Jurnal SPIRIT Vol. 14 No. 2 Nopember 2022, hal 23-29 P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X

PERTAHANAN PENCEGAHAN SERANGAN SOCIAL ENGINEERING MENGGUNAKAN TWO FACTOR AUTHENTICATION (2FA) BERBASIS SMS (SHORT MESSAGE SYSTEM)

Slamet[1)]
Prodi S1 Sistem Informasi, Universitas Dinamika, Surabaya, Indonesia[1)]
email: slamet@dinamika.ac.id[1)]

***ABSTRACT**: Advances in digital technology have made communication between humans faster and easier. On the other hand, a lot of personal information is available online through social media and services that do not have security measures in place to protect this information. Therefore, the communication system is very vulnerable and easily penetrated by intruder due to social engineering attacks. This attack aims to deceive individuals or companies by taking actions that benefit the attacker. The trick is to provide personal data such as PIN numbers, health records, and passwords. This attack phenomenon is one of the biggest challenges in maintaining the security of personal data because this attack model takes advantage of human nature which is easy to trust others. This paper provides an in-depth survey of high-success social engineering attacks, using a 2 Factor Authentication (2FA) model by examining user accounts, to detect and avoid attempted account fraud via SMS (Short Message System). Experimental results show that attack success can be reduced to 10% and aggressive intruders can be caught by 70% of users in forwarding user verification code.*

***Keywords:** Social Engineering, Security, 2FA, SMS*

1. Pendahuluan

Social engineering muncul sebagai salah satu jenis ancaman keamanan *cyber* terhadap individu, organisasi dan masyarakat [1]. Serangan s*ocial engineering* meningkat pesat di jaringan saat ini dan melemahkan rantai keamanan *cyber*. Serangan ini melakukan memanipulasi dengan membocorkan data penting demi kepentingan *intruder* [2]. Model serangan ini berusaha menantang beragam sistem keamanan jaringan seperti kekuatan *firewall*, metode kriptografi, sistem deteksi intrusi, dan anti-virus.

Dalam hal kepercayaan, sifat dasar manusia lebih cenderung mempercayai manusia lain dibandingkan kepada komputer atau teknologi. Oleh karena itu, kecenderungan sifat manusia ini menjadi mata rantai terlemah dalam rantai keamanan. Kegiatan jahat yang dilakukan dengan interaksi manusia dapat mempengaruhi seseorang secara psikologis, seperti mengungkapkan informasi rahasia atau melanggar prosedur-prosedur keamanan [3].

Teknik serangan *social engineering* adalah serangan yang paling kuat karena memanfaatkan interaksi manusia dan mengancam semua sistem dan jaringan. Mereka tidak dapat dicegah dengan menggunakan solusi perangkat lunak atau perangkat keras selama orang tidak dilatih untuk mencegah serangan ini. Umumnya para *intruder* memilih serangan ini ketika tidak ada cara untuk meretas sistem yang tanpa kerentanan teknis [4].

Dalam sepuluh tahun terakhir, *social engineering* sudah menjadi senjata andalan, baik bagi *intruder* berskala kecil atau *intruder* yang didukung oleh negara. Serangan ini digunakan untuk mengelabui pengguna seperti menginstal *malware*, membocorkan informasi-informasi rahasia dan bahkan untuk mentransfer keuangan dalam jumlah tertentu [5]. Model penyerangan ini sering menyasar pencurian data-data pribadi, dimana *intruder* mencuri *password* korban dan memungkinkan untuk mengambil alih akun tersebut sehingga dapat mengakses informasi-informasi yang sama dengan korbannya.

Mengaktifkan *Two Factor Authentication* (2FA) [6] adalah salah satu langkah paling efektif untuk memerangi pencurian data pribadi. 2FA

membutuhkan informasi lain selain *username* dan *password*. Informasi ini dapat berupa hal-hal yang terkait dengan pengetahuan (sesuatu yang diketahui pengguna, misalnya PIN), hal-hal yang berhubungan dengan kepemilikan (sesuatu yang dimiliki pengguna, misalnya token keamanan, perangkat seluler, atau aplikasi smartphone), atau faktor biometrik (misalnya sidik jari, pengenalan wajah, dan suara).

Dengan menyediakan otentikasi dua lapisan, 2FA meningkatkan keamanan data ke tingkat yang jauh lebih kuat. Apabila misalnya, *password* disusupi *intruder*, 2FA masih menawarkan lapisan perlindungan lain untuk memblokir akses-akses yang tidak sah.

Dalam makalah ini, kami memperkenalkan 2FA berbasis SMS untuk melindungi pengguna dari serangan *social engineering* dalam menipu korban dan membajak kartu SIM ponsel dari korbannya.

2. Landasan Teori

2.1. Serangan *Social Engineering*

Saat ini, serangan *social engineering* adalah ancaman terbesar yang dihadapi keamanan *cyber* [7]. Menurut penulis [8], mereka dapat dideteksi tetapi tidak bisa dihentikan. S*ocial engineering* memanfaatkan korban untuk mendapatkan informasi penting yang dapat digunakan untuk tujuan tertentu, dijual di pasar gelap atau diinvestasikan di jaringan gelap. Dengan munculnya *big data*, *intruder* menggunakan *big data* dan memanfaatkannya demi tujuan bisnis [9]. Mereka mengemas data dalam jumlah besar untuk dijual sebagai barang dagangan masa kini [9].

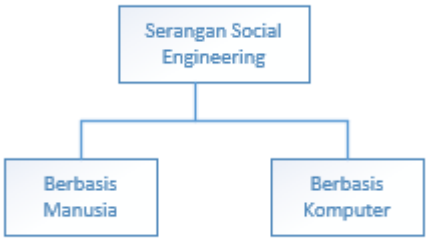
Meskipun serangan *social engineering* berbeda satu dengan lain, mereka memiliki pola yang sama dengan tahapan yang serupa. Pola umum yang sering digunakan oleh *intruder* terdiri dari empat tahapan: (1) mengumpulkan informasi-informasi tentang korban; (2) mengembangkan hubungan lebih lanjut dengan target (calon korban); (3) mengeksploitasi informasi yang didapatkan dan berlanjut melakukan serangan; dan (4) keluar tanpa jejak [13]. Gambar 1 mengilustrasikan tahapan-tahapan serangan *social engineering*.

Gambar 1. Tahapan serangan *Social Engineering*

Pada tahap pertama (fase pengumpulan informasi), *intruder* memilih korban berdasarkan: persyaratan-persyaratan yang sudah direncanakan. Pada tahap pengembangan hubungan, *intruder* mulai mendapatkan kepercayaan dari korban melalui kontak atau berkomunikasi secara langsung. Pada tahap eksploitasi, *intruder* mempengaruhi korban secara emosional untuk memberikan informasi penting atau melakukan kesalahan keamanan. Pada tahap terakhir (keluar), *intruder* sudah berhasil melakukan aksinya dan berhenti tanpa meninggalkan bukti atau jejak apapun [10].

2.2. Klasifikasi Serangan *Social Engineering*

Serangan *social engineering* diklasifikasikan ke dalam dua kategori, yaitu serangan berbasis manusia dan serangan berbasis komputer [11] sebagaimana diilustrasikan pada gambar 2.



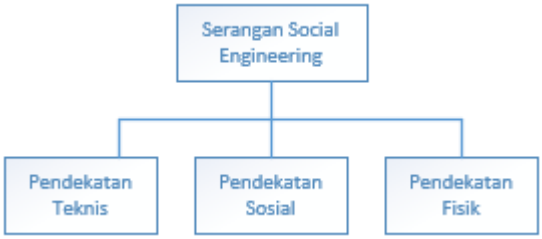
Gambar 2. Klasifikasi serangan *Social Engineering*

Dalam serangan berbasis manusia, *intruder* melakukan serangan dengan cara interaksi secara langsung dengan tujuan untuk mengumpulkan informasi yang diinginkan. Dengan demikian, *intruder* dapat mempengaruhi korban dalam jumlah tertentu. Serangan berbasis komputer dilakukan menggunakan perangkat komputer atau ponsel untuk mendapatkan informasi dari target. Dalam model ini, *intruder* dapat menyerang banyak korban dalam waktu beberapa detik. Salah satu serangan berbasis komputer yang sering digunakan, terutama untuk *phishing email* [12] adalah *Social Engineering Toolkit* (SET).

2.3. Cara Serangan *Social Engineering*

Menurut cara serangannya, *social engineering* dilakukan dengan tiga pendekatan, yaitu: pendekatan sosial, pendekatan teknis, dan

pendekatan fisik [11], seperti yang diilustrasikan pada gambar 3.



Gambar 3. Cara serangan *Social Engineering*

2.3.1. Pendekatan Teknis

Serangan dengan pendekatan teknis dilakukan melalui internet, seperti lewat media sosial dan layanan *web online*. Dalam pendekatan ini, *intruder* mengumpulkan informasi yang diinginkan seperti *password*, detail kartu kredit, dan jawaban pertanyaan-pertanyaan keamanan [9] dari sistem.

Dalam penelitian [13] mencatat bahwa internet sangat menarik bagi perekayasa sosial untuk mencari-cari *password*, karena pengguna sering menggunakan *password* (sederhana) yang sama untuk akun sama di tempat yang berbeda. Kebanyakan orang juga tidak menyadari bahwa mereka memberikan banyak informasi pribadi secara bebas kepada *intruder* (atau siapa pun yang akan mencarinya).

Intruder sering menggunakan mesin pencari dalam mengumpulkan informasi pribadi tentang calon korbannya. Selain itu, ada juga alat atau *website* yang bisa mengumpulkan dan mengagregasi informasi dari *web* yang berbeda. Situs media sosial juga menjadi sumber dalam mencari informasi yang berharga.

2.3.2. Pendekatan Sosial

Serangan dengan pendekatan sosial dilakukan melalui hubungan yang mempermainkan psikologi dan emosi calon korban. Serangan ini adalah serangan yang paling berbahaya dan seringkali paling berhasil karena melibatkan interaksi manusia secara langsung [9].

Dengan pendekatan ini, *intruder* mengandalkan teknik sosio-psikologis seperti prinsip persuasi [14] dalam memanipulasi korbannya. Contoh metode persuasi yang digunakan dalam serangan-serangan ini, seperti sifat rasa ingin tahu dari manusia. Untuk meningkatkan peluang keberhasilan serangan tersebut, para *intruder* sering melakukan dengan mengembangkan hubungan yang lebih dekat kepada calon korban. Menurut [15], jenis serangan sosial yang paling umum dilakukan dalam pendekatan ini adalah melalui telepon, *baiting* dan *spear phishing*.

2.3.3. Pendekatan Fisik

Serangan dengan pendekatan fisik mengacu pada tindakan fisik yang dilakukan oleh *intruder* dalam mengumpulkan informasi tentang calon korbannya. Informasi-informasi yang dikumpulkan seperti informasi pribadi (misalnya: nama, NIK, nomor kartu kredit, tanggal lahir) sampai kepada informasi penting yang digunakan oleh calon korban pada sistem komputernya.

Metode yang sering digunakan dalam pendekatan ini adalah *dumpster diving* [16], yaitu, dengan menelusuri sampah di suatu organisasi. Tempat sampah dapat menjadi sumber informasi yang berharga bagi *intruder* dalam menemukan data pribadi karyawan, tulisan-tulisan kecil, *print-out* informasi penting, seperti *username, password* dan sebagainya. Jika misalnya, *intruder* memperoleh akses ke kantor atau organisasi yang ditargetkan, *intruder* akan berusaha menemukan informasi seperti *password* yang tertulis di catatan kecil. Serangan fisik juga bisa dilakukan dengan pencurian atau pemerasan untuk mendapatkan informasi kepada calon korban.

Selain ketiga pendekatan di atas, serangan *social engineering* dapat menggabungkan berbagai pendekatan yang telah dibahas sebelumnya.

Contoh berbagai serangan *social engineering* yang sering digunakan adalah *phishing*, pemalsuan identitas, panggilan *help desk*, *diversion theft*, *fake software*, *baiting*, *pretexting*, *tailgating*, *pop-up windows*, r*obocalls*, *ransomware*, *online social engineering*, *reverse social engineering*, dan *phone social engineering* [17].

2.4. *Two Factor Authentication* (2FA)

Multi Factor Authentication, [18] juga sering disebut sebagai *Two Factor Authentication* (2FA), adalah sistem keamanan yang membutuhkan lebih dari satu jenis autentikasi yang dilakukan penggunanya. Dalam 2FA, pengguna harus menggunakan metode yang berbeda secara bersamaan untuk memverifikasi bahwa mereka adalah yang mereka katakan sebelum diberikan akses ke sistem informasi.

Solusi 2FA dapat terdiri dari kombinasi *one time password* (OTP), dengan menggunakan ponsel

untuk menerima atau menolak *login/token* dengan *password* yang ditampilkan.

Secara umum, faktor otentikasi menggunakan tiga filosofi dasar, yaitu: sesuatu yang Anda ketahui (seperti *password*), sesuatu yang Anda miliki (seperti *token*), atau sesuatu tentang Anda (seperti data biometrik) [19].

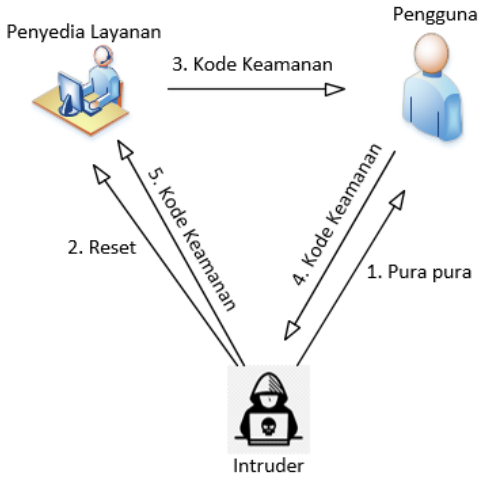
Two Factor Authentication biasanya terdiri dari sesuatu yang dimiliki pengguna dan sesuatu yang diketahui pengguna. Sebagai contoh, pengguna dapat memiliki token fisik yang dihubungkan ke komputer mereka atau *generator* token di ponsel mereka, atau mengetahui *password* atau nomor identifikasi pribadi (PIN). *Token* dan PIN digabungkan sebagai cara mengotentikasi sehingga dikatakan 2FA. Contoh lainnya, dalam penggunaan token berbasis ponsel dimana perangkat bisa dibuka kuncinya menggunakan fungsi *biometric* sebagai autentikasi yang digunakan secara *default*.

Multi Factor Authentication memastikan tingkat keamanan yang lebih tinggi dan dapat memberikan atau menolak akses berdasarkan berbagai kemungkinan dan titik data [20].

3. Metode Penelitian

Di bagian ini, kami menjelaskan metodologi untuk menemukan pesan verifikasi yang efektif dan mengurangi kerentanan menggunakan 2FA berbasis SMS.

Dalam mekanisme 2FA, pertama-tama *intruder* memulainya dengan aktifitas sensitif seperti: mengatur ulang *password*, mengatur *username*. Sistem otentikasi akan menghasilkan informasi penting dan kode acak (juga dikenal sebagai "Kode Verifikasi" atau "Kode Keamanan"), kemudian sistem mengirimkannya ke pengguna melalui SMS menggunakan nomor di ponsel pengguna. Saat menerima kode, pengguna meneruskan kembali ke Penyedia Layanan menggunakan saluran *web* untuk pengaturan ulang *password*. Jika kode yang dimasukkan cocok dengan yang dikirim, pengguna akan diautentikasi dan aktifitas yang diminta berhasil dilakukan. Model 2FA dari *social engineering* diilustrasikan pada gambar 4.



Gambar 4. Model 2FA dari *Social Engineering* berbasis SMS

Gambar 4 mendeskripsikan aliran 2FA dari serangan *social engineering*, dimana *intruder* menggunakan penipuan untuk mengelabui korban agar meneruskan kode keamanan yang memungkinkan *intruder* untuk menyusup ke akun korban. Tujuan utama dari otentikasi ini adalah untuk membangun lapisan otentikasi kedua yang dapat digunakan ketika data-data pribadi telah diketahui oleh *intruder*. Informasi tentang data-data pribadi pengguna adalah ancaman realistis mengingat potensi terjadinya pelanggaran data begitu besar dan tingkat keberhasilan serangan phishing yang dilakukan oleh *malware* yang juga besar [21].

Selanjutnya, aktifitas lainnya dalam mengekploitasi akun adalah dengan melakukan pembajakan terhadap kartu SIM dari ponsel korban [22]. Dalam serangan ini, *intruder* tidak berinteraksi dengan korban secara langsung. Namun, dia dapat meminta kepada operator ponsel untuk mengubah pemetaan dari nomor ponsel korban kepada kartu SIM *intruder*, sehingga panggilan atau SMS apapun akan ditujukan kepada *intruder*.

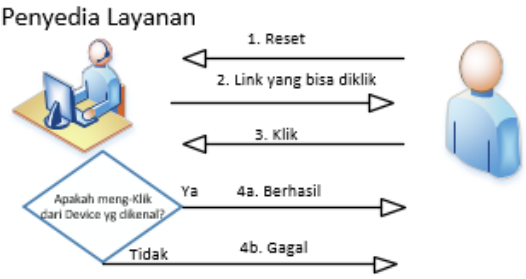
Setelah ini dilakukan, *intruder* mendapatkan akses ke salah satu akun korban yang diamankan dengan 2FA berbasis SMS, dengan memulai pengaturan ulang *password* atas nama korban. Demikian juga saat *provider* telpon mengirimkan pengaturan ulang kode *password* ke nomor telepon korban.

4. Hasil Dan Pembahasan

Dalam eksperimen yang telah dilakukan, Penyedia Layanan mengirimkan pesan 2FA yang berisi kode keamanan dengan satu atau dua tautan yang dapat di-klik. Tautan ekperimen 2FA ditunjukkan pada gambar 5.

Gambar. 5. Ekperimen 2FA dengan dua tautan yang dapat di-klik

Gambar 5 menunjukkan tautan ekperimen 2FA. Jika pengguna mengklik salah satu tautan, Penyedia Layanan akan menerima: *request* dari *browser* pengguna, *cookie* HTML dan pelacak lainnya, yang digunakan untuk menentukan apakah klik tersebut berasal dari perangkat yang dikenali sebagai pemilik akun resmi. Apabila standar SMS tidak mendukung HTML, maka aplikasi SMS akan menafsirkan teks SMS dan mengidentifikasi URL. Setelah itu, penyedia layanan melakukan verifikasi terhadap informasi yang diterima dari perangkat tersebut. Proses ini diilustrasikan pada gambar 6.



Gambar 6. Proses Verifikasi Perangkat

Gambar 6 menjelaskan alur verifikasi perangkat pada 2FA. Pertama-tama, 2FA dipicu oleh permintaan pengguna saat ada aktifitas-aktifitas sensitif, seperti mengubah *password*, mengubah alamat pengiriman, melakukan *transfer* dana dalam jumlah yang besar, atau melakukan tindakan-tindakan anomali (aktifitas di luar kebiasaan pengguna).

Ekperimen 2FA dikatakan berhasil jika perangkat pengguna dikenali oleh sistem. Pengguna kemudian diizinkan untuk melakukan aktifitas pada perangkat yang sama yang digunakan untuk menjawab ekperimen. Hal ini memastikan bahwa pengguna mengetahui tindakan apa yang sedang dilakukan secara menyeluruh.

Jika perangkat pengguna tidak dikenali, maka dilanjutkan dengan proses eskalasi. Proses ini melibatkan penggunaan perangkat lain yang sudah terdaftar dalam *database* Penyedia Layanan untuk melewati proses kedua. Proses untuk melakukan otentikasi menggunakan pertanyaan-pertanyaan berbasis pengetahuan. Proses ini ditunjukkan pada gambar 7.

Gambar 7. Ilustrasi tindakan yang diambil dalam ekperimen 2FA

Pada gambar 7, Pengguna diminta untuk meneruskan atau menyetujui aktifitas yang membuat 2FA terpicu. Persetujuan atau pembatalan perlu dilakukan oleh pengguna untuk merespons ekperimen 2FA pada perangkat yang digunakan. Apabila dipilih "Lanjut" maka aktifitas 2FA akan diteruskan, dan apabila dipilih "Tidak" maka aktifitas 2FA akan dibatalkan.

Dengan adanya informasi perangkat yang sudah tercatat pada *database* Penyedia Layanan, *social engineering* yang bertujuan untuk mengelabui korban tidak akan berarti lagi. Hal ini karena perangkat *intruder* tidak akan dikenali sebagai pemilik akun karena *intruder* tidak memiliki *cookies* (dan pengenal lain) yang dimiliki pengguna asli. Demikian juga dengan pembajakan kartu SIM tidak akan berhasil dilakukan karena semua informasi tentang pengguna resmi telah tercatat pada *server* Penyedia Layanan.

Apabila *intruder* melakukan tindakan yang menyebabkan 2FA terkirim kepada korban yang dituju, maka Penyedia Layanan akan memberikan 2FA dengan tantangan-tantangan berupa pertanyaan yang harus dijawab dengan benar oleh *intruder*. Namun begitu, pemilik akun harus tetap menyetujuinya agar tantangan bisa dilanjutkan, misalnya pemilik akun diminta menyetujui alamat baru, seperti yang diilustrasikan pada gambar 7, atau diminta untuk mengatur *password* baru.

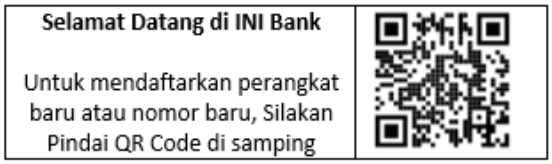
Proses penyelesaian tantangan ini harus dilakukan pada perangkat yang digunakan untuk melewati tantangan 2FA (mis., telepon pengguna).

Apabila 2FA mendapatkan tantangan baru, seperti adanya perangkat baru yang digunakan untuk mengganti perangkat lama atau mengganti nomer telponnya dengan nomor baru, maka 2FA akan menentukan apakah perangkat ini berasal dari *intruder* atau pengguna asli. Masalah seperti ini diatasi dengan menggunakan metode eskalasi. Eskalasi dilakukan dengan meminta pengguna

untuk menjawab pertanyaan-pertanyaan berbasis pengetahuan; atau dapat membuktikan akses ke sumber daya tertentu terkait dengan pengguna.

Proses eskalasi yang tepat tergantung pada jenis layanan terkait dengan tantangan 2FA. Oleh karena itu, fungsi sistem yang penting adalah untuk mendaftar perangkat baru atau nomor baru yang terkait dengan akun pengguna.

Profil perangkat dapat dilakukan selama *setup* akun dengan teknik *bootstrap* ketika pengguna mendaftarkan perangkat atau nomornya, dengan meminta informasi yang sudah dikenali (saat *login*) sehingga pengguna bisa mendaftarkan perangkat atau nomor barunya, seperti yang diilustrasikan pada gambar 8.



Gambar 8. Pendaftaran Perangkat dan atau Nomor Telpon Baru oleh Pengguna

Gambar 8 mengilustrasikan pendaftaran perangkat baru atau nomor baru dari pengguna apabila ingin mengganti data yang lama. Pengguna memindai kode QR dari perangkat barunya, dan permintaan dikirim ke halaman web yang URL-nya dikodekan menggunakan kode QR. Saat permintaan diterima, maka data perangkat tersebut disimpan oleh Penyedia Layanan. Perangkat juga dapat didaftarkan secara otomatis dengan eskalasi tertentu.

Sebagai contoh, jika pengguna gagal *login* karena perangkatnya tidak terdaftar, maka pengguna dapat diminta untuk mengkonfirmasi bahwa dia melakukan akses yang gagal; kemudian dilanjutkan dengan proses eskalasi untuk menjawab pertanyaan-pertanyaan tertentu terkait dengan profil dari pengguna resmi. Apabila lolos dalam proses eskalasi, maka perangkat tersebut akan secara otomatis terdaftar. Dan apabila tidak berhasil menjawab pertanyaan-pertanyaan tantangan, maka proses eskalasi gagal. Beberapa perangkat atau nomor yang bisa didaftarkan misalnya komputer, laptop, tablet, dan ponsel.

5. Kesimpulan

Paper ini menjelaskan solusi teknis yang membahas serangan *social engineering* dengan *2 Factor Authentication* berbasis SMS. Pendekatan yang digunakan dalam penelitian ini adalah: berdasarkan pada perangkat pengguna yang dikenali oleh penyedia layanan, model eskalasi dengan mengambil tantangan dari data atau pengalaman pengguna asli.

Melalui percobaan, kami mengamati bahwa *intruder* agresif dapat terjaring oleh 70% pengguna asli dalam meneruskan kode verifikasi mereka. Hasilnya bahwa, pesan SMS yang berisi kode verifikasi yang dikirim oleh penyedia layanan dapat memainkan peran penting dalam mengurangi serangan ini. Solusi ini juga dapat mengatasi serangan seperti pembajakan kartu SIM dimana saluran pengiriman berusaha dicuri.

Kami mengembangkan prinsip rancangan verifikasi anti-penyalahgunaan pesan untuk mengurangi kerentanan pengguna dalam meneruskan kode verifikasi kepada *intruder*. Sejumlah pesan SMS yang masuk, dievaluasi menggunakan eksperimen lapangan. Hasil percobaan kami menunjukkan bahwa keberhasilan serangan dapat dikurangi menjadi hanya 10%.

Daftar Pustaka

[1] Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, 198, 656-661..

[2] Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021, July). Social engineering attacks: Recent advances and challenges. In International Conference on Human-Computer Interaction (pp. 417-431). Springer, Cham.

[3] Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. IEEE Access.

[4] Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Chipfumbu-Kangara, C. (2022). Enhanced social engineering framework mitigating against social engineering attacks in higher education. Security and Privacy, 5(5), e237.

[5] Indarta, Y., Ranuhardja, F., Ashari, I. F., Sihotang, J. I., Simarmata, J., Harmayani, H., ... & Idris, M. (2022). Keamanan Siber: Tantangan di Era Revolusi Industri 4.0. Yayasan Kita Menulis.

[6] Tirfe, D., & Anand, V. K. (2022). A survey on trends of two-factor authentication. In Contemporary Issues in Communication, Cloud and Big Data Analytics (pp. 285-296). Springer, Singapore.

[7] Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895-11910.

[8] Tulkarm, P. (2021). A Survey of Social Engineering Attacks: Detection and Prevention Tools. Journal of Theoretical and Applied Information Technology, 99(18).

[9] Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. Ieee Access, 9, 7152-7169.

[10] Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., & Wei, Z. (2021). Understanding and deciphering of social engineering attack scenarios. Security and Privacy, 4(4), e161.

[11] Subbalakshmi, C., Pareek, P. K., & Sayal, R. (2022). A Study on Social Engineering Attacks in Cybersecurity. In Innovations in Computer Science and Engineering (pp. 59-71). Springer, Singapore.

[12] Barik, K., Konar, K., Banerjee, A., Das, S., & Abirami, A. (2022). An Exploration of Attack Patterns and Protection Approaches Using Penetration Testing. In Intelligent Data Communication Technologies and Internet of Things (pp. 491-503). Springer, Singapore.

[13] Duarte, N., Coelho, N., & Guarda, T. (2021, November). Social Engineering: The Art of Attacks. In International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability (pp. 474-483). Springer, Cham.

[14] Cialdini, R. B. (2009) Influence: the psychology of persuasion. HarperCollins e-books

[15] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[16] Conteh, N. Y. (2021). The dynamics of social engineering and cybercrime in the digital age. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 144-149). IGI Global.

[17] Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12), 6042.

[18] Mahmood Saqib, R., Shahid Khan, A., Javed, Y., Ahmad, S., Nisar, K., A Abbasi, I., ... & Ahmadi Julaihi, A. (2022). Analysis and intellectual structure of the multi-factor authentication in information security. Intelligent Automation & Soft Computing, 32(3), 1633-1647.

[19] Matelski, S. (2022, June). Human-Computable OTP Generator as an Alternative of the Two-Factor Authentication. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference (pp. 64-71).

[20] Suhyana, F. A., Suseno, S., & Ramli, T. S. (2021). Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain. SIGn Jurnal Hukum, 2(2), 138-156.

[21] Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan dan Pengelabuan (Cybercrime). UNES Law Review, 4(3), 297-308.

[22] Faircloth, C., Hartzell, G., Callahan, N., & Bhunia, S. (2022, June). A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft. In 2022 IEEE World AI IoT Congress (AIIoT) (pp. 501-507). IEEE.