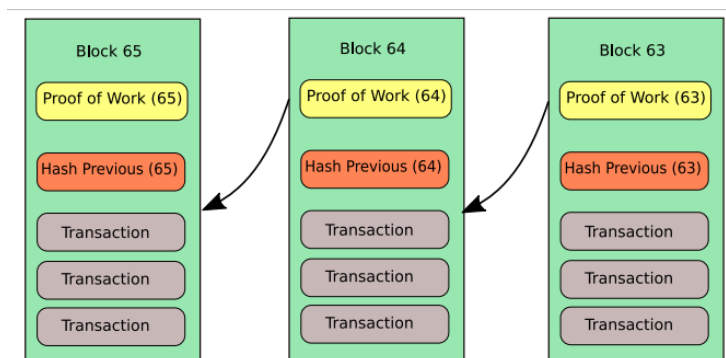
BAB I

PENDAHULUAN

1.1 Latar Belakang

Kata *Internet of Things* sudah tidak asing lagi bagi kebanyakan orang jaman sekarang. Menjadi salah satu perkembangan teknologi yang sangat penting pada masa ini, teknologi ini sering digunakan dan dipakai oleh berbagai pihak seperti Hotel, Resort, Apartemen dan Rumah Pribadi yang merupakan rangkaian sensor pintar dengan asisten dan robot yang terdapat pada *smart home*, manusia dapat berinteraksi dengan rumahnya dan berhasil menghubungkan semua perangkat dan peralatan rumah tangga ke unit pusat sistem kontrol [1]. Hal ini memudahkan kegiatan setiap orang yang dimana mereka sibuk dengan pekerjaannya, tetapi dengan adanya teknologi pintar ini semua dapat dilakukan dengan mudah. Dengan kemampuan yang dimiliki oleh *Internet of Things*, *smart home* dapat berinteraksi dan bekerja sama untuk menyediakan berbagai layanan. Setiap perangkat yang digunakan oleh Pengguna harus dapat dijangkau dan menghasilkan informasi yang dapat diambil oleh Pengguna terlepas dari lokasi mereka. Namun sangat penting bahwa Pengguna yang diautentikasi dan berwenang yang dapat menggunakan sistem. Apabila tidak, maka rentan terhadap berbagai resiko keamanan yang ada seperti pencurian informasi, monitoring informasi, pengubahan data, dan perampasan informasi pribadi [2]. Pada dasarnya perangkat pintar ini memberikan keuntungan kepada Pengguna tidak terlepas juga pada kelemahan yang dimana kebanyakan Pengguna merasa takut jika kerahasiaan atau data pribadinya dapat diketahui oleh orang lain atau bisa menyebabkan kerugian finansial [3]. Keterbatasan penyimpanan dan daya pemrosesan perangkat dapat membuat perangkat rentan terhadap berbagai macam serangan, keamanan tradisional telah gagal mengatasi masalah keamanan terkait perangkat pintar [4].

Ada dua mata uang elektronik yang familiar di tahun 2022 dan sering digunakan yaitu, *ethereum* dan *bitcoin*. Kedua uang elektronik ini sangat sering digunakan dalam dunia digital, contohnya *ethereum* digunakan untuk memperjual belikan gambar digital NFT (*Not Fungible Token*). Dibalik mata uang elektronik terdapat keamanan data yaitu *blockchain* merupakan sistem penting yang digunakan oleh kedua mata uang tersebut untuk mengamankan data transaksi, yang dimana basis data terdistribusi menyimpan daftar catatan yang terurut dan terus bertambah yang disebut blok. *Blockchain* berfungsi sebagai buku besar yang mencatat semua transaksi [5], [6].



Gambar 1. 1 Struktur Blockchain

Struktur Blockchain [6]

Gambar 1.1 merupakan struktur yang ada pada *blockchain*, Sebuah blok dalam arsitektur blockchain merupakan sekumpulan data yang dikumpulkan, yang setiap bloknnya dapat diidentifikasi menggunakan fungsi hash. Blok yang terbentuk akan berisi hash dari blok sebelumnya sehingga semua data dapat dihubungkan melalui struktur daftar tertaut. Secara khusus, blok tersebut berisi header dan data transaksi yang relevan [6]. Pada jurnal Singh et al. [7] dengan algoritma konsensus *Proof of Authority*, dimana terdapat entitas terpercaya yang disebut validator. Pada proses pembuatan blok yang diminta oleh validator akan dibuktikan jika valid maka akan tersimpan, jika tidak valid maka validator lain akan melakukan *voting* dengan

mayoritas menentang validator dan kemudian validator akan dianggap berbahaya dan dihapus dari sistem. *Blockchain* ini akan digunakan sebagai sistem keamanan yang ada pada perangkat *smart home*, sehingga dapat meminimalisir terjadinya pencurian data pribadi yang bersifat asli. Demi kenyamanan penggunaan IoT dalam rumah, maka sistem rumah pintar akan menggunakan keamanan berlapis seperti yang digunakan oleh mata uang digital seperti *ethereum* dan *bitcoin* yaitu *blockchain*. Tujuan dari penelitian ini, Penulis ingin menerapkan blockchain untuk mengamankan data pada sistem smart home yang nantinya blockchain dapat mengamankan data Pengguna dari serangan *cyber* yang tidak diinginkan dan juga memiliki data akurasi yang sesuai. Dari uraian diatas, maka Penulis memilih judul Skripsi “Penerapan Blockchain untuk Mengamankan Data pada Sistem *Smart Home*”

1.2 Perumusan Masalah

Dari uraian pada latar belakang, penelitian ini dilakukan dikarenakan beberapa hal sebagai berikut:

1. *Smart Home* merupakan rumah yang berbasis teknologi yang artinya Pengguna *smart home* bisa mengatur peralatan rumahnya melalui *smartphone* atau website. Terlihat fleksibel dan mudah untuk digunakan, dibalik teknologi ini aplikasi *smart home* bertukar data dengan perangkat rumah dalam mekanisme yang kurang aman dan kurangnya enkripsi data dapat menyebabkan hilangnya informasi atau kebocoran data pada jaringan sehingga meningkatkan ancaman keamanan *cyber*.
2. *Blockchain* sebagai jaringan yang diterapkan dan berkomunikasi antar node serta menjadi pengaman data pada *smart home* dari pihak yang tidak bertanggung jawab.
3. Sebuah sistem tidak lepas dari akurasi data, pada *smart home* sendiri akurasi dibutuhkan untuk melihat ketepatan penyimpanan data terhadap datanya. Hal ini dilakukan untuk menyediakan data yang sebenarnya pada *smart home*.

1.3 Batasan Masalah

Dalam permasalahan yang diangkat oleh Penulis pada penelitian ini, agar tidak jauh dari pembahasan dan lebih terfokus maka Penulis akan membatasi masalah yang diteliti sebagai berikut:

1. Penelitian ini berfokus pada penerapan *blockchain* untuk mengamankan data yang ada pada *smart home* dengan dataset *smart home* yang didapatkan pada website *kaggle*.
2. Simulasi dengan menggunakan *localhost* yang bersifat *private blockchain* dengan input dari dataset yang diperoleh.
3. Hasil yang diperoleh berupa beberapa sampel dataset yang masuk ke dalam website serta adanya pengujian akurasi data dan keamanan data.

1.4 Tujuan

Adapun tujuan yang ingin dicapai oleh Penulis dalam penelitian ini sebagai berikut:

1. Mencegah terjadinya perubahan informasi data dan kebocoran data pada *Smart Home* yang dapat merugikan Pengguna.
2. Mengimplementasikan *blockchain* untuk mengamankan data berupa informasi dari *smart home*.
3. Membuktikan bahwa data yang diamankan dengan *blockchain* dapat lebih akurat.

1.5 Manfaat

Adapun manfaat dari penelitian ini sebagai berikut:

1. Memberikan kenyamanan kepada Pengguna ketika menggunakan *smart home* tanpa ada rasa takut jika adanya monitoring data atau kebocoran data.
2. Memberikan sistem *smart home* yang mudah diakses.
3. Mampu mendapatkan informasi dan akurasi yang sesuai dengan menggunakan *blockchain*.

1.6 Metodologi Penelitian

1.6.1 Metode Studi Pustaka dan Literatur

Pada metode ini mengumpulkan dan mencari referensi yang bersesuaian dengan permasalahan yang dibahas. Referensi ini terdapat pada jurnal ilmiah, buku dan artikel ilmiah mengenai penerapan *Blockchain* untuk mengamankan data pada sistem *Smart Home*.

1.6.2 Metode Konsultasi

Pada metode ini melakukan konsultasi kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui Penulis dalam tugas akhir penerapan *Blockchain* untuk mengamankan data pada sistem *Smart Home*.

1.6.3 Metode Pembuatan Model

Pada metode ini membuat perancangan model dengan menggunakan program dan simulasi menggunakan perangkat lunak agar bisa memperlancar proses pembuatan model.

1.6.4 Metode Pengujian

Pada metode ini melakukan pengujian terhadap program dan simulasi yang telah dibuat dengan hasil pengujian dapat berupa akurasi, efisiensi dan faktor yang mempengaruhi tingkat keberhasilan pengujian.

1.6.5 Metode Analisa dan Kesimpulan

Hasil dari pengujian pada tugas akhir ini akan dianalisis baik kelebihan maupun kekurangannya dan menganalisis bagaimana proses yang akan terjadi dalam penerapan *Blockchain* untuk mengamankan data pada sistem *Smart Home*.

DAFTAR PUSTAKA

- [1] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K. K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," *IEEE Internet Things J*, vol. 7, no. 2, pp. 818–829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400.
- [2] A. Mohanty and M. Sridhar, "HybriDiagnostics: Evaluating Security Issues in Hybrid SmartHome Companion Apps," in *Proceedings - 2021 IEEE Symposium on Security and Privacy Workshops, SPW 2021*, May 2021, pp. 228–234. doi: 10.1109/SPW53761.2021.00037.
- [3] S. K. Karimi Khaoula, "Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges," 2019.
- [4] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating Smart Home Security: Is Blockchain the Answer?," *IEEE Access*, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.
- [5] L. Wu, X. Du, W. Wang, and B. Lin, "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology," 2018.
- [6] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.
- [7] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, "Managing smart home appliances with proof of authority and blockchain," in *Communications in Computer and Information Science*, 2019, vol. 1041, pp. 221–232. doi: 10.1007/978-3-030-22482-0_16.
- [8] C. Lin, D. He, X. Huang, K. K. R. Choo, and A. v. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer*

- Applications*, vol. 116, pp. 42–52, Aug. 2018, doi: 10.1016/j.jnca.2018.05.005.
- [9] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of Trust: A decentralized blockchain-based authentication system for IoT,” *Comput Secur*, vol. 78, pp. 126–142, Sep. 2018, doi: 10.1016/j.cose.2018.06.004.
- [10] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, “A blockchain-based smart home gateway architecture for preventing data forgery,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, Dec. 2020, doi: 10.1186/s13673-020-0214-5.
- [11] D. Yoan Rizaldi and I. Febry Kurniawan, “Implementasi Multichain sebagai Alternatif Solusi Keamanan dan Privasi Data pada Komunikasi Perangkat Pintar Rumah,” 2019.
- [12] A. M. Mabruroh, F. Dewanta, and A. A. Wardana, “Implementasi Ethereum Blockchain dan Smart Contract pada Jaringan Smart Energy Meter,” 2021.
- [13] H. F. Putra, “PENERAPAN BLOCKCHAIN DAN KRIPTOGRAFI UNTUK KEAMANAN DATA PADA JARINGAN SMART GRID.”
- [14] Othmar Kyas, *How To Smart Home A Step by Step Guide for Smart Homes & Building Automation A Key Concept Book by*, 5th Edition. KEY CONCEPT PRESS, 2017. [Online]. Available: www.keyconceptpress.com
- [15] D. Briere and P. Hurley, *Smart Homes for Dummies*. Indiana: Wiley Publishing , 2007.
- [16] Abideen Sainul, *BLOCKCHAIN E-BOOK*. Cybrosys Technologies, 2018. [Online]. Available: www.cybrosys.comwww.blockchainexpert.uk
- [17] N. Pathak and A. Bhandari, *IoT, AI, and Blockchain for .NET*. Apress, 2018. doi: 10.1007/978-1-4842-3709-0.
- [18] M. Fajar Asy’ari, A. Budiyo, and A. Widjajarto, “ETHEREUM PARAMETER ANALYSIS OF PEER TO PEER BLOCKCHAIN

NETWORK IN COIN TRANSFER APPLICATIONS ON ASPECT PROCESSORS,” 2019.

- [19] D. E. R. Denning, *Cryptography and data security*. Addison-Wesley, 1982.
- [20] S. K. Kuanar, B. Kishore Mishra, S.-L. Peng, and D. D. Dasig, “The Role of IoT and Blockchain: Techniques and Applications.”
- [21] D. Métrologie Légale, *International Vocabulary of Metrology-Basic and General Concepts and Associated Terms (VIM) 3rd Edition Vocabulaire international de métrologie-Concepts fondamentaux et généraux et termes associés (VIM) 3 ème Édition OIML V 2-200 Edition 2007 (E/F) ORGANISATION INTERNATIONALE*. 2007.
- [22] G. Dahlquist and Å. Björck, “Numerical Methods in Scientific Computing, Volume I.”
- [23] Ridho Sayid, “ALAT PENETAS TELUR OTOMATIS BERBASIS MIKROKONTROLER,” pp. 35–36, 2019.
- [24] T. H. Saputro, N. Hidayati, and E. I. H. Ujianto, “JIP (Jurnal Informatika Polinema) SURVEI TENTANG ALGORITMA KRIPTOGRAFI ASIMETRIS,” 2020.