CLUSTERING SERANGAN MAN IN THE MIDDLE (MITM) PADA BLOCKCHAIN BERBASIS CHAIN DAN GRAPH DI JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN K-MEANS

OLEH:
SARI NUZULASTRI
09012682125020

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

CLUSTERING SERANGAN MAN IN THE MIDDLE (MITM) PADA BLOCKCHAIN BERBASIS CHAIN DAN GRAPH DI JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN K-MEANS

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister Ilmu Komputer

OLEH:
SARI NUZULASTRI
09012682125020

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

CLUSTERING SERANGAN MAN IN THE MIDDLE (MITM) PADA BLOCKCHAIN BERBASIS CHAIN DAN GRAPH DI JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN K-MEANS

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Magister

OLEH:

SARI NUZULASTRI

09012682125020

Palembang, Januari 2024

Pembimbing I

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Pembimbing II

Hadipurnawan Satria, Ph.D.
NIP. 198004182020121001

Mengetahui,
Koordinator Program Studi Magister Ilmu Komputer

Hadipurnawan Satria, Ph.D.
NIP. 198004182020121001

HALAMAN PERSETUJUAN

Pada hari kamis tanggal 11 Januari 2024 telah dilaksanakan ujian sidang tesis oleh Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Sari Nuzulastri

NIM : 09012682125020

Judul : *Clustering* Serangan *Man in the Middle (MITM)* pada *Blockchain* Berbasis *Chain* dan *Graph* di Jaringan *Internet of Things (IoT)* Menggunakan *K-Means*

1. Pembimbing I

   Prof. Deris Stiawan, M.T., Ph.D.
   NIP. 197880617200604100 2

2. Pembimbing II

   Hadipurnawan Satria, Ph.D.
   NIP. 198804182020121001

3. Penguji I

   Dian Palupi Rini, M.Kom., Ph.D.
   NIP. 197802232006042002

4. Penguji II

   Dr. Ahmad Zarkasi, M.T.
   NIP. 197908252023211007

Mengetahui,
Koordinator Program Studi Magister Ilmu Komputer

Hadipurnawan Satria, Ph.D.
NIP. 198004182020121001

LEMBAR PERNYATAAN

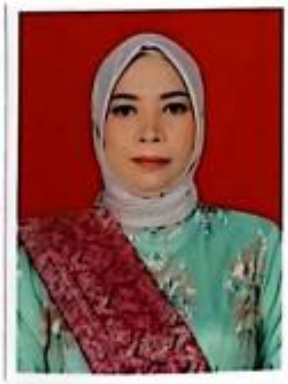
Yang bertanda tangan di bawah ini:

Nama	: Sari Nuzulastri
NIM	: 09012682125020
Program Studi	: Magister Ilmu Komputer
Judul Tesis	: Clustering Serangan Man in The Middle (MITM) pada Blockchain Berbasis Chain dan Graph di Jaringan IoT Menggunakan K-Means

Hasil Pengecekan Software Ithenticate/Turnitin: 18 %

Menyatakan bahwa laporan tesis saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tesis ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Palembang, 11 Januari 2024

Sari Nuzulastri
NIM. 09012682125020

KATA PENGANTAR

Puji syukur dipanjatkan kepada Allah SWT atas limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tesis dengan judul **"*Clustering* Serangan *Man in The Middle* (MITM) pada *Blockchain* Berbasis *Chain* dan *Graph* di Jaringan *Internet of Things* (IoT) Menggunakan K-Means"**. Tesis ini diajukan untuk melengkapi salah satu syarat memperoleh gelar Magister di program studi Magister Teknik Informatika Universitas Sriwijaya.

Penulis berharap Tesis ini dapat bermanfaat bagi orang banyak, meski masih banyak kekurangan dan jauh dari kesempurnaan. Dalam penyusunan Tesis ini, penulis banyak mendapat bimbingan, dukungan dan bantuan dari berbagai pihak, baik moril maupun materil, sehingga Tesis ini dapat diselesaikan. Dengan ketulusan hati, penulis mengucapkan terimakasih kepada:

1. Orang tua, alm. Papa tersayang A. Nawawi dan Hj. Rogayah, H. Azwan dan Hj. Maryani atas doa dan ridho yang diberikan kepada penulis.
2. Suami, Ahmad Farnanda dan anak tercinta Fathir, atas dukungan, cinta, semangat dan motivasi yang diberikan kepada penulis.
3. Saudara kandung penulis yang tidak dapat disebut satu persatu, atas semangat dan kontribusi positifnya terhadap penulis.
4. Prof. Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Hadipurnawan Satria, Ph.D selaku Koordinator Program Studi Magister Teknik Informatika Universitas Sriwijaya dan pembimbing Tesis atas dukungannya selama penulisan ini.
6. Prof. Deris Stiawan, M.T., Ph.D., selaku Pembimbing I Tesis yang selalu mengarahkan, memberi nasihat dan dukungan selama penulisan.
7. Dian Palupi Rini, M.Kom., Ph.D. dan Dr. Ahmad Zarkasi, M.T., selaku penguji
8. Pak Huda, Pak Rifai, Pak Rossi, Naufal, Dimas dan Ipul atas sharing ilmu, bantuan, support dan masukkannya.

9. Semua Dosen dan Staff Magister Ilmu Komputer yang selama ini telah melimpahkan ilmunya kepada penulis selama proses belajar mengajar dan membantu dalam memperlancar kegiatan akademik di Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Geng bukit yang selalu memberikan semangat moril dalam menyelesaikan Tesis.
11. Semua pihak yang telah membantu secara langsung maupun secara tidak langsung.

Akhir kata, dengan segala kerendahan hati dan keterbatasan, penulis berharap Tesis ini menghasilkan sesuatu yang bermanfaat, khusunya bagi Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Palembang, Januari 2024
Penulis,

Sari Nuzulastri

CLUSTERING MAN IN THE MIDDLE (MITM) ATTACKS ON CHAIN AND GRAPH-BASED BLOCKCHAIN IN IOT NETWORKS USING K-MEANS

Sari Nuzulastri (09012682125020)
Dept. of Master Computer Science, Computer Science, Sriwijaya University
Email: sari@ilkom.unsri.ac.id

ABSTRACT

Network security on *Internet of Thing* (IoT) devices in the IoT development process may open rooms for hackers and other problems if not properly protected, particularly in the addition of internet connectivity to computing device systems that are interrelated in transferring data automatically over the network. This study implements network detection on IoT network security resembles security systems from *man in the middle* (MITM) attacks on *blockchains*. Security systems exist on blockchains are decentralized and have peer to peer characteristics which are categorized into several parts based on the type of architecture that suits their use cases such as *blockchain chain based* and *graph based*. This study uses the principal component analysis (PCA) to extract features from the transaction data processing on the blockchain process and produces 9 features before the K- Means algorithm with the elbow technique was used for classifying the types of MITM attacks on IoT networks and comparing the types of *blockchain chain-based* and *graph-based* architectures in the form of visualizations as well. Experimental results shows 97.16% of normal data and 2.84% of MITM attack data were observered.

Keywords : Internet of Things, network security, man in the middle (MITM), blockchain, k-means

CLUSTERING SERANGAN MAN IN THE MIDDLE (MITM) PADA BLOCKCHAIN BERBASIS CHAIN DAN GRAPH DI JARINGAN IOT MENGGUNAKAN K-MEANS

Sari Nuzulastri (09012682125020)
Jurusan Magister Ilmu Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya
Email: sari@ilkom.unsri.ac.id

ABSTRAK

Keamanan jaringan pada perangkat *Internet of Thing* (IoT) dalam proses pengembangan IoT yang memberikan akses dan informasi di dalam jaringan internet yang dapat membuka celah bagi peretas dan masalah lainnya jika tidak terlindungi dengan baik, terutama pada penambahan konektivitas internet ke sistem perangkat komputasi yang saling terkait dalam mentransfer data secara otomatis melalui jaringan. Pendeteksian jaringan yang diimplementasikan pada keamanan jaringan IoT seperti sistem keamanan dari serangan *man in the midlle* (MITM) pada *blockhchain*. Sistem keamanan yang ada pada *blockchain* yang sifatnya terdesentralisasi dan berkarakteristik *peer to peer* dapat dikategorikan menjadi beberapa bagian berdasarkan jenis arsitekturnya yang sesuai dengan kasus penggunaannya seperti *blockchain chain based* dan *graph based.* Dalam penelitian ini menggunakan PCA sebagai ekstraksi fitur pada proses pengolahan data yang menghasilkan 9 fitur sebelum menggunakan algoritma K-Means dengan menggunakan teknik elbow yang digunakan dalam proses pengelompokkan jenis serangan MITM pada jaringan IoT serta membandingkan jenis arsitektur *blockchain chain based* dan *graph based* dalam bentuk visualisasi. Dari hasil visualisasi didapat 97,16% data normal dan 2,84% data serangan MITM.

Kata kunci : *internet of things, man in the middle (MITM), blockchain, chain base, graph base, k-means*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Pendahuluan bab ini menjelaskan tentang latar belakang dilakukannya penelitian yang berjudul: "*Clustering* Serangan *Man in The Middle (MITM)* pada *Blockchain* Berbasis *Chain* dan *Graph* di Jaringan IoT Menggunakan K-Means". Pada bab ini akan dimulai dengan alasan penulis mengangkat tentang data serangan yang ada pada jaringan IoT dan beberapa alasan penulis dalam mengklasifikasi serangan tersebut serta pada sub bab selanjutnya menjelaskan tentang rumusan masalah dan batasan masalah. Kemudian terdapat tujuan dari penelitian ini dan metodologi yang akan digunakan dalam peneltian tersebut.

1.1 Latar Belakang

Internet of Things (IoT) adalah paradigma baru yang telah mengubah cara hidup tradisional menjadi gaya hidup berteknologi tinggi. Menurut penelitian (S. Kumar, Tiwari, and Zymbler 2019) penggunaan perangkat IoT sebagai perangkat pintar dan internet yang memberikan solusi inovatif dalam berbagai tantangan atau masalah yang terkait dalam bidang bisnis, pemerintahan dan publik/swasta serta industri. Diperkirakan pada tahun 2030 akan banyak perangkat IoT yang terhubung ke internet (Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical 2023) diseluruh dunia dengan perkiraan sekitar 650 milyar USD (Internet of Things (IoT) total annual revenue worldwide from 2020 to 2030 2023). Kenaikan penggunaan perangkat IoT pada tahun 2023 sekitar 15 milyar perangkat dengan pendapatan sekitar 300 milyar USD, sehingga diperkirakan 90% sampai 95% dari jumlah perangkat menggunakan media nirkabel (Sinha 2023) seperti WiFi (IEEE802.11x), Bluetooth (IEEE802.15.1), ZigBee (IEEE802.15.4), atau GSM (NBIoT, LPWA, 5G).

Internet of Things (IoT) merupakan teknologi yang mengubah dunia pada jaringan yang berkembang dari perangkat fisik dan virtual yang terhubung satu sama lain ke internet, yang ditujukan untuk mengumpulkan data, mengendalikan

alat lain untuk melakukan hal tertentu secara spesifik melalui jaringan internet. Jaringan internet 4G maupun 5G mendukung konektivitas IoT (Mistry et al. 2020) yang akan disusul dengan munculnya teknologi 6G (Rathod et al. 2022; Vaghani, Sood, and Yu 2022) , karena semakin banyak perangkat IoT yang terhubung ke jaringan maka dibutuhkan kapasitas yang lebih besar agar jaringan tetap stabil dan tidak mengalami gangguan.

Perkembangan IoT yang berkembang seiring dengan kemajuan teknologi, dengan itu membutuhkan media penyimpanan dan pemrosesan data dengan karakteristik yang unik pada keterbatasan sumber daya (Borgia 2014), (Zhou et al. 2017) dimana *cloud* adalah salah satu alternatif penyimpanan data untuk IoT. Namun, pengorganisasian mandiri dan komunikasi yang menggunakan *cloud* sebagai salah satu media dalam penyimpanan data yang rentan terhadap serangan, karena semakin banyak perangkat yang terhubung dengan internet. Keamanan jaringan pada perangkat IoT merupakan peranan penting dalam memproteksi data agar tetap aman yang melibatkan penambahan konektivitas internet ke sistem perangkat komputasi yang saling terkait dan mampu mentransfer data secara otomatis melalui jaringan

Distributed Ledger Technology (DLT) merupakan suatu sistem digital yang mencatat transaksi secara terdesentralisasi, yang berfungsi untuk mengawasi adanya manipulasi data, dan semua informasi yang tersimpan aman dan akurat yang berperan seperti kunci pengaman, sehingga informasi yang tersimpan dalam *database* tidak dapat diubah dan diatur oleh jaringan luar. Pada tahun 2021 penelitian dari (Singh, Sanwar Hosen, and Yoon 2021) menjelaskan bahwa DLT merupakan bagian jenis dari *blockchain*, dengan adanya konsep *blockchain* yang menyediakan sistem manajemen data yang terdesentralisasi dalam penyimpan dan berbagi data pada setiap transaksi dalam jaringan yang memberikan analisis terperinci pada pola serangan keamanan yang diterapkan dalam perangkat IoT. Sistem keamanan yang ada pada *blockchain* yang sifatnya terdesentralisasi dan berkarakteristik *peer to peer* pada dunia nyata yang ada pada masalah keamanan, tantangan, kerentanan dan serangan yang menghambat pada peningkatan teknologi *blockchain* dalam berbagai aspek kehidupan.

Teknologi *blockchain* yang dapat dikategorikan menjadi beberapa bagian berdasarkan jenis arsitekturnya yang sesuai dengan kasus penggunaannya, sedangkan secara konteks *blockchain chain based* dan *graph based* merupakan dua jenis struktur data yang digunakan oleh *blockchain* untuk menyimpan transaksi dan membangun bukti konsensus. Penelitian (Wu et al. 2022) menjelaskan bahwa *blockchain chain based* struktur datanya pada setiap blok membentuk rantai dan terus bertambah sedangkan *graph based* menggunakan struktur data berbentuk grafik acak dan setiap transaksi dapat langsung terhubung dengan beberapa transaksi lainnya dalam jaringan, adapun penggunaanya tergantung dari tujuan pada aplikasi *blockchain* yang akan digunakan.

Penelitian (J. Choi et al. 2021) pada penelitiannya menjelaskan mengenai sistem keamanan *man in the middle* (MITM) yang berbasis *blockchain*. Metode yang mendeteksi serangan dari MITM dengan melakukan penyaringan data jaringan, pendeteksian jaringan, perbandingan jaringan yang diimplementasikan pada sistem keamanan jaringan *blockchain internet of thing* (IoT).

Beberapa penelitian yang menunjukkan tentang jenis dari serangan MITM (Mallik et al. 2019) merupakan jenis serangan yang bertujuan untuk mengambil data informasi secara sembunyi – sembunyi atau meniru salah satu pihak melalui sebuah protokol atau serangan SSL/TLS MITM. Teknik utama dari serangan MITM (Nayak and Samaddar 2010) yang digunakan dalam peretasan berbasis komputer seperti serangan *spoofing* DNS yang memberikan data yang berbeda (pemalsuan data).

Penggunaan algortima K-Means pada jaringan IoT berfungsi untuk melakukan pengelompokan data berdasarkan karakteristik, menurut penelitian (Stiawan et al. 2021) dengan menggunakan algoritma K-Means yang menghasilkan hasil dari pengelompokkan jumlah rata-rata paket dalam *cluster* serangan adalah 95.931 paket, dan rata-rata *cluster* normal adalah 4.068 paket dengan akurasi *clustering* menggunakan metode K-Means sebesar 99,94% dengan akurasi pada *confusion matrix* pada bagian *true negative* sebesar 98,62%, *true positif* sebesar 100%, *false negative* sebesar 0,00% dan *false positif sebesar 1,38%*.

Pada penelitian ini, akan dilakukan perbandingan performa antara *graph based* dengan *chain based* dari data serangan MITM yang ada pada jaringan IoT, untuk esktraksi fitur menggunakan PCA dan *clustering* menggunakan metode K-Means yang hasilnya akan ditampilkan dalam bentuk visualisasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, untuk mendapatkan perbandingan dari beberapa *platform* DLT (*Distributed Ledger Technology*) yang terdesentralisasi dan memiliki karakteristik pada masalah sistem keamanan, serta serangan yang akan menghambat pada sistem kerja jaringan *blockchain* dapat dirumuskan dalam penelitian ini yaitu:

1. Bagaimana sistem keamanan dari data transaksi yang ada di jaringan *blockchain* IoT (*Internet of Things*)?
2. Bagaimana *clustering* dari serangan *Man in The Middle (MITM)* yang ada pada jaringan *blockchain* di jaringan IoT (*Internet of Things*)?
3. Bagaimana untuk mendapatkan perbandingan performa antara DLT *graph based* dengan *chain based*?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang akan dirancang dalam tesis ini yaitu:

1. Dataset yang digunakan adalah data *public* yang diambil dari paper tentang *graph based* (Guo et al. 2020) IOTA Emperical Data Analysis.
2. Penelitian ini hanya dibatasi pada sistem keamanan data transaksi dari serangan *Man in The Middle (MITM).*
3. Metode *machine learning* yang digunakan dalam proses *clustering* adalah K-Means.

1.4 Tujuan

Tujuan dalam penelitian tesis ini adalah sebagai berikut:

1. Membuat karakteristik dari sistem keamanan data transaksi yang ada pada jaringan *blockchain* IoT.
2. Menganalisis jenis tipe serangan *Man in The Middle (MITM)* pada jaringan *blockchain* IoT.
3. Menganalisa perbedaan antara DLT *graph based* dengan *chain based.*

1.5 Manfaat

Adapun manfaat yang diperoleh dari penelitian ini adalah sebagai berikut:

1. Dapat diketahui bagaimana karakteristik sistem keamanan dari data transaksi yang ada pada jaringan *blockchain* IoT.
2. Dapat diketahui hasil *clustering* yang ada pada perangkat jaringan *blockchain* IoT.
3. Diketahui perbedaan dari sistem kinerja antara DLT *graph based* dengan *chain based* pada perangkat jaringan *blockchain* IoT.

1.6 Sistematika Penulisan

Agar mendapatkan gambaran yang jelas mengenai penelitian ini, maka dibuatlah sistematika penulisan yang berisi gambaran dalam tiap bab penelitian ini, yaitu:

1. BAB I : Pendahuluan

   Bab I berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat dari topik yang dipilih berupa suatu sistem keamanan pada jaringan yang terhubung pada perangkat IoT (*Internet of Things*).

2. BAB II : Tinjauan Pustaka

   Bab II ini menjelaskan mengenai *literature riview* yang berhubungan dengan masalah *blockchain* IoT yang berhubungan dengan sistem keamanan pada perangkat IoT

(*Internet of Things*) pada beberapa penelitian publikasi. Kemudian menjelaskan dataset yang akan digunakan.

3. BAB III : Metodologi Penelitian

   Bab III berisi metodologi yang menjelaskan secara bertahap dan terperinci tentang langkah-langkah yang digunakan untuk mencari, mengumpulkan dan menganalisa terkait dengan data perbandingan sistem keamanan antara *graph based* dengan *chain based* pada penelitian ini.

4. BAB IV : Hasil dan Analisa

   Bab IV ini berisi tentang hasil pengujian yang telah dilakukan, data yang diambil akan dianalisa dengan menggunakan berbagai macam teknik serta hasil dari validasi.

5. BAB V : Kesimpulan dan Saran

   Bab V ini menjelaskan kesimpulan dari hasil yang diperoleh, serta merupakan dari jawaban yang diperoleh dari tujuan yang dicapai. Kemudian terdapat saran dan kekurangan untuk kemajuan yang dapat dikembangkan dalam penelitian berikutnya.

DAFTAR PUSTAKA

Abdelmaboud, Abdelzahir et al. 2022. "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions." *Electronics (Switzerland)* 11(4): 1–35.

Ahmed, Mohiuddin, Raihan Seraj, and Syed Mohammed Shamsul Islam. 2020. "The K-Means Algorithm: A Comprehensive Survey and Performance Evaluation." *Electronics (Switzerland)* 9(8): 1–12.

Arifeen, Murshedul et al. 2022. "Autoencoder Based Consensus Mechanism for Blockchain-Enabled Industrial Internet of Things." *Internet of Things (Netherlands)* 19(July 2021): 100575. https://doi.org/10.1016/j.iot.2022.100575.

Bhushan, Bharat, G. Sahoo, and Amit Kumar Rai. 2018. "Man-in-the-Middle Attack in Wireless and Computer Networking - A Review." *Proceedings - 2017 3rd International Conference on Advances in Computing, Communication and Automation (Fall), ICACCA 2017* 2018-Janua: 1–6.

Borgia, Eleonora. 2014. "The Internet of Things Vision: Key Features, Applications and Open Issues." *Computer Communications* 54: 1–31.

Brusco, Michael J., Emilie Shireman, and Douglas Steinley. 2017. "A Comparison of Latent Class, K -Means, and K -Median Methods for Clustering Dichotomous Data." *Psychological Methods* 22(3): 563–80.

Canteaut, Anne, María Naya-Plasencia, and Bastien Vayssière. 2013. "Sieve-in-the-Middle: Improved MITM Attacks." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8042 LNCS(PART 1): 222–40.

Celebi, M. Emre, Hassan A. Kingravi, and Patricio A. Vela. 2013. "A Comparative Study of Efficient Initialization Methods for the K-Means Clustering Algorithm." *Expert Systems with Applications* 40(1): 200–210.

Choi, Hyunsang, and Heejo Lee. 2005. "PCAV: Internet Attack Visualization on Parallel Coordinates." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 3783 LNCS: 454–66.

Choi, Hyunsang, Heejo Lee, and Hyogon Kim. 2009. "Fast Detection and Visualization of Network Attacks on Parallel Coordinates." *Computers and Security* 28(5): 276–88. http://dx.doi.org/10.1016/j.cose.2008.12.003.

Choi, Jinchun et al. 2021. "Blockchain-Based Man-in-the-Middle (MITM) Attack Detection for Photovoltaic Systems." *2021 IEEE Design Methodologies Conference, DMC 2021* (August 2022).

Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. 2016. “A Survey of Man in the Middle Attacks.” *IEEE Communications Surveys and Tutorials* 18(3): 2027–51.

Cullen, Andrew, Pietro Ferraro, Christopher King, and Robert Shorten. 2019. “Distributed Ledger Technology for IoT: Parasite Chain Attacks.” : 1–11. http://arxiv.org/abs/1904.00996%0Ahttp://dx.doi.org/10.1109/JIOT.2020.2983401.

Dinata, Rozzi Kesuma, Safwandi Safwandi, Novia Hasdyna, and Nur Azizah. 2020. “Analisis K-Means Clustering Pada Data Sepeda Motor.” *INFORMAL: Informatics Journal* 5(1): 10.

Eigner, Oliver, Philipp Kreimel, and Paul Tavolato. 2017. “Detection of Man-in-the-Middle Attacks on Industrial Control Networks.” *Proceedings - 2016 International Conference on Software Security and Assurance, ICSSA 2016* (August): 64–69.

Emira, Hosny. H. Abo. 2020. “Authenticating IoT Devices Issues Based on Blockchain.” *Journal of Cybersecurity and Information Management* (January): 35–40.

Fan, Caixiang, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek. 2020. “Performance Evaluation of Blockchain Systems: A Systematic Survey.” *IEEE Access* 8(July): 126927–50.

Fan, Qing, Jianhua Chen, Lazarus Jegatha Deborah, and Min Luo. 2021. “A Secure and Efficient Authentication and Data Sharing Scheme for Internet of Things Based on Blockchain.” *Journal of Systems Architecture* 117(July 2020): 102112. https://doi.org/10.1016/j.sysarc.2021.102112.

Ferraro, Pietro, Christopher King, and Robert Shorten. 2018. “IOTA-Based Directed Acyclic Graphs without Orphans.” : 1–13. http://arxiv.org/abs/1901.07302%0Ahttp://dx.doi.org/10.1109/TAC.2019.2950873.

Gugueoth, Vinay, Sunitha Safavat, Sachin Shetty, and Danda Rawat. 2023. “A Review of IoT Security and Privacy Using Decentralized Blockchain Techniques.” *Computer Science Review* 50: 100585. https://doi.org/10.1016/j.cosrev.2023.100585.

Guo, Fengyang, Xun Xiao, Artur Hecker, and Schahram Dustdar. 2020. “Characterizing IOTA Tangle with Empirical Data.” *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*.

“Internet of Things (IoT) Total Annual Revenue Worldwide from 2020 to 2030.” 2023. *Transforma Insights*. https://www.statista.com/statistics/1194709/iot-revenue-worldwide/.

Kably, Salaheddine, Mounir Arioua, and Nabih Alaoui. 2022. “Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment.” *Computers, Materials and Continua* 71(2): 5271–91.

Kumar, Prabhat et al. 2023. “A Blockchain-Orchestrated Deep Learning Approach for Secure Data Transmission in IoT-Enabled Healthcare System.” *Journal of Parallel and Distributed Computing* 172: 69–83. https://doi.org/10.1016/j.jpdc.2022.10.002.

Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. 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.

Li, Jennifer, and Mohamad Kassem. 2021. “Applications of Distributed Ledger Technology (DLT) and Blockchain-Enabled Smart Contracts in Construction.” *Automation in Construction* 132(April): 103955. https://doi.org/10.1016/j.autcon.2021.103955.

Mallik, Avijit, Abid Ahsan, Mhia Md Zaglul Shahadat, and Jia Chi Tsou. 2019. “Man-in-the-Middle-Attack: Understanding in Simple Words.” *International Journal of Data and Network Science* 3(2): 77–92.

Mistry, Ishan, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. 2020. “Blockchain for 5G-Enabled IoT for Industrial Automation: A Systematic Review, Solutions, and Challenges.” *Mechanical Systems and Signal Processing* 135: 106382. https://doi.org/10.1016/j.ymssp.2019.106382.

Mohanta, Bhabendu Kumar et al. 2021. “Addressing Security and Privacy Issues of IoT Using Blockchain Technology.” *IEEE Internet of Things Journal* 8(2): 881–88.

Nayak, Gopi Nath, and Shefalika Ghosh Samaddar. 2010. “Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions.” *Proceedings - 2010 3rd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2010* 5: 491–95.

“Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2030, by Vertical.” 2023. *Transforma Insights*. https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/.

Paulavičius, Remigijus, Saulius Grigaitis, Aleksandr Igumenov, and Ernestas Filatovas. 2019. “A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions.” *Informatica (Netherlands)* 30(4): 729–48.

Popov, Serguei, Olivia Saa, and Paulo Finardi. 2019. “Equilibria in the Tangle.” *Computers and Industrial Engineering* 136(July): 160–72. https://doi.org/10.1016/j.cie.2019.07.025.

Rathod, Tejal et al. 2022. “Blockchain for Future Wireless Networks: A Decade Survey.” *Sensors* 22(11): 1–36.

Sagala, Ray Mondow. 2021. “Prediksi Kelulusan Mahasiswa Menggunakan Data Mining Algoritma K-Means.” *TeIKa* 11(2): 131–42.

Sedlmeir, Johannes, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. 2020. “The Energy Consumption of Blockchain Technology: Beyond Myth.” *Business and Information Systems Engineering* 62(6): 599–608. https://doi.org/10.1007/s12599-020-00656-x.

Sicari, S., A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. 2015. “Security, Privacy and Trust in Internet of Things: The Road Ahead.” *Computer Networks* 76: 146–64. http://dx.doi.org/10.1016/j.comnet.2014.11.008.

Singh, Saurabh, A. S.M. Sanwar Hosen, and Byungun Yoon. 2021. “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.” *IEEE Access* 9: 13938–59.

Sinha, Satyajit. 2023. “State of IoT 2023: Number of Connected IoT Devices Growing 16% to 16.7 Billion Globally.” *iot-analytics*. https://iot-analytics.com/number-connected-iot-devices/ (August 1, 2023).

Sivasankari, N., and S. Kamalakkannan. 2022. “Detection and Prevention of Man-in-the-Middle Attack in Iot Network Using Regression Modeling.” *Advances in Engineering Software* 169(April): 103126. https://doi.org/10.1016/j.advengsoft.2022.103126.

Smith, Lindsay. 2006. “A Tutorial on PCSA.” *Department of Computer Science, University of Otago.*: 12–28.

Stiawan, Deris et al. 2021. “Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network.” *IEEE Access* 9: 116475–84.

Tsoulias, Konstantinos et al. 2020. “A Graph Model Based Blockchain Implementation for Increasing Performance and Security in Decentralized Ledger Systems.” *IEEE Access* 8: 130952–65.

Vaghani, Anjali, Keshav Sood, and Shui Yu. 2022. “Security and QoS Issues in Blockchain Enabled Next-Generation Smart Logistic Networks: A Tutorial.” *Blockchain: Research and Applications* 3(3): 100082. https://doi.org/10.1016/j.bcra.2022.100082.

Wu, Huan Yu et al. 2022. “Chain or DAG? Underlying Data Structures, Architectures, Topologies and Consensus in Distributed Ledger Technology: A Review, Taxonomy and Research Issues.” *Journal of Systems Architecture* 131(August).

Zhou, Jun, Zhenfu Cao, Xiaolei Dong, and VasilakosAthanasios V. 2017. "Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos The." *IEEE Communications Magazine* (January): 26–33.

Zhu, Qing, Jun Pei, Xinbao Liu, and Zhiping Zhou. 2019. "Analyzing Commercial Aircraft Fuel Consumption during Descent: A Case Study Using an Improved K-Means Clustering Algorithm." *Journal of Cleaner Production* 223: 869–82.