IMPLEMENTASI PROTOTYPE KEAMANAN *TWO-FACTOR AUTHENTICATION (*2FA*)* PADA SISTEM INFORMASI AKADEMIK (STUDI KASUS: UIN SULTAN MAULANA HASANUDDIN BANTEN)

http://dx.doi.org/10.28932/jutisi.vXiX.X

Riwayat Artikel
Received: xx Bulan 20xx | *Final Revision*: xx Bulan 20xx | *Accepted*: xx Bulan 20xx

Abstrak — **Sistem Informasi Akademik (SIAKAD) menyimpan data mahasiswa yang penting, seperti nilai, Kartu Rencana Studi, dan informasi pribadi, sehingga keamanannya memerlukan perhatian khusus. Sistem otentikasi pada SIAKAD UIN Sultan Maulana Hasanuddin Banten saat ini hanya menggunakan satu faktor—kombinasi Nomor Induk Mahasiswa (NIM) dan PIN—tanpa langkah verifikasi tambahan. Artinya, jika seseorang mengetahui atau menebak detail login tersebut, ia dapat mengambil alih akun tersebut. Penelitian ini bertujuan untuk merancang dan mengimplementasikan prototipe antarmuka Otentikasi Dua Faktor *(*2FA*)* untuk sistem SIAKAD dengan tetap mematuhi prinsip-prinsip Interaksi Manusia-Komputer *(HCI)*, guna memastikan bahwa peningkatan keamanan tidak mengorbankan kenyamanan pengguna. Metode yang digunakan adalah penelitian berbasis desain, yang mencakup tinjauan pustaka mengenai prinsip-prinsip *HCI* dan metode *2FA*, analisis mekanisme otentikasi yang ada dalam sistem SIAKAD, desain *wireframe*, serta pembuatan prototipe interaktif menggunakan Figma. Prototipe ini terdiri dari empat komponen: halaman login, verifikasi dua faktor menggunakan *OTP* melalui email, verifikasi dua faktor dengan *Google Authenticator (TOTP),* dan notifikasi untuk deteksi perangkat baru. Setiap komponen dirancang dengan menerapkan prinsip-prinsip visibilitas status sistem, pencegahan dan pemulihan kesalahan, serta kontrol dan kebebasan pengguna. Hasil pengujian menunjukkan bahwa penggunaan ketiga metode verifikasi ini secara bersamaan menambah lapisan keamanan ekstra pada proses login tanpa mempersulit pengguna. Pengguna tetap dapat memilih metode verifikasi yang mereka sukai dan menentukan berapa lama mereka mempercayai perangkat yang sedang mereka gunakan. Penelitian ini diharapkan dapat menjadi acuan untuk meningkatkan keamanan sistem akademik daring di perguruan tinggi yang masih menggunakan otentikasi satu faktor.**

Kata kunci— **sistem informasi akademik; otentikasi; interaksi manusia-komputer; keamanan sistem informasi; otentikasi dua factor**

Implementation of a *TWO-FACTOR AUTHENTICATION (*2FA*)* Security Prototype for an Academic Information System (Case Study: UIN Sultan Maulana Hasanuddin Banten)

Abstract — **The Academic Information System (SIAKAD) keeps important student data, such as grades, Study Plan Cards, and personal information, so its security needs special attention. The authentication system in the SIAKAD of UIN Sultan Maulana Hasanuddin Banten currently uses only one factor, which is just a combination of NIM and PIN, without any extra verification steps.This means that if someone finds out or guesses these login details, they could take over the account. This study aims to design and implement a prototype for a TWO-FACTOR AUTHENTICATION (2FA) interface on the SIAKAD system while still following the principles of Human-Computer Interaction (HCI), ensuring that improved security does not compromise the user's comfort. The method used is design-based research, which includes a literature study on HCI principles and 2FA methods, analysis of the current authentication mechanism in the SIAKAD system, design of wireframes, and creation of an interactive prototype using Figma. The prototype includes four components: the login page, two-factor verification using email OTP, two-factor verification.**

with *Google Authenticator (TOTP),* and a new device detection notification. Each component is designed by applying the principles of visibility of system status, error prevention and recovery, and user control and freedom. Test results show that using all three verification methods together adds extra security to the login process without making it harder for users.Users can still choose their preferred verification method and set how long they trust the device they're using. This study is expected to serve as a reference for improving the security of university online academic systems that still use single-factor authentication.

Keywords— academic information system; authentication; human-computer interaction; information system security; two-factor authentication

I. PENDAHULUAN

Autentikasi berbasis satu faktor yang hanya mengandalkan kata sandi masih memiliki berbagai kelemahan keamanan karena pengguna cenderung memilih kata sandi yang mudah diingat sehingga lebih rentan terhadap serangan seperti *password guessing* dan *shoulder surfing*. Oleh karena itu, diperlukan mekanisme autentikasi yang lebih aman, seperti *Two-Factor Authentication (2FA*), untuk memberikan lapisan verifikasi tambahan sekaligus mempertahankan kemudahan penggunaan. [18]. Jika informasi akun pengguna bocor melalui serangan phishing atau kebocoran data di layanan lain, penyerang bisa dengan mudah masuk ke akun tanpa kesulitan [8] [16]. Pemeriksaan terhadap SIAKAD Universitas Islam Negeri (UIN) Sultan Maulana Hasanuddin Banten menunjukkan bahwa proses login di sistem tersebut masih hanya memerlukan NIM dan PIN, sehingga bisa mengalami risiko yang sama.

Autentikasi dengan satu faktor dianggap tidak aman karena risiko akun bisa dicuri, seperti yang ditunjukkan oleh penelitian besar yang menunjukkan bahwa pengguna sering memilih kata sandi yang pendek dan mudah ditebak [18]. Jika informasi akun pengguna bocor melalui serangan phishing atau kebocoran data di layanan lain, penyerang bisa dengan mudah masuk ke akun tanpa kesulitan [8] [16]. Pemeriksaan terhadap SIAKAD Universitas Islam Negeri (UIN) Sultan Maulana Hasanuddin Banten menunjukkan bahwa proses login di sistem tersebut masih hanya memerlukan NIM dan PIN, sehingga bisa mengalami risiko yang sama.

Autentikasi dua faktor *(2FA)* adalah salah satu cara umum yang digunakan untuk mengatasi kelemahan dari autentikasi satu faktor.*2FA* memerlukan kombinasi dua jenis faktor verifikasi yang berbeda, yaitu sesuatu yang diketahui pengguna seperti kata sandi atau PIN, serta sesuatu yang dimiliki pengguna seperti kode *One-Time Password (OTP)* yang dikirim lewat email atau kode *Time-based One-Time Password (TOTP)* yang dihasilkan oleh aplikasi authenticator [22] [23]. Penambahan *2FA* secara signifikan dapat menurunkan risiko akun direbut, karena penyerang harus memiliki akses ke faktor kedua yang biasanya tidak bisa didapatkan hanya dari kebocoran informasi login [21] [22].

Persepsi mengenai keamanan dan privasi memengaruhi perilaku pengguna terkait mekanisme keamanan seperti kata sandi dan autentikasi multifaktor. Pengguna cenderung mempraktikkan perilaku yang tidak aman berdasarkan persepsi mereka tentang keamanan dan kenyamanan. Makalah ini menyoroti keselarasan antara persepsi privasi dan keamanan serta potensi penerapan kognisi yang diperluas *(augmented cognition)* dalam bidang Interaksi Manusia-Komputer (HCI) dan desain instruksional untuk meningkatkan perilaku terkait keamanan dalam hal akses. [7] [17]. Prinsip *Human-Computer Interaction (HCI)* penting untuk diperhatikan dalam merancang *2FA*, terutama prinsip seperti visibilitas status sistem, pencegahan dan pemulihan kesalahan, serta kontrol dan kebebasan pengguna [1] [2] [20], agar penambahan lapisan keamanan tetap mudah dipahami dan tidak memberatkan pengguna. Konsep keamanan yang dapat digunakan menggabungkan kebutuhan akan keamanan dengan kemudahan dalam penggunaan, sehingga pengguna tetap bisa menjalankan proses keamanan tanpa merasa kesulitan [6] [14].

Penelitian sebelumnya mengenai survei mekanisme Multi-Factor Authentication telah mengidentifikasi berbagai metode *2FA* dengan tingkat keamanan dan tingkat kemudahan penggunaan yang berbeda, mulai dari *OTP* melalui SMS atau email hingga *TOT*P melalui aplikasi [22] [23]. Penelitian tentang keamanan yang ramah pengguna juga membahas betapa pentingnya membuat sistem keamanan yang memperhatikan kebutuhan pengguna agar lebih banyak orang mau menggunakannya [14] [24]. Namun, sebagian besar penelitian tersebut belum secara khusus menggabungkan desain *2FA* dengan prinsip HCI dalam satu prototipe antarmuka pada studi kasus sistem informasi akademik perguruan tinggi di Indonesia. Kondisi ini menjadi celah dalam penelitian yang kemudian diisi oleh penelitian ini.

Berdasarkan penjelasan tersebut, penelitian ini bertujuan untuk membuat dan menerapkan prototipe antarmuka keamanan *2FA* di SIAKAD, dengan mengambil SIAKAD UIN Sultan Maulana Hasanuddin Banten sebagai contoh studi.Antarmuka ini melibatkan tiga mekanisme verifikasi, yaitu *OTP* melalui email, *Google Authenticator (TOTP)*, serta notifikasi untuk mendeteksi perangkat baru. Kebaruan penelitian ini terletak pada cara desain yang menggabungkan prinsip *HCI* secara jelas dalam setiap bagian dari *2FA* yang dibuat, sehingga dapat meningkatkan keamanan sistem akademik tanpa mengurangi kepraktisan dan kemudahan penggunaan bagi mahasiswa sebagai pengguna utama sistem tersebut.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan design-based research, yaitu pendekatan yang tidak hanya mengamati kondisi yang ada, tetapi juga menyusun rancangan dan membangun prototype nyata sebagai solusi atas permasalahan yang ditemukan [19]. Pendekatan ini dipilih karena sesuai untuk penelitian *HCI* yang bersifat iteratif, mencakup tahap

perancangan desain, evaluasi, dan revisi [1] [2] [19]. Penelitian dilaksanakan dalam beberapa tahapan, yaitu kajian literatur, analisis permasalahan, perancangan wireframe dan prototype, serta evaluasi rancangan berdasarkan prinsip *HCI*

A. Kajian Literatur

Langkah pertama dilakukan dengan mengumpulkan dan mengamati berbagai bacaan yang berkaitan dengan dua dasar utama, yaitu prinsip *Human-Computer Interaction* dan konsep *Two-Factor Authentication*. Prinsip-prinsip *HCI* yang dianalisis mencakup sepuluh *heuristik usability* yang diajukan oleh Nielsen [1] [2],dengan penekanan pada tiga prinsip yang paling berkaitan dengan keamanan, yaitu visibilitas status sistem, pencegahan dan pemulihan kesalahan, serta kontrol dan kebebasan pengguna [20]. Konsep *2FA* yang dianalisis mencakup metode *OTP* melalui email, *TOTP* melalui aplikasi authenticator, serta cara mendeteksi perangkat baru [22] [23].

B. Analisis Permasalahan Autentikasi

Tahap kedua dilakukan dengan menganalisis cara kerja mekanisme autentikasi di SIAKAD UIN Sultan Maulana Hasanuddin Banten, dengan cara mengamati langsung proses login pada sistem tersebut. Analisis ini berfokus pada mengidentifikasi risiko yang muncul dari penggunaan mekanisme autentikasi satu faktor, berdasarkan studi tentang kebiasaan pengguna dalam menggunakan password [18] serta studi mengenai penolakan pengguna terhadap saran keamanan yang dianggap merepotkan [8]. Hasil dari analisis ini digunakan sebagai dasar untuk menentukan kombinasi metode *2FA* yang akan dirancang di tahap selanjutnya.

C. Perancangan Wireframe dan Prototype

Tahap ketiga dilakukan dengan merancang wireframe sederhana yang kemudian dikembangkan menjadi prototype interaktif menggunakan aplikasi *Figma*. Perancangan dilakukan secara iteratif, yaitu rancangan awal didiskusikan dan direvisi secara berulang hingga menghasilkan prototype akhir yang dianggap sesuai dengan kebutuhan penelitian [12] [19]. Terdapat empat komponen utama yang dirancang, yaitu:

1) Halaman login: menyediakan kolom NIM/Username dan PIN, dilengkapi opsi alternatif untuk masuk langsung menggunakan Google Authenticator.

2) Verifikasi Email OTP: menampilkan kode *OTP* enam digit yang dikirim ke email terdaftar, dengan batas waktu berlaku selama dua menit serta opsi kirim ulang kode.

3) Verifikasi Google Authenticator: menampilkan simulasi kode *TOTP* enam digit pada aplikasi authenticator yang berubah otomatis setiap 30 detik, dilengkapi indikator hitung mundur.

4) Notifikasi deteksi perangkat baru: menampilkan rincian informasi perangkat (browser, sistem operasi, lokasi, alamat IP, dan waktu login) setiap kali sistem mendeteksi login dari perangkat yang berbeda dari biasanya, disertai pilihan durasi kepercayaan perangkat selama satu jam atau dua puluh empat jam.

D. Evaluasi Rancangan Berdasarkan Prinsip HCI

Tahap terakhir adalah mengevaluasi setiap bagian dari prototype yang sudah dibuat, agar bisa memastikan bahwa desain tersebut telah memenuhi tiga prinsip dasar *HCI* yang digunakan, yaitu visibilitas status sistem, pencegahan dan pemulihan kesalahan, serta kontrol dan kebebasan pengguna [1] [2] [20]. Evaluasi dilakukan dengan cara deskriptif kualitatif, yaitu dengan menganalisis setiap bagian antarmuka pada prototype, lalu membandingkannya dengan definisi dan indikator dari setiap prinsip *HCI* yang digunakan sebagai acuan [13].

III. HASIL DAN PEMBAHASAN

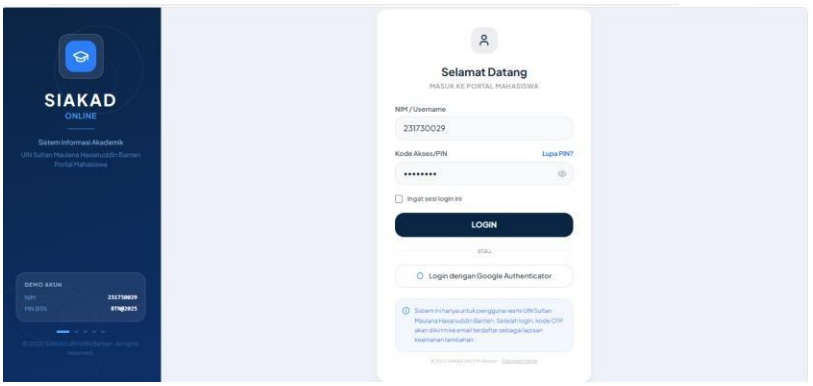
A. Analisis Mekanisme Autentikasi SIAKAD

Dari pengamatan terhadap SIAKAD UIN Sultan Maulana Hasanuddin Banten, terlihat bahwa proses login di sistem tersebut hanya membutuhkan dua data, yaitu NIM dan PIN, tanpa ada tahap verifikasi tambahan lainnya. Berdasarkan penelitian sebelumnya, kondisi ini menyebabkan setidaknya tiga risiko utama. Pertama, akun bisa diakses orang lain jika PIN diketahui atau berhasil ditebak, karena banyak pengguna memilih kombinasi angka yang mudah ditebak [18]. Kedua, tidak ada sistem yang menginformasikan pemilik akun ketika ada login dari perangkat atau lokasi yang tidak biasa [7] [8]. Ketiga, tidak ada lapisan verifikasi tambahan yang bisa menghalangi serangan meskipun PIN sudah diketahui [22] [23]. Ketiga risiko tersebut menjadi dasar dalam membuat prototype *2FA* yang akan dijelaskan di bagian berikutnya. Simpulan merupakan pernyataan yang merujuk pada tujuan penelitian yang dihubungkan dengan hasil dan pembahasan dari penelitian. Rencana penelitian lanjutan juga dapat disebutkan dalam bagian ini.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

Halaman Login

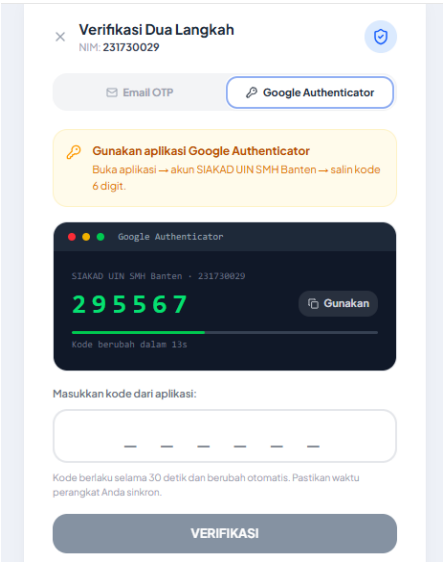
Halaman login dirancang sesederhana mungkin agar tidak membingungkan pengguna, sekaligus tetap mengarahkan pengguna pada opsi keamanan tambahan, seperti terlihat pada Gambar 1. Pengguna memasukkan NIM/Username dan PIN seperti pada mekanisme yang sudah ada, namun ditambahkan opsi "Login dengan *Google Authenticator*" sebagai alternatif metode masuk yang lebih cepat bagi pengguna yang telah mengaktifkan *TOTP*. Informasi keamanan pada bagian bawah formulir, yang menjelaskan bahwa kode *OTP* akan dikirim ke email terdaftar sebagai lapisan keamanan tambahan, merupakan penerapan prinsip visibility of system status [1] [2] sehingga pengguna mengetahui sejak awal bahwa proses login akan melalui verifikasi tambahan.



Gambar 1. Prototype Halaman Login SIAKAD

C. Prototype Verifikasi Dua Langkah

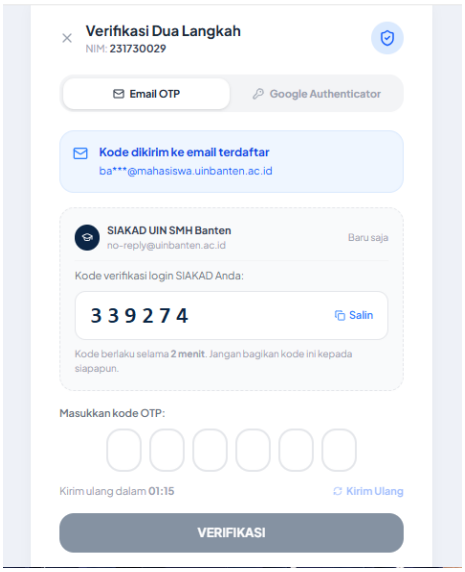
Komponen verifikasi dua langkah menyediakan dua pilihan metode, yaitu *Google Authenticator* dan Email *OTP*, yang dapat dipilih melalui tab pada bagian atas tampilan. Pada metode *Google Authenticator*, seperti terlihat pada Gambar 2, pengguna diminta menyalin kode *TOTP* enam digit dari aplikasi authenticator, dilengkapi indikator waktu berupa progress bar yang menghitung mundur sebelum kode berubah. Tombol "Gunakan" pada pojok kanan kode memudahkan pengguna untuk langsung menyalin kode ke kolom input tanpa perlu mengetik manual, sejalan dengan prinsip error prevention, karena pengetikan manual berisiko menimbulkan kesalahan input [1] [20].



Gambar 2. Prototype Verifikasi Dua Langkah Menggunakan Google Authenticator

Pada metode Email *OTP*, seperti terlihat pada Gambar 3, sistem menampilkan keterangan bahwa kode verifikasi telah dikirim ke alamat email terdaftar, dengan sebagian alamat email disamarkan demi menjaga privasi pengguna. Tersedia enam kotak input terpisah untuk memasukkan kode *OTP*, penghitung mundur waktu kirim ulang, serta tautan "Kirim Ulang" yang aktif kembali setelah hitungan mundur berakhir. Rancangan ini menerapkan prinsip error prevention and

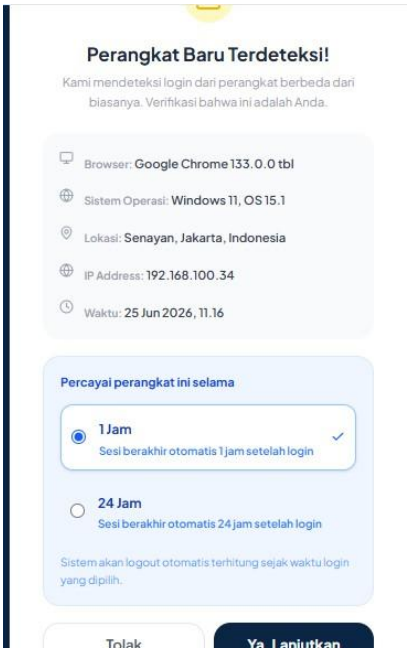
recovery, karena pengguna diberikan jalan keluar yang jelas apabila kode tidak diterima atau telah kedaluwarsa, tanpa harus mengulang seluruh proses login dari awal [1] [6].



Gambar 3. Prototype Verifikasi Dua Langkah Menggunakan Email OTP

D. Prototype Notifikasi Deteksi Perangkat Baru

Komponen keamanan tambahan berupa notifikasi deteksi perangkat baru, seperti terlihat pada Gambar 4, akan muncul setiap kali sistem mendeteksi proses login dari perangkat yang berbeda dari biasanya. Notifikasi menampilkan rincian informasi perangkat secara transparan, meliputi jenis browser, sistem operasi, lokasi, alamat IP, dan waktu login, sehingga pengguna dapat menilai sendiri apakah aktivitas login tersebut benar dilakukan olehnya atau tidak [7] [8]. Pengguna kemudian diminta menentukan tingkat kepercayaan terhadap perangkat tersebut, dengan dua pilihan durasi (satu jam atau dua puluh empat jam), serta dua tombol aksi, yaitu “Tolak” dan “Ya, Lanjutkan”. Rancangan ini menerapkan prinsip user control and freedom, karena pengguna diberi kendali penuh untuk menerima atau menolak akses dari perangkat baru sekaligus mengatur sendiri durasi kepercayaan sesuai kebutuhan [1] [2] [20].



Gambar 4. Prototype Notifikasi Deteksi Perangkat Baru

E. Pembahasan

Keempat komponen prototype yang dirancang menunjukkan bahwa penambahan mekanisme *2FA* pada SIAKAD dapat dilakukan tanpa harus mengorbankan kemudahan penggunaan. Penyediaan dua pilihan metode verifikasi, yaitu Email *OTP* dan *Google Authenticator*, Evaluasi heuristik (HE) adalah metode inspeksi kegunaan (usability) yang populer, yang memungkinkan evaluator ahli untuk mendokumentasikan masalah kegunaan pada desain antarmuka. Kebutuhan sumber daya yang relatif rendah serta manfaat besar dalam mengidentifikasi masalah kegunaan dan menyarankan aspek perbaikannya menjadikan HE metode yang sangat dapat diterapkan dalam skala luas. Namun, terdapat beberapa keterbatasan dan kendala dalam menerapkan HE di perusahaan berskala besar; oleh karena itu, edukasi dan komunikasi, serta penggabungan HE dengan teknik kegunaan lainnya, dapat sangat meningkatkan nilai dan manfaat dari pelaksanaan metode ini. [1] [2]. Pengguna yang sudah familiar dengan aplikasi authenticator dapat memilih metode *TOTP* yang lebih cepat, sementara pengguna yang belum terbiasa dapat tetap mengandalkan metode Email *OTP* yang lebih familiar [22].

Penerapan indikator waktu pada kode *TOTP* maupun Email *OTP*, serta notifikasi deteksi perangkat baru yang menampilkan rincian informasi perangkat secara transparan, merupakan bentuk konkret penerapan prinsip *visibility of system status*. Prinsip ini penting agar pengguna tidak merasa kebingungan atau khawatir berlebihan terhadap proses verifikasi yang berlangsung [6] [14]. Dari sisi keamanan, kombinasi tiga mekanisme tersebut secara signifikan mengurangi risiko pengambilalihan akun yang hanya mengandalkan PIN semata, karena penyerang yang berhasil memperoleh PIN tetap harus melewati lapisan verifikasi kedua berupa kode *OTP* atau *TOTP*, atau terdeteksi melalui notifikasi perangkat baru [18] [22] [23].

Teknologi keamanan sering kali menerapkan pendekatan desain sistem yang berfokus pada komponen, bukan pada pengguna. Akibatnya, kebutuhan dan nilai-nilai pengguna tidak terakomodasi dengan memadai, yang pada gilirannya berdampak pada aspek kegunaan *(usability)* keamanan. Dalam makalah ini, kami memaparkan pelajaran yang diperoleh dari penerapan proses desain keamanan yang berpusat pada pengguna untuk mengatasi tantangan kegunaan keamanan yang sudah lama dikenal, yaitu autentikasi kunci dalam layanan pesan instan yang aman. Pengguna jarang melakukan prosedur autentikasi kunci ini, sehingga komunikasi mereka yang menggunakan enkripsi ujung-ke-ujung *(end-to-end)* menjadi rentan. Pendekatan kami mencakup lokakarya desain kolaboratif, evaluasi oleh ahli, pembuatan prototipe *storyboard* secara iteratif, dan evaluasi daring. Meskipun kami tidak dapat membuktikan bahwa pendekatan desain kami menghasilkan peningkatan kegunaan atau pengalaman pengguna, kami menemukan bahwa prototipe yang berpusat pada pengguna dapat meningkatkan pemahaman pengguna mengenai implikasi keamanan. Oleh karena itu, prototipe yang didasarkan pada intuisi, kebutuhan, dan nilai-nilai pengguna merupakan titik awal yang bermanfaat untuk menangani tantangan keamanan yang telah lama ada. Penerapan pendekatan desain yang saling melengkapi dapat lebih meningkatkan kegunaan dan pengalaman pengguna. [5] Metode Cognitive Walkthrough digunakan untuk mengevaluasi kemudahan pengguna dalam menyelesaikan tugas pada antarmuka sistem [3] [4]. Pengujian tersebut menjadi salah satu rekomendasi penting bagi penelitian lanjutan.

IV. SIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan prototype antarmuka keamanan *TWO-FACTOR AUTHENTICATION (2FA)* pada Sistem Informasi Akademik, dengan studi kasus SIAKAD UIN Sultan Maulana Hasanuddin Banten, yang sebelumnya hanya menerapkan autentikasi satu faktor berupa kombinasi NIM dan PIN tanpa lapisan verifikasi tambahan. Prototype yang dihasilkan terdiri atas tiga mekanisme verifikasi, yaitu Email *OTP*, *Google Authenticator* berbasis *TOTP*, dan notifikasi deteksi perangkat baru, yang seluruhnya dirancang dengan menerapkan prinsip *Human-Computer Interaction,* yaitu *visibility of system status*, *error prevention and recovery*, dan *user control and freedom*. Hasil evaluasi rancangan menunjukkan bahwa penambahan lapisan keamanan *2FA* pada SIAKAD dapat dirancang tanpa mengorbankan kenyamanan dan kemudahan penggunaan bagi mahasiswa sebagai pengguna utama sistem. Penelitian lanjutan disarankan untuk mengembangkan prototype ini menjadi sistem yang berfungsi penuh serta melakukan pengujian usability secara kuantitatif, misalnya menggunakan *System Usability Scale*, agar efektivitas rancangan *2FA* dapat diukur secara objektif.

UCAPAN TERIMA KASIH

Penghargaan disampaikan kepada Badan Riset dan Inovasi Nasional (BRIN), khususnya Kelompok Riset *Human-Computer Interaction and Visualization* pada Pusat Riset Sains Data dan Informasi di Kawasan Sains dan Teknologi B.J. Habibie Serpong, atas bimbingan dan fasilitas riset yang diberikan selama proses perancangan prototype ini. Penghargaan juga disampaikan kepada Program Studi Informatika, Universitas Islam Negeri Sultan Maulana Hasanuddin Banten, atas dukungan akademik yang diberikan.

DAFTAR PUSTAKA

1] G.-C. Yang, Q. Hu, M. R. Asghar, and H. Kim, "TIM: Secure and Usable Authentication for Smartphones," *Journal of Information Security and Applications*, vol. 71, Art. no. 103374, 2022, doi:

[2] H. J. A. Fuller, T. Arnold, K. D. Maddox, and K. Adams, "Considerations and Strategies for Operationalizing Heuristic Evaluation Work," in *Healthcare and Medical Devices*, vol. 51, *Proceedings of the 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022), 2022, pp. 239–247, doi: 10.54941/ahfe1002123.*

[3] M. Farzandipour, E. Nabovati, and M. S. Jabali, "Comparison of usability evaluation methods for a health information system: heuristic evaluation versus cognitive walkthrough method," *BMC Medical Informatics and Decision Making*, vol. 22, no. 157, pp. 1–13, 2022, doi: 10.1186/s12911-022-01905-7.

[4] T. Tullis and B. Albert, Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics, 2nd ed. Waltham, MA, USA: Morgan Kaufmann, 2013.

[5] . M. Fassl, L. T. Gröber, and K. Krombholz, "Exploring User-Centered Security Design for Usable Authentication Ceremonies," in *Proc. 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*, Yokohama, Japan (Virtual), May 2021, pp. 1–15, doi: 10.1145/3411764.3445164.

[6] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis, IN, USA: Wiley, 2020.

[7] A. R. Y. Wang, M. S. Endsley, and D. Kaber, "Privacy and Security Perceptions in Augmented Cognition Applications," in *Lecture Notes in Computer Science*, vol. 14036, *Proc. 15th International Conference on Applied Human Factors and Ergonomics (AHFE 2023)*. Cham, Switzerland: Springer, 2023, pp. 242–250, doi: 10.1007/978-3-031-35897-3_28.

[8] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in Proc. Workshop New Security Paradigms (NSPW), 2009, pp. 133–144.

[9] International Organization for Standardization, Information Security, Cybersecurity and Privacy Protection — Information Security Controls, ISO/IEC 27002:2022, 2022.

[10] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, Panduan Penyelenggaraan Sistem Informasi Akademik Perguruan Tinggi. Jakarta, Indonesia: Kemendikbudristek, 2023.

[11] Badan Riset dan Inovasi Nasional, Profil Kawasan Sains dan Teknologi B.J. Habibie. Tangerang Selatan, Indonesia: BRIN, 2024.

[12] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 6th ed. Thousand Oaks, CA, USA: SAGE Publications, 2023.

[13] B. Shneiderman, C. Plaisant, M. Cohen, S. Jacobs, N. Elmqvist, and N. Diakopoulos, Designing the User Interface: Strategies for Effective Human-Computer Interaction, 6th ed. Boston, MA, USA: Pearson, 2018.

[14] L. F. Cranor and S. Garfinkel, Eds., Security and Usability: Designing Secure Systems that People Can Use. Sebastopol, CA, USA: O'Reilly Media, 2005.

[15] J. Sauro and J. R. Lewis, Quantifying the User Experience: Practical Statistics for User Research, 2nd ed. Cambridge, MA, USA: Morgan Kaufmann, 2016.

[16] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security and Privacy, 2012, pp. 553–567.

[17] C. Reuter, L. Lo Iacono, and A. Benlian, "A Quarter Century of Usable Security and Privacy Research: Transparency, Tailorability, and the Road Ahead," *Behaviour & Information Technology*, vol. 41, no. 10, pp. 2035–2048, 2022, doi: 10.1080/0144929X.2022.2080908.

[18] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web (WWW), 2007, pp. 657–666.

[19] A. Collins, D. Joseph, and K. Bielaczyc, "Design research: Theoretical and methodological issues," J. Learn. Sci., vol. 13, no. 1, pp. 15–42, 2004.

[20] D. Norman, The Design of Everyday Things, Revised and Expanded ed. New York, NY, USA: Basic Books, 2013.

[21] National Institute of Standards and Technology, "Digital identity guidelines: Authentication and lifecycle management," NIST, Gaithersburg, MD, USA, Special Publication 800-63B, 2023.

[22] M. Dasgupta, A. K. Nag, and D. Bhattacharyya, "A survey of multi-factor authentication mechanisms in modern web applications," J. Inf. Secur. Appl., vol. 73, 2023, Art. no. 103440.

[23] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA), 2009, pp. 641–644.

[24] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards implementing inclusive authentication technologies for older adults," in Proc. SOUPS Workshop Inclusive Privacy and Security (WIPS), 2019.