Integrasi Distribusi Data Radar Menggunakan Teknologi Blockchain dan Kriptograf

Fahmi Rosyadi[1], Masbah R.T. Siregar[2,] Abdul Multi[3]

Program Studi Magister Teknik Elektro
Fakultas Pascasarjana
Institut Sains Dan Teknologi Nasional
Email : fahmi22a3@gmail.com

Abstrak

Saat ini radar banyak digunakan diberbagai bidang seperti meteorologi, militer, kepolisian, pelayaran, penerbangan, pertanian, kebencanaan, dan riset. Sedangkan saat ini penggunaan radar masih berbentuk sektoral, parsial, dan terpecah-pecah sehingga penggunaan data radar hanya sebatas internal. Dengan kondisi geogrfis Indonesia yang sangat luas dan belum maksimalnya integrasi dan distribusi data radar menyebabkan minimnya wilayah geografis Indonesia yang terjangkau oleh radar. Penggunaan atau pertukaran data radar masih menggunakan teknologi informasi berbasis *client-server*, dan dengan penyimpanan bersifat *centralized* yang memiliki faktor risiko keamanan informasi dan privasi yang rentan disalah gunakan atau dieksploitasi. Selain itu kemungkinan terjadinya kehilangan data yang mengakibatkan sulit didapatkan kembali datanya, bahkan ketika sudah menerapkan sistem cadangan dengan *cloud* atau perlindungan lainnya, masih terdapat risiko hilang data sepenuhnya jika dibandingkan dengan menerapkan *platform decentralized*. Oleh karena itu diperlukan integrasi dan distribusi data radar dengan *platform decentralized* sehingga data radar tidak berbentuk sektoral, parsial, dan terpecah-pecah. Integrasi dan distribusi data radar ini nantinya dapat memaksimalkan penggunaaan radar lintas bidang sehingga satu radar bisa digunakan lebih optimal bagi semua bidang termasuk meteorologi, militer, kepolisian, pelayaran, penerbangan, pertanian, kebencanaan, dan riset. Salah satu teknologi yang dapat digunakan untuk integrasi distribusi radar adalah *blockchain* dan kriptografi. Blockchain dan kriptografi asimetris selain dapat meningkatkan kemanan data, juga dapat menjamin bahwa data yang masuk ke sistem blockchain dari sumber yang benar. Semakin besar bit kunci kriptografi asimentris yang digunakan, semakin aman sebuah data.

Kata Kunci — Radar, Blockchain, kriptografi, Integrasi Distribusi

Abstract

Currently radar is widely used in various fields such as meteorology, military, police, shipping, aviation, agriculture, disaster, and research. Meanwhile, currently the use of radar is still in the form of sectoral, partial, and fragmented so that the use of radar data is only internal. With Indonesia's geographical condition which is very broad and the integration and distribution of radar data has not been maximized, this has resulted in the lack of geographic area of Indonesia that is reached by radar. The use or exchange of radar data still uses client-server-based information technology, and with centralized storage which has risk factors for information security and privacy that are vulnerable to being misused or exploited. In addition, there is the possibility of data loss which makes it difficult to get data back, even when you have implemented a backup system with cloud or other protection, there is still a risk of complete data loss when compared to implementing a decentralized platform. Therefore, it is necessary to integrate and distribute radar data with a decentralized platform so that the radar data is not sectoral, partial, and fragmented. This integration and distribution of radar data will later be able to maximize the use of cross-field radar so that one radar can be used more optimally for all fields including meteorology, military, police, shipping, aviation, agriculture, disaster, and research. One technology that can be used for the integration of radar distribution is blockchain and cryptography. Blockchain and asymmetric cryptography in addition to increasing data security, can also guarantee that data entering the blockchain system comes from the correct source. The larger the bit asymmetric cryptographic key used, the more secure the data.

Keywords — Radar, Blockchain, Cryptography, Integrated Distribution.

DOI: https://doi.org/10.37277/stch.v32i3 (https://ejournal.istn.ac.id/index.php/sainstech/article/view/1343/893)

I. PENDAHULUAN

Radar (*Radio Detection and Ranging*) merupakan sistem gelombang elektromagnetik yang digunakan untuk mendeteksi, mengukur jarak dan membuat map benda-benda seperti pesawat terbang, kendaraan bermotor dan informasi cuaca/hujan. Gelombang radio/sinyal yang dipancarkan dari suatu benda dapat ditangkap oleh radar kemudian dianalisa untuk mengetahui lokasi dan bahkan jenis benda tersebut (Akhmad Fadholi,2013).

Dengan kondisi geografis Indonesia yang sangat luas dan penggunaan data radar yang masih sektoral, parsial dan terpecah-pecah mengakibatkan jumlah radar yang dibutuhkan sangat banyak sedangkan harga radar itu sendiri terhitung masih mahal. Alhasil wilayah geografis Indonesia masih minim terjangkau oleh radar(Widjaya dkk.,2022).

Oleh karena itu diperlukan integrasi dan distribusi data radar sehingga data radar tidak berbentuk sektoral, parsial, dan terpecah-pecah. Integrasi dan distribusi data radar ini nantinya dapat memaksimalkan penggunaaan radar lintas bidang sehingga satu radar bisa digunakan oleh semua bidang termasuk meteorologi, militer, kepolisian, pelayaran, penerbangan, pertanian, kebencanaan, dan riset. Penggunaan radar secara bersama-sama ini tentunya dapat menghemat anggaran pembelian radar secara nasional(Widjaya dkk.,2022).

Pada saat ini penggunaan atau pertukaran data radar masih menggunakan teknologi informasi dengan sistem distribusi berbasis *client-server*, dan data radar disimpan dalam satu gudang data yang bersifat *centralized*. Dengan penyimpanan secara *centralized* memiliki faktor risiko terkait dengan keamanan informasi dan privasi yang lebih tinggi, adanya kemungkinan informasi akan disalah gunakan atau dieksploitasi (Mudliar dkk., 2018). Selain itu kemungkinan terjadinya kehilangan data yang mengakibatkan sulit didapatkan kembali datanya, bahkan ketika sudah menerapkan sistem cadangan dengan *cloud* atau perlindungan lainnya, masih terdapat risiko hilang data sepenuhnya jika dibandingkan dengan menerapkan *platform decentralized* (Jha dkk., 2019).

Solusi terkait integrasi data radar, distribusi data radar, ketersediaan data radar, keamanan data radar, dan kemudahan dalam pemutakhiran data radar yang dilakukan secara bersama dapat diselesaikan dengan menerapkan penyimpanan data dengan *platform decentralized*. Salah satu teknologi yang dapat mengakomodir hal tersebut adalah dengan teknologi *blockchain* dan kriptografi.

Blockchain merupakan sebuah rekaman autentik dari seluruh aktivitas yang terjadi dalam suatu jaringan, tersebar di seluruh komponen jaringan, dan saling terkait dalam suatu rangkaian blok data. *Blockchain* memberikan keamanan tambahan untuk penyimpanan data pada pusat pengatur jaringan. Di sisi lain, sistem kriptografi juga diterapkan untuk keamanan dan autentikasi data yang dikirimkan sehingga data tersebut hanya bisa diakses oleh pengirim dan penerima, serta keasliannya juga terjamin(Fadilla, 2021).

II. TINJAUAN PUSTAKA

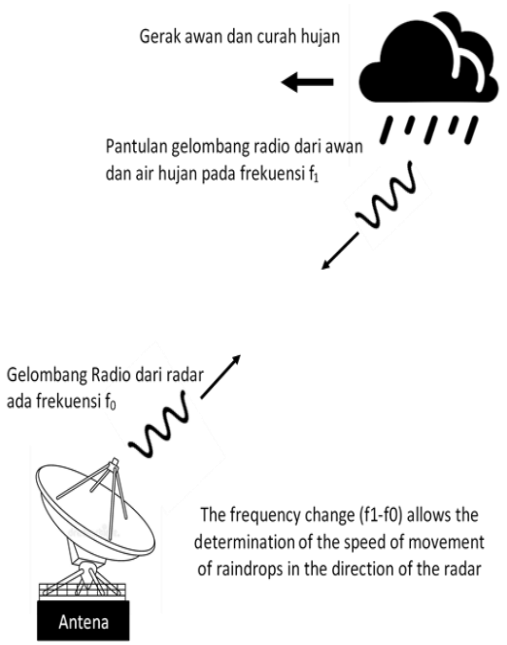
A. Radar (Radio Detection and Ranging)

Radar (*Radio Detection and Ranging*) merupakan suatu alat yang sistemnya memancarkan gelombang elektromagnetik berupa gelombang radio dan gelombang mikro. Pantulan dari gelombang yang dipancarkan kemudian digunakan untuk mendeteksi obyek yang berada di atmosfer. Gelombang radio/sinyal yang dipancarkan dari suatu benda dapat ditangkap oleh radar kemudian dianalisa untuk mengetahui lokasi dan bahkan jenis benda tersebut. Walaupun sinyal yang diterima relatif lemah, namun radar dapat dengan mudah mendeteksi dan memperkuat sinyal tersebut(Akhmad Fadholi,2013).

B. Radar Cuaca

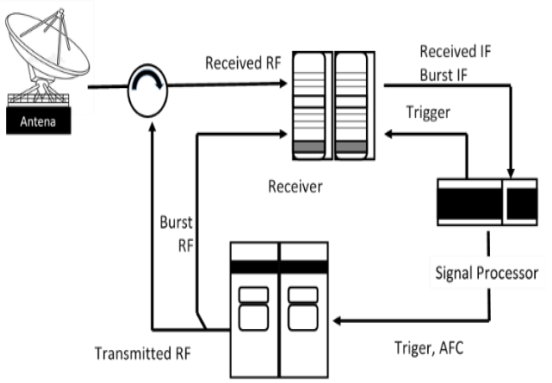
Radar cuaca bekerja berdasar efek Doppler yang artinya proses pendeteksian suatu objek oleh gelombang radio

berdasarkan selisih frekuensi pantul f_1 dari pergeseran frekuensi kerja radar f_0 akibat pergerakan objek tersebut. Semakin banyak objek tersebut dan bergerak cepat maka efek Doppler yang dihasilkan akan semakin besar. Efek Doppler inilah yang akan dikonversi menjadi redaman curah hujan dalam bentuk kode-kode warna (Anantia dkk., 2019). Prinsip kerjanya dapat dilihat pada Gambar 1 berikut.

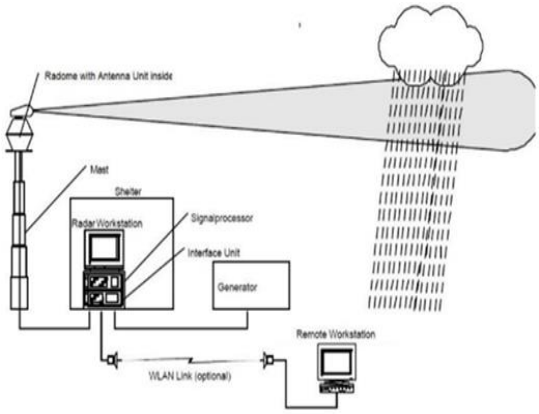


Gambar 1. Prinsip Kerja Radar Cuaca Berdasarkan Efek Doppler (Sumber : Anantia dkk., 2019)

Radar Cuaca di Indonesia kebanyakan masih menggunakan teknologi pemancar magnetron ataupun klystron. Tipikal blok diagram dari radar cuaca polarisasi tunggal (*single polarization*) dan polarisasi ganda (*dual polarization*) yang menggunakan pamancar magnetrón. Detail sistem radar cuaca dapat dilihat pada Gambar 2 berikut.



(a) Magnetron Transmitter



(b) Magnetron Polarisasi Tunggal

Gambar 2. Detil Sistem Radar Cuaca Magnetron Polarisasi Tunggal (Sumber : Anantia dkk., 2019)

C. Pengolahan Data Radar Cuaca

Radar Cuaca mengasilkan beberapa data, secara periodik data diperbaharui setiap 4 menit. Data-data ini disimpan di dalam komputer pemroses data menggunakan perangkat lunak *IRIS Sigmet*. Data akan dipisahkan ke dalam beberapa direktori sesuai dengan jenis data dan alur proses datanya.

Direktori /usr/iris_data yang ada dalam sistem radar terdiri dari :

- *ingest* : direktori hasil scan radar bersifat analog untuk diproses lagi menjadi data bersifat digital (*Cartesian*)
- Product : berisikan data-data digital (*Cartesian*) hasil scan radar cuaca yang sudah dipisahkan menjadi beberapa jenis data (PPI, CAP PI, *Rainfall* dan lain-lain)

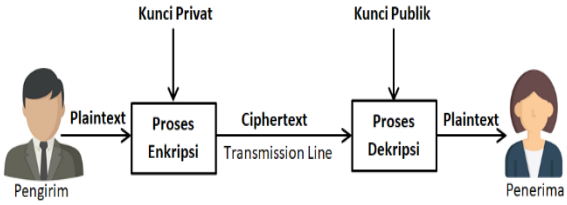
DOI: https://doi.org/10.37277/stch.v32i3 (https://ejournal.istn.ac.id/index.php/sainstech/article/view/1343/893)

- *Weatherscout* : direktori ini berisikan data yang sama dengan direktori *Product*, direktori ini diperlukan sistem radar untuk meletakan data-data yang akan digunakan perangkat lunak *Weatherscout* agar dapat ditampilkan ke dalam format grafis.
- *Images* : berisi data dalam bentuk gambar (*image*) hasil pengolahan dari data-data *Cartesian* yang sudah diplot sesuai dengan letak piksel-piksel yang dihasilkan oleh radar.
- *Archive* : berisikan data-data yang bersifat arsip. Data-data *cartesian* satu hari sebelumnya akan di gandakan ke direktori ini secara otomatis.

Radar akan membuat data secara periodik setiap 4 menit dimana data yang dihasilkan adalah berupa data *cartesian* dan *image* (gambar). Data *cartesian* dapat diubah menjadi dalam bentuk *textfile* menggunakan *utility software Iris-Sigmet (product examiner)*. Dengan utility ini akan dihasilkan data *text file* yang berisi header (keterangan dari data) dan data radar itu sendiri yang masih dalam nilai desible (dB) serta perlu dirubah menjadi nilai dBz (decible of Z). Nilai dBz (reflektifitas) selanjutnya dirubah menjadi Rainrate

D. Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan tersebut dikirim dari suatu tempat ke tempat lain. Kriptografi asimetris adalah salah satu jenis algoritma kriptografi yang sering juga disebut dengan algoritma kunci-publik. Artinya, kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Seperti terlihat pada Gambar 3 berikut.



Gambar 3. Proses enkripsi dan dekripsi menggunakan kriptografi asimetris.

Dalam kriptografi asimentris, ada beberapa komponen dasar yang membangunnya yaitu:

- *Plaintext* (teks-biasa) adalah pesan atau informasi asli yang ingin disampaikan di antara dua pihak.
- *Ciphertext* (teks-kode) adalah pesan atau informasi yang telah melalui proses enkripsi. *Ciphertext* berupa data yang terlihat acak atau tidak bermakna.
- Kunci pribadi (*private key*) adalah kunci yang dirahasiakan atau hanya boleh diketahui oleh satu orang..
- Kunci umum (*public key*) adalah kunci yang boleh semua orang tahu (dipublikasikan).
- Enkripsi adalah sebuah proses untuk mengubah *plaintext* menjadi *ciphertext* melalui suatu algoritma tertentu. Proses ini dilakukan oleh pihak pengirim.
- Dekripsi adalah sebuah proses untuk mengubah *ciphertext* menjadi *plaintext* kembali melalui suatu algoritma tertentu. Proses ini dilakukan oleh pihak penerima.

Salah satu jenis kriptografi asimetris adalah algoritma RSA. Algoritma RSA dikembangkan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman dari MIT (Massachusetts Institute of Technology) sebagai jawaban dari tantangan untuk membuat sistem kriptografi kunci publik yang aman. Mereka berhasil menemukan algoritma yang menurut mereka sulit dipecahkan tetapi perhitungan yang digunakan tetap sederhana.

RSA menggunakan skema dengan memodelkan *plaintext* dan *ciphertext* menjadi sebuah bilangan bulat antara nol dan n–1 untuk nilai n. Nilai dari n biasanya sebesar 1024 bit atau 309 digit desimal dan memanfaatkan prinsip dari eksponensial. Secara ringkas, berikut ini adalah langkah-langkah algoritma RSA:

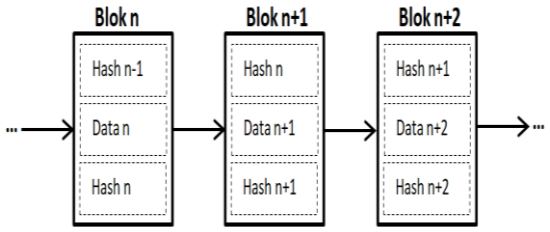
- Bilangan prima p dan q dipilih dengan $p \neq q$
- n dihitung dengan cara $n = p \times q$

- Φ(n) dihitung dengan $\phi(n) = (p-1)(q-1)$
- e dipilih sehingga memenuhi FPB $(\phi(n), e) = 1$ dan $1 < e < \phi(n)$
- d dicari sehingga memenuhi persamaan $e \cdot d \equiv 1 \pmod{(\phi(n))}$ atau $d \equiv e^{-1} \pmod{(\phi(n))}$
- Kunci publik PU adalah $[e, n]$
- Kunci privat PR adalah $[d, n]$
- Proses enkripsi : $C = M^e \bmod (n)$, dengan syarat $M < n$
- Proses dekripsi : $M = C^d \bmod (n)$Plaintext (teks-biasa)

E. Blockchain

Blokchain adalah sebuah rangkaian blok data yang berisikan informasi unik dan dilengkapi dengan kode hash sebagai bukti keterkaitan tiap blok yang dihasilkan.

Blockchain dapat diasumsikan sebagai arsip transaksi yang dikumpulkan pada blok-blok dengan penanda waktu atau *timestamp*. Setiap blok teridentifikasi dengan suatu nilai hash. Namun, setiap blok tersebut mereferensikan nilai hash dari blok yang ada sebelumnya. Oleh karena itu, ikatan antar blok akan terjadi dan membuat sebuah rantai blok atau *blockchain* seperti pada Gambar 4.



Gambar 4. Skema blockchain.

Skema tersebut akan berulang untuk blok-blok selanjutnya, tetapi pengecualian terjadi pada blok pertama dari rantai tersebut, yang dinamakan *genesis*. Blok *genesis* ini akan menjadi penanda secara umum pada seluruh jaringan *blockchain*, dan tanpa memiliki blok pendahulu. *Blockchain* memiliki karakteristik sebagai berikut :

- Konsensus: Sebuah data dapat dinyatakan *valid* ketika semua partisipan setuju dengan validitasnya.
- Asal: Partisipan mengetahui sumber datangnya data.
- Kekekalan: Tidak ada yang dapat merubah sebuah data setelah tercatat di jaringan *blockchain*.

Hash pada *blockchain* merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi hash yang paling sering digunakan adalah *Secure Hash Algorithm* (SHA). Hal itu dikarenakan kelemahan dasar dari fungsi hash lainnya telah ditemukan melalui *cryptanalysis*. SHA sendiri menjadi salah satu dari beberapa fungsi hash yang terstandarisasi. Hingga saat ini, ada dua versi SHA yang masih belum terbobol secara praktis, yaitu SHA2 dan SHA-3. Pada penelitian ini menggunakan algoritma SHA-2 yaitu SHA-256.

SHA-2 menggunakan enam fungsi logis, di mana setiap fungsi beroperasi pada kata 32-bit, yang direpresentasikan sebagai x, y, dan z. Hasil dari setiap fungsi adalah kata 32-bit baru.

$Ch(x, y, z) = (x \wedge y) \oplus (x \wedge z)$ (1)

$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$ (2)

$\sum_0^{\{256\}}(x) = RTOR^2(x) \oplus RTOR^{13}(x) \oplus RTOR^{22}(x)$ (3)

$\sum_1^{\{256\}}(x) = RTOR^6(x) \oplus RTOR^{11}(x) \oplus RTOR^{25}(x)$ (4)

$\sigma_0^{\{256\}}(x) = RTOR^7(x) \oplus RTOR^{18}(x) \oplus SHR^3(x)$...(5)

$\sigma_1^{\{256\}}(x) = RTOR^{17}(x) \oplus RTOR^{19}(x) \oplus SHR^{10}(x)$.(6)

III. METODE PENELITIAN

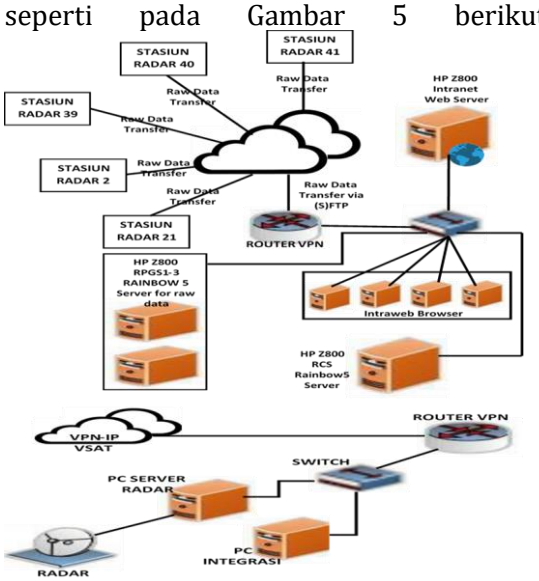
A. Identifikasi Sistem Eksisting

Radar terintegrasi yang sudah beroperasi adalah radar cuaca, seperti di Amerika dengan nama NEXRAD, atau OPERA yang dioperasikan negara-negara di Eropa. Sedangkan di Indonesia sendri, PT. LEN menjembatani sistem integrasi radar cuaca yang dioperasikan BMKG di berbagai wilayah Indonesia. Ada 41 radar yang sudah diintegrasikan. Pengintegrasian radar tersebut meliputi konektivitas setiap radar

dalam satu sistem jaringan radar dan juga penyatuan data radar untuk melihat profil cuaca utuh Indonesia secara bersamaan (*concurrently*).

Radar cuaca menghasilkan data secara berkesinambungan (*continue*) setiap 10 menit sekali (*setting observation interval* bervariasi antara 5 menit sampai 10 menit), data tersebut akan tersimpan pada tempat penyimpanan lokal di lokasi radar. Tingginya frekuensi pengamatan oleh radar menyebabkan data radar cuaca yang disimpan berukuran cukup besar dan bervariasi tergantung pada jenis produk radar. Kemudian data tersebut akan di transfer dan di-*backup* ke stasiun pusat. Bila proses transfer tidak terjadi dan atau tempat penyimpanan data di lokasi radar sudah penuh, maka data radar yang baru akan menggantikan data yang lama (*over-written*).

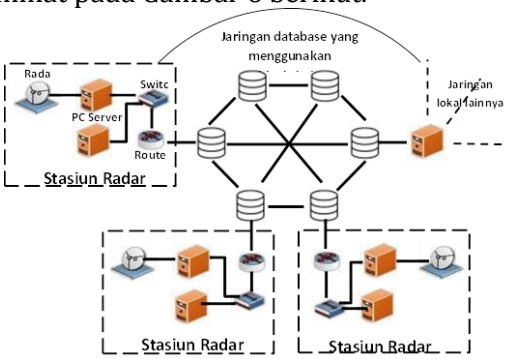
Selain terintegrasinya radar selanjutnya mendistribusikan data/informasi yang tersedia. Untuk mengintegrasikan radar cuaca pada jaringan telekomunikasi maka ditempatkanlah perangkat-perangkat baru diantara radar dan jaringan telekomunikasi tersebut. Dengan penambahan perangkat baru tersebut topologi jaringan radar cuaca seperti pada Gambar 5 berikut.



Gambar 5. Blok diagram sistem integrasi radar eksisting.

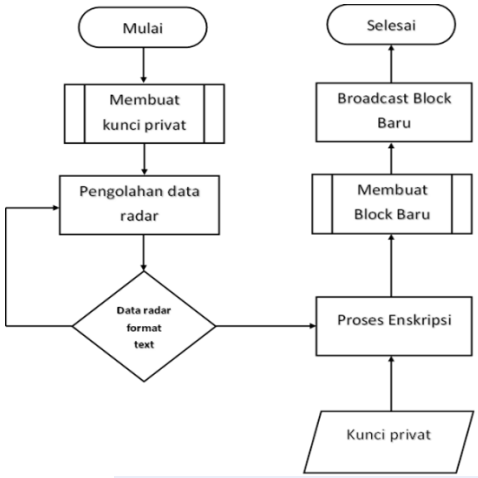
B. Sistem Integrasi Distribusi Data Radar Menggunakan Blockchain dan Kriptografi

Teknologi *blockchain* pada sistem integrasi distribusi data radar sebagian besar cara kerjanya sama dengan teknologi *blockchain* yang terdapat dalam sistem *Bitcoin* dan berfokus pada pencatatan *database*. Node yang terlibat dalam *Blockchain* yang telah digunakan oleh *Bitcoin* adalah independen bersifat acak dan tidak dihitung (Wu dkk., 2017). Tetapi pada sistem ini digunakan permission *blockchain*, node dibuat bersifat sebaliknya dari sistem *Bitcoin*. Metode ini bertujuan untuk menjaga integritas data yang terlindungi dari manipulasi sehingga data radar lebih terjamin keamanan datanya. Blok diagram Sistem Integrasi radar eksisting dapat dilihat pada Gambar 6 berikut.

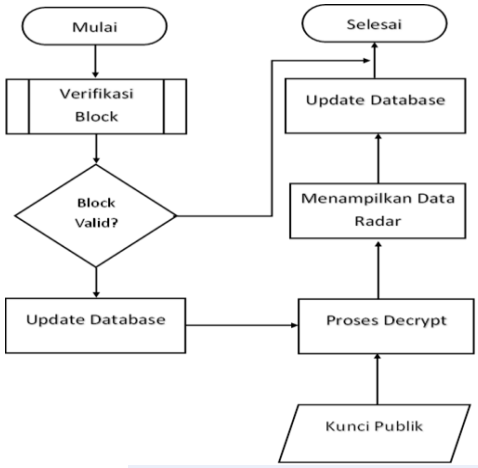


Gambar 6. Blok diagram sistem integrasi radar eksisting.

Secara garis besar alir proses integrasi dan distribusi data radar menggunakan *blockhain* dan kriptografi adalah sebagai mana terlihat pada Gambar 7 dan 8 berikut :

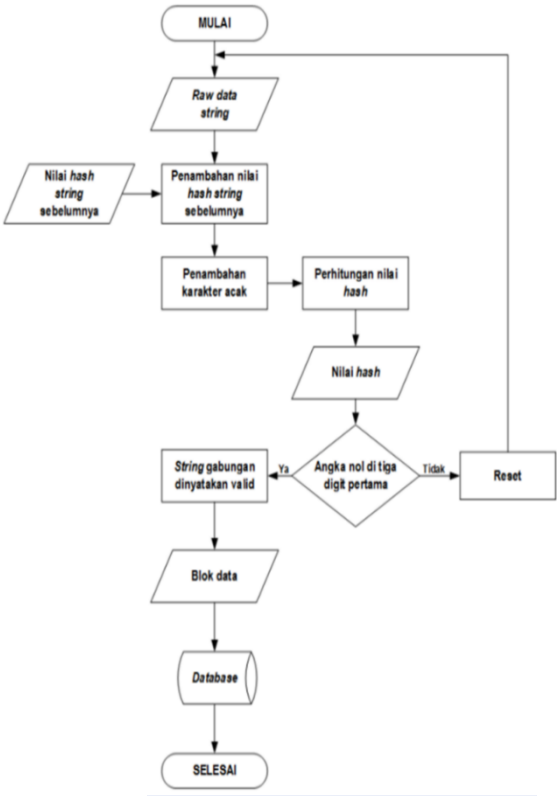


Gambar 7. Diagram Alir Node Pengirim Data Radar.



Gambar 8. Diagram Alir Node Penerima Data Radar.

Langkah Penyusunan blok dari blockchain dapat dilihat pada Gambar 9 berikut.



Gambar 9. Diagram alir penyusunan blok dari blockchain.

Proses ini dimulai saat pembacaan data radar pada setiap node dilaksanakan. Sebelum proses pembacaan radar dimulai, node yang terhubug dengan radar membangkitkan *private key* dan *public key*. Setiap node penerima data radar harus memiliki *public key* seluruh node yang terhubung langsung dengan radar. Node akan mengumpulkan hasil pengolahan data radar kemudian data tersebut di enskripsi. Apabila proses enskripsi data radar telah selesai, maka node akan membuat blok. Blok yang telah dibuat akan di distribuskan keseluruh node. Setibanya blok pada tiap node, node penerima akan melakukan verifikasi untuk mengetahui valid atau tidaknya block tersebut. Apabila blok dinyatakann *valid*, maka data akan ditambahkan ke *database*. Langkah terakhir adalah melakukan *decrypt* dari data yang diterima node dengan menggunakan *public key*.

IV. HASIL DAN PEMBAHASAN

A. Pengambilan Data Radar

Integrasi dan distribusi data radar menggunakan blockchain dan kriptografi dimulai dari pengambilan data radar . Pengambilan data radar menghasilkan data sebagaimana terlihat pada Tabel 1 berikut:

TABEL I. DATA RADAR CURAH HUJAN TERHADAP SATUAN WAKTU

No	Akum. Waktu	Posisi 1 (106.0-106.4999)			Posisi 2 (106.5-106.9999)		
		CH /6m	CH /30 m	CH /60m	CH /6m	CH /30m	CH /60 m
1	6	0.38			0.02		
2	12	0.28			0.05		
3	18	0.36	1.65		0.11	0.26	
4	24	0.30			0.04		
5	30	0.33		2.86	0.04		0.71
6	36	0.29			0.10		
7	42	0.24			0.06		
8	48	0.22	1.21		0.01	0.45	
9	54	0.23			0.03		
	…						
240	1440	0.11			0.09		

B. Pengujian Pembangkitan Kunci Privat dan Publik

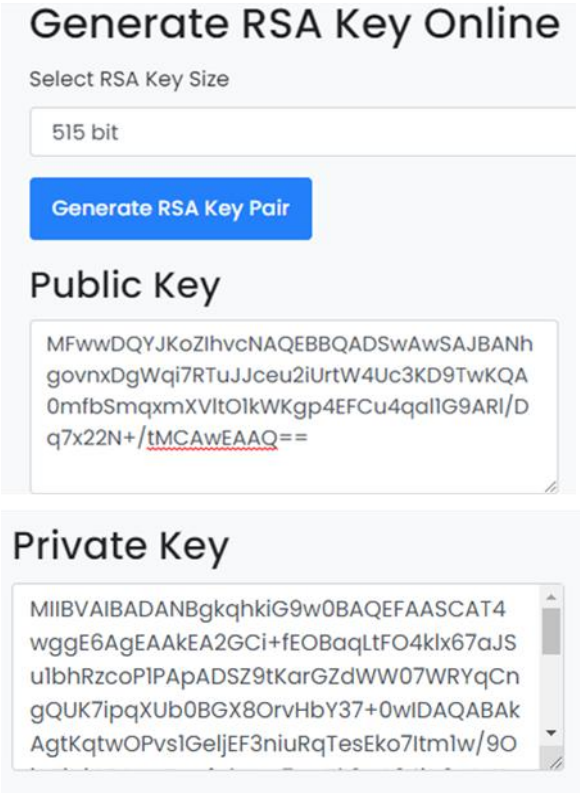
Sebelum data radar tersebut dimasukkan ke dalam proses enskripsi, terlebih dahulu dibuat kunci publik dan kunci privat. Pembangkitan kunci Privat dan Publik ini menggunakan *Generate RSA Key Online* (Gambar 10 dan 11 serta Tabel 2) dan didapat hasil sebagai berikut :

Kunci Privat :

MIIBVAIBADANBgkqhkiG9w0BAQEFAAS
CAT4wggE6AgEAAkEA2GCi+fEOBaqLtFO4
klx67aJSu1bhRzcoP1PApADSZ9tKarGZdW
W07WRYqCngQUK7ipqXUb0BGX8OrvHbY
37+0wIDAQABAkAgtKqtwOPvs1GeljEF3ni
uRqTesEko7Itm1w/9OiqTi+jGEGVvTMyfal
Wex5qaZk0YO24jA0uBNPmuPKsHCRlhAiE
A9H+nJUE/yUYqbpMP5fzZZewTX/8McW
MhcBpaonxei+sCIQDijlZ/K0CKbTXAtHgP0f
SkEIiaIoh90Ot5YxEQmHUmuQIgIpN627Xig
2A81+5MLUYYqGU+SDEVXWObcvMHJjtY
U4kCIQCyl13cFW5lML3k0N6sKefdxSLJzls
mQyC8qbl0CZqgEQIgXVu0FZKL8+mDfs/b
7mcpJiHlfxwaQ01r5G5sFc82Y7w=

Kunci Publik :

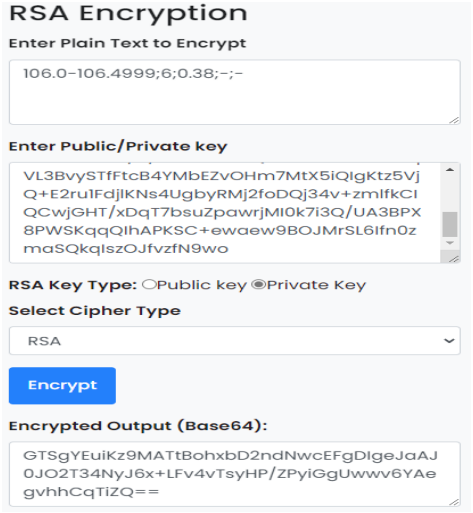
MFwwDQYJKoZIhvcNAQEBBQADSwAwS
AJBANhgovnxDgWqi7RTuJJceu2iUrtW4Uc3
KD9TwKQA0mfbSmqxmXVltO1kWKgp4EF
Cu4qal1G9ARl/Dq7x22N+/tMCAwEAAQ=
=



Gambar 10. Generate RSA Key.

C. Pengujian Enkripsi

Setelah mendapatkan kunci privat dan kunci publik, data radar di enkripsi menggunakan kunci privat.



Gambar 11. Enkripsi RSA.

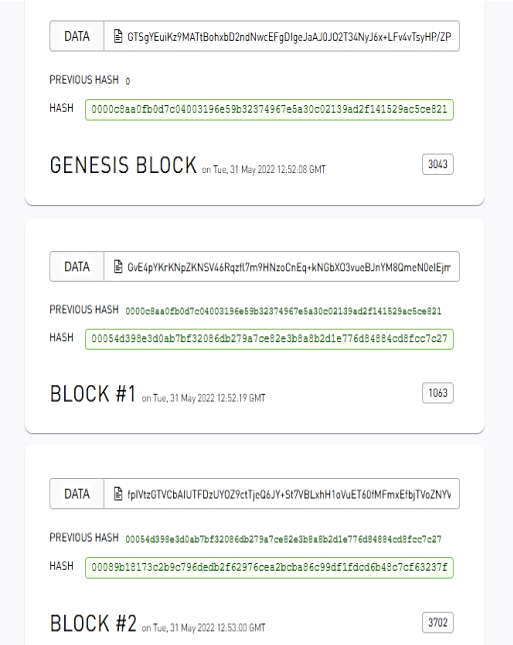
TABEL 2. DATA HASIL ENKRIPSI MENGGUNAKAN KUNCI PRIVAT

No	Plaintext	Chipertext
1	106.0-106.4999;6;0.38;-;-	GTSgYEuiKz9MATtBohxbD2ndNwcEFgDIgeJaAJ0JO2T34NyJ6x+LFv4vTsyHP/ZPyiGgUwwv6YAegvhhCqTiZQ==
2	106.0-106.4999;12;0.28;-;-	GvE4pYKrKNpZKNSV46Rqzfl7m9HNzoCnEq+kNGbXO3vueBJnYM8QmeN0eIEjmAKO4Z79Xc3PRsEAXbQircXPpg==
3	106.0-106.4999;18;0.36;1.65;-	fpIVtzGTVCbAIUTFDzUYOZ9ctTjeQ6JY+St7VBLxhH1oVuET60fMFmxEfbjTVoZNYVUq/z4tdea6Hgp4MfCqcg==
4	106.0-106.4999;24;0.30;-;-	EA89d9Lhvd1JWuif0+oYmDFMPOX8qkotyX39qsV4D4EQBluffAf6l3fitdSHbweH9AJRE5pbLkZr2tJ8Jb6eFg==
5	106.0-106.4999;30;0.33;-;2.86	enw50APUqJOgaisJA+NIE4ajqg5WJpN4GLRbW8IL67+IK9bFrH6SQDSef8X/Q25vIb/Gn6TqSCZC/MmkVGPflA==
6	106.0-106.4999;36;0.29;-;-	aoSJ0IfQ+DlXrBMYq45hIJtoTKabKyIkCA4PJP+wYULvseogKm8th/iBQMoDL0Bnex7AxV2p9xSglDR2Kenx9A==

7	106.0-106.4999;42;0.24;-;-	YNpSXVr2hEJSYPSw46C7AwmnywKBkZK+6KsbJvi5y9qgqHsFOZz6MIN2GJZ/670McnAX1smx4fBsUBW52TQObA==
8	106.0-106.4999;48;0.22;1.21;-	WAa4srk/lMbOFCjZE8CqnHbFLvIP9sXBc/feP1AfB5OfoE1P7kPhiVvjkRxE3d5/ClCdweX07DZ6LjJUzlohow==
…		
240	106.0-106.4999;1440;0.11;-;-	3baT/OTroZp0XopXjgahzXcBUuMF65d/YqrQKa4eNwVoh7oe3AWmJrw8kdgrprlv6W/GpUjfYwYu0qC9KYdvfA==

D. Pengujian Blockchain

Data enkripsi yang didapat kemudian dimasukkan kedalam system blockchain



Gambar 12. Proses Blockchain.

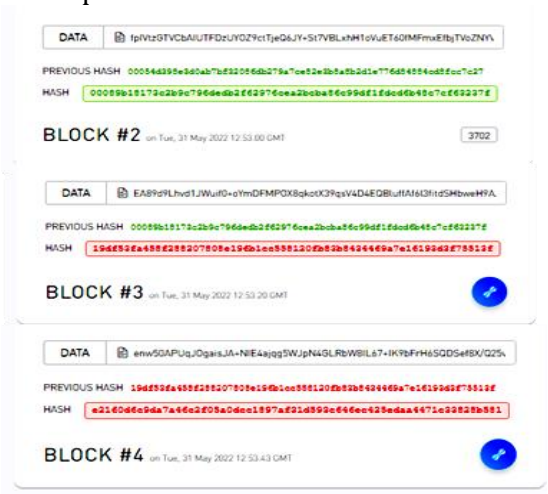
TABEL 3. DATA BLOCKCHAIN

Block	**Data (Baris 1),Previous Hash (Baris 2), Hash (Baris3), Nounce(Baris 4)**
Genesis	GTSgYEuiKz9MATtBohxbD2ndNwcEFgDIgeJaAJ0JO2T34NyJ6x+LFv4vTsyHP/ZPyiGgUwwv6YAegvhhCqTiZQ==
	0
	000aeb9f4d3f7e8a50d1266afaddd6b57371f6c61d77d0668d1fd6dc26fe7897
	5792
Block #1	GvE4pYKrKNpZKNSV46Rqzfl7m9HNzoCnEq+kNGbXO3vueBJnYM8QmeN0eIEjmAKO4Z79Xc3PRsEAXbQircXPpg==
	000aeb9f4d3f7e8a50d1266afaddd6b57371f6c61d77d0668d1fd6dc26fe7897
	000fa62f5fcd6ff495d368ee0393c1566e5e8c1f939fdccca0adcfeea2db42fc
	4043
Block #2	fpIVtzGTVCbAIUTFDzUYOZ9ctTjeQ6JY+St7VBLxhH1oVuET60fMFmxEfbjTVoZNYVUq/z4tdea6Hgp4MfCqcg==
	000fa62f5fcd6ff495d368ee0393c1566e5e8c1f939fdccca0adcfeea2db42fc
	00021065e2fb394a345c5a2f3e092b0014141360f4479b8901e885c5260738f5
	7341
…	
Block #239	aoSJ0IfQ+DlXrBMYq45hIJtoTKabKyIkCA4PJP+wYULvseogKm8th/iBQMoDL0Bnex7AxV2p9xSglDR2Kenx9A==
	000080d81bff09dfd6fb098511cec1766530974a93d1585aeccd7552c5d95112
	0001aa19c7db5ca49017c21237e271999b681c2b9842626cf42b09c22677a77d
	864

Block-block yang terbentuk akan dikirim ke semua node secara real-time. Pada terjadi kerusakan data yang disengaja atau tidak disengaja maka block yang mengalami perubahan data dan dinyatakan tidak valid

DOI: https://doi.org/10.37277/stch.v32i3 (https://ejournal.istn.ac.id/index.php/sainstech/article/view/1343/893)

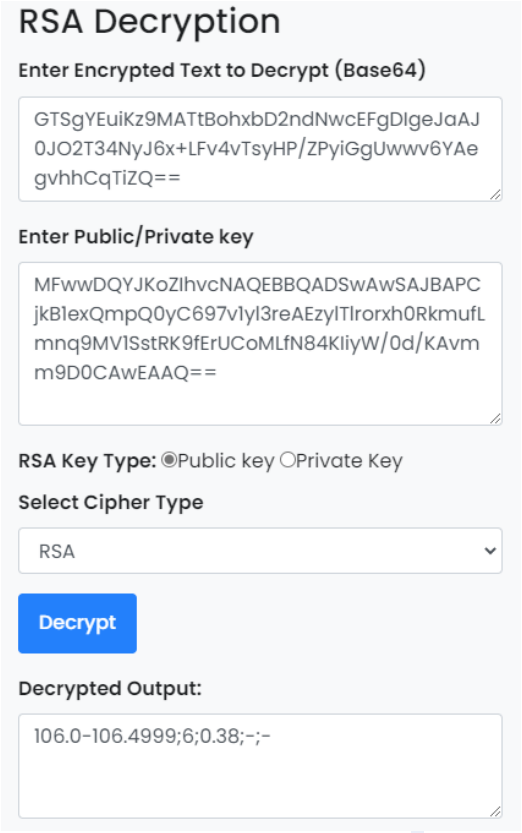
serta ditandai dengan warna merah, Seperti terlibat pada Gambar 13 berikut.



Gambar 13. Block Mengalami Perubahan Data.

E. Pengujian Dekripsi

Block yang dinyatakan valid di node penerima perlu dilakukan proses dekripsi untuk mendapatkan data radar (Gambar 14).



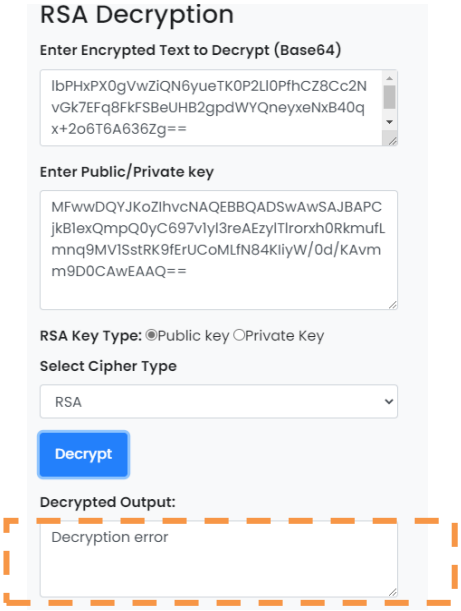
Gambar 14. Dekripsi RSA .

Hasil deskripsi terlihat pada Tabel 4 berikut.

TABEL 4. HASIL DEKRIPSI MENGGUNAKAN KUNCI PUBLIK

No	Chipertext	Plaintext
1	GTSgYEuiKz9MATtBohxbD2ndNwcEFgDIgeJaAJ0JO2T34NyJ6x+LFv4vTsyHP/ZPyiGgUwwv6YAegvhhCqTiZQ==	106.0-106.4999;6;0.38;-;
2	GvE4pYKrKNpZKNSV46Rqzfl7m9HNzoCnEq+kNGbXO3vueBJnYM8QmeN0eIEjmAKO4Z79Xc3PRsEAXbQircXPpg==	106.0-106.4999;12;0.28;-;-
3	fpIVtzGTVCbAIUTFDzUYOZ9ctTjeQ6JY+St7VBLxhH1oVuET60fMFmxEfbjTVoZNYVUq/z4tdea6Hgp4MfCqcg==	106.0-106.4999;18;0.36;1.65;-
4	EA89d9Lhvd1JWuif0+oYmDFMPOX8qkotyX39qsV4D4EQBluffAf6l3fitdSHbweH9AJRE5pbLkZr2tJ8Jb6eFg==	106.0-106.4999;24;0.30;-;-
...		
240	3baT/OTroZp0XopXjgahzXcBUuMF65d/YqrQKa4eNwVoh7oe3AWmJrw8kdgrprlv6W/GpUjfYwYu0qC9KYdvfA==	106.0-106.4999;1440;0.11;-;-

Pengujian dekripsi ini akan berhasil dilakukan, bila menghasilkan *plaintext* kembali seperti data awal. Perubahan data meskipun hanya satu huruf akan menyebabkan proses dekripsi *error* seperti Gambar 15 berikut ini :



Gambar 15. Proses Dekripsi Error Akibat Manipulasi Data .

V. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan dapat kita simpulkan bahwa integrasi dan distribusi data radar menggunakan sistem *blockchain* bisa lebih efektif dibanding sitem eksisting yang ada. Keamanan data radar pada sistem *blockchain* dan kriptografi memiliki tingkat keamanan yang tinggi dan semakin terjamin keaslian data karena proteksi keamanan data dilakukan secara berlapis. *Blockchain* dan kriptografi asimetris selain dapat meningkatkan kemanan data, juga dapat menjamin bahwa data yang masuk ke sistem *blockchain* dari sumber yang benar. Semakin besar bit kunci kriptografi asimentris yang digunakan, semakin aman sebuah data.

REFERENSI

T. Debora Mayke M, Processing Daata Radar Cuaca C-Band Doppler untuk Curah Hujan, skripsi, Institut Pertanian Bogor, Jan. 2011.

Pusat Penelitian dan Pengembangan Sumber Daya Air. 2014. Optimasi Pemanfaatan Radar Cuaca untuk Siaga Bencana di Daerah Gunung Merapi. Badan Penelitian dan Pengembangan Kementerian Pekerjaan Umum, Jakarta. 30 hal.

P. Anantia, dan U. Fitria Dwi, Sistem Informasi Radar Cuaca Terintegrasi BMKG, *Journal of Telecommunication, Elektronics Engineering (JTECE).*, vol. 01, no. 02, pp. 09-19, Jul. 2019.

W. Dwi Fitra H. S., Perancangan dan Implementasi Teknologi Blockchain Pemilu Berdasarkan Formulir C1 Pindaian KPU, tesis, Institut Teknologi Bandung, Jan. 2019.

F. Rana Zaini, Sistem Keamanan Penyimpanan Data Identitas Nasional Terintegrasi dengan Teknologi Blockchain, tesis, Institut Teknologi Bandung, Mar. 2020.

M. Fadilla Nur A., Perancangan dan Implementasi Sistem Pencatatan Izin Mendirikan Bangunan Menggunakan Teknologi Blockchain, tesis, Institut Teknologi Bandung, Jan. 2021.

D. Widjaya, Akuntabilitas Kinerja Deteksi Dini Bencana Alam Geologi dan Hidrometeorologi di Indonesia, Pusat Kajian Akuntabilitas Keuangan Negara Badan Keahlian DPR RI, Jun. 2022.

A. Fadholi, RADAR : Radio Detection and Ranging,http://www.fisikanet.lipi.go.id/utama.cgi?fenomena&1364039911, Apr. 2022.

D. Milosav, and M. Nistoskaya, Blockchain Technology, Working Paper Series 20022:2, QoG The Quality of Government Insitute, Mar. 2022.

F. Nova Hulu, Metode Analisi Enkripsi dan Dekripsi Dengan Penerapan Algoritma Kriptografi Klasik Ke Dalam Chiper, Jurnal Elektro dan Telkomunikasi, [S.l.], v. 8, n. 01, p. 26 - 34, mar. 2022.