Analisis Penerapan Blockchain dan Kriptografi untuk Keamanan Data

Pada Sistem Jaringan Tenaga Listrik

Christopher Davin Leoputra (18219037)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: christopherdavin08@gmail.com

***Abstract*—Perkembangan teknologi di masa ini sudah tak dapat dibendung lagi dan berlaku pada seluruh aspek kehidupan masyarakat. Seiring dengan perkembangan tersebut, faktor faktor lain seperti manusia, pengetahuan, dan lingkungan mendorong adanya tuntutan akan kehidupan yang lebih layak tak terkecuali di perkotaan. Untuk memenuhi hal tersebut, dibutuhkan manajemen kota melalui pendekatan konsep perencanaan yang berkelanjutan. Konsep yang berkembang saat ini yaitu konsep smart city atau kota cerdas. Smart city adalah sebuah konsep kota yang mengandalkan teknologi Internet of Things dan memanfaatkan teknologi informasi untuk mengintegrasikan seluruh infrastruktur dan pelayanan dari pemerintah kepada warga masyarakat untuk membantu meningkatkan kualitas kota tersebut [1]. Salah satu contoh komponen utama dari smart city adalah smart energy melalui *smart grid* yang memperkenalkan komunikasi dua arah antara pelanggan dengan perusahaan penyedia listrik. Sistem smart grid diimplementasikan sebagai interpretasi modern dari jaringan listrik tradisional untuk menemukan cara paling efisien untuk menggabungkan energi terbarukan dan teknologi penyimpanan. Salah satu masalah yang dapat terjadi pada jaringan smart grid adalah kemungkinan data pelanggan disalahgunakan oleh pihak yang tidak bertanggungjawab karena saluran transmisi yang tidak aman. Penerapan kriptografi dalam menjaga keamanan data pelanggan dapat menjadi jawaban permasalahan tersebut melalui penggunaan blockchain dan algoritma kriptografi yang diterapkan pada jaringan smart grid. Blockchain memberikan keamanan tambahan untuk penyimpanan data pada pusat pengatur jaringan dan kriptografi memberikan kerahasiaan serta autentikasi pada pertukaran data dalam jaringan. Maka dari itu, pada makalah ini akan dibahas mengenai analisis penerapan blockchain dan algoritma kriptografi yakni algoritma RSA yang digunakan untuk menjaga keamanan data sistem jaringan listrik smart grid.**

Keywords—smart grid, blockchain, RSA, pertukaran data

I. Pendahuluan

Di era Society 5.0, dimana seluruh kehidupan masyarakat terhubung dengan jaringan internet, keamanan data dan informasi menjadi salah satu hal yang menjadi perhatian. Tak bisa dipungkiri, kemajuan teknologi turut serta membawa implikasi kompleks dalam kehidupan manusia. Banyak oknum pelaku kejahatan melalui jaringan internet atau yang lebih dikenal dengan sebutan kejahatan siber berusaha mencuri, merusak, menyebarkan maupun memanipulasi data melalui sekecil apapun celah keamanan yang ada. Di Indonesia sendiri, telah tercatat setidaknya sekitar 1,6 miliar serangan siber telah terjadi di sepanjang tahun 2021 [4]. Catatan ini menunjukkan bahwa pertukaran data melalui jaringan internet masih rawan terhadap serangan siber. Seiring dengan perkembangan zaman, data menjadi salah satu aset penting dan bahkan ada istilah yang mengatakan "*Data is the new oil*" akibat besarnya nilai yang diberikan oleh sebuah data.

Pemanfaatan data di beberapa tahun terakhir ini telah menciptakan banyak hal hal baru yang mempermudah kehidupan masyarakat. Salah satunya adalah terciptanya konsep smart city. Smart city merupakan sebuah konsep kota yang mengandalkan teknologi Internet of Things (IoT) dan memanfaatkan teknologi informasi untuk mengintegrasikan seluruh infrastruktur dan pelayanan dari pemerintah kepada warga masyarakat untuk membantu meningkatkan kualitas kota tersebut. Dalam mewujudkan konsep ini, dibutuhkan banyak komponen komponen lain, salah satunya adalah smart energy yaitu suatu sistem terbaru dari pemanfaatan energi.

Inovasi teknologi dalam penciptaan smart energy yang cukup banyak digunakan adalah *smart grid*. *Smart grid* merupakan teknologi yang memanfaatkan kemajuan teknologi komunikasi, komputer, dan siber untuk dapat melakukan pengendalian dan pengoperasian sistem tenaga listrik dalam menyalurkan tenaga listrik [5]. Pada jaringan smart grid, akan ada pertukaran data secara dua arah antara pengguna listrik dengan perusahaan penyedia listrik. Data inilah yang diincar oleh oknum tidak bertanggungjawab melalui celah saluran transmisi yang kurang aman. Data yang didapatkan nantinya dapat disalahgunakan sehingga merugikan pelanggan maupun perusahaan penyedia listrik [6]. Contoh data yang dapat diambil adalah data dari meteran listrik pengguna berupa nilai tegangan, arus, dan *power factor*.

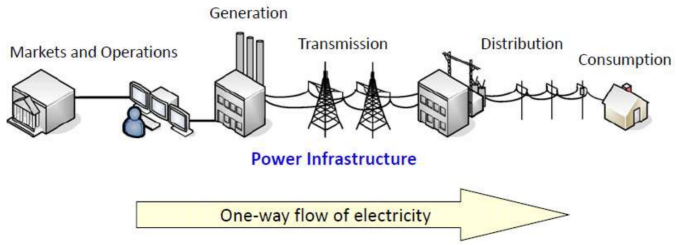
Hal yang dapat diterapkan untuk menangani dan menyelesaikan serangan ini adalah dengan menggunakan blockchain dan algoritma kriptografi RSA yang diterapkan pada jaringan *smart grid*. Maka dari itu, pada makalah ini akan dibahas topik mengenai penerapan blockchain dan kriptografi untuk keamanan data khususnya pada sistem

jaringan tenaga listrik atau *smart grid* guna meningkatkan efisiensi, kualitas, dan keandalan sistem ketenagalistrikan.

II. Landasan Teori

A. Smart Grid

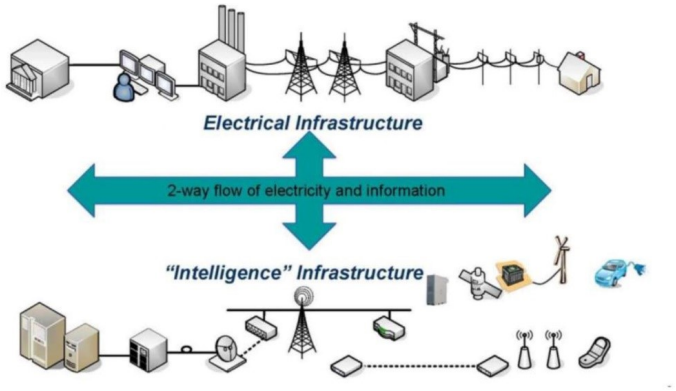
Smart grid merupakan teknologi yang memanfaatkan kemajuan teknologi komunikasi, komputer, dan siber untuk dapat melakukan pengendalian dan pengoperasian sistem tenaga listrik dalam menyalurkan tenaga listrik. Pengimplementasian *smart grid* akan memberikan keuntungan yang lebih besar karena jumlah pembangkit terbarukan dan unit penyimpan yang terdistribusi dan terintegrasi meningkat dan tentunya emisi CO2 menurun, keandalan meningkat melalui optimalisasi jaringan karena memiliki kemampuan mengoreksi diri atau penyembuhan diri [5]. Pengaplikasian *smart grid* menggantikan jaringan listrik konvensional diharapkan dapat meningkatkan keandalan, kualitasdan efisiensi jaringan listrik, meminimalisasi kebutuhan akan pembangkit cadangan untuk memenuhi beban puncak, dan meningkatkan penetrasi energi terbarukan



Gambar 1. Skema jaringan listrik tradisional

Sumber: https://www.interregsolarise.eu/

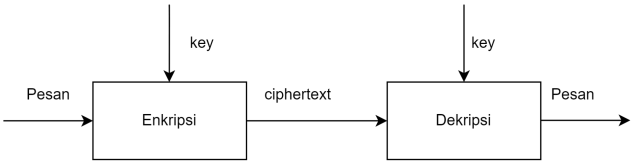
Sistem *smart grid* melakukan pertukaran data secara dua arah antara pengguna listrik dengan perusahaan penyedia listrik. Maka dari itu, perlu adanya sistem pengamanan terhadap aliran pertukaran data yang terjadi agar meminimalisir tindakan penyalahgunaan data pengguna dan penyedia listrik.



Gambar 2. Skema Smart Grid

Sumber: https://pltfrmrsrcs.sagepub.com/

B. Algoritma Kunci Publik RSA



Gambar 3. Alur kriptografi

Kriptografi kunci-publik diciptakan untuk menyelesaikan permasalahan pada kriptografi kunci-simetris dimana proses enkripsi dan dekripsi dilakukan menggunakan kunci yang sama. Permasalahan muncul ketika seseorang harus mengirimkan kunci tersebut kepada penerimanya agar pesan dapat tersampaikan. Untuk menghindari serangan terhadap pesan, kunci harus dikirimkan melalui saluran kedua yang benar-benar aman.[8]. Salah satu algoritma kunci publik yang paling terkenal adalah algoritma RSA.

Algoritma RSA merupakan algoritma kunci-publik yang paling banyak pengaplikasiannya. Algoritma ini ditemukan pada tahun 1976 oleh tiga peneliti asal MIT yaitu Ronald Rivest, Adi Shamir, dan Len Adleman. Keamanan algoritma RSA ini terletak pada sulitnya memfaktorkan bilangan bulat yang besar menjadi faktor-faktor prima [7]. Terdapat dua bagian utama dalam algoritma RSA, yaitu proses pembangkitan sepasang kunci dan proses enkripsi/dekripsi pesan yang dituliskan dengan langkah dan persamaan sebagai berikut:

Proses pembangkitan sepasang kunci dilakukan dengan langkah-langkah sebagai berikut:

1. Pilih dua bilangan prima, p dan q yang bersifat rahasia
2. Hitung nilai n yang merupakan hasil perkalian dari bilangan p dan q
3. Hitung Φ (*totient euler*) dari n yang merupakan hasil dari perkalian nilai (p – 1) dan (q – 1).
4. Pilih sebuah bilangan bulat e sebagai kunci publik, dengan nilai e relatif prima terhadap n..
5. Hitung kunci dekripsi, d, dengan persamaaan

$$ed \equiv 1 \pmod{\Phi(n)} \text{ atau } d\ e\ -1 \bmod (\Phi(n))$$

Kunci publik yang akan digunakan adalah pasangan nilai e dan n, sedangkan nilai kunci privat merupakan pasangan dari nilai d dan n.

Persamaan enkripsi pesan

$$c_i = m_i^{\ e} \bmod n$$

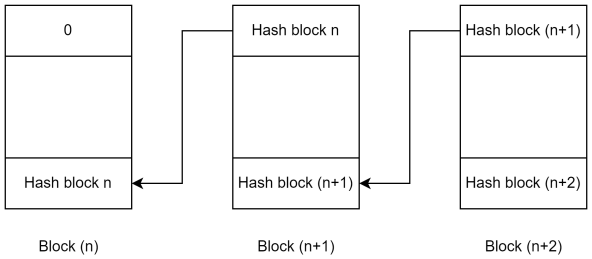
Persamaan dekripsi pesan:

$$m_i = c_i^{\ d} \bmod n$$

C. Blockchain

Blockchain merupakan buku besar (ledger) terbuka yang terdesentralisasi (decentralized) atau terdistibusi (distributed ledger). Sistem yang digunakan pada blockchain adalah *chaining blocks* dari fungsi hash menggunakan hash pointer [9]. Fungsi hash merupakan suatu fungsi matematika yang

mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi ini digunakan pada berbagai aplikasi pengamanan dan protokol internet. Beberapa contoh kegunaan fungsi hash adalah untuk autentikasi pesan, tanda tangan digital, hingga penyimpanan password.



Gambar 4. Ilustrasi Blockchain

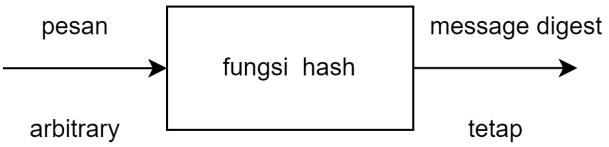
Cara kerja blockchain yaitu setiap blok dapat menyimpan sejumlah informasi tertentu. Setiap block yang telah terisi informasi akan terhubung dengan block sebelumnya dan juga dengan block setelahnya, sehingga membentuk sebuah rangkaian yang dinamakan blockchain. Block yang sudah dimasukkan ke dalam rangkaian akan menjadi catatan data permanen yang tidak dapat diubah ataupun dihapus, data ini disimpan dengan informasi waktu yang jelas, dan terhubung ke jaringan tanpa batas.

Terdapat lima sifat blockchain. Sifat pertama adalah blockchain merupakan sistem yang transparan karena dikembangkan dengan konsep *Open-source*.Sifat kedua adalah *Decentralized*, yang membuat sistem lebih baik dari sistem terpusat dalam menghadirkan sebuah sistem pencatatan transaksi yang transparan dan terpercaya. Sifat ketiga adalah *Immutable*, artinya seluruh block data yang sudah lulus protokol konsensus dan dimasukkan ke dalam blockchain adalah final dan tidak dapat diganggu gugat oleh siapapunSifat keempat adalah *Independent* dan *Personal*, artinya blockchain memungkinkan kita untuk berinteraksi secara langsung dengan aset kita tanpa harus menggunakan pihak ketiga sebagai perantara. Sifat kelima adalah *Disruptive*, artinya teknologi ini akan mengubah banyak sekali aspek kehidupan umat manusia [9].

Dengan adanya blockchain, keamanan dan juga privasi data dapat ditingkatkan. Dimana blockchain menciptakan catatan transaksi yang tidak bisa diubah dengan enkripsi dari ujung ke ujung karena perubahan pada satu block akan mempengaruhi block block lainnya.

D. Fungsi hash

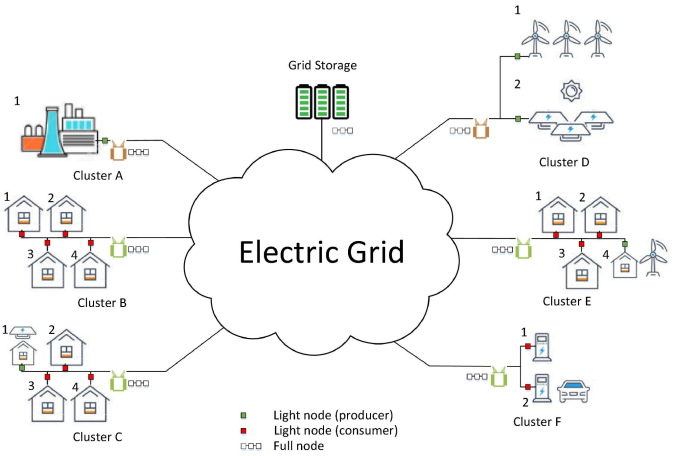
Fungsi hash merupakan sebuah fungsi yang dapat digunakan untuk memetakan data dengan ukuran arbitrer atau sembarang ke sebuah nilai berukuran tetap. Hasil yang diperoleh dari fungsi ini berupa sebuah message digest yaitu string berukuran tertentu dan panjangnya tetap. Nilai yang dikembalikan dari fungsi hash bersifat satu arah dan tidak dapat dikembalikan menjadi pesan semula



Gambar 5. Skema fungsi hash

III. SKEMA RANCANGAN

Rancangan alur sistem pengamanan data pada jaringan *smart grid* terbgi menjadi 2 yaitu algoritma RSA dan fungsi hash. Jaringan smart grid ini dirancang sebagai jaringan yang terhubung dengan server lokal. Selain itu, server lokal terhubung dengan sebuah database. Database ini berperan dalam penyimpanan data yang menggunakan sistem blockchain.

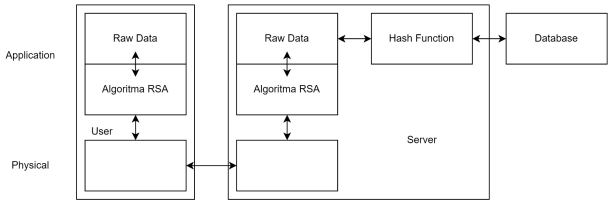


Gambar 6. Ilustrasi jaringan *smart grid*

Sumber: https://ars.els-cdn.com/content/image/1-s2.0-S1319157819309000-gr4.jpg

Skema alur pengamanan data dalam jaringan *smart grid* ini bekerja seperti jaringan telekomunikasi pada umumnya, program akan dirancang untuk bisa kompatibel dengan desain jaringan telekomunikasi yang sudah ada. Alur dimulai dari algoritma RSA yang diletakkan dekat dengan raw data atau data kasar pada application layer pada user. Peletakan program RSA pada application layer bertujuan agar program dapat diletakkan pada berbagai jenis jaringan seperti TCP/IP.

Raw data ini memuat beberapa informasi yang terdiri dari kode identifikasi pelanggan, unix time, pemakaian listrik, dan daya terukur. Pengambilan data pada jaringan smart grid akan dilakukan setiap satuan waktu. Keluaran dari fungsi enkripsi berupa matriks baris dari bilangan yang sebanding dengan kunci RSA.



Gambar 7. Alur algoritma RSA *smart grid*

Fungsi hash diletakkan sebelum proses penyimpanan oleh server. Fungsi hash yang diletakkan pada tahap akhir sebelum penyimpanan data pada jaringan smart grid berfungsi untuk merepresentasikan proses penyusunan blok dari blockchain oleh server. Fungsi ini akan memerlukan waktu yang lebih lama dikarenakan adanya ketentuan yang dibuat untuk memperoleh nilai hash yang diinginkan.

Nilai hash yang diperoleh harus memenuhi sebuah ketentuan agar dapat menjadi bukti bahwa pekerjaan untuk menghitung nilai hash telah dilakukan untuk sebuah masukan data berupa string. Cara kerja yang dilakukan pada fungsi hash ini hampir mirip dengan cara kerja yang dilakukan pada transakasi Bitcoin, namun pada Bitcoin memiliki perbedaan dimana nilai hash yang dihasilkan harus berada di bawah suatu nilai atau dikenal dengan istilah target [11].

Tiap satu siklus aliran data didefinisikan dengan pengiriman data dari tiap pengguna menuju server dan juga sebaliknya. Untuk pengiriman dari server, data string akan memuat kode identifikasi pelanggan, kode perintah, dan karakter pengisi.

Algoritma RSA pada jaringan *smart grid* ini perlu memerhatikan beberapa informasi terkait antara lain:

- Raw data berupa string yang memuat informasi data sepanjang 32 karakter dari informasi kode pelanggan, waktu, pemakaian listrik dan daya listrik yang digunakan yang terpisah dengan tanda pagar

  Contoh raw data yang diperoleh:

  BC23K1#7538509173#115356#12243

- Untuk pengukuran waktu dilakukan terhadap satuan waktu. Diasumsikan pengambilan data dilakukan setiap satu menit.
- Ukuran kunci RSA yang digunakan mengikuti standar NIST yaitu lebih dari 1024 bit, sebesar 1536 bit.
- Hasil dari enkripsi RSA akan berupa matriks berukuran sama dengan kunci yang dipilih. Untuk cluster akan dipasangkan ukuran 1x192 x 9bit signed integer
- Pengiriman data server berisi data string yang memuat identifikasi pelanggan, kode dan karakter sejumlah maksimal 32 karakter

  Contoh data yang diperoleh:

  BC23I0#42#XXXXXXXXXXXXXXXXXXXXXX

IV. Analisis dan Pembahasan

Dalam perhitungan algoritma RSA, salah satu aspek penting yang mempengaruhi hasil yang diperoleh adalah ukuran kunci yang digunakan. Semakin kecil ukuran kunci yang digunakan, sebuah sistem akan lebih mudah untuk dibobol oleh pihak yang tidak bertanggungjawab. Standar yang digunakan untuk ukuran kunci RSA yang digunakan sebesar 1024 bit atau lebih besar agar data dapat terproteksi secara kompleks.

Untuk setiap nilai ukuran kunci RSA yang berbeda akan menghasilkan waktu komputasi yang berbeda. Semakin besar kunci yang digunakan, maka akan semakin tinggi nilai rata-rata waktu perhitungannya. Sehingga, terbukti jika ukuran kunci RSA berpengaruh secara eksponensial terhadap waktu komputasi proses pengamanan raw data yang dibutuhkan. Terdapat beberapa asumsi yang digunakan dalam rancangan sistem pengamanan data *smart grid* ini seperti saluran transmisi yang bersifat sempurna sehingga tidak menghasilkan galat yang dapat menyebabkan kesalahan dalam perhitungan.

Tabel 1. Perbandingan ketentuan nilai hash terhadap waktu

Digit nol	**2**	**3**	**4**
Waktu minimum (detik)	0.0011	0.0008	0.4201
Waktu rata-rata (detik)	0.0832	1.4381	20.7356
Waktu maksimum (detik)	0.5386	8.1352	141.2345

Untuk mencari satu nilai hash yang memenuhi ketentuan nilai hash dengan jumlah digit nol awal pada nilai hash, dilakukan pengujian waktu berdasarkan jumlah digit nol 2, 3, dan 4 sebanyak 100 kali perhitungan untuk mencari waktu minimal, maksimal dan waktu rata ratanya.

Algoritma RSA akan melakukan enkripsi dan dekripsi pesan berupa informasi listrik pelanggan sebagai perintah dari pelanggan ke server dan juga sebaliknya server akan memberikan perintah ke pengguna. Fungsi hash digunakan dalam jaringan *smart grid* untuk merepresentasikan alur keterhubungan block pada blockchain di server. Untuk memperoleh ketentuan nilai hash yang akan digunakan, dilakukan perhitungan waktu yang diperlukan untuk mencari satu nilai hash sehingga dapat diperoleh jumlah digit nol yang mengawali nilai hash yang akan dijadikan sebagai ketentuan nilai hash.

Tabel 2. Perhitungan waktu dengan simulasi RSA

Minimum (detik)	Maksimum (detik)	Rata-rata (detik)

7.043	13.004	9.013

Sebagai contoh nilai hash dengan ketentuan berdasarkan digit nol awal:

- 0000C3B891D189A6EDB060ADF56FBCDA6EDA 6EDBDB2C737B5D5A189A29E

Dapat dilihat pada nilai hash diatas, terdapat 4 digit nilai 0 yang akan digunakan sebagai ketentuan nilai hash.

Pada block yang menyusun sebuah blockchain terdiri dari nilai hash block dari block sebelumnya raw data berupa string terdiri dari informasi pelanggan seperti besar pemakaian listrik, kode waktu dan besar daya listrik. Pada karakter terakhir akan ditambahkan karakter acak untuk memenuhi syarat ketentuan nilai hash yang telah diperoleh tadi berdasarkan jumlah nol pada digit pertama nilai hash.

Contoh block pada rangkaian blockchain yang digunakan:

00000000000000000000000000000000#UWTYK6#3542933540#437.57#2335.16#KLIL44A443E0PO7FFAR8JF21U37C4I
00044A4ACE6E68DFDBE76021CB51B921#YJDK4X#3542933540#60.712#431.027#KI21RQNMWW1LFF8OFHPOAFK2C5F64EC

Secara utuh, tiap block berisi 96 karakter dan sudah termasuk dengan pagar sebagai pembatas antar informasi raw data.

Tabel 3. Perhitungan waktu dengan blockchain

Minimum (detik)	Maksimum (detik)	Rata-rata (detik)
46.371	92.442	67.314

Dapat dilihat pada perhitungan waktu dengan blockchain ini memakan waktu yang cukup panjang sehingga dalam kondisi nyata dalam penerapannya pada jaringan *smart grid*, hal ini tidak dapat dijadikan sebagai gambaran. Salah satu aspek pertimbangan yang digunakan dalam metode perhitungan blockchain ini adalah spesifikasi alat yang digunakan untuk melakukan proses berintensitas tinggi.

V. Kesimpulan

Smart Grid merupakan inovasi teknologi yang memanfaatkan kemajuan teknologi komunikasi, komputer, dan siber untuk dapat melakukan pengendalian dan pengoperasian sistem tenaga listrik dalam penyaluran tenaga listrik. Namun, sistem ini memiliki celah keamanan pada saluran transmisi yang tidak aman saat melakukan pertukaran data. Penerapan blockchain pada pengamanan data sistem *smart grid* memberikan keamanan dalam penyimpanan data ke dalam database setelah sebelumnya dilakukan algoritma RSA untuk merahasiakan transmisi data antara user dan server. Pembentukan blockchain yang hanya dikhusukan pada suatu perangkat memungkinkan adanya pembagian tanggung jawab dalam penggunaan data. Dalam perhitungan nilai hash pada pembentukan blockchain, waktu yang diperoleh akan semakin lama karena kesulitan dalam pemenuhan ketentuan nilai hash. Perbedaan 1 digit pada ketentuan nilai hash menghasilkan perbedaan yang cukup jauh terhadap waktu pencarian nilai hash

Ucapan Terima Kasih

Ucapan terima kasih dan puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan karunia-Nya, penulis dapat menyelesaikan makalah ini dengan lancar. Penulis juga mengucapkan terima kasih kepada Dr. Rinaldi Munir selaku dosen pengampu mata kuliah II4031 Kriptografi dan Koding atas dedikasinya dalam memberikan ilmu pengetahuan, khususnya mengenai mata kuliah kriptografi selama satu semester ini sehingga penulis dapat memberikan kontribusi nyata dengan merumuskan ide melalui makalah ini.

Daftar Pustaka

[1] C. Puspitasari, "Sejarah dan Konsep Smart City dalam Dunia Teknologi Informasi", [online]. Available: https://binus.ac.id/malang/2021/04/sejarah-dan-konsep-smart-city-dalam-dunia-teknologi-informasi/#:~:text=Smart%20city%20merupakan%20sebuah%20konsep,dari%20pemerintah%20kepada%20warga%20masyarakat.

[2] A Pribadi, "25 Sistem Smart Grid Dibangun Hingga 2024", [online]. Available: https://www.esdm.go.id/id/media-center/arsip-berita/25-sistem-smart-grid-dibangun-hingga-2024#:~:text=Dalam%20meningkatkan%20keandalan%20sistem%20tenaga,Variable%20Renewable%20Energy%20(VRE).

[3] I. B. K. Sugirianta, I N. Sukarma , "Keandalan Sistem Smart Grid", [online]. Available: http://repository.univ-tridinanti.ac.id/1625/1/BAB%20I.pdf

[4] V. Mantalean , "BSSN Sebut Ada 1,6 Miliar Serangan Siber Selama 2021", [online]. Available: https://nasional.kompas.com/read/2022/03/07/20162321/bssn-sebut-ada-16-miliar-serangan-siber-selama-2021#:~:text=JAKARTA%2C%20KOMPAS.com%20%2D%20Badan,7%2F3%2F2022).

[5] Pusyantek BRIN, "Klaster Teknologi Energi Sistem Smart Grid", [online]. Available: http://pusyantek.bppt.go.id/id/pages/klaster-teknologi/energi/sistem-smart-grid#:~:text=Pusyantek%20%7C%20Technology%20solution%20provider&text=Inovasi%20Teknologi%20Smart%20Grid%20merupakan,listrik%20dalam%20menyalurkan%20tenaga%20listrik.

[6] J. Gao et al., "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," [online]. Available: https://ieeexplore.ieee.org/document/8303679

[7] R. Munir, "Algoritma RSA", [online]. Available: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/12%20-%20Algoritma-RSA-2021.pdf

[8] R. Munir, "Kriptografi Kunci Publik", [online]. Available: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/11%20-%20Kriptografi-Kunci-Publik-2021.pdf

[9] R. Munir, "Penggunaan Hash di dalam Blockchain", [online]. Available: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/23%20-%20Penggunaan-hash-di-dalam-blockchain.pdf

[10] A. Triorizka, "Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature dengan .NET", [online]. Available: https://repository.amikom.ac.id/files/Publikasi_06.12.1748.pdf

[11] G. Walker, “Learn Me a Bitcoin - Target,”, [online]. Available: http://learnmeabitcoin.com/glossary/target.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Mei 2022

Christopher Davin Leoputra (18219037)