JUTIS (Jurnal Teknik Informatika Unis)
Vol. 13 No. 2 Bulan November 2025 **p-ISSN: 2252-5351**
Program Studi Teknik Informatika – Fakultas Teknik **e-ISSN: 2656-0860**
Universitas Islam Syekh-Yusuf Tangerang

Strategi Keamanan Data di Era Transformasi Digital: Tantangan Cloud Computing, Internet of Things, dan Blockchain

Nabila Nurasyifa[1], Farwah Assyifaurrohmah[2], Daffa Wahid sya'bani[3]
[123]Informatika, Sains dan Teknologi, UIN Sultan Maulana Hasanudin Banten, 42171

aan.ansori@uinbanten.ac.id [1], Asyifan707@gmail.com [2], aestheticpple@gmail.com[3], wahiddaffa332@gmail.com[4]

Abstrak
Melalui penggunaan teknologi seperti blockchain, cloud computing, dan Internet of Things (IoT), transformasi digital telah sepenuhnya mengubah cara data dikelola, diakses, dan disimpan. Teknologi ini memberikan kemudahan dan efisiensi, tetapi juga menimbulkan risiko keamanan data yang signifikan. Meskipun cloud computing memfasilitasi penyimpanan dan akses data, ada risiko yang mungkin saja terjadi, termasuk potensi serangan siber, dan hilangnya kendali atas data. Dengan jaringan perangkat yang terhubung, Internet of Things rentan terhadap risiko eksploitasi perangkat, akses ilegal, dan serangan fisik dan digital yang dapat membahayakan data pengguna. Blockchain menyediakan solusi keamanan berbasis kriptografi terdesentralisasi yang dapat menjaga transparansi transaksi dan integritas data, tetapi masih rentan terhadap masalah serangan sampai 51%. Terlepas dari keamanan teknologi.. Untuk mengatasi risiko yang dapat mengancam keamanan data, dengan menggunakan metodologi deskriptif studi ini membahas sejumlah teknik mitigasi, termasuk kontrol akses yang ketat, enkripsi data, pemantauan infrastruktur, dan penerapan teknologi blockchain. Individu dan organisasi dapat melindungi data dari penyalahgunaan dan mendorong pengelolaan yang bertanggung jawab dengan menerapkan langkah-langkah tersebut dan memiliki pemahaman yang menyeluruh tentang bahayanya. keberlanjutan Teknologi digital yang aman bergantung pada strategi terintegrasi yang menggabungkan edukasi pengguna, implementasi kebijakan privasi, dan penguatan teknologi. Studi ini menyoroti betapa pentingnya inovasi dalam keamanan dan kepatuhan untuk mengatasi masalah-masalah di dunia digital yang semakin rentan keamanannya.

Kata kunci: *Blockchain, cloud computing, keamanan data, transformasi digital Internet of Things.*

A. Pendahuluan

Data telah muncul sebagai salah satu sumber daya paling berharga yang menggerakkan banyak aspek kehidupan di era transformasi digital, termasuk pemerintahan, industri, dan pendidikan. Teknologi seperti *blockchain, Cloud Computing, dan Internet of Things (IoT)* telah sepenuhnya mengubah cara data dikelola, diakses, dan disimpan. Efisiensi dan kenyamanan dihasilkan oleh perubahan ini, namun terdapat juga masalah signifikan terkait keamanan data, privasi, dan pertahanan terhadap kemungkinan ancaman siber. Mengingat pesatnya perkembangan teknologi digital memerlukan langkah-langkah mitigasi yang cerdas dan efisien untuk menjaga kepercayaan masyarakat terhadap teknologi, maka arti penting tema ini menjadi semakin relevan.

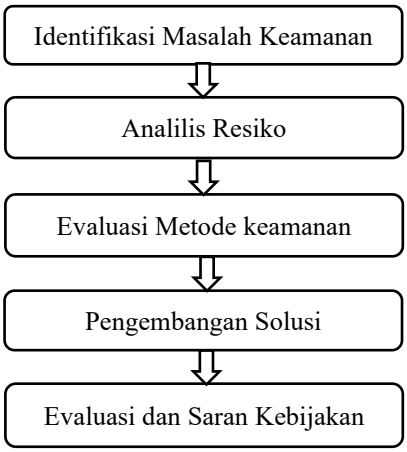
Setiap teknologi memiliki kelemahan keamanan meskipun faktanya memberikan sejumlah kemudahan. Misalnya, *cloud computing* menyimpan data di server jauh yang rentan terhadap peretasan, kebocoran data, dan kehilangan data. Karena jaringan perangkatnya yang luas, *IoT* menimbulkan bahaya tambahan, termasuk kemungkinan eksploitasi perangkat dan akses yang tidak diinginkan. Bahkan *blockchain*, yang sering dianggap sebagai teknologi aman, rentan terhadap masalah seperti skalabilitas dan serangan 51%. Menurut data literatur, 74% bisnis yang menggunakan komputasi awan memiliki masalah keamanan data. Publikasi lain menunjukkan bahwa potensi pelanggaran keamanan serius meningkat dengan adanya lebih dari 25 miliar perangkat *IoT* yang terhubung.

Sejumlah penelitian sebelumnya telah berusaha memberikan jawaban teoretis terhadap masalah keamanan ini. Beberapa taktik terpenting yang berhasil dengan baik untuk menjaga data dalam cloud computing adalah pemantauan infrastruktur, aturan akses yang ketat, dan enkripsi data. Namun, pengembangan metode keamanan berbasis kriptografi dan penggunaan otentikasi biometrik sangat penting untuk mengurangi bahaya dalam *blockchain* dan *Internet of Things*. Menurut penelitian utama, metode desentralisasi seperti *blockchain* dapat meningkatkan integritas data hingga 95%; namun demikian, mereka masih perlu diperbaiki untuk mengatasi kekurangannya.

Studi ini menyarankan strategi terintegrasi sebagai konsep solusi yang mencakup pendidikan pengguna, peraturan privasi yang ketat, dan peningkatan teknologi keamanan. Tujuan dari langkah ini adalah untuk menciptakan lingkungan digital yang lebih aman dan andal. Dengan menggunakan teknik dan teknologi enkripsi mutakhir *seperti Google Cloud Platform (GCP),* strategi ini memberikan solusi yang bisa diterapkan luas. Tujuan studi ini adalah untuk membuat daftar permasalahan keamanan data utama di era transformasi digital, menilai kebijakan dan teknologi saat ini, dan memberikan saran mengenai teknik mitigasi yang bisa diterapkan dan berbasis bukti. Tujuan dari studi ini adalah untuk membantu keberlanjutan transformasi digital yang inklusif dan tepercaya dengan memberikan panduan kepada individu dan organisasi mengenai pengelolaan data yang aman dan bertanggung jawab.

B. Metode

Studi ini dilakukan dengan menggunakan metodologi deskriptif yang fokus pada langkah-langkah konkret untuk mengidentifikasi dan mengatasi isu keamanan data di zaman revolusi digital. Menemukan berbagai masalah keamanan yang dihadapi oleh teknologi penting seperti *blockchain, Cloud Computing*, *dan Internet of Things (IoT)* adalah langkah pertama. Untuk menilai risiko tertentu, seperti serangan siber, dan pencurian data yang sering muncul dalam penggunaan teknologi ini, informasi dikumpulkan dari studi kasus dan literatur.



Gambar 1. Alur metode penelitian

Setelah identifikasi masalah, penelitian ini menilai berbagai metode keamanan dan teknologi yang telah diterapkan. Menerapkan enkripsi data, kontrol akses, dan pemantauan arsitektur server yang dapat menghentikan akses yang tidak diinginkan merupakan topik utama diskusi dalam *cloud computing*. Di sisi lain, analisis *IoT* berkonsentrasi pada bahaya kerentanan perangkat terhadap serangan digital dan fisik, serta strategi mitigasi seperti enkripsi dan otentikasi. Studi ini menekankan pada bahaya yang mungkin terjadi, dan manfaat teknologi *blockchain* dalam hal keamanan melalui desentralisasi dan kriptografi.

Mengembangkan teknik mitigasi untuk mengurangi ancaman keamanan yang teridentifikasi adalah langkah selanjutnya. Menerapkan standar keamanan terbaik, seperti *firewall* yang ketat, *enkripsi end-to-end,* dan otentikasi berbasis biometrik, adalah salah satu dari taktik ini. Untuk menjamin ketersediaan layanan yang berkelanjutan, penelitian ini juga merekomendasikan konfigurasi arsitektur server yang lebih aman, yang mencakup penggunaan penyeimbang beban dan *failover* pada platform cloud. Selain itu, sejumlah situasi terkait digunakan untuk menerapkan metode keamanan yang diusulkan. Misalnya, infrastruktur server berbasis cloud yang aman diimplementasikan dengan menggunakan fitur keamanan *Google Cloud Platform (GCP*) seperti enkripsi data dan penskalaan otomatis. Fitur keamanan tambahan seperti pemantauan waktu nyata digunakan dalam sistem *IoT* untuk mengidentifikasi aktivitas yang meragukan pada perangkat yang terhubung. Untuk memastikan mekanisme mitigasi berjalan efektif, penerapannya dievaluasi dengan menggunakan simulasi serangan.

C. Hasil dan Pembahasan

Keamanan Data di Era Transformasi Digital

Melalui penggunaan teknologi kontemporer seperti komputasi awan, *Internet of Things (IoT), dan blockchain,* era transformasi digital telah mengubah cara kita menyimpan, mengakses, dan mengelola data. Kenyamanan dan efisiensi adalah manfaat dari

perubahan ini, tetapi masalah keamanan data juga harus diselesaikan untuk memastikan keselamatan dan keamanan informasi. Data pengguna dalam *cloud computing* disimpan di server jauh yang dapat diakses secara online. Meskipun hal ini memudahkan untuk diakses dari lokasi mana pun, keamanan data menjadi masalah yang signifikan karena berbagai pihak dapat mengakses data tersebut melalui jaringan internet, yang rentan terhadap serangan siber. Sebagai contoh, orang yang tidak berwenang dapat mengakses data sensitif jika kontrol aksesnya lemah. Selain itu, privasi dan kepatuhan merupakan masalah penting saat menggunakan *cloud*, seperti halnya kompatibilitas aplikasi, ketersediaan layanan, kehilangan data, dan kerentanan terhadap serangan *GCP*, yang menawarkan sejumlah fitur keamanan seperti pengaturan akses, enkripsi data, dan pemantauan keamanan, merupakan salah satu langkah mitigasi yang dapat digunakan untuk mengurangi risiko ini. Menerapkan praktik terbaik keamanan, seperti konfigurasi firewall yang ketat, penggunaan HTTPS, dan manajemen akses terbatas, juga penting untuk aplikasi ini. Komponen penting dari solusi ini adalah pengelolaan dan pemantauan infrastruktur server.

Sementara itu, *di Internet of Things (IoT),* keamanan data menghadapi tantangan tambahan karena *IoT* terdiri dari jaringan perangkat yang saling terhubung yang sering kali memiliki sumber daya terbatas untuk mengimplementasikan enkripsi dan kontrol keamanan. Perangkat-perangkat ini, mulai dari sensor di pabrik hingga perangkat pintar di rumah, sering kali tidak dirancang dengan lapisan keamanan yang kuat dan mudah diakses tanpa izin. Akibatnya, banyaknya entitas dan data yang terlibat membuat *IoT* terekspos pada risiko keamanan yang dapat mengancam dan membahayakan konsumen.

Bahaya ini terutama berbentuk membantu serangan terhadap sistem lain, membahayakan keselamatan pengguna, dan memungkinkan orang yang tidak berwenang untuk mengakses data dan menyalahgunakan informasi pribadi. *IoT* juga rentan terhadap serangan yang berfokus pada konektivitas atau kerentanan perangkat. Informasi yang dikumpulkan pada perangkat *IoT* dapat dicuri jika berhasil disusupi. *Blockchain* menjadi pilihan keamanan yang semakin disukai, terutama dalam hal menangani dan menjaga informasi pribadi. Teknik ini menggunakan kriptografi untuk menjaga integritas data, menghasilkan sistem penyimpanan yang transparan dan aman. Sangat sulit untuk mengubah data pada *blockchain* tanpa diketahui karena setiap transaksi dan modifikasi data didokumentasikan dalam blok-blok yang terikat satu sama lain. Akan tetapi, *blockchain* tidak bebas dari risiko selalu ada kekhawatiran mengenai kemungkinan serangan terhadap keamanan jaringan *blockchain,* seperti serangan 51%, dimana satu pihak dapat mengambil alih sebagian besar jaringan.

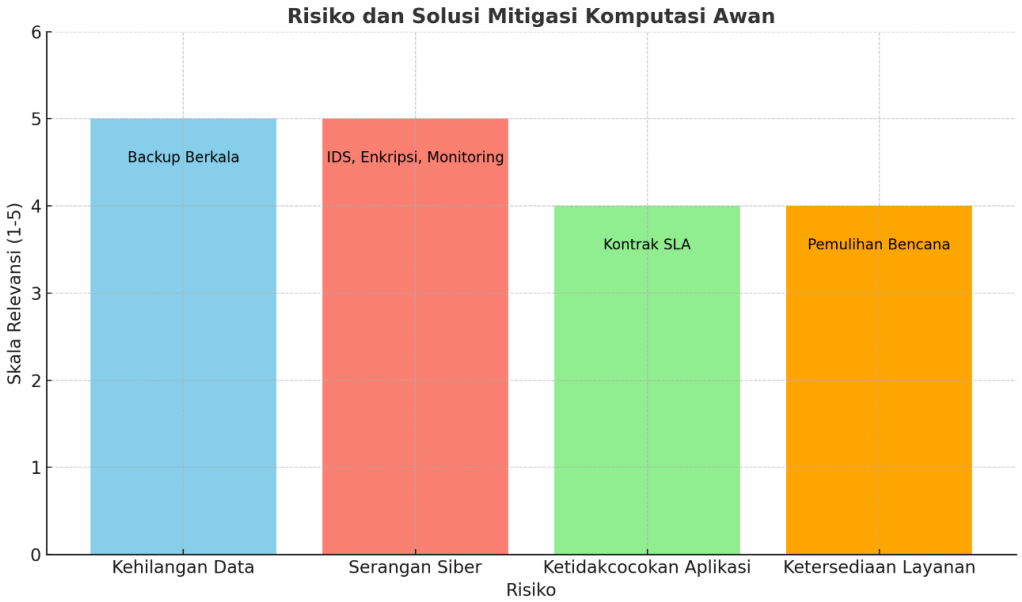
Tantangan keamanan dalam cloud computing

Kombinasi teknologi komputer (komputasi) dan pengembangan berbasis Internet (awan) dikenal sebagai *cloud computing*. *cloud computing* adalah teknik komputer di mana fitur-fitur yang berhubungan dengan teknologi informasi ditawarkan sebagai layanan, yang memungkinkan pelanggan untuk mengaksesnya secara online. Bagi banyak bisnis dan orang-orang *cloud computing* telah muncul sebagai pilihan utama untuk penyimpanan dan akses data. Aksesibilitas dan kemampuan beradaptasi *cloud computing* membuatnya

menjadi pilihan yang populer bagi para konsumennya, namun seiring dengan semakin populernya *cloud computing* sejumlah masalah keamanan data baru juga bermunculan. Risiko keamanan yang membahayakan privasi data yang disimpan di cloud semakin meningkat di era digital saat ini. Cara bisnis dan individu menyimpan dan mengakses data telah berubah secara signifikan di era digital saat ini. Meskipun *cloud computing* membuat penyimpanan data dan akses jarak jauh menjadi sederhana dan efektif, *cloud computing* juga menimbulkan risiko baru terhadap keamanan data. Baik individu maupun perusahaan harus menyadari risiko ini dan mengetahui cara melindungi data mereka, pengguna *cloud computing* sangat memperhatikan keselamatan dan keamanan data mereka. Oleh karena itu, sangat penting untuk memastikan bahwa *cloud computing* aman.

Ada sejumlah bahaya yang terkait dengan penyimpanan data *cloud computing* seperti kompatibilitas aplikasi, ketersediaan layanan, kehilangan data, dan kerentanan terhadap serangan. Karena data yang disimpan di *cloud* sering kali berisi informasi sensitif dan berharga, seperti data pelanggan, perusahaan, dan pribadi, keamanan *cloud computing* menjadi perhatian penting. Klien yang menggunakan layanan *cloud* perlu memiliki keyakinan bahwa penyedia layanan cloud akan melindungi ketersediaan, kerahasiaan, dan integritas data mereka. Kemungkinan pencurian data, kejahatan siber, dan aktivitas yang merugikan pengguna lainnya adalah salah satu kekhawatiran yang terkait dengan *cloud computing* Sistem yang kemungkinan besar menyimpan data sensitif dari pelanggan *cloud computing* akan diserang oleh peretas.

Oleh karena itu, sangat penting untuk memahami ancaman terhadap keamanan data saat menggunakan *cloud computing* Pengguna dapat meningkatkan keamanan data mereka di lingkungan *cloud computing* dan melindunginya dari potensi risiko keamanan dengan menggunakan prosedur keamanan yang tepat. Karena keserbagunaan dan keefektifannya dalam manajemen dan penyimpanan data, *cloud computing* semakin populer dalam beberapa tahun terakhir. Namun, ada masalah dengan keamanan data yang disimpan dalam database *cloud computing*. Berikut resiko dan mitigasi dari *cloud computing*.



Gambar 2. Grafik risiko dan solusi mitigasi cloud computing

Serangan, kehilangan data, kehilangan kendali atas data, ketersediaan layanan, dan kompatibilitas aplikasi merupakan risiko yang terkait dengan penggunaan *cloud computing*. Oleh karena itu, teknik mitigasi berikut ini dapat digunakan untuk mengurangi risiko-risiko tersebut :

1. Keamanan yang kuat : Untuk melindungi data dari ancaman internal dan eksternal, buatlah langkah-langkah keamanan yang ketat, enkripsi data, dan pantau dengan cermat izin akses pengguna.
2. Penyimpanan cadangan yang efisien : Untuk mengatasi potensi kehilangan data, buatlah cadangan data Anda secara teratur dan simpan di lokasi yang aman.
3. Kontrak yang tidak ambigu : Buatlah kontrak terperinci dengan penyedia layanan komputasi awan yang mencakup topik-topik seperti ketersediaan layanan, pemulihan bencana, dan kebijakan privasi.
4. Pemantauan aktif : Mengawasi lingkungan komputasi awan untuk mengidentifikasi risiko atau modifikasi apa pun yang dapat membahayakan keamanan dan kelangsungan layanan.
5. Pemulihan bencana : Ciptakan strategi pemulihan bencana menyeluruh yang mencakup protokol pemulihan, pengujian yang sering dilakukan, dan pemulihan cepat jika terjadi keadaan darurat.
6. Pendidikan dan pelatihan : Berikan instruksi yang cukup kepada pengguna komputasi awan untuk membantu mereka memahami bahaya dan langkah-langkah yang perlu dilakukan untuk mengatasinya.

Ketika kita menyimpan file yang akan dipindahkan ke basis data online, seperti yang sering dilakukan akhir-akhir ini dengan menyimpan data di email, *Google Drive, atau Dropbox*, kita sering mengalami keterbatasan dalam penyimpanan data. Pendekatan ini sering disarankan untuk meredakan kekhawatiran akan kehilangan data dengan melakukan hal ini,

kita dapat merasa tenang karena memiliki data cadangan yang tersimpan di *Dropbox, Google Drive*, dan email Suryati et al., (2019). Menurut Haynes J. (2014), keamanan sistem informasi dan keamanan siber mencakup tujuan-tujuan berikut :

1. Kerahasiaan : Menjunjung tinggi batasan hukum tentang akses dan pengungkapan informasi, termasuk strategi untuk melindungi data hak milik dan privasi individu. Integritas: Mencegah perubahan atau penghancuran informasi yang tidak benar, serta menjamin keabsahan informasi dan tidak adanya penyangkalan.
2. Ketersediaan : Memastikan akses yang cepat dan dapat diandalkan untuk penggunaan informasi. M. Nieles, (2017)
3. Otentikasi : Mengonfirmasi identitas pengguna, proses, atau perangkat, sering kali sebagai prasyarat untuk memberikan akses ke sumber daya informasi.
4. Non-repudiasi : Perlindungan terhadap individu yang telah dengan tulus dan ikhlas melakukan tindakan tertentu. Memberikan kemampuan untuk menentukan apakah individu tertentu mampu melakukan tindakan yang tepat, seperti membuat informasi, menerima informasi, dan mengevaluasi informasi. Salah satu sistem yang paling aman adalah tanda tangan digital.

Tanda tangan digital berfungsi untuk memverifikasi keaslian dan integritas sebuah dokumen digital serta dapat mengidentifikasi perubahan dokumen akibat hasil manipulasi. Salah satu metode untuk melengkapi tanda tangan digital pada suatu dokumen adalah dengan menggunakan fungsi hash, yang tentunya akan menghasilkan digest. Tujuan dari jurnal penelitian ini adalah mengembangkan aplikasi verifikasi identitas digital dengan mengimplementasikan tanda tangan digital. Memanfaatkan fungsi hash adalah salah satu metode penandatanganan dokumen secara digital; fungsi ini akan menghasilkan sebuah intisari. Dengan menggunakan tanda tangan digital, luaran dari jurnal penelitian ini adalah sebuah aplikasi pengembangan sertifikat tanah digital. Salah satu ide dalam kritik kontemporer adalah tanda tangan digital. Dalam hal keamanan kriptografi, tanda tangan digital memiliki tujuan utama untuk *non-repudiation* atau *anti-denial*, yang berarti bahwa jika sebuah dokumen sah, pengirim tidak dapat menyangkal bahwa dokumen tersebut dikirim oleh pengirim yang bersangkutan. Tanda tangan digital beroperasi dalam beberapa cara yaitu Pengirim pada awalnya menerapkan *algoritme hashing* pada pesan untuk menghasilkan intisari pesan dari dokumen yang akan dikirim. Tanda tangan digital dihasilkan ketika pengirim menandatangani intisari pesan menggunakan kunci publik setelah proses *hashing* selesai. Penerima kemudian menerima dokumen dan tanda tangan digital ini. Penerima mengonfirmasi keabsahan pesan setelah menerimanya. Penerima dapat membuat kembali message digest dari dokumen yang telah di-*hash* dengan menggunakan *private key* untuk membatalkan tanda tangan digital selama fase verifikasi ini. Komunikasi dianggap sah dan berasal dari pengirim asli jika *message digest* yang didapatkan sesuai dengan yang dikirimkan. Di sisi lain, jika intisari pesan berbeda, hal ini menunjukkan Sistem keamanan *cloud computing* menggunakan teknologi seperti *intrusion prevention system (IPS*) dan *intrusion detection system (IDS)* untuk melindungi data dari ancaman yang dapat membahayakan integritas, kerahasiaan, dan ketersediaannya. Perangkat lunak sumber terbuka sering kali digunakan

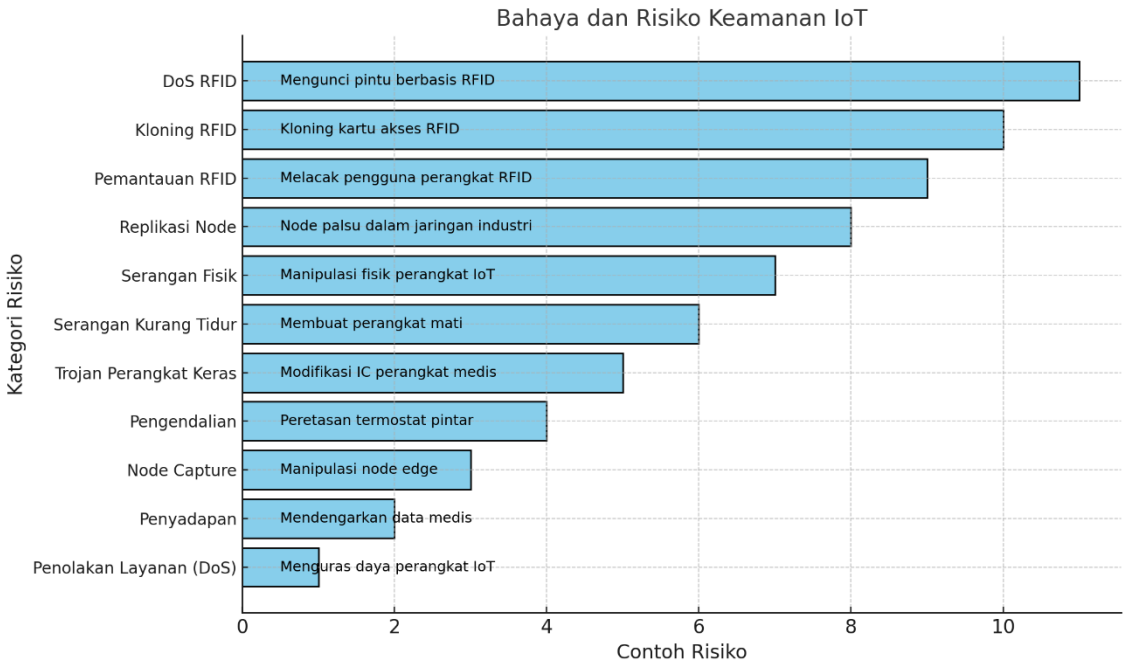
untuk membantu operasi di lingkungan komputasi awan untuk menerapkan keamanan ini.

Layanan web semakin banyak di-*host* pada arsitektur server yang berbasis *cloud computing*. Salah satu pemasok layanan komputasi awan teratas, *Google Cloud Platform (GCP)* menyediakan berbagai layanan infrastruktur, seperti jaringan, penyimpanan, komputasi, dan manajemen aplikasi. Ada banyak manfaat dalam mengadopsi *GCP* untuk mengimplementasikan infrastruktur server berbasis komputasi awan untuk layanan web, termasuk efektivitas biaya, skalabilitas, ketergantungan, dan keamanan. Ada beberapa teknik implementasi server dengan ketersediaan tinggi untuk infrastruktur server berbasis komputasi awan.Saat menerapkan infrastruktur server berbasis komputasi awan, keamanan juga menjadi pertimbangan penting. Kontrol akses, enkripsi data, dan pemantauan keamanan hanyalah beberapa fitur keamanan yang ditawarkan *GCP*. Menerapkan praktik terbaik keamanan, seperti konfigurasi firewall yang ketat, penggunaan HTTPS, dan manajemen akses terbatas, juga penting untuk aplikasi ini. Komponen penting dari solusi ini adalah manajemen dan pemantauan infrastruktur server. Pemantauan *cloud*, pencatatan *cloud*, dan jejak awan hanyalah beberapa dari kemampuan pemantauan dan manajemen komprehensif yang ditawarkan *GCP*. Teknologi-teknologi ini memungkinkan untuk melacak kinerja aplikasi, menemukan masalah, dan mengimplementasikan perbaikan.

Keamanan data dalam IoT (*Internet of Things*)

Kevin Ashton pertama kali mempresentasikan *Internet of Things (IoT)* pada tahun 1999. Kapasitas untuk menghubungkan benda-benda cerdas dan memungkinkan interaksinya dengan benda lain, lingkungan, dan perangkat komputasi cerdas lainnya melalui jaringan internet dikenal sebagai *Internet of Things (IoT).* IoT memiliki dampak yang signifikan pada pengguna individu di domain rumah, termasuk rumah pintar dan aplikasi otomotif. IoT memiliki dampak yang signifikan pada pengguna bisnis dalam beberapa hal, termasuk manajemen rantai pasokan, mengurangi waktu ketika produk tidak tersedia di pasar ritel, memantau distribusi barang, memerangi pemalsuan, dan meningkatkan kuantitas dan kualitas manufaktur.

Aspek keamanan merupakan salah satu kendala yang perlu diatasi untuk mendorong adopsi *IoT* secara luas. *IoT* adalah sistem yang rumit. Kerumitan ini disebabkan oleh berbagai peralatan dengan kemampuan komunikasi dan pemrosesan data di samping keterlibatan entitas yang berbeda seperti data, mesin, *RFID,* sensor, dan lainnya. *IoT* rentan terhadap ancaman keamanan yang dapat membahayakan dan mengancam konsumen karena banyaknya organisasi dan data yang terlibat. Bahaya ini terutama berbentuk membantu serangan terhadap sistem lain, membahayakan keselamatan pengguna, dan mengizinkan orang yang tidak berwenang untuk mengakses data dan menyalahgunakan informasi pribadi. Tergantung pada target serangan, entitas IoT mungkin rentan terhadap berbagai macam serangan. Bahaya IoT termasuk dalam kategori berikut :



Gambar 3. Grafik Bahaya dan Risiko keamanan IoT

Internet of Things adalah *sistem multi-komponen* dan kompleks. Kompleksitasnya berasal dari fakta bahwa sistem ini melibatkan berbagai peralatan dengan berbagai kemampuan komunikasi dan pemrosesan data di samping keterlibatan beberapa entitas seperti data, perangkat, jalur komunikasi, sensor, dll. Sejumlah besar entitas dan data terlibat. Akses tidak sah ke data dan penyalahgunaan informasi pribadi, membantu serangan terhadap sistem lain, dan membahayakan keselamatan pengguna adalah beberapa risiko terhadap *Internet of Things*. Tergantung pada target serangan, entitas *IoT* mungkin rentan terhadap berbagai macam serangan. Solusi *IoT* tidak dapat diintegrasikan secara langsung dengan sistem keamanan biasa. Hal ini disebabkan oleh sifat dinamis dari objek *IoT*, yang memungkinkan perangkat untuk dengan mudah bergabung atau meninggalkan komunitas *IoT* tempat mereka tertanam. Sumber daya perangkat *IoT* yang terbatas, termasuk yang terkait dengan listrik, kecepatan CPU, memori, kapasitas saluran (bandwidth), dan faktor lainnya, adalah fitur lain yang sangat signifikan. Karena fitur-fitur ini, model keamanan di *Internet of Things* berbeda dengan sistem keamanan jaringan tradisional. *CIA-Triad*, atau kerahasiaan, integritas, dan ketersediaan, adalah tiga kategori besar di mana fitur keamanan sistem teknologi informasi dapat dibagi. Fitur keamanan sistem yang membutuhkan kerja sama antara beberapa pihak, seperti *Internet of Things*, tidak dapat didefinisikan secara memadai oleh paradigma *CIA-Triad*. Dengan memeriksa berbagai sumber informasi dan literatur terkait keamanan, daftar atribut keamanan yang lebih menyeluruh telah dihasilkan. Di antara risiko keamanan *IoT* adalah risiko Keamanan *IoT* pada Lapisan Node Aplikasi mulai dari pemantauan kesehatan pribadi hingga manajemen industri menggunakan sistem dan aplikasi *IoT*. Oleh karena itu, penyerang dapat memilih untuk menargetkan sistem dan aplikasi *IoT* dengan alasan apa pun. Pencurian informasi pribadi, termasuk kata sandi rekening bank, nomor kartu kredit, data

lokasi, dan data terkait kesehatan, dengan memanfaatkan kelemahan pada perangkat IoT adalah salah satu alasan mengapa penyerang menargetkan sistem ini.

Edge node sebagian besar diserang oleh trojan perangkat keras. Dengan mengubah *Integrated Circuit (IC*), serangan trojan perangkat keras memungkinkan penyerang untuk mengakses data atau perangkat lunak yang beroperasi pada *IC*. Sebelum atau selama fabrikasi, penyerang memodifikasi desain *IC* dan memilih mekanisme pemicu yang akan mengaktifkan Trojan untuk memasukkannya. Trojan dapat diaktifkan dengan dua cara: secara eksternal, dengan menggunakan antena atau sensor yang dapat berkomunikasi dengan dunia luar, atau secara internal, dengan mengaktifkan Trojan ketika kondisi yang telah ditentukan tercapai. Serangan menggunakan saluran sisi non-jaringan. Bahkan ketika perangkat tidak menggunakan media komunikasi nirkabel, seperti suar yang secara konstan menyiarkan status perangkat, setiap node dapat mengungkapkan informasi penting dalam kondisi fungsi yang umum. Dalam sistem medis, kerentanan seperti ini dapat menyebabkan masalah terkait privasi. Sebagai ilustrasi, seorang pasien yang mengenakan peralatan medis yang menandakan kondisi medis yang terstigma secara sosial. data kesehatan pribadi seperti tekanan darah, kadar gula darah, dan detail lainnya dapat diungkapkan oleh perangkat IoT medis.

Perangkat *IoT* biasanya hanya memiliki baterai berkapasitas kecil karena keterbatasan fisik. Karena gadget akan mengalami kegagalan fungsi dan tidak dapat mengumpulkan data, terutama saat keadaan darurat, serangan ini dapat memberikan dampak yang signifikan, misalnya, penyerang dapat menonaktifkan peringatan sistem deteksi kebakaran gedung jika mereka menemukan cara untuk menghabiskan baterai detektor asap. Dalam skenario yang berbeda, penyerang dapat membombardir perangkat *IoT* dengan ribuan atau jutaan paket acak yang meminta respons, menguras baterai perangkat. Perangkat dengan kapasitas energi yang rendah adalah target serangan gaya *DOS* ini. Penyerang mengirimkan beberapa pertanyaan yang tampak otentik dalam serangan ini. Akibatnya, lebih sulit untuk mengidentifikasi serangan semacam ini. Serangan kurang tidur adalah salah satu eksploitasi yang menargetkan gadget dengan daya tahan baterai rendah. Serangan dengan pemadaman listrik. Ketika perangkat *IoT (edge node)* mengalami malfungsi, serangan ini terjadi. Terkadang perangkat yang berkoordinasi atau beberapa perangkat berhenti bekerja. Kesalahan dalam proses pembuatan, kehabisan baterai, injeksi kode, atau akses yang tidak sah secara fisik ke perangkat, semuanya dapat menyebabkan kegagalan ini. Serangan injeksi kode *Stuxnet* pada program kontrol proses nuklir Iran adalah contoh yang terkenal.

Serangan fisik, atau gangguan. Perangkat *IoT* rentan terhadap serangan fisik karena sering ditemukan di area yang rentan secara fisik (jalan raya, pertanian, perikanan, dll.). Seorang penyerang dapat memperbarui sistem operasi, mengubah kode program, memanipulasi sirkuit, dan mengekstrak informasi kriptografi dengan akses langsung. Lebih jauh lagi, barang tersebut dapat dirusak secara permanen oleh penyerang. Sebagai ilustrasi, pertimbangkan serangan *Nest Thermostat*, di mana peretas mencoba mengganti perangkat lunak asli dengan yang palsu. Dengan cara ini, bahkan setelah kehilangan akses langsung, penyerang masih dapat mengoperasikan termostat. Serangan replikasi node.

Dengan meniru salah satu identitas dari node lain, penyerang menambahkan node baru ke sekelompok node lain. Serangan menggunakan kamuflase. Untuk menyembunyikan keberadaan serangan, penyerang dalam jenis serangan ini menyisipkan node palsu atau mengubah node asli. Setelah itu, node yang diubah dapat berfungsi seperti biasa.

Identifikasi *RFID: Tag RFID* adalah perangkat *edge-node* yang umum digunakan dalam sistem Internet of Things. Tag RFID rentan terhadap berbagai serangan, seperti Pemantauan. Teknologi *RFID* memiliki identitas yang berbeda. Akibatnya, penyerang dapat membaca identitas tag *RFID* menggunakan peralatan pembaca *RFID* yang tidak sah. Penyerang dapat melacak objek yang menjadi target serangan dengan menggunakan kesempatan membaca. Jenis tag tertentu memiliki informasi penting tentang produk yang dipasangi *RFID*. Misalnya, kode produksi dan kode produk adalah dua bagian dari tag *Electronic Product Code (EPC).* Agar pembaca tag dapat memverifikasi hal-hal yang dimiliki oleh pemiliknya, seseorang dengan tag *EPC* biasanya menggunakan standar inventarisasi. Masalah privasi muncul dari ancaman ini. Sebagai contoh, seorang penyerang mungkin dapat mengidentifikasi jenis gadget medis tertentu, seperti pompa insulin pasien, dan dengan demikian menentukan bahwa korban menderita diabetes.

Kloning tag. Peretas bisa mendapatkan keuntungan besar dari serangan *kloning tag (spoofing)*, tetapi mereka juga bisa merusak merek perusahaan secara serius, dengan mengotomatiskan serangan, kerugiannya bisa meningkat. Dengan menggunakan *kloning tag*, penyerang dapat memperoleh akses ke data sensitif, detail rekening bank, dan wilayah bisnis yang dibatasi. Serangan *DoS*. *Serangan denial-of-service (DoS)* pada tag *RFID* mengganggu saluran frekuensi radio, sehingga tidak memungkinkan pembaca tag untuk membaca tag dan dengan demikian membuat layanan tidak tersedia. Misalnya, dengan mengganggu semua pintu berbasis *RFID*, penyerang dapat mengunci seluruh fasilitas. Penelitian sebelumnya telah membahas kelemahan tambahan dari sistem autentikasi *RFID* terhadap serangan *DOS*.

Blockchain dan keamanan data

Teknologi *Blockchain* dimulai dengan sebuah ide tentang data digital yang, karena terdesentralisasi, dapat ditransmisikan dan disimpan dengan aman tanpa diretas atau diubah. Tujuan dari keamanan informasi adalah untuk melindungi data dan informasi dari bahaya, kehilangan, atau akses ilegal. Dengan semakin banyaknya data yang disimpan dan ditransfer oleh teknologi digital di era modern, keamanan data informasi menjadi semakin penting. Sebagai contoh, *blockchain* dan kriptografi adalah dua metode yang digunakan oleh bisnis dan lainnya untuk mencoba mengamankan data mereka. Ilmu yang memastikan keamanan pesan dikenal sebagai kriptografi, studi tentang metode matematika yang berkaitan dengan fitur keamanan informasi termasuk kerahasiaan, integritas data, dan otentikasi adalah definisi lain dari kriptografi. Studi kriptografi berfokus untuk memastikan bahwa dokumen dan pesan kita aman dan tidak dapat dibaca oleh orang yang tidak berwenang.

Sistem login adalah salah satu elemen internet yang harus diperhitungkan

keamanannya ketika menggunakan teknologi *blockchain* untuk mengoptimalkan keamanan web server terhadap serangan otentikasi yang rusak, menurut artikel jurnal oleh Iman Riadi, dkk.(2021). Karena mudah diatur, nama pengguna dan kata sandi biasanya digunakan oleh sistem login sebagai metode autentikasi. Karena kata sandi dan nama pengguna sangat rentan terhadap peretasan, keamanan sistem login harus diperkuat Teknologi terdesentralisasi yang disebut *blockchain* memungkinkan transaksi antara dua pihak yang tidak dapat dipercaya tanpa memerlukan perantara. Karena blockchain menyimpan data secara terdesentralisasi di seluruh jaringan, satu orang tidak dapat mengubahnya tanpa persetujuan jaringan. Selain itu, *blockchain* dapat meningkatkan akuntabilitas dan transparansi manajemen data. Karena data dapat diakses oleh pihak yang tidak berwenang dan dieksploitasi untuk tujuan jahat, keamanan data menjadi hal yang krusial dalam transformasi digital Nugroho et al., & Situmeang, (2021). Teknologi *blockchain* dapat meningkatkan keamanan data dalam hal ini dengan beberapa cara. Pertama, *blockchain* meningkatkan keamanan data dengan memungkinkan penyimpanan data yang terdesentralisasi dan terenkripsi, sehingga sulit bagi seseorang untuk mengubah atau mencuri data tanpa persetujuan dari seluruh jaringan *blockchain* karena data tersebut tidak disimpan secara terpusat. Kedua, semua pihak dapat memverifikasi setiap transaksi dan bagian dari data dalam teknologi *blockchain*. Hal ini menurunkan kemungkinan penipuan dan meningkatkan transparansi. Ketiga, karena teknologi *blockchain* meniadakan kebutuhan akan perantara atau pihak ketiga, verifikasi dan validasi menjadi proses yang sangat cepat dan efisien. Namun, ada juga bahaya yang terkait dengan penggunaan teknologi *blockchain*, seperti ketergantungan pada sistem, ancaman keamanan, dan masalah skalabilitas. Jika teknologi *blockchain* mengalami masalah atau kerusakan, data dan transaksi yang tersimpan dalam blockchain juga akan terpengaruh. Selain itu, menggunakan teknologi *blockchain* untuk perlindungan data memiliki risiko masalah keamanan yang signifikan. Walaupun teknologi blockchain dianggap sangat aman, sebuah serangan masih dapat terjadi jika berhasil melewati langkah-langkah keamanannya. *Blockchain* rentan terhadap berbagai macam serangan, seperti *Sybil attack* , serangan *double spending*, dan serangan 51%.

Ketika penyerang mendapatkan kontrol lebih dari 50% kekuatan jaringan *blockchain*, ini dikenal sebagai serangan 51% (Trinowo, 2020). Penyerang dapat mengubah catatan transaksi sebelumnya dan memalsukan transaksi jika mereka memiliki lebih dari 50% kekuatan jaringan. Keamanan data dalam blockchain dapat terancam, dan integritas data dapat dirusak. Ketika seorang penyerang mencoba menggunakan aset mata uang digital yang sama untuk menyelesaikan transaksi yang sama dua kali, hal ini dikenal sebagai serangan *double-spending*. Setiap transaksi pada blockchain harus dikonfirmasi dan diotorisasi oleh jaringan secara keseluruhan. Sebaliknya, serangan pengeluaran ganda bertujuan untuk mengirimkan aset kripto yang sama ke dua alamat yang berbeda pada saat yang sama dalam upaya untuk memalsukan transaksi. Orang yang menerima aset mata uang kripto dapat mengalami kerugian finansial yang besar sebagai akibatnya. Pelaku *Sybil attack* membuat banyak identitas palsu yang tampaknya berasal dari berbagai node jaringan. Hal ini dapat meningkatkan pengaruh penyerang di seluruh jaringan dan

memungkinkan mereka untuk memalsukan data dan transaksi Bashar et al.,(2022).

Penerapan teknologi *blockchain* dalam transformasi digital memiliki kendala skalabilitas selain ancaman keamanan. Ukuran dan volume transaksi yang dapat diproses oleh teknologi *blockchain* dibatasi. Ketika diterapkan pada proyek transformasi digital yang luas dan rumit, hal ini menjadi masalah Lin & Liao & Bashar et al., (2022). Lebih banyak penelitian dan pengembangan masih diperlukan untuk meningkatkan kapasitas transaksi yang dapat ditangani, meskipun sejumlah teknologi *blockchain* telah dikembangkan untuk meningkatkan skalabilitas Teknologi *blockchain* dapat menawarkan keuntungan besar untuk keamanan data dalam transformasi digital, terlepas dari bahaya dan batasan tertentu. Memilih jenis *blockchain* yang paling sesuai dengan kebutuhan perusahaan dan mempertimbangkan keuntungan dan kerugian dalam menggunakan *blockchain* sangat penting ketika mengadopsi *blockchain* untuk keamanan data. Selain itu, sangat penting untuk mempertimbangkan perlunya mengintegrasikan dengan sistem yang ada saat ini dan potensi untuk mengatasi kekurangan teknologi blockchain Lin & Liao & Liu et al.,(2019).

D. Kesimpulan

Jurnal ini memberikan pemahaman terkait keamanan data pada transformasi digital yang terjadi akibat teknologi modern seperti dalam *cloud computing, Internet of Things (IoT),* dan *blockchain.* Meskipun kemajuan ini meningkatkan efisiensi dan kenyamanan, hal ini juga menimbulkan masalah keamanan data yang signifikan. Tantangan utama teknologi *cloud computing* mencakup risiko serangan data, kehilangan data, dan masalah privasi. Data yang disimpan di server jarak jauh dapat diakses secara ilegal jika prosedur keamanan lemah. Langkah-langkah mitigasi mencakup kontrol akses yang ketat, enkripsi data, dan penerapan solusi seperti *Google Cloud Platform (GCP),* yang memberikan kemampuan keamanan tingkat lanjut seperti pemantauan dan pengelolaan server secara *real-time*. *IoT* menghadapi tantangan tambahan karena terdiri dari perangkat yang terhubung dengan sumber daya terbatas. Perangkat ini rentan terhadap berbagai ancaman, termasuk penolakan layanan, pencurian data, dan serangan fisik. Prosedur keamanan konvensional belum tentu sesuai untuk *IoT*, sehingga tindakan mitigasi seperti autentikasi biometrik dan enkripsi ujung ke ujung diperlukan.

Teknologi *Blockchain* memberikan solusi keamanan menggunakan sistem desentralisasi dan kriptografi. Teknologi ini menjamin integritas data dan transparansi transaksi. Namun, blockchain rentan terhadap bahaya seperti serangan 51%, masalah skalabilitas, dan ketergantungan pada teknologi. Meskipun demikian, keunggulan blockchain dalam keamanan data menjadikannya teknologi yang menjanjikan, khususnya dalam hal meminimalkan penipuan dan meningkatkan transparansi. Studi ini menekankan pentingnya strategi komprehensif yang mencakup peningkatan teknologi, serta mendidik masyarakat. Studi ini memberikan rekomendasi strategi mitigasi, seperti penggunaan teknologi modern, dan pemasangan infrastruktur yang lebih aman tentang ancaman keamanan digital. Temuan ini menunjukkan bahwa kombinasi langkah-langkah ini dapat membantu terciptanya lingkungan digital yang aman dan terpercaya.

Daftar Pustaka

Abiezal, M. E., & Afrianto, I. Tinjauan Literatur: Keamanan Cloud di Era Digital Menangani Ancaman Saat Ini dan Memastikan Privasi Data.

Fauziah, Y. (2014). Tinjauan keamanan sistem pada teknologi cloud computing. *Jurnal Informatika Ahmad Dahlan*, *8*(1), 103259.

Febryan, F. B. Trend Keamanan Cloud Computing.

Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), 6719-6742.

Hidayat, T. S., & Abdurrahman, L. (2023). Keamanan Dan Privasi Teknologi Pembayaran Digital Pada Umkm Dengan Menggunakan Platform Blockchain Hyperledger Fabric. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *9*(2).

Meutia, E. D. (2015). Internet of things–Keamanan dan Privasi. In *Seminar Nasional dan Expo Teknik Elektro* (Vol. 1, No. 1, pp. 85-89).

Najib, W., & Sulistyo, S. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, *9*(4), 375-384.

Putra, A. (2023). Penggunaan Teknologi Blockchain Dalam Upaya Meningkatkan Keamanan Data Di Massa Era Digital. *no. April*, 1-11.

Sari, D. R. (2024). Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT). *Technologia Journal*, *1*(2), 1-10.

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55-68.