Analisis Penggunaan Blockchain untuk Meningkatkan Keamanan Gmail dari Serangan Phising

Muhammad Tsaqib Al [1], Fauzi Nur Azis[2], Alfito Muhammad Fernanda[3*]

[1]*Teknik Informatika*
Universitas Duta Bangsa Surakarta
[1]220103067@mhs.udb.ac.id

[2] *Teknik Informatika*
Universitas Duta Bangsa Surakarta
[2]220103058@mhs.udb.ac.id

[3]*Teknik Informatika*
Universitas Duta Bangsa Surakarta
[3]*220103045@mhs.udb.ac.id*

***Abstrak*— Perkembangan teknologi informasi yang peat telah mempermudah manusia dalam berbagai asperk kehidupan, termasuk dalam komunikasi dan penyimpanan data. Salah satu bentuk komunikasi digital yang paling seting digunakan adalah Email. Namun, meningkatnya penggunaan email juga diikuti oleh meningkatnya ancaman keamanan, salah satunya adalah serangan phishing. Penelitian ini bertujuan untuk menganalisis penggunaan teknologi blockchain dalam meningkatkan keamanan email Gmail dari serangan phishing. Metode penelitian yang digunakan adalah kuantitatif asosiatif dengan pengambilan data melalui survei kuesioner yang disebarkan kepada 50 responden pengguna Gmail. Data yang dikumpulkan mencakup pemahaman responden terhadap teknologi blockchain, pengalaman mereka terkait serangan phishing, serta pandangan mereka tentang efektivitas blockchain dalam meningkatkan keamanan email. Dari data kuesioner, terungkap bahwa 24% responden sangat familiar dengan teknologi blockchain, 36% cukup familiar, dan 40% tidak familiar. Hasil penelitian menunjukkan bahwa meskipun pemahaman tentang teknologi blockchain masih terbatas, terdapat minat yang signifikan terhadap penerapannya untuk meningkatkan keamanan email. Penelitian ini menyimpulkan bahwa edukasi lebih lanjut dan demonstrasi manfaat teknologi blockchain dapat mendorong adopsi yang lebih luas dan meningkatkan keamanan email dari serangan phishing.**
Kata kunci— Keamanan email, blockchain, phishing, gmail, teknologi informasi.

***Abstract*— The rapid advancement of information technology has significantly eased various aspects of human life, including communication and data storage. One of the most widely used forms of digital communication is email. However, the increased use of email is accompanied by rising security threats, such as phishing attacks. This research aims to analyze the use of blockchain technology in enhancing the security of Gmail emails against phishing attacks. The research methodology employed is quantitative associative, utilizing data gathered through a questionnaire survey distributed to 50 respondents who are Gmail users. The collected data includes respondents' understanding of blockchain technology, their experiences with phishing attacks, and their views on the effectiveness of blockchain in enhancing email security. From the questionnaire data, it was found that 24% of respondents are very familiar with blockchain technology, 36% are somewhat familiar, and 40% are not familiar. The research results indicate that despite limited understanding of blockchain technology, there is significant interest in its application to enhance email security. The study concludes that further education and demonstration of blockchain benefits could drive wider adoption and improve email security against phishing attacks.**
Keywords— Email security, blockchain, phishing, Gmail, information technology.

I. PENDAHULUAN

Perkembangan teknologi informasi saat ini berlangsung sangat pesat, termasuk di Indonesia. Teknologi pada dasarnya dirancang untuk memudahkan kehidupan manusia[1]. Salah satu perkembangan teknologi yang paling pesat adalah pada bidang teknologi komunikasi. Perkembangan teknologi komunikasi yang sangat pesat membawa berbagai peluang dan tantangan[2]. Salah satu teknologi komunikasi yang paling banyka digunakan di seluruh dunia adalah email. Email merupakan aplikasi yang sangat populer dan digunakan setiap hari untuk keperluan pribadi, bisnis, atau publik[3]. Email memegang peranan yang sangat penting dalam pekerjaan. Karena itu, banyak penjahat mencoba mencuri privasi atau menggunakan email untuk tujuan lain[4].

Ancaman email yang harus diwaspadai yaitu: (1) spam, (2) penipuan, (3) phishing, (4) penyebaran malware, (5) spoofing. Hingga saat ini, belum ada peraturan yang menjamin perlindungan khusus terhadap masyarakat atas berbagai permasalahan terkait penyalahgunaan data pribadi dalam penggunaan teknologi informasi[5].

Phising merupakan bentuk penipuan elektronik yang bertujuan untuk memperoleh informasi sensitif seperti username, password, dan detail kartu kredit. Dalam praktiknya, pelaku phising

akan meniru identitas entitas yang terpercaya atau organisasi sah dan berkomunikasi melalui media elektronik[6].

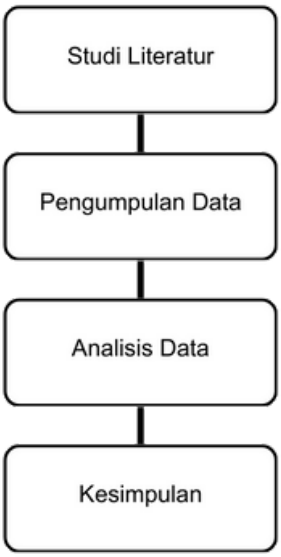
Perusahaan logistik dan pelayaran semakin sering menjadi sasaran serangan phishing. Dalam serangan phishing, pelaku kejahatan siber menghubungi organisasi yang menjadi target melalui email (phishing), telepon (vishing), atau pesan teks (SMSishing), dan menyamar sebagai individu atau organisasi yang tepercaya. Tujuan dari serangan ini adalah untuk mengelabui penerima agar memberikan informasi sensitif dan kata sandi sehingga pelaku dapat mengakses data secara ilegal demi keuntungan finansial[7].

Gmail, sebagai salah satu layanan email terbesar di dunia, juga tidak kebal terhadap serangan phising. Meskipun Google telah menerapkan berbagai mekanisme keamanan seperti filter spam dan teknologi machine learning untuk mendeteksi email berbahaya, penjahat siber terus mencari celah baru untuk mengecoh pengguna. Oleh karena itu, diperlukan pendekatan baru yang lebih kuat untuk meningkatkan keamanan email melindungi pengguna dari serangan phising[8].

Blockchain adalah teknologi yang memberikan tingkat keamanan yang tinggi pada data dengan menggunakan sistem database yang terdesentralisasi dan terenkripsi, sehingga mencegah manipulasi data atau akses yang tidak sah. Selain itu, teknologi blockchain dilengkapi dengan sistem pengauditan yang kuat yang dapat meningkatkan transparansi dalam pengelolaan data[9].

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dan kuantitatif untuk menganalisis penggunaan blockchain dalam meningkatkan keamanan email Gmail dari serangan phishing. Metodologi yang digunakan dalam penelitian ini meliputi beberapa tahapan, tahapan penelitian dapat dijelaskan pada Gambar 1 berikut:



Gambar 1. Diagram Blok Metode Penelitian

Berdasarkan Gambar 1berikut adalah langkah proses dari penelitian ini :

1. Melakukan studi literatur terkait blockchain,keamanan email, dan phishing.
2. Mengumpulkan data melalui kuesioner kepada pengguna Gmail.
3. Menganalisis data kuesioner untuk menilai efektivitas blockchain.
4. Melakukan kesimpulan dari analisis data.

Pemilihan metode blockchain didasarkan pada pertimbangan bahwa Gmail memerlukan tingkat keamanan yang sangat tinggi untuk meelindungi data pengguna. Salah satu yang dipilih adalah blockchain dengan algoritma kriptografi canggih yang menjamin ekripsi data yang kuat dan tahan terhadap upaya intruksi oleh pihak yang tidak berwenang. Selain itu, blockchain juga dapat digunakan untuk menerapkan sistem verifikasi multi-faktor yang lebih aman. Hal ini memungkinkan Gmail untuk menyimpan lapisan verifikasi tambahan di blockchain, memastikan hanya pengguna yang benar-benar berwenang yang dapat mengakses akun mereka.

III. HASIL DAN PEMBAHASAN

A. Cara Kerja Phising pada Gmail

Cara kerja serangan Email Phishing diawali dengan serangan dimana seorang penyerang mengambil alih server web, kemudian mengirimkan email phising/ email palsu kepada korban dengan tautan berbahaya atau konten palsu yang meminta informasi pribadi. Saat korban mengklik tautan tersebut, mereka diarahkan ke situs web yang telah dikompromi ileh penyerang. Situs web phishing palsu muncul, menipu korban untuk memasukkan informasi pribadi. Setelah mendapatkan informasi yang diinginkan, penyerang dapat menyalahgunakan informasi tersebut untuk keuntungan probadi atau bahkan melakukan pemerasan terhadap korban[10].

B. Persentase Serangan dalam Gmail

Tabel ini menunjukkan presentase relatif dari kasus email phishing yang terdeteksi di Indonesia selama tahun 2020 menurut laporan Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas)[11].

"Pusopskamsinas pada tahun 2020 mendeteksi terjadinya email phishing sebanyak 2.549 kasus."

Jenis Waktu Pengiriman	Presentase Serangan%
Jam Kerja (09.00 – 17.00)	55,53 %
Di Luar Jam Kerja	44,37 %

Tabel 1. Presentase Serangan Gmail

C. Dampak Serangan Phising dalam Gmail

Dampak serangan phishing dalam Gmail dapat sangat merugikan bagi pengguna dan organisasi. Antara lain sebagai berikut:

1. Spammer akan menggunakan akun yang sudah terkena phishing untuk mengirimkan banyak email palsu atau scam. Dengan Demikian, email server UI diblokir oleh mail server yang lain, sehingga pengguna tidak dapat mengirimkan email resmi, baik dari UI ke mail server lain maupun dari mail server di luar UL.

2. Pelaku Phishing akan menggunakan data atau informasi yang mereka peroleh untuk melakukan tindakan yang merugikan dari sisi keamanan seperti mencuri dengan mengatasnamakan diri sendiri, meretas sistem komputer, dll.

D. Potensi Blockchain dalam Keamanan Email

1. Blockchain dapat memberikan keamanan tambahan melalui pencatatan transaksi yang tidak dapat diubah.
2. Transparansi dan desentralisasi blockchain membuatnya sulit bagi penyerang untuk memalsukan identitas pengirim atau isi pesan.

E. Hasil Survei Pengguna Gmail

Penelitian ini bertujuan untuk menganalisis penggunaan blockchain dalam meningkatkan keamanan email Gmail dari serangan phishing. Penelitian menggunakan metode kuantitatif dengan pengambilan data melalui survei. Data dikumpulkan melalui kuesioner yang disebarkan kepada responden untuk menilai efektivitas blockchain dalam meningkatkan keamanan email dan kesadaran pengguna terhadap teknologi blockchain seta serangan phishing. Berikut adalah hasil dan pembahasan dari penelitian ini berdasarkan data yang diperoleh dari 50 responden yang dijelaskan pada Tabel 2.

Tabel 2. Data Kuesioner

No	Pertanyaan	Jawaban	Jumlah Responden	Presentase
1	Seberapa familiar Anda dengan teknologi Blockchain	Sangat Familiar	12	24%
		Cukup Familiar	18	36%
		Tidak Familiar	20	40%
2	Apakah Anda tahu apa itu Phising?	Sangat Familiar	35	70&
		Cukup Familiar	10	20%
		Tidak Familiar	5	10%
3		Pernah	12	24%

	Apakah Anda pernah menjadi korban phising?	Belum	30	60%
		Tidak Yakin	8	16%
4	Seberapa sering Anda menerima email Phising?	Sering	10	20%
		Jarang	20	40%
		Tidak Pernah	20	40%
5	Menurut Anda, seberapa aman Gmail dari serangan phising?	Sangat Aman	15	30%
		Cukup Aman	20	40%
		Tidak Aman	15	30%
6	Seberapa penting keamanan email bagi Anda	Sangat Penting	30	60%
		Cukup Penting	15	30%
		Tidak Penting	5	10%
7	Apakah Anda setuju bahwa penggunaan blockchain dapat meningkatkan keamanan Gmail?	Setuju	20	40%
		Netral	15	30%
		Tidak Setuju	15	30%
8	Apakah Anda merasa Gmail akan lebih aman dengan menggunakan teknologi blockchain?	Ya	18	36%
		Tidak	20	40%
		Tidak Tahu	12	24%
9	Seberapa besar kesediaan anda untuk menggunakan layanan email yang dilindungi oleh teknologi blockchain?	Bersedia	22	44%
		Netral	15	30%
		Tidak Bersedia	13	26%
10	Seberapa penting menurut Anda, investasi dalam teknologi blockchain untuk keamanan email?	Sangat Penting	25	50%
		Cukup Penting	15	15%
		Tidak Penting	10	10%

Dari data kuesioner table di atas menyatakan beberapa hal, yaitu:

1. Pemahaman Terhadap Teknologi Blockchain.

   Data menunjukkan bahwa pemahaman responden mengenai teknologi blockchain cukup beragam. Sebanyak 24% responden sangat familiar dengan teknologi ini, 36% cukup familiar, dan 40% tidak familiar. Hal ini menunjukkan bahwa meskipun blockchain adalah teknologi yang potensial, masih banyak pengguna yang belum memahami sepenuhnya cara kerjanya dan manfaat yang dapat diberikannya. Ini menandakan kebutuhan akan edukasi yang lebih intensif mengenai blockchain agar pengguna dapat memahami dan memanfaatkan teknologi ini dengan baik dalam meningkatkan keamanan email.

2. Kesadaran Tentang Phising.

   Sebanyak 70% responden sangat familiar dengan konsep phishing, 20% cukup familiar, dan hanya 10% yang tidak familiar. Tingginya tingkat kesadaran ini penting karena menunjukkan bahwa sebagian besar pengguna sudah menyadari adanya ancaman phishing. Namun, tingginya kesadaran ini juga perlu diimbangi dengan tindakan pencegahan yang efektif untuk mengurangi risiko serangan phishing.

3. Pengalaman Menjadi Korban Phising.

   Sebanyak 24% responden pernah menjadi korban phishing, sementara 60% belum pernah, dan 16% tidak yakin. Angka ini menunjukkan bahwa hampir seperempat dari responden telah mengalami serangan phishing secara langsung, yang menunjukkan adanya ancaman yang nyata dan signifikan. Pengalaman ini dapat mendorong pengguna untuk lebih waspada dan mencari solusi keamanan yang lebih baik, seperti teknologi blockchain.

4. Persepsi Terhadap Keamanan Gmail dari Serangan Phishing.

   Hanya 30% responden merasa bahwa Gmail sangat aman dari serangan phishing, sementara 40% merasa cukup aman, dan 30% merasa tidak aman. Ini menunjukkan bahwa meskipun Gmail telah menerapkan berbagai mekanisme keamanan, masih ada kekhawatiran di antara pengguna mengenai efektivitas langkah-langkah tersebut. Penggunaan teknologi blockchain bisa menjadi solusi untuk meningkatkan kepercayaan pengguna terhadap keamanan layanan email.

5. Pandangan Terhadap Penggunaan Blockchain untuk Keamanan Gmail.

   Sebanyak 40% responden setuju bahwa penggunaan blockchain dapat meningkatkan keamanan Gmail, 30% netral, dan 30% tidak setuju. Ini menunjukkan adanya minat yang signifikan terhadap solusi baru seperti blockchain, meskipun ada juga keraguan dan ketidakpastian di antara pengguna. Edukasi lebih lanjut dan

demonstrasi kasus penggunaan yang sukses dapat membantu mengatasi keraguan ini.

6. Kesediaan Menggunakan Layanan Email dengan Blockchain.

   Sebanyak 44% responden bersedia menggunakan layanan email yang dilindungi oleh teknologi blockchain, 30% netral, dan 26% tidak bersedia. Ini menunjukkan bahwa hampir setengah dari responden melihat nilai potensial dalam menggunakan blockchain untuk keamanan email. Kesediaan ini menunjukkan bahwa ada pasar yang siap menerima teknologi baru jika manfaatnya dapat ditunjukkan dengan jelas.

F. Cara Menggunakan Blockchain untuk Meningkatkan Keamanan Gmail dari Seranga Phising.

Berikut adalah beberapa cara untuk menggunakan teknologi blockchain dalam meningkatkan keamanan Gmail dari serangan phishing:

1. Verifikasi Identitas yang Lebih Aman:

   Blockchain dapat digunakan untuk membuat sistem verifikasi identitas yang lebih aman. Setiap pengguna Gmail dapat memiliki identitas *computerized* yang unik dan terenkripsi di blockchain, sehingga hanya pengguna yang benar-benar sah yang dapat mengakses akun mereka.

2. Pencacatan Transaksi yang Tidak Dapat Diubah:

   Dengan blockchain, semua transaksi dan aktivitas dalam e-mail dapat dicata secara permanen dan tidak dapat diubah. Hal ini membuat lebih sulit bagi penyerang untuk menyembunyikan jejak mereka atau memalsukan aktivitas email.

3. Keamanan Data yang Lebih Tinggi:

   Data yang disimpan di blockchain dilindungi oleh algoritma kriptografi yang canggih. Ini berarti data email pengguna akan lebih sulit diaksees oleh pihak yang tidak berwenang.

4. Pendeteksian Serangan yang Lebih Efektif:

   Dengan menggunakan *smart contracts,* blockchain dapat digunakan untuk mendeteksi aktivvitas yang mencurigakan secara otomatis. Misalnya, jika ada upaya login yang mencurigakan, sistem dapat secara otomatis memicu tindakan keamanan tambahan.

5. Desentralisasi untuk Mencegah Titik Kegagalan Tunggal:

   Sistem berbasis blockchain berdifat desentralisasi, yang berarti tidak ada titik kegagalan tunggal. Ini mengurangi risiko bahwa penyerrang dapat mengambil alih seluruh sistem e-mail dengan menyerang satu server pusat.

Dengan menerapkan teknologi blockchain, Gmail dapat meningkatkan lapisan keamanan mereka dan memberikan perlindungan yang lebih baok terhadap serangan phishing.

IV. KESIMPULAN

Penelitian ini menghasilkan beberapa temuan penting terkait penggunaan teknologi blockchain untuk meningkatkan keamanan email Gmail dari serangan phishing:

1. Tingkat Pemahaman dan Minat terhadap Blockchain**:** Pemahaman responden mengenai teknologi blockchain masih terbatas, namun ada minat yang cukup signifikan terhadap penerapannya untuk meningkatkan keamanan email. Edukasi lebih lanjut mengenai teknologi ini diperlukan agar pengguna dapat memanfaatkan blockchain secara efektif.
2. Kesadaran terhadap Phishing**:** Tingkat kesadaran responden tentang serangan phishing cukup tinggi. Meskipun demikian, pengalaman menjadi korban phishing

menunjukkan bahwa ancaman ini masih sangat nyata dan memerlukan solusi yang lebih efektif.

3. Persepsi Terhadap Keamanan Gmail**:** Kepercayaan pengguna terhadap keamanan Gmail bervariasi, menunjukkan bahwa langkah-langkah keamanan saat ini mungkin belum cukup untuk melindungi dari serangan phishing. Ini menunjukkan perlunya peningkatan mekanisme keamanan yang lebih kuat.
4. Potensi Blockchain sebagai Solusi Keamanan**:** Responden menunjukkan pandangan yang positif terhadap penggunaan blockchain untuk meningkatkan keamanan email, meskipun ada beberapa yang masih netral atau tidak setuju. Ini menandakan bahwa manfaat blockchain perlu ditunjukkan secara jelas untuk meningkatkan adopsi.
5. Dukungan terhadap Investasi dalam Teknologi Keamanan**:** Mayoritas responden setuju bahwa investasi dalam teknologi baru seperti blockchain sangat penting untuk meningkatkan keamanan email, menunjukkan dukungan kuat dari pengguna untuk inovasi di bidang keamanan siber.

Secara keseluruhan, penelitian ini menunjukkan bahwa teknologi blockchain memiliki potensi besar untuk meningkatkan keamanan email Gmail dari serangan phishing. Namun, adopsi teknologi ini memerlukan edukasi yang intensif dan demonstrasi manfaat nyata dari penggunaannya. Dengan demikian, blockchain dapat menjadi solusi yang efektif dalam melindungi data dan informasi pengguna dari ancaman siber.

UCAPAN TERIMA KASIH

Kami ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dalam proses penulisan artikel ini. Kami tidak akan dapat menyampaikan hasil penelitian ini. Kami tidak akan dapat menyampaikan hasil penelitain ini tanpa bantuan dan dorongan dari berbagai pihak.

Pertama, kami ingin mengucapkan terima kasih kepada pihak SENATIB dari Universitas Duta Bangsa Surakarta atas dukungan mereka selama proses penulisan dan publikasi artikel ini. Dukungan yang diberikkan telah membantu kami dalam menyelesaikan penelitian ini dengan baik.

Kami juga ingin berterima kasih kepada seluruh staf dan rekan-rekan di Fakultas Ilmu Komputer Universitas Duta Bangsa Surakarta atas bantuan teknis dan diskusi yang konstruktif selama penelitian ini berlangsung. Kontribusi mereka sangat berharga daalam memastikan kualitas dan vaiditas hasil penelitian kami.

Tidak lupa, kami juga ingin mengucapkan terima kasih kepada para responden yang telah berpatisipasi dalam penelitain ini. Partisipasi dan wawasan yang mereka berikan sangat penting untuk keberhasilan penelitian ini.

Dengan dukungan dan kerja sama dari berbagai pihak, artikel ini diharapkan dapat meingkatkan pemahaman dan kesadaran akan keamanan datadi era digital saat ini. Semoga semua orang yang membaca dapat mengambil manfaat dati hasil penelitian ini.

REFERENSI

[1] L. Yana Siregar, M. Irwan Padli Nasution Prodi Manajemen, and U. Negeri Islam Sumatera Utara, “HIRARKI Jurnal Ilmiah Manajemen dan Bisnis DEVELOPMENT OF INFORMATION TECHNOLOGY ON INCREASING BUSINESS ONLINE,” vol.2, no. 1, pp. 71–75, 2020, doi: 10.30606/hjimb.

[2] I. A. Afandi, A. Kusyanti, and N. H. Wardani. 2017. Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. 1(9): 783–792.

[3] Chhabra, G. S., & Bajwa, D. S. 2012. Review of E-mail System, Security Protocols and Email Forensics. International Journal of Computer Science & Communication Networks. 5(3): 201–211.

[4] Hidayat, W., Musdira, N., Rasyid, N., Khairi, M., & Juharman, M. (2023). Analisis Ancaman Terhadap Keamanan Data Pribadi pada Email. Jurnal Pendidikan Terapan, 7-12.

[5] Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. Jurnal Ham, 11(2), 285-299.

[6] Dian Rachmawati, ”Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber,” Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211

[7] Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkyanfi, M. W. (2023). Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem

Logistik Di Era Digital. *Jurnal Bisnis, Logistik Dan Supply Chain (Blogchain)*, *3*(1), 23-32.

[8] Pratama, A., & Wibisono, A. (2022). "Efektivitas Penerapan Teknologi Keamanan Email pada Layanan Gmail". Jurnal Keamanan Informasi, 10(2), 99-108.

[9] Praveena Anjelin, D., Ganesh Kumar, S. (2021). "Blockchain Technology for Data Sharing in Decentralized Storage System." In: Dash, S.S., Das, S., Panigrahi, B.K. (eds) Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 1172. Springer, Singapore.

[10] Verma, P., Goyal, A., & Gigras, Y. (2020). Email phishing: Text classification using natural language processing. *Computer Science and Information Technologies*, *1*(1), 1-12.

[11] Laporan Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), 6 Maret 2021.