Jurnal Filsafat Indonesia, Vol 7 No 2 Tahun 2024
ISSN: E-ISSN 2620-7982, P-ISSN: 2620-7990

Keamanan Data *Internet of Things* dalam Perspektif Pseudosains Mario Bunge

Aditya Pradana[1], Yoanes Bandung[2], Dimitri Mahayana[3], Yusep Rosmansyah[4]
[1.2.3,4] Program Studi Teknik Elektro dan Informatika, Sekolah Teknik Elektro dan Informatika, Bandung, Indonesia
E-mail: 33223014@std.stei.itb.ac.id[1], yoanes.bandung@itb.ac.id[2], dimitri@lskk.ee.itb.ac.id[3], yusep@stei.itb.ac.id[4]

Diterima: 19-12-2023	Direview: 12-01-2024	Publikasi: 30-06-2024

Abstrak

Keamanan data menjadi perhatian utama dalam *Internet of Things* (IoT) yang berkembang pesat. Artikel ini menyelidiki aspek keamanan data pada IoT dengan perspektif pseudosains yang terinspirasi oleh Mario Bunge. Tujuan penelitian ini adalah untuk memahami dan mengatasi tantangan keamanan data di lingkungan IoT. Pertama, penulis mengidentifikasi dan mengevaluasi potensi kerentanan dan ancaman terhadap data, risiko peretasan, dan kebutuhan enkripsi data. Penulis kemudian menganalisis metode dan strategi keamanan yang umum digunakan, termasuk *blockchain*, *fog computing, edge computing*, dan *machine learning*. Pendekatan pseudosains Bunge membantu dalam memahami dan menganalisis keamanan data IoT secara komprehensif. Hasilnya menunjukkan pemahaman yang lebih dalam tentang tantangan keamanan data di IoT, serta rekomendasi terperinci untuk mitigasi risiko. Penelitian ini menyoroti pentingnya pendekatan holistik yang memadukan aspek teknis dan filosofis untuk mengatasi masalah keamanan data di IoT. Perspektif pseudosains membantu dalam mengembangkan kerangka konseptual yang kokoh dan mendorong pemikiran kritis dalam merumuskan strategi keamanan yang efektif. Kesimpulannya, artikel ini memberikan kontribusi penting dalam memahami dan mengatasi kompleksitas keamanan data di IoT.

Kata Kunci: keamanan data; internet of things; pseudosains; Mario Bunge

Abstract

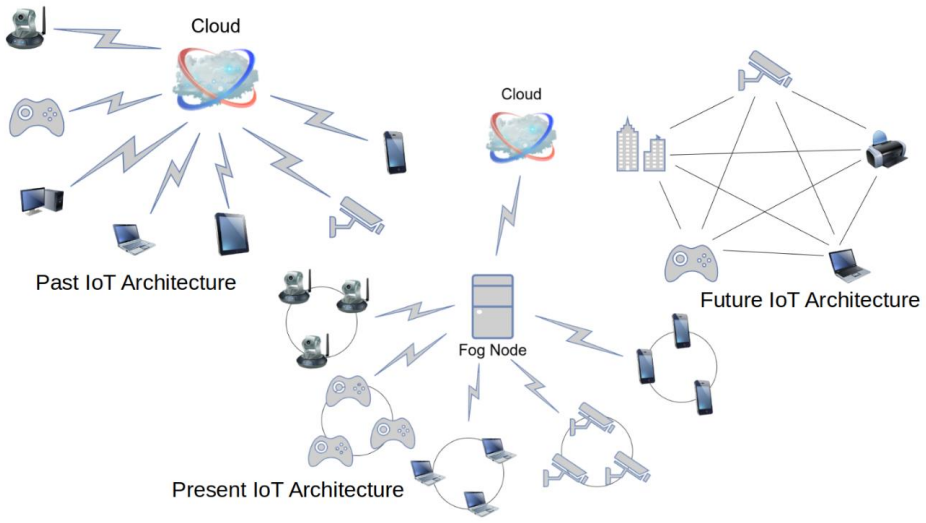
Data security is a major concern in the rapidly growing Internet of Things (IoT). This paper investigates the data security aspects of IoT with a pseudoscience perspective inspired by Mario Bunge. The purpose of this research is to understand and address data security challenges in IoT environments. First, researcher identify and evaluate potential vulnerabilities and threats to data, hacking risks, and data encryption needs. Then, researcher analyze commonly used security methods and strategies, including blockchain, fog computing, edge computing, and machine learning. Bunge's pseudoscience approach helps in comprehensively understanding and analyzing IoT data security. The results show a deeper understanding of the data security challenges in IoT, as well as detailed recommendations for risk mitigation. This research highlights the importance of a holistic approach that blends technical and philosophical aspects to address data security issues in IoT. The pseudoscience perspective helps in developing a solid conceptual framework and encourages critical thinking in formulating effective security strategies. In conclusion, this paper makes an important contribution in understanding and addressing the complexities of data security in IoT.

Keywords: data security; internet of things; pseudosains; Mario Bunge

1. Pendahuluan

Laju pertumbuhan perangkat yang terhubung ke Internet semakin meningkat, salah satunya adalah penggunaan Internet of Things (IoT) di masyarakat. Faktanya, jumlah perangkat IoT kini melebihi jumlah perangkat non-IoT. Menurut statistik, terdapat lebih dari 15 milyar (15,14 milyar) perangkat IoT yang terhubung di seluruh dunia (Duarte, 2023). Jumlah tersebut lebih

banyak dari jumlah user yang menggunakan internet di dunia, yaitu 5,16 milyar (Kemp, 2023). Teknologi IoT semakin banyak diimplementasikan pada berbagai bidang. Gambar 1 menampilkan perbedaan mengenai arsitektur Iot pada masa lalu, sekarang, dan masa depan. Di masa yang akan datang, perangkat IoT dapat saling berkomunikasi secara langsung (*peer to peer*) (Hassija dkk., 2019). Komunikasi antar perangkat IoT secara langsung, akan meningkatkan efisiensi pada jaringan, mengurangi latensi, memudahkan dalam skalabilitas, serta meningkatkan keamanan karena tidak melibatkan server yang terpusat sehingga potensi serangan terhadap satu titik tunggal dapat berkurang. Hal tersebut membuat lebih banyak aplikasi IoT yang dikembangkan untuk memenuhi kebutuhan manusia.



Gambar 1. Arsitektur IoT Masa Lalu, Sekarang, dan Masa Depan (Hassija Dkk., 2019)

Banyaknya aplikasi pada IoT telah memunculkan Multimedia Internet of Things (M-IoT). M-IoT adalah konsep yang menggabungkan IoT dan teknologi multimedia untuk menciptakan lingkungan dengan kemampuan berbagi dan mengelola jenis konten multimedia seperti *audio*, *video*, gambar, dan data berukuran besar dari sensor. Perangkat M-IoT membutuhkan bandwidth yang lebih tinggi, sumber daya memori yang besar, dan daya komputasi yang lebih tinggi untuk menganalisis dan memproses data multimedia yang diperoleh. Tabel 1 menunjukkan perbedaan antara data IoT skalar dan multimedia. Aplikasi multimedia tradisional melibatkan transmisi data point-to-point, point-to-multipoint, atau multipoint-to-multipoint. Sebaliknya, aplikasi M-IoT membutuhkan transmisi data yang sangat besar selama komunikasi multipoint-to-point (misalnya, sistem pengawasan seluruh kota pintar) atau multipoint-to-multipoint.

Semakin bertambahnya penggunaan IoT, maka diperlukan juga mekanisme untuk memastikan keamanannya. Penelitian mengenai keamanan IoT yang terpublikasikan sudah dilakukan sejak tahun 1980-an. Tahun 1980-an istilah IoT belum ada, namun terdapat istilah ”komputasi pervasif” yang mengeksplorasi gagasan bahwa komputer dan teknologi dapat menyatu dengan lingkungan sehari-hari. Grafik jumlah paper yang meneliti mengenai keamanan IoT di IEEE dan ACM memperlihatkan bahwa topik tersebut semakin banyak diteliti pada tahun 2000-an. Mayoritas paper fokus membahas mengenai keamanan IoT dalam beberapa tahun terakhir ini, diantaranya adalah paper yang membahas mengenai klasifikasi *intrusion detection systems* pada IoT (Arisdakessian dkk., 2023), penggunaan teknologi *fog computing* untuk meningkatkan keamanan data pada aplikasi IoT (Burhan dkk., 2023), hingga penggunaan teknologi *image processing* dalam aplikasi keamanan berdasarkan wajah pada IoT (Al-Ghaili dkk., 2023).

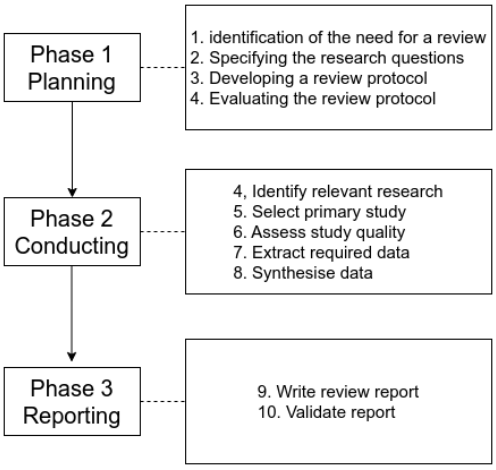
Artikel ini disusun dengan tujuan mengidentifikasi dan memberikan pandangan kritis terhadap pendekatan mengenai keamanan data pada IoT yang mungkin tidak ilmiah atau tidak valid. Mario Bunge menekankan perlunya dasar logis dan bukti empiris, sehingga dapat menilai klaim atau solusi yang mungkin tidak didasarkan pada metofologi yang dapat diuji atau argumentasi logis yang konsisten.

Tabel 1. Perbedaan Data Iot Skalar dan Multimedia (Nauman Dkk., 2020)

Parameter	Data Skalar	Data Multimedia
Ukuran data	Bytes – Kilobytes	Megabytes – Gigabytes
Memori	Kilobytes – Megabytes	Megabytes – Gigabytes
Pemrosesan	Kilohertz – Megahertz	Megahertz – Gigahertz
Storage	Kilobytes - Megabytes	Gigabytes
Bandwidth	Kilobytes	Megabytes
Delay sensitivity	Rendah	Tinggi
Konsumsi daya	Rendah	Tinggi

2. Metode

Proses penyusunan artikel ini menggunakan metode *Systematic Literature Review* (SLR) dengan mengikuti langkah-langkah seperti pada gambar 2 (Kitchenham, 2007). Pencarian dimulai dengan melakukan elaborasi beberapa review paper yang relevan dengan keamanan data multimedia pada IoT. Sumber utama pencarian artikel tersebut adalah jurnal IEEE dan ACM. Proses pencarian dilakukan dalam dua tahap, yaitu pencarian secara manual dan pencarian otomatis menggunakan Parsifal. Pencarian manual dilakukan dengan kata kunci “security”, “multimedia”, “internet of things”. Hasil pencarian manual tersebut didapatkan review paper sebagai rujukan awal. Beberapa kata kunci yang didapatkan dari paper-paper tersebut digunakan sebagai referensi untuk pencarian otomatis. Kata kunci tersebut dimasukkan pada form Population, Intervention, Comparison, Outcome, dan Context (PICOC). PICOC dapat membantu dalam membuat string pencarian. Query yang didapatkan adalah (”*internet of multimedia things*” OR ”iomt” OR ”*internet of things*” OR ”iot”) AND (”blockchain” OR ”*edge computing*” OR ”*fog computing*” OR ”*machine learning*”) AND (”*security*”) AND (”*approach*” OR ”*architecture*” OR ”*method*”). Hasil pencarian tersebut diberi filter bahwa hasil nya berupa jurnal riset dan diterbutkan dalam lima tahun terakhir, dengan topik spesifik (*internet of things, computer network security, data privacy, security*). Selanjutnya dilakukan pembahasan mengenai pseudosain menurut pandangan Mario Bunge.



Gambar 2. SLR Kitchenham and Charters (Kitchenham, 2007)

3. Hasil dan Pembahasan

a. Kerangka Kerja Bidang Kognitif Mario Bunge

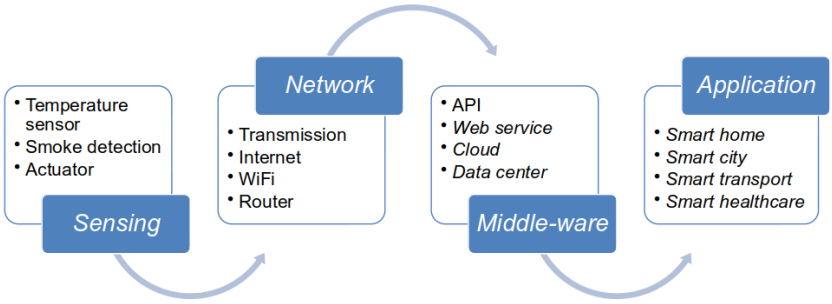
Mario Bunge, seorang filsuf dan epistemologis Argentina-Kanada, mendefinisikan pseudosains sebagai klaim atau pernyataan ilmiah yang tidak dapat diuji secara empiris, tidak dapat dibuktikan atau dibantah oleh pengamatan atau eksperimen. Menurut Mario Bunge, masyarakat akan mencirikan sebuah ilmu pengetahuan dan juga pseudosains sebagai bidang kognitif, yaitu sebuah sektor dari aktivitas manusia yang bertujuan untuk mendapatkan, menyebarkan, atau memanfaatkan pengetahuan, baik pengetahuan tersebut benar atau salah (Bunge, 1983). Mario Bunge merangkum karakteristik-karakteristik dari bidang kognitif sebagai berikut:

E = (C, S, D, G, F, B, P, K, A, M)

Keterangan:
C = Komunitas kognitif
S = Masyarakat yang menaungi C
G = Pandangan umum, atau pandangan dunia, atau filosofi dari C
D = Domain atau semesta wacana dari E: objek-objek yang dibahas oleh E
F = Latar belakang formal: perangkat logika dan matematika yang dapat digunakan dalam E
B = Latar belakang khusus, atau pra-anggapan tentang D yang diambil dari bidang pengetahuan selain E
P = Problematika atau sekumpulan masalah yang dapat ditangani oleh E
K = Pengetahuan khusus yang diakumulasikan oleh E
A = Aims atau tujuan dari komunitas C dalam mengolah E
M = Metode atau kumpulan metode yang dapat digunakan dalam E

Beberapa karakteristik dari pseudosains adalah klaim yang berlebihan, kontradiktif, tidak dapat difalsifikasi, adanya bias konfirmasi, tidak terbuka, dan tidak menggunakan praktik sistematis (Mahayana, 2023). Salah satu cara yang dapat dilakukan untuk mengembangkan literasi sains serta meningkatkan pendidikan adalah mencegah dan menghindari pseudosains. Hal tersebut dapat dilakukan agar masyarakat tidak terjebak pada kepercayaan terhadap teori konspirasi secara berlebihan. Bidang kognitif Mario Bunge adalah salah satu kerangka kerja yang dapat diikuti agar penelitian yang dilakukan tidak menjadi pseudosains. Kerangka kerja bidang kognitif Mario Bunge yang memiliki rumus **E = (C, S, D, G, F, B, P, K, A, M)** membantu penulis dapat memahami metode, subjek, atau penelitian yang berkaitan dengan topik tertentu, termasuk dalam konteks keamanan data pada IoT.

1) Komunitas kognitif (C)
   Komunitas kognitif (C) akan mewakili komunitas peneliti, profesional, serta ahli yang berfokus pada memahami dan mengatasi tantangan keamanan di IoT. Komunitas peneliti terlihat dari banyaknya peneliti yang membahas mengenai topik keamanan data pada IoT. Berdasarkan metode SLR Kitchenham, pencarian otomatis mendapatkan 1978 paper yang relevan. Tahap berikutnya adalah melakukan seleksi dan membagi paper tersebut menjadi 3 kategori: review paper mengenai keamanan IoT (52 paper), keamanan IoT (854 paper), dan keamanan data multimedia pada IoT (35 paper). Pencarian secara manual mendapatkan 532 paper yang relevan. Pencarian tersebut difokuskan pada artikel berupa jurnal, terbit 5 tahun terakhir, dengan topik spesifik (*internet of things, computer network security, data privacy, security of data, cryptography, telecommunication security*).
2) Masyarakat (**S**)
   S mengacu pada konteks sosial yang lebih luas dalam mendukung komunitas kognitif. Hal ini termasuk lembaga, organisasi serta pemangku kepentingan yang terlibat dalam pengembangan, implementasi, dan regulasi teknologi IoT. Beberapa komunitas utama yang memiliki peran penting dalam ekosistem IoT adalah *International Telecomunication Union* (ITU), *Institute of Electrical and Electronics Engineers* (IEEE), *European Telecommunications Standars Institute* (ETSI), *Open Connectivity Foundation* (OCF), *National Institute of Standards and Technology* (NIST), dll.
3) Pandangan Umum (**G**)
   Komunitas kognitif umumnya berkomitmen untuk menjaga privasi, mengolah data dengan cara yang etis, dan mengamankan IoT untuk memastikan kendalan dari sistem tersebut.
4) Domain (**D**)
   Objek-objek yang dibahas melibatkan perangkat yang terhubung, jaringan, transmisi data, serta ekosistem dari IoT secara keseluruhan. Secara umum terdapat empat *layer* pada IoT yaitu, *sensing layer*, *middleware layer*, *network layer*, dan *application layer* (Hassija dkk., 2019), seperti yang terlihat pada g cxambar 3.



Gambar 3. Layer pada IoT (Hassija dkk., 2019)

5) Latar belakang formal (**F**)
Latar belakang formal mencakup logika dan matematika yang digunakan dalam melakukan analisis dan pengembangan protokol keamanan untuk IoT. Ini termasuk teknologi untuk meningkatkan keamanan, metode kriptografi, protokol keamanan jaringan, serta metode untuk melakukan verifikasi keamanan sistem IoT. Teknologi yang digunakan untuk meningkatkan keamanan adalah *blockchain*, *fog computing*, *edge computing*, dan *machine learning* (Hassija dkk., 2019). Penelitian menggunakan *blockchain* untuk meningkatkan kemanan data dilakukan untuk autentikasi sistem *smart home* (Lin dkk., 2020), mengamankan *pattern recognition* dan eksploitasi pada proses informasi multimedia (Ghazal dkk., 2022), mengamankan data privasi pasien pada sistem medis (Wu dkk., 2021). Teknologi *edge computing* digunakan pada pengamanan *framework* untuk aplikasi multimedia di jaringan 5G (Krishnan dkk., 2021), mengamankan layanan *Internet of Multimedia Things* (Xu dkk., 2021), mengamankan video *reporting* pada *vechicular network* (Zhong dkk., 2023), membuat framework berdasarkan autentikasi-agregasi-lokal diferensial privasi untuk IoMT (Usman dkk., 2020). Teknologi *machine learning* digunakan untuk mengamankan *microphone* pada perangkat *smart home* (Bhattacharya dkk., 2020), mengamankan suara pada aplikasi *voice assistant* (Y. Wang dkk., 2019), mengamankan sensor suara pada perangkat *mobile* (L. Wang dkk., 2023). Penelitian yang menggabungkan berbagai teknologi untuk meningkatkan keamanan data pada IoT juga dilakukan. Penelitian tersebut diantaranya adalah penggabungan *blockchain* dan *machine learning* dalam mengamankan data *image* pada bidang medis (Xiang dkk., 2023); *edge computing* dan *machine learning* dalam mengamankan data privasi berupa *image* (Fagbohungbe dkk., 2022), mengamankan data multimedia pasien (Xue dkk., 2021); serta kombinasi *blockchain* dan *fog computing* dalam mengamankan data multimedia pada IoT (Liang dkk., 2021).

6) Latar belakang khusus (**B**)
Latar belakang spesifik mencakup wawasan yang diambil dari bidang ilmu komputer, teknologi informasi, telekomunikasi jaringan, khususnya pengetahuan yang berkontribusi untuk memahami dan mengatasi masalah keamanan pada IoT. Metode khusus yang digunakan untuk meningkatkan keamanan diantaranya menggunakan *feature selection* untuk mendeteksi pola drone (Alsoliman dkk., 2023), *Convolutional Neural Networks* (CNNs) pada perintah *computer vision* (Lachtar dkk., 2023), algoritma *Motion Fusion* untuk mendeteksi objek pada aplikasi kamera (Aribilola dkk., 2023), *autoencoder* untuk mengamankan data privasi dan mengurangi *noise* pada data (Fagbohungbe dkk., 2022).

7) Problematika (**P**)
Salah satu masalah keamanan data IoT adalah cara melakukan identifikasi serangan sehingga dapat dicari solusi untuk menngatasi kerentanannya. Kerentanan seperti akses yang tidak sah, kerentanan perangkat, dan memastikan kerahasiaan dan integritas dari data adalah contoh dari kerentanan ini. Serangan yang banyak diteliti dikelompokkan menjadi beberapa tipe serangan, yaitu sebagai berikut.
   a) Serangan terhadap akses dan otentikasi berupa serangan *access control*, *guessing password*, *impersonation, priviledge-insider, spoofing, Man in the Middle, relay, replay,* dan *self-similarity*.
   b) Serangan terhadap data dan kriptografi berupa serangan *adversarial, chipertext, chosen-plaintext, cloning, crypto-analytical, data injection, differential, known-plaintext, malicious cropping, modification,* dan *morphing*.

c) Serangan terhadap jaringan dan layanan berupa serangan *brute force, Denial of Service, Distribution Denial of Service, jamming, remote hijacking*, dan *sinkhole*.
d) Serangan terhadap sensor dan data gambar berupa serangan *compression, cropping, histogram equalization, motion blur, noise, scaling, shearing,* dan *statistical*.
e) Serangan terhadap identitas pengguna berupa serangan *eavesdropping, social engineering, speaker recognition, stealthy*, dan *sybil*.

8) Pengetahuan (**K**)
Pengetahuan diwakilkan dengan temuan penelitian terbaru serta wawasan praktis yang relevan dalam mengamankan sistem IoT. Salah satu ciri dari penelitian ilmiah adalah keberlanjutan, bahwa topik tersebut masih relevan dan masih berkembang dalam beberapa waktu terakhir. Penelitian mengenai keamanan data IoT telah menemukan beberapa perkembangan, termasuk *framework Blockchain-based Medical Image Fusion* yang lebih efisien dan aman (Xiang dkk., 2023), metode *feature selection* untuk mengetahui *unprofiled drone* (Alsoliman dkk., 2023), pendeteksi *ransomware* dengan akurasi tinggi pada *platform* yang berbeda (Lachtar dkk., 2023).
9) Aims atau tujuan (**A**)
Tujuan dalam topik ini adalah mendorong ekosisten IoT yang aman, dapat diandalkan, menjamin privasi pengguna, serta dapat berkontribusi terkait keamanan data IoT.
10) Metode (**M**)
Metode ilmiah merupakan suatu siklus pengamatan, pertanyaan, hipotesis, eksperimen, analisis, dan kesimpulan yang berkelanjutan (Mahayana, 2022). Berbeda dengan penelitian pada bidang sosial yang biasanya menggunakan pendekatan kualitatif dan kuantitatif, penelitian di bidang ini dapat menggunakan pendekatan *Design Research Methodology* (DRM) atau *Design Science Research Methodhology* (DSRM). Tahapan yang perlu dilakukan pada DRM yaitu *Research Clarification, Descriptive Study I, Prescriptive Study,* dan *Descriptive Study II* (Blessing & Chakrabarti, 2009). Tahapan yang perlu dilakukan pada DSRM terdiri dari lima tahap, yaitu desain konseptual, membangun arsitektur sistem, menganalisis desain, membuat prototype (termasuk pengembangan produk), dan evaluasi (Brocke dkk., 2020).

b. Filosofi Penelitian dan Bawang Penelitian

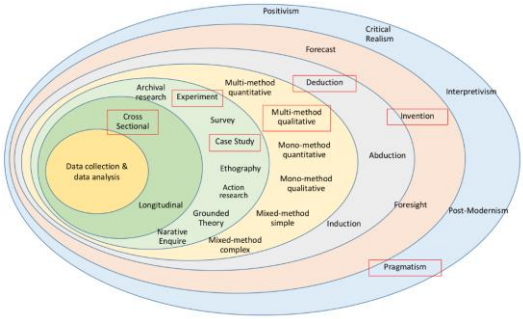
Setidaknya terdapat lima filosofi penelitian/paradigma dalam filsafat sains, yaitu *logical positivism*, *critical realism*, *interpretivism*, *post-modernism*, dan *pragmatism* (Mahayana, 2022). Kelima filosofi dasar tersebut digunakan untuk mencari realitas dalam bidang sains. Uraian berikut merupakan refleksi dalam kelima paradigma tersebut.

1) Paradigma *Logical Positivism* menekankan adanya hal yang nyata, independen, dan terdapat realitas tunggal. Hal tersebut membuat pentingnya mengukur dan memverifikasi setiap langkah dalam proses pengembangan metode keamanan. Data yang dapat diverifikasi dan diukur secara empiris dianggap sebagai data yang benar.
2) Paradigma *Critical Realism* menyarankan bahwa terdapat realitas yang harus dihadapi, sehingga penulis perlu mempertimbangkan berbagai keragaman perspektif dan pemahaman tentang keamanan data. Hal ini mencakup pertimbangan etika, sosial, dan budaya yang berbeda dalam tiap pengembangan metode keamanan.
3) Paradigma *Interpretivism* menyoroti masalah yang kompleks, sosial, dan bagaimana pemahaman individu tentang keamanan data dapat bervariasi berdasarkan konteks dan pengalaman masyarakat. Penulis perlu membuat pendekatan yang lebih berfokus pada pengembangan metode yang dapat disesuaikan dengan berbagai persepsi dan pemahaman tiap pengguna.
4) Paradigma *Post-modernism* menekankan bagaimana konsep keamanan itu sendiri adalah konstruksi sosial yang dipengaruhi oleh kekuatan, budaya, dan bahasa. Hal tersebut akan mendorong pemikiran kritis tentang bagaimana kekuatan dan bahasa mempengaruhi definisi dan implementasi keamanan data multimedia.
5) Paradigma *Pragmatism* menekankan pentingnya mengembangkan metode yang efektif dan dapat diterapkan dalam situasi nyata. Pragmatisme akan mendukung penelitian dan pengembangan metode keamanan yang fokus pada hasil konkret dan manfaat yang dapat diberikan kepada pengguna.

Paradigma penelitian yang akan digunakan cenderung menggabungkan beberapa paradigma. Ini akan mencerminkan kompleksitas dan interdisiplinaritas dari topik tersebut. Paradigma penelitian yang lebih mendekati dalam topik keamanan data IoT ini mungkin adalah

paradigma interpretif dengan elemen dari paradigma pragmatisme. Paradigma *Interpretivism* relevan dalam konteks keamanan data multimedia karena menekankan pemahaman makna subjektif yang diberikan oleh individu, yaitu pengguna. Pengembangan metode keamanan memerlukan pemahaman bagaimana nilai, etika, dan perspektif pengguna memengaruhi pemahaman keamanan dan implementasi praktisnya. Paradigma *Pragmatism* dapat mencerminkan fokus pada hasil yang berguna dan praktis dalam pengembangan metode keamanan. Keamanan data IoT harus memenuhi kebutuhan praktis pengguna, sehingga paradigma pragmatisme relevan untuk menghasilkan solusi yang efektif. Pergeseran paradigma penelitian dalam topik ini mungkin telah terjadi seiring perkembangan teknologi dan pemahaman tentang keamanan data di IoT. Awalnya, paradigma penelitian mungkin lebih cenderung positivistis, dengan fokus pada pengukuran dan verifikasi empiris. Seiring dengan munculnya isu-isu etika, privasi, dan kompleksitas sosial dalam IoT, paradigma interpretif dan realisme kritis menjadi semakin mendominasi.

Secara umum, kelima filosofi penelitian tersebut memberikan kriteria untuk membedakan antara sains dan pseudosains. Pseudosains dianggap tidak ilmiah karena tidak memenuhi kriteria-kriteria tersebut, seperti verifiability, koherensi, interpretasi, realitas objektif, dan kegunaan. Mario Bunge mendefinisikan pseudosains sebagai "sekelompok kepercayaan yang tidak ilmiah karena tidak dapat diverifikasi, koheren, atau berguna." Bunge mengkritik pseudosains karena menyesatkan dan berbahaya, dan dia menyerukan untuk mempromosikan sains dan pemikiran kritis. Kelima filosofi penelitian yang disebutkan di atas dapat digunakan untuk menilai apakah suatu sistem kepercayaan merupakan pseudosains. *Logical positivism* menekankan pada *verifiability, critical realism* menekankan pada koherensi, *interpretivism* menekankan pada interpretasi, post-modernism mempertanyakan konsep realitas dan kebenaran, dan pragmatism menekankan pada kegunaan. Jika suatu sistem kepercayaan tidak memenuhi kriteria-kriteria tersebut, maka kemungkinan besar itu adalah pseudosains.



Gambar 4. Bawang Penelitian

Penjelasan tersebut dapat direpresentasikan dalam visualisasi lain, yaitu ”bawang penelitian” (Mahayana, 2022). Visualisasi tersebut memperlihatkan beberapa pendekatan baru yang disesuaikan berdasarkan konteks dari penelitian yang dilakukan. Bawang penelitian ini dapat menghubungkan filsafat sains dengan kerangka kerja saintifik yang digunakan. Visualisasi dari bawang penelitian pada topik ini diperlihatkan pada gambar 4.

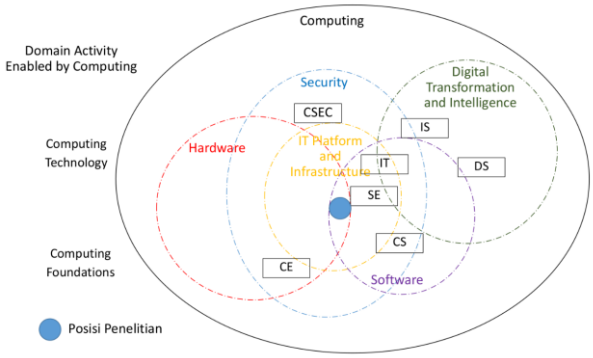
c. Posisi Penelitian

Domain Activity Enabled by Computing merujuk pada suatu area penelitian yang melibatkan aktivitas atau kegiatan yang dimungkinkan dalam bidang komputasi. Penelitian dalam domain keamanan data IoT ini dapat dianggap bukan pseudosains jika memenuhi kriteria ilmiah yang diakui. Posisi penelitian pada topik ini mengacu pada ACM Computing Curricula 2020. ACM Computing Curricula 2020 adalah panduan kurikulum resmi yang dikeluarkan oleh Association for Computing Machinery (ACM) untuk pendidikan dalam bidang ilmu komputer. Domain Activity Enabled by Computing (DAEC) merupakan salah satu domain dalam kurikulum tersebut, dan penelitian yang dilakukan dalam domain ini lebih mementingkan kegiatan yang dapat diwujudkan dalam bidang komputasi (CC2020 Task Force, 2021).

Penelitian di dalam domain kegiatan yang dimungkinkan oleh komputasi diharapkan mengikuti metodologi ilmiah yang ketat. Ini termasuk pembentukan hipotesis yang dapat diuji, pengumpulan data, analisis data, dan pengambilan kesimpulan berdasarkan bukti empiris. Pseudosains seringkali sulit atau bahkan tidak mungkin direproduksi. Penelitian di DAEC,

sebagaimana dicontohkan oleh Computing Curricula 2020, seharusnya dapat direproduksi oleh peneliti lain. Ini menciptakan dasar yang kuat untuk membedakan antara penelitian ilmiah dan pseudosains. Penelitian di dalam DAEC akan memberikan kontribusi yang signifikan terhadap pemahaman tentang kegiatan yang dimungkinkan dalam ranah komputasi. Penelitian semacam itu diakui oleh komunitas ilmiah dan dapat membantu mengembangkan teori atau praktik yang terkait dengan perkembangan di bidang komputasi. Pseudosains sering kali tidak memenuhi standar validitas dan kredibilitas. Penelitian di DAEC diharapkan mematuhi standar-standar ini, termasuk penggunaan metode penelitian yang sesuai dan publikasi hasil penelitian dalam jurnal-jurnal yang diakui oleh komunitas ilmiah.

Penelitian di DAEC diarahkan pada aktivitas yang dimungkinkan dalam ranah komputasi, yang mencakup berbagai bidang seperti perangkat keras, perangkat lunak, infrastruktur IT, transformasi digital dan kecerdasan, dan dalam bidang keamanan. Keberadaan keterkaitan yang jelas dengan bidang komputasi membantu menegaskan bahwa penelitian tersebut relevan dan sah. Dalam penelitian ilmiah DAEC, rekan sejawat akan menilai dan memvalidasi kualitas dan relevansi penelitian. Ini adalah langkah penting dalam mengidentifikasi penelitian yang sah dan mencegah pseudosains. Gambar 5 menunjukkan posisi penelitian dengan topik keamanan data pada IoT berdasarkan DAEC yang mengacu pada ACM Computing Curricula 2020. Penelitian yang dilakukan berada di dalam domain *security* dan infrastruktur yang juga mencakup *hardware* dan *software*.



Gambar 5. Posisi penelitian

4. Simpulan dan Saran

Artikel ini membahas tentang keamanan data dalam Internet of Things (IoT) dengan menggunakan perspektif pseudosains Mario Bunge. Penelitian ini menunjukkan bahwa keamanan data menjadi perhatian utama dalam IoT. Pertama, artikel ini mengidentifikasi dan mengevaluasi potensi kerentanan dan ancaman terhadap data, risiko peretasan, dan kebutuhan enkripsi data. Langkah selanjutnya, artikel ini menganalisis metode dan strategi keamanan yang umum digunakan dalam IoT, seperti blockchain, fog computing, edge computing, dan machine learning. Pendekatan pseudosains Bunge membantu dalam memahami dan menganalisis keamanan data IoT secara komprehensif. Hasilnya menunjukkan pemahaman yang lebih dalam tentang tantangan keamanan data di IoT, serta rekomendasi terperinci untuk mitigasi risiko. Artikel ini menekankan pentingnya pendekatan holistik yang memadukan aspek teknis dan filosofis untuk mengatasi masalah keamanan data di IoT. Perspektif pseudosains membantu dalam mengembangkan kerangka konseptual yang kokoh dan mendorong pemikiran kritis dalam merumuskan strategi keamanan data IoT yang efektif. Artikel ini memberikan kontribusi penting dalam memahami dan mengatasi kompleksitas keamanan data di IoT. Keamanan data IoT adalah bidang yang kompleks dan terus berkembang, bidang ini didasarkan pada prinsip-prinsip ilmiah yang kokoh, diantaranya kriptografi, jaringan dan keamanan komputer, serta teori informasi. Kesimpulan yang didapat, keamanan data IoT tidak diklasifikasikan sebagai pseudosains dalam perspektif Mario Bunge.

5. Daftar Pustaka

Al-Ghaili, A. M., Gunasekaran, S. S., Jamil, N., Alyasseri, Z. A., Al-Hada, N. M., Ibrahim, Z.-A., Bakar, A. A., Kasim, H., Hosseini, E., Omar, R., Kasmani, R. Md., & Razali, R. A. (2023).

A Review on Role of Image Processing Techniques to Enhancing Security of Iot Applications. *IEEE Access*, 1–1. https://doi.org/10.1109/access.2023.3312682.

Alsoliman, A., Rigoni, G., Callegaro, D., Levorato, M., Pinotti, C. M., & Conti, M. (2023). Intrusion Detection Framework for Invasive FPV Drones Using Video Streaming Characteristics. *ACM Transactions on Cyber-Physical Systems*, *7*(2). https://doi.org/10.1145/3579999.

Aribilola, I., Asghar, M. N., Kanwal, N., Fleury, M., & Lee, B. (2023). SecureCam: Selective Detection and Encryption Enabled Application for Dynamic Camera Surveillance Videos. *IEEE Transactions on Consumer Electronics*, *69*(2), 156–169. https://doi.org/10.1109/TCE.2022.3228679.

Arisdakessian, S., Wahab, O. A., Mourad, A., Otrok, H., & Guizani, M. (2023). A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions. *IEEE Internet of Things Journal*, *10*(5), 4059–4092. https://doi.org/10.1109/JIOT.2022.3203249.

Bhattacharya, S., Manousakas, Di., Ramos, A. G. C. P., Venieris, S. I., Lane, N. D., & Mascolo, C. (2020). Countering Acoustic Adversarial Attacks in Microphone-equipped Smart Home Devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *4*(2). https://doi.org/10.1145/3397332.

Blessing, L. T. M., & Chakrabarti, A. (2009). *DRM, a Design Research Methodology*. Springer.

Brocke, J. vom, Hevner, A., & Maedche, A. (2020). Design Science Research. *Springer*. https://doi.org/10.1201/b16768-26.

Bunge, M. (1983). What Is Pseudoscience? *The Skeptical Inquirer*, *9*, 36–46.

Burhan, M., Alam, H., Arsalan, A., Rehman, R. A., Anwar, M., Faheem, M., & Ashraf, M. W. (2023). A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-Based IoT Applications: Layered Architecture, Real-Time Security Issues, and Solutions. *IEEE Access*, *11*, 73303–73329. https://doi.org/10.1109/ACCESS.2023.3294479.

CC2020 Task Force. (2021). Computing Curricula 2020. Paradigms for Global Computing Education. Dalam *Computing Curricula 2020*. https://dl.acm.org/doi/book/10.1145/3467967.

Duarte, F. (2023). *Number of IoT Devices (2023)*. Exploding Topics. https://explodingtopics.com/blog/number-of-iot-devices.

Fagbohungbe, O., Reza, S. R., Dong, X., & Qian, L. (2022). Efficient Privacy Preserving Edge Intelligent Computing Framework for Image Classification in IoT. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *6*(4), 941–956. https://doi.org/10.1109/TETCI.2021.3111636.

Ghazal, T. M., Hasan, M. K., Abdallah, S. N. H., & Abubakkar, K. A. (2022). Secure IoMT Pattern Recognition and Exploitation for Multimedia Information Processing using Private Blockchain and Fuzzy Logic. *ACM Transactions on Asian and Low-Resource Language Information Processing*. https://doi.org/10.1145/3523283.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. Dalam *IEEE Access* (Vol. 7, hlm. 82721–82743). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2924045.

Kemp, S. (2023). *Digital 2023: Global Overview Report*. Data Reportal. https://datareportal.com/reports/digital-2023-global-overview-report.

Kitchenham, B. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. https://www.researchgate.net/publication/302924724.

Krishnan, P., Jain, K., Jose, P. G., Achuthan, K., & Buyya, R. (2021). SDN Enabled QoE and Security Framework for Multimedia Applications in 5G Networks. *ACM Transactions on Multimedia Computing, Communications and Applications*, *17*(2). https://doi.org/10.1145/3377390.

Lachtar, N., Ibdah, D., Khan, H., & Bacha, A. (2023). RansomShield: A Visualization Approach to Defending Mobile Systems Against Ransomware. *ACM Transactions on Privacy and Security*, *26*(3). https://doi.org/10.1145/3579822.

Liang, H., Wu, J., Zheng, X., Zhang, M., Li, J., & Jolfaei, A. (2021). Fog-Based Secure Service Discovery for Internet of Multimedia Things: A Cross-Blockchain Approach. *ACM Transactions on Multimedia Computing, Communications and Applications*, *16*(3s). https://doi.org/10.1145/3415151.

Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. R. (2020). HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. *IEEE Internet of Things Journal*, *7*(2), 818–829. https://doi.org/10.1109/JIOT.2019.2944400.

Mahayana, D. (2022). *Filsafat Sains: Dari Newton, Einstein hingga Sains-Data* (E. Warsidi, Ed.). ITB Press.

Mahayana, D. (2023). *Pseudoscience, Big Data Analytics & Artificial Intelligence*. Paper presented at lecturer for Filsafat Sains, STEI ITB.

Usman, M., Jan, M. A., & Puthal, D. (2020). PAAL: A Framework Based on Authentication, Aggregation, and Local Differential Privacy for Internet of Multimedia Things. *IEEE Internet of Things Journal*, *7*(4), 2501–2508. https://doi.org/10.1109/JIOT.2019.2936512

Wang, L., Chen, M., Lu, L., Ba, Z., Lin, F., & Ren, K. (2023). VoiceListener: A Training-free and Universal Eavesdropping Attack on Built-in Speakers of Mobile Devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *7*(1). https://doi.org/10.1145/3580789.

Wang, Y., Cai, W., Gu, T., Shao, W., Li, Y., & Yu, Y. (2019). Secure your voice: An Oral Airflow-Based Continuous Liveness Detection for Voice Assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *3*(4). https://doi.org/10.1145/3369811.

Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. *ACM Transactions on Multimedia Computing, Communications and Applications*, *17*(2s). https://doi.org/10.1145/3408321

Xiang, T., Zeng, H., Chen, B., & Guo, S. (2023). BMIF: Privacy-preserving Blockchain-based Medical Image Fusion. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *19*(1). https://doi.org/10.1145/3531016.

Xu, X., Huang, Q., Zhang, Y., Li, S., Qi, L., & Dou, W. (2021). An LSH-based Offloading Method for IoMT Services in Integrated Cloud-Edge Environment. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *16*(3s). https://doi.org/10.1145/3408319.

Xue, Z., Zhou, P., Xu, Z., Wang, X., Xie, Y., Ding, X., & Wen, S. (2021). A Resource-Constrained and Privacy-Preserving Edge-Computing-Enabled Clinical Decision System: A Federated Reinforcement Learning Approach. *IEEE Internet of Things Journal*, *8*(11), 9122–9138. https://doi.org/10.1109/JIOT.2021.3057653.

Zhong, H., Wang, L., Cui, J., Zhang, J., & Bolodurina, I. (2023). Secure Edge Computing-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks. *IEEE Transactions on Information Forensics and Security*, *18*, 3774–3786. https://doi.org/10.1109/TIFS.2023.3287731.