Jurnal Ilmiah Ilmu Komputer Vol. 8, No. 2, Septemner 2022 (P) ISSN 2442-451X
Fakultas Ilmu Komputer (O) ISSN 2503-3832
Universitas AL Asyariah Mandar

RANCANG BANGUN APLIKASI GAMIFIKASI UNTUK MENINGKATKAN KESADARAN KEAMANAN SIBER

Raden Budiarto Hadiprakoso[1], Wian Agus Satria[2]

[1,2]Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
[1]raden.budiarto@, [2]wian.agus@poltekssn.ac.id

ABSTRAK

Pada awal tahun 2021 Badan Siber dan Sandi Negara melaporkan data serangan siber yang terjadi di Indonesia. Jumlah serangan yang diterima pada kuartal pertama tahun 2021 lebih dari 88 juta serangan. Serangan pengumpulan informasi menyumbang sebanyak 43% dari serangan ini. Serangan pengumpulan informasi menyumbang sebanyak 43% dari serangan ini. Sangat penting untuk menemukan cara untuk meningkatkan kesadaran keamanan siber untuk mencegah serangan pengumpulan informasi semacam itu. Akibatnya, sebuah penelitian dilakukan untuk menggunakan gamifikasi instruksional kesadaran keamanan siber untuk meningkatkan kesadaran keamanan siber komunitas. Menggunakan *Software Development Lifecycle* (SDLC) *Personal Xtreme Programming*, aplikasi gamifikasi SadarSiber ini dibuat dalam bentuk permainan kuis. Berdasarkan hasil kuesioner yang dibagikan kepada responden, aplikasi gamifikasi SadarSiber dapat meningkatkan kesadaran keamanan siber dan mencegah pengguna mengekspos data pribadinya kepada pihak yang tidak dikenal.

Kata Kunci— aplikasi android, kesadaran keamanan siber pembelajaran gamifikasi, personal extreme programming.

ABSTRACT

The National Cyber and Crypto Agency (BSSN) provided data about cyber-attacks in Indonesia in early 2021. The number of attacks received in the first quarter of 2021 exceeds 88 million. Information gathering attacks account for up to 43% of these attacks. Information gathering attacks account for up to 43% of these attacks. To prevent such information-gathering attacks, it is critical to find a way to improve cybersecurity awareness. As a result, a study was conducted to determine the effectiveness of cybersecurity awareness instructional gamification in raising community cybersecurity awareness. This SadarSiber gamification application is designed in the form of a quiz game using Software Development Lifecycle (SDLC) Personal Xtreme Programming. The SadarSiber gamification application, according to the questionnaire results supplied to respondents, can enhance cybersecurity awareness and protect users from revealing their sensitive data to unknown parties.
Keywords— android app, cyber-security awareness, gamification learning, personal extreme programming.

1. PENDAHULUAN

Menurut data Badan Siber dan Sandi Negara, telah terjadi 88.414.296 serangan yang telah dilancarkan dari awal tahun 2021 hingga 12 April 2021. Dari 88 juta serangan tersebut, 43% tergolong serangan tipe pencurian informasi (*Information Gathering*) [1]. *Information Gathering* merupakan kegiatan mengumpulkan informasi sebanyak-banyaknya mengenai suatu sasaran tertentu [2]. Pada penelitian [3] Jeon, dkk. mendefinisikan aset pada sistem informasi menjadi tiga: informasi pribadi, perangkat, dan aplikasi. Informasi pribadi, dalam hal ini, mencakup semua data yang tersimpan pada sistem, seperti buku alamat, riwayat panggilan, informasi lokasi, email dan lampiran, layanan pesan singkat (SMS), file media. Jenis serangan siber yang mengumpulkan informasi bisa berakibat fatal ketika penyerang mendapatkan informasi pribadi pengguna. Kerentanan yang mengancam aset tersebut salah satunya disebabkan karena ketidaksadaran pengguna terhadap keamanan siber.

Kementerian Komunikasi dan Informasi Republik Indonesia menyatakan bahwa penggunaan *smartphone* di Indonesia sangat tinggi. Fakta ini didorong oleh tarif internet yang murah dan jumlah pengguna *smartphone* yang besar mencapai 167 juta orang atau 89% dari total penduduk Indonesia pada tahun 2021 [4]. Jika menghubungkan serangan pengumpulan informasi dengan banyak pengguna *smartphone*, masalah pengumpulan informasi menjadi hal yang menarik untuk dipelajari. Untuk itu, diperlukan suatu

(P) ISSN 2442-451X
(O) ISSN 2503-3832

metode agar pengguna terhindar dari serangan siber khususnya pengumpulan informasi.

Berdasarkan permasalahan tersebut, solusi yang disajikan dalam makalah ini adalah teknik gamifikasi pendidikan. Berdasarkan penelitian dari Scholefield dan Shepherd mengenai teknik *gamification* yang dinyatakan efektif sebagai metode pengajaran *cybersecurity*. Teknik gamifikasi juga mendapat respons yang baik dari pengguna untuk meningkatkan kesadaran keamanan siber, terutama mengenai kekuatan kata sandi [5]. Dikarenakan media hiburan yang banyak diminati dan diakses oleh pengguna internet melalui *smartphone*, maka solusi yang dihadirkan adalah pengenalan dunia siber berbasis *game* untuk meningkatkan kesadaran keamanan siber.

Aplikasi SadarSiber yang dikembangkan akan mengimplementasikan *Software Development Lifecycle* (SDLC). Metode SDLC yang digunakan adalah Personal Extreme Programming (PXP) [6]. Metode ini dipilih karena metode PXP digunakan untuk memaksimalkan proses pengembangan program yang dilakukan oleh seorang *programmer* (pemrogram tunggal) [7]. PXP muncul dari metodologi agile modern, *Extreme Programming* (XP) dan *Personal Software Process* (PSP). Metodologi ini telah ditujukan untuk pengembang otonom yang bertujuan untuk mengkonsolidasikan prinsip-prinsip XP dalam pengembangan aplikasi perangkat lunak [8].

Penelitian ini bertujuan untuk mengeksplorasi metodologi *Personal Extreme Programming* dalam mengembangkan perangkat lunak gamifikasi pembelajaran yang dilakukan sebagai pengembang tunggal. Selain itu, untuk mengukur dampak penerapan gamifikasi terhadap peningkatan kesadaran keamanan siber. Dampak dari penelitian ini adalah memberikan solusi terkait pencegahan kebocoran data pribadi pada *smartphone*. Manfaat ini dapat dicapai melalui media pendidikan yang menghibur dalam bentuk permainan. *Game* hasil gamifikasi edukasi kesadaran keamanan siber yang dikemas dalam bentuk game, sehingga diharapkan dapat meningkatkan semangat *masyarakat* awam dalam belajar dan meningkatkan kesadaran keamanan siber

2. TINJAUAN PUSTAKA

Pada makalah [9], Scholefield dan Shepherd menjelaskan teknik gamifikasi dalam mendidik pengguna biasa tentang keamanan kata sandi untuk meningkatkan kesadaran keamanan umum. Penelitian ini menggunakan aplikasi *role-playing quiz*, dan hasil yang diperoleh pengguna merasa nyaman belajar melalui *game* tersebut. Penelitian ini berfokus pada keamanan *password* dan hanya meningkatkan pengetahuan pengguna melalui soal-soal ujian pada kuis. Sebagai perbandingan, penelitian yang dilakukan di sini akan fokus pada keamanan informasi pengguna secara umum di dunia maya dan informasi yang disajikan dalam bentuk teks narasi tertulis pada aplikasi untuk menjelaskan jawaban atas pertanyaan yang terdapat dalam kuis. Selain itu ada juga permainan kuis untuk menguji pengetahuan yang diperoleh dengan memahami materi aplikasi.

Dalam makalah [10], penulis mendeskripsikan gamifikasi, terdapat tiga struktur utama, yaitu elemen *game*, yaitu teknik desain *game*, dan konteks *non-game*. Elemen *game* ini terdiri dari elemen-elemen khas dalam sebuah *game*, seperti skor tertinggi, *badge*, dan *achievement*. Teknik desain game yang dimaksud adalah desain *software* dengan nuansa *game*.

Jagust dkk. di kertas [11] memperkenalkan *gamification* untuk pembelajaran digital. Objek penelitian dalam tulisan ini adalah siswa sekolah dasar. Makalah ini lebih lanjut menjelaskan strategi gamifikasi dalam mempengaruhi pengguna dan meningkatkan minat belajar siswa. Hasil penelitian menunjukkan bahwa gamifikasi dapat mempertahankan minat belajar siswa lebih baik daripada pendekatan pembelajaran non-gamifikasi dalam sumber digital.

Penelitian [12] menggunakan pendekatan gamifikasi dan pembelajaran langsung untuk mempelajari topik keamanan siber. Penelitian ini disusun menggunakan pendekatan kuantitatif dengan pengukuran kompetensi dan pengukuran motivasi menggunakan angket. Hasil penelitian menemukan bahwa salah satu faktor pembentuk motivasi intrinsik yang mendukung pencapaian kompetensi dapat ditingkatkan sekitar 62% dengan menggunakan pendekatan *hands-on learning* dengan *gamification*.

3. METODE YANG DIUSULKAN

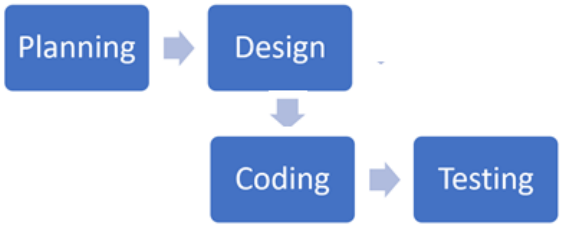
Objek penelitian dalam penelitian ini adalah penerapan *gamification* untuk mengukur dan meningkatkan kesadaran keamanan siber. Akan diukur apakah ada peningkatan pemahaman kesadaran keamanan siber pengguna dengan menggunakan aplikasi gamification yang dibuat dalam penelitian ini. Soal-soal dalam aplikasi ini didasarkan pada penelitian yang berjudul "*Survey on Cyber Security awareness on collage student*" oleh Senthilkumar dan Easwaramoorthy [13]. Hasil kuesioner ini akan dilihat dan dianalisis terkait perbedaan pemahaman pengguna sebelum dan sesudah menggunakan aplikasi *gamification*.

Penelitian ini akan mengambil metode penelitian dan pengembangan. Metode penelitian dan pengembangan adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk [14]. Objek penelitian ini juga akan diuji keefektifan produk, baik dalam bentuk aplikasinya (melalui pengujian perangkat lunak) maupun dampak yang diberikan aplikasi untuk meningkatkan kesadaran keamanan siber (diukur melalui Kuesioner Kesadaran Keamanan Informasi Pengguna) [15].

Metode pengembangan perangkat lunak yang diguankan adalah *Personal Extreme Programming* (PXP) dengan menerapkan metode penelitian *Research and Development* [16]. Metode pengembangan perangkat lunak ini dipilih karena ideal untuk membuat perangkat lunak baru dan menyelesaikan proyek dengan cepat. PXP akan lebih efektif ketika pengguna tidak mengerti apa yang mereka

(P) ISSN 2442-451X
(O) ISSN 2503-3832

inginkan [17]. Penelitian ini tentunya akan sangat efektif karena fitur *game* yang dikembangkan disesuaikan dengan minat pengguna. Tahapan proses dalam metodologi PXP diilustrasikan pada Gambar 1.



Gambar 1. Proses pada PXP

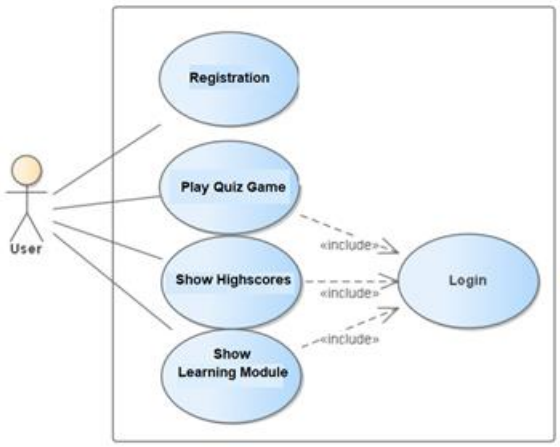
3.1. Perencanaan

Pada tahap ini dilakukan perencanaan perangkat lunak sebagai inisiasi awal dalam mempersiapkan pekerjaan proyek. Perencanaan dimulai dengan penetapan standar pengkodean yang akan memandu proses pengkodean aplikasi. Setelah itu, data kuantitatif dikumpulkan melalui survei atau wawancara untuk mendapatkan cerita pengguna yang berisi masalah dan solusi yang diharapkan oleh pengguna. Dari cerita pengguna ini, pengembang harus memecah masalah yang ada dan mengelompokkan solusi ke dalam serangkaian fitur yang dibuat dalam aplikasi (juga dikenal sebagai *FeatureSets*). Sementara itu, cerita pengguna terkadang tidak sepenuhnya menggambarkan masalah dan solusi yang ada, sehingga perlu ada inisiatif pengembang dalam menyelesaikan *FeatureSets* yang dibuat sesuai dengan kebutuhan pengguna. Selanjutnya, direncanakan untuk memperkirakan waktu pengembangan perangkat lunak dari semua *FeatureSet*. *FeatureSets* kemudian diprioritaskan berdasarkan tingkat urgensi kebutuhan.

3.2. Desain

Aplikasi dirancang berdasarkan persyaratan dalam Kumpulan Fitur dan cerita pengguna. Menjelaskan desain dengan *Unified Model Language* (UML) agar klien dapat memahami desain dari aplikasi yang akan dibuat. Pada penelitian ini, aplikasi *Enterprise Architect* akan digunakan untuk membuat desain *use case, activity diagram*, dan *sequence diagram*. Diagram UML yang dibuat dalam penelitian ini meliputi *use case diagram* dan *class diagram*.

Use Case adalah salah satu diagram UML yang menggambarkan interaksi antara satu atau lebih aktor dengan tujuannya (*use case*) dalam sistem. *Use case* bukanlah diagram dari sebuah *use case* tetapi terdiri dari beberapa *use case. Use case* diagram dengan *use case* tidak saling menggantikan tetapi *use case* diagram dibuat setelah *use case* dibuat. Banyak orang salah paham bahwa *use case* sama dengan diagram kasus padahal sebenarnya ini adalah dua hal yang berbeda. *Use case* diagram digunakan untuk mengumpulkan beberapa use case yang telah dibuat sebelumnya. Dalam *use case* diagram, kita dapat melihat bagaimana para aktor berinteraksi dalam sistem. Use case diagram dapat membantu merumuskan persyaratan sistem dan mengkomunikasikan desain dengan pelanggan atau pemangku kepentingan. Diagram *use case* dari aplikasi yang diusulkan ditunjukkan pada Gambar 2.



Gambar 2. Use case diagram

Gambar 2 menampilkan diagram *use case* yang menjelaskan apa yang dapat dilakukan aktor dengan aplikasi gamifikasi ini. Diagram *use case* aplikasi ini hanya terdiri dari satu aktor yaitu pengguna aplikasi. Aktor dapat melakukan empat kasus penggunaan: pendaftaran akun, bermain *game* kuis, melihat skor tinggi, dan melihat materi modul pembelajaran.

Tahapan perancangan aplikasi selanjutnya adalah membuat diagram kelas. Diagram kelas adalah jenis diagram UML yang statis dan menggambarkan struktur suatu sistem dengan menunjukkan kelas, atribut, operasi, dan hubungan antar kelas. Diagram kelas digunakan untuk memvisualisasikan dan mendokumentasikan berbagai aspek sistem dan juga digunakan untuk membangun kode program aplikasi perangkat lunak. Diagram kelas menunjukkan struktur kelas dan hubungan antar kelas atau objeknya, termasuk pewarisan, antarmuka, dan asosiasi. Class diagram merupakan diagram UML yang populer digunakan dalam pemodelan sistem berorientasi objek karena merupakan diagram UML yang dapat dipetakan secara langsung ke dalam bahasa pemrograman berorientasi objek. Rancangan diagram kelas ditunjukkan pada Gambar 3.

3.3 Pengkodean & Pengujian

Pengembang menentukan pengujian unit untuk setiap cerita. Tes unit ini akan menjadi penguji dalam peningkatan perangkat lunak. Proses pengkodean (*coding*)di XP dan PXP berjalan terus menerus dengan testing di mana ada iterasi terus menerus untuk menguji *source code* dan terus memperbaikinya. Proses ini melibatkan iterasi sampai pengguna akhir menerima program dengan baik. Proses *coding* pada aplikasi ini akan menggunakan Android Studio IDE, dengan OS berbasis Ubuntu 18.04 pada perangkat

(P) ISSN 2442-451X
(O) ISSN 2503-3832

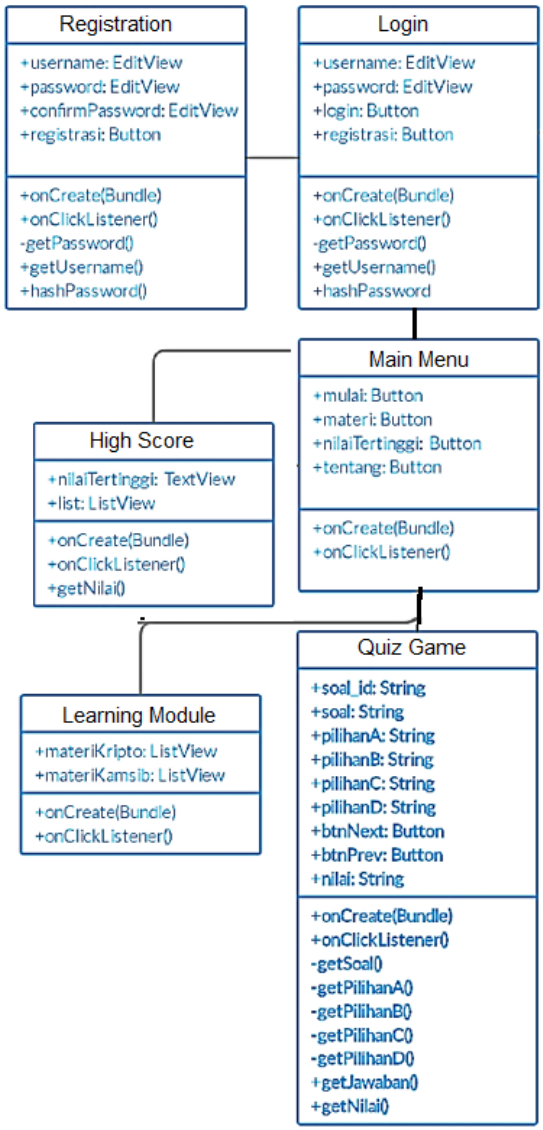
dengan spesifikasi RAM 10 GB, prosesor Intel Core i3 5005U-2.0Ghz.

Proses pengujian berjalan secara berurutan yaitu *unit testing*, *integration testing*, dan *acceptance testing*, bersamaan dengan proses *coding*. Proses ini dilakukan karena pada XP, setiap kali terjadi ketidaksesuaian pada saat proses pengujian, maka akan segera dilakukan *coding* ulang hingga mencapai kondisi ideal. Pengujian yang akan dilakukan adalah pengujian unit untuk menguji fitur-fitur pada aplikasi. Pengujian integrasi dilakukan agar setiap fitur terintegrasi dengan baik dengan aplikasi. Terakhir, pengujian penerimaan pengguna dilakukan untuk memastikan bahwa pengguna akan sepenuhnya menerima aplikasi. Responden penguji aplikasi diambil secara acak sebagai pengguna akhir aplikasi.

Peneliti [13] menggunakan kerangka kerja untuk mendefinisikan pertanyaan inti yang terkait dengan pemahaman pengguna dan kesadaran keamanan siber dalam berbagai aspek. Mereka menerapkan aspek-aspek ini dibagi sebagai berikut:

1. Kesadaran akan *User* ID dan *password*
2. Kesadaran akan perlindungan komputer
3. Kesadaran pemasangan *firewall* dan anti-virus
4. Kesadaran virus

Dari aspek tersebut, kemudian ditetapkan sebanyak 20 pertanyaan untuk menguji kesadaran keamanan siber pengguna. Kemudian kuesioner disebarkan kepada 30 responden yang dibagikan secara acak melalui *google form*. Responden dibatasi untuk usia pelajar tingkat SMA di kota Jakarta. Responden akan diminta untuk mengisi dua kuesioner. Terdapat kuesioner awal untuk mengukur tingkat kesadaran keamanan siber responden sebelum menggunakan aplikasi SadarSiber dan kuesioner terakhir untuk mengukur dampak penggunaan aplikasi terhadap tingkat kesadaran keamanan siber responden. Dari 30 kuesioner, 29 responden mengisi kuesioner dengan lengkap dan melakukan semua langkah dalam pengumpulan data

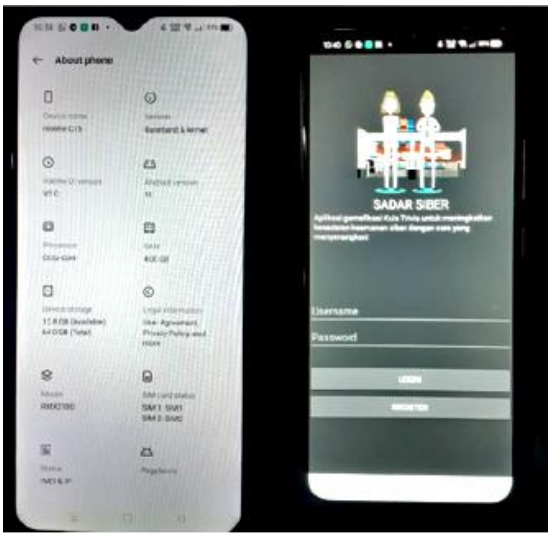


Gambar 3. Class diagram

4. HASIL PENELITIAN

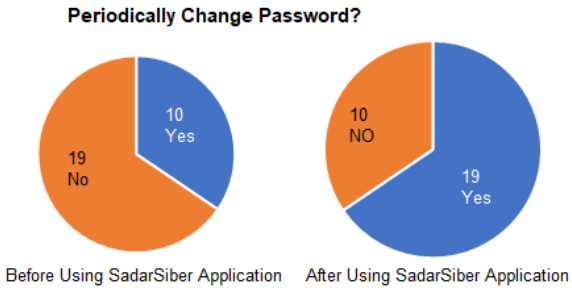
Pengujian pertama yang dilakukan setelah aplikasi dibuat adalah pengujian kompatibilitas. Pengujian ini dimaksudkan untuk mengetahui apakah aplikasi dapat berjalan di perangkat Android dengan sistem operasi Android 6 sampai dengan versi sistem operasi Android 11. Pengujian dilakukan dengan menginstal APK langsung di perangkat Android. Gambar 4 merupakan tampilan perangkat yang sudah dapat menjalankan aplikasi SadarSiber.

(P) ISSN 2442-451X
(O) ISSN 2503-3832



Gambar 4. Tampilan aplikasi SadarSiber

Bagian berikut akan memaparkan hasil penelitian berdasarkan data yang diperoleh dari responden. Dalam penelitian berikut, salah satu pertanyaan pada kuesioner terkait apakah responden secara berkala mengganti *password* yang digunakan atau tidak. Pada kuesioner tahap awal, didapatkan hasil 10 dari 29 responden yang melakukan perubahan *password* yang digunakan secara berkala. Setelah menggunakan aplikasi SadarSiber, responden diminta kembali untuk mengisi kuesioner. Hasil penelitian menunjukkan bahwa 19 responden menjawab ya sedangkan sisanya menjawab tidak. Dengan demikian, aplikasi SadarSiber dapat memberikan pemahaman yang baik tentang kesadaran keamanan siber bagi penggunanya. Gambar 5 menunjukkan grafik hasil tersebut.



Gambar 5. Hasil kuesioner

Gambar 5 menunjukkan bahwa dari 29 responden, 19 orang menyatakan sering mengganti *password*, dan sepuluh lainnya masih menggunakan *password* yang sama tanpa mengubahnya. Terjadi peningkatan di mana awalnya 10 orang menyatakan akan mengganti *password* secara berkala, menjadi 19 orang yang menyatakan akan mengganti *password* secara berkala. Hasil ini menunjukkan bahwa pengguna sadar akan perubahan kata sandi yang digunakan secara teratur. Selain pertanyaan tersebut terdapat 19 pertanyaan lain yang dijelaskan pada tabel 1.

Kolom 'C' pada tabel 1 membandingkan jumlah jawaban yang berubah dari responden sebelum menggunakan aplikasi SadarSiber dan setelah menggunakan aplikasi SadarSiber. Jawaban negatif berarti responden telah mengubah jawaban menjadi pilihan yang salah dari yang semula benar. Sedangkan jawaban positif berarti responden telah mengganti jawaban yang semula salah menjadi benar.

Dari tabel 1, dampak penggunaan aplikasi SadarSiber memberikan nilai perubahan positif yang berarti pengguna lebih sadar akan keamanan siber. Jawaban lengkap berubah menjadi jawaban benar dari jawaban awal salah pada angket sebanyak 52 jawaban. Kemudian, jawaban lengkap berubah menjadi salah dari yang semula benar pada kuesioner, yaitu tiga jawaban. Dari hasil tersebut, pengguna aplikasi SadarSiber telah melakukan perubahan yang signifikan menjadi lebih baik kepada pengguna akhir. Aplikasi ini juga memberikan informasi kepada responden untuk lebih waspada terhadap keamanan siber, terutama mengikuti materi-materi yang telah disajikan dalam aplikasi.

Tabel 1 Hasil Kuesioner

Pertanyaan	Pre		Post		C
	Y	T	Y	T	
Apabila keluarga saya meminta password dari akun layanan keuangan saya melalui email, maka akan saya beritahukan melalui email	6	23	4	25	2
Apabila keluarga saya meminta password dari akun layanan keuangan saya melalui email, maka akan saya beritahukan melalui layanan pesan singkat	26	3	27	2	1
Saya pernah mendapat email/pesan mencurigakan yang memberikan saya iming-iming hadiah yang sangat besar	25	4	23	6	-2
Apabila mendapat email/pesan mencurigakan, saya akan mencari tau link atau lampiran yang terdapat pada email tersebut dengan mengunjungi atau mengunduhnya	10	19	3	26	7
Melaporkan kepada pihak berwenang dan penyelenggara layanan email/pesan apabila mendapat email/pesan yang mencurigakan	2	27	1	28	1
Apabila ditelepon oleh orang tidak dikenal yang mengaku sebagai pihak berwenang, maka saya akan memberikan data yang mereka perlukan sepeti nomor KTP, tanggal lahir, alamat rumah, dan sebagainya apabila diminta dikarenakan saya warga negara yang patuh hukum.	1	28	1	28	0

(P) ISSN 2442-451X
(O) ISSN 2503-3832

Jika saya menemukan *flashdisk* di jalan, maka saya akan acuh dan meninggalkannya	25	4	25	4	0
Jika saya menemukan *flashdisk* di jalan, maka saya akan mencari tahu identitas pemiliknya dengan melihat isi *flashdisk* tersebut	1	28	1	28	0
Saya sering melakukan *backup* data pada perangkat saya ke penyimpanan eksternal setelah membuat perubahan pada data tersebut	10	19	23	6	13
Melakukan penyimpanan sebagai data cadangan pada layanan cloud terpercaya	1	28	1	28	0
Saya memahami beberapa istilah virus seperti *worm, malware*, serta kiat menghindarinya	11	18	9	20	2
Saya pernah terkena ransomware	10	19	6	23	4
Saya akan membayar jaminan apabila terkena *ransomware* untuk memulihkan file berharga atau foto kenangan yang tidak sempat saya cadangkan	20	9	26	3	6
Ketika saya melihat suatu website memiliki tanda gembok dan diawali dengan HTTPS, maka saya yakin 100% bahwa website tersebut valid dan terpercaya untuk melakukan transaksi *online*	19	10	26	3	7
Fitur incognito pada browser yang saya miliki dapat membuat saya tidak diketahui riwayat browsingnya bahkan oleh penyedia layanan internet (ISP) yang saya gunakan	27	2	28	1	1
Apabila keluarga saya meminta *password* dari akun layanan keuangan saya melalui email, maka akan saya beritahukan melalui email	3	26	2	27	1
Apabila keluarga saya meminta *password* dari akun layanan keuangan saya melalui email, maka akan saya beritahukan melalui layanan pesan singkat	8	21	6	23	2
Saya pernah mendapat email/pesan mencurigakan yang memberikan saya iming-iming hadiah yang sangat besar	16	13	12	17	4
Apabila mendapat email/pesan mencurigakan, saya akan mencari tahu link atau lampiran yang terdapat pada email tersebut dengan mengunjungi atau mengunduhnya	11	18	9	20	2

5. KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan sebagai berikut: Penerapan metode PXP SDLC dapat digunakan dengan tepat dan membantu pengembangan perangkat lunak *game* edukasi. Uji penerimaan pengguna menyatakan bahwa aplikasi ini sesuai dengan apa yang diharapkan pengguna dari pernyataannya untuk cerita pengguna. Penerapan teknik gamifikasi dapat meningkatkan kesadaran keamanan siber pengguna. Berdasarkan hasil pengujian, terdapat peningkatan kesadaran keamanan siber pengguna pada aspek kesadaran yang telah ditetapkan. Selain itu, dari kuesioner setelah menggunakan aplikasi, semua responden menyatakan bahwa menggunakan aplikasi SadarSiber dapat memberikan informasi untuk meningkatkan kesadaran keamanan siber pengguna.

Saran berikut dapat diajukan untuk penelitian selanjutnya, yaitu menerapkan bentuk permainan lain untuk gamifikasi yang berbeda, menerapkan SDLC lain untuk dibandingkan dengan penerapan PXP dalam penelitian ini. Selain itu, disarankan untuk menggunakan bentuk survei atau indikator lain untuk mengukur tingkat kesadaran keamanan siber dari responden. Penelitian lanjutan juga dapat dilakukan dengan jumlah responden yang lebih besar.

Daftar Pustaka

[1] Badan Siber dan Sandi Negara, "Rekap Serangan Siber (Januari – April 2021)," Rekap Serangan Siber, Apr-2021. [Online]. Available: https://cloud.bssn.go.id/s/qpBD4mbZCmL3F85. [Accessed: 08-Oct-2021].

[2] A. Roy, L. Mejia, P. Helling, and A. Olmsted, "Automation of cyber-reconnaissance: A Java-based open source tool for information gathering," 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), 2017.

[3] W. Jeon, K. Jeeyeon, D. Won, and Y. Lee, "A Practical Analysis of Smartphone Security," Human Interface and the Management of Information. Interacting with Information. Human Interface 2011, vol. 6771, 2011.

[4] Badan Pusat Statistik, Telekomunikasi Indonesia 2018, 02-Dec-2019. [Online]. Available: https://www.bps.go.id/publication/2019/12/02/6799f23db22e9bdcf52c8e03/statistik-telekomunikasi-indonesia-2018.html. [Accessed: 08-Oct-2020].

[5] S. Scholefield and L. A. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," HCI for Cybersecurity, Privacy and Trust Lecture Notes in Computer Science, pp. 191–203, 2019.

[6] Y. Dzhurov, "Personal Extreme Programming – An Agile Process for Autonomous Developers", Proceedings of International Conference on SOFTWARE, SERVICES & SEMANTIC TECHNOLOGIES, ISBN 978-954-9526-62-2, 2009

[7] R. Agarwal dan D. Umphress, "Extreme Programming for a Single Person Team", Computer Science &

(P) ISSN 2442-451X
(O) ISSN 2503-3832

Software Engineering 107 Dunstan Hall Auburn University, 2008

[8] Y. A. Younis, K. Kifayat, Q. Shi, E. Matthews, G. Griffiths, and R. Lambertse, "Teaching Cryptography Using CYPHER (InteraCtive CrYPtograpHic Protocol TEaching and LeaRning)," Proceedings of the 6th International Conference on Engineering & MIS 2020, 2020.

[9] M. Hendrix, A. Al-Sherbaz, and V. Bloom, "Game Based Cyber Security Training: are Serious Games suitable for cyber security training?" International Journal of Serious Games, vol. 3, no. 1, 2016.

[10] T. Jagust, I. Boticki, V. Mornar, and H.-J. So, "Gamified Digital Math Lessons for Lower Primary School Students," 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), 2017.

[11] M. M. Muller and W. F. Tichy, "Case study: extreme programming in a university environment," Proceedings of the 23rd International Conference on Software Engineering. ICSE, 2001.

[12] P. A. W. Putro, Y. R. Pramadi, H. Setiawan, N. K. Gunawan, R. B. Hadiprakoso and H. Kabetta, "Correlation Between Motivation and Achievement of Competencies in the Hands-On Learning Method," 2019 5th International Conference on Education and Technology (ICET), 2019, pp. 29-32, doi: 10.1109/ICET48172.2019.8987209.

[13] K. Senthilkumar and S. Easwaramoorthy, "A Survey on Cyber Security awareness among college students in Tamil Nadu," IOP Conference Series: Materials Science and Engineering, vol. 263, p. 042043, 2017.

[14] Sugiyono, METODE PENELITIAN KUANTITATIF, KUALITATIF, R&D, 19th ed. Bandung, Indonesia: Alfabeta, Publisher 2013.

[15] A. Cockburn, "Crystal Clear: A Human-Powered Methodology for Small Teams (The Agile Software Development Series)", Addison-Wesley Professional, 2004.

[16] R. Pinter, "Willingness of Online Access Panel Members to Participate in Smartphone Application-Based Research," Mobile Research Methods: Opportunities and challenges of mobile research methodologies, 2015.

[17] S. Asri, Prihatini PM, Setiawan W. "Comparing Traditional and Agile Software Development Approaches: Case of Personal Extreme Programming". In International Conference on Science and Technology. 2018.