BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan digital memiliki peran krusial dalam menjaga kerahasiaan informasi pribadi pengguna, terutama di tengah transformasi teknologi yang pesat pada era Revolusi Industri 4.0. Keamanan digital sudah diterapkan pada beberapa aplikasi yang umum digunakan masyarakat, misalnya: aplikasi pemerintahan, dunia perbankan, institusi pendidikan, organisasi kemiliteran, organisasi kepolisian, dan lain sebagainya. Kemajuan teknologi yang pesat dalam layanan daring telah mendorong peningkatan jumlah identitas digital, seiring dengan tuntutan dan kebutuhan pengguna. Dilansir "Katadata Media Network" yang mengutip laporan dari "*We are Social*". Jumlah pengguna internet di Indonesia menunjukkan tren peningkatan signifikan antara tahun 2018 hingga Januari 2022, yakni sebesar 132,7 juta pengguna pada tahun 2018, 150 juta pada 2019, 175,4 juta pada 2020, 202,6 juta pada 2021, dan mencapai 204,7 juta pengguna pada tahun 2022. Sementara itu, menurut laporan terbaru APJII tahun 2023, jumlah tersebut telah meningkat menjadi 215,6 juta pengguna. Dapat diasumsikan bahwa tren jumlah pengguna yang menggunakan internet dalam 6 tahun terakhir (2018-2023) khususnya di Indonesia, mengalami peningkatan karena terdorong oleh penggunaan internet yang sudah menjadi kebutuhan masyarakat.

Dalam keamanan digital, penggunaan *password* dan *username* menjadi metode pengamanan yang umum digunakan hingga sekarang (WIJAYA, n.d.). Namun penggunaan metode tersebut tidak menjamin bahwa akses hak pengguna tidak bisa ditembus sama sekali oleh pengguna lain Contoh sederhana dari pelanggaran keamanan terjadi ketika individu yang tidak memiliki otorisasi berhasil memperoleh akses ke sistem basis data, sehingga dapat mengakses dan mengambil data kredensial seperti nama pengguna dan kata sandi yang tersimpan. Kerahasiaan menjadi faktor krusial untuk menjaga isi informasi dari siapapun, kecuali pihak berwenang yang mempunyai otoritas untuk mengakses informasi tersebut (Yahya & Amini, 2018). Melansir survei KIC (Katadata Insight Center) bersama Kementerian Komunikasi & Informatika (Menkominfo) pada tahun

2021, Dengan jumlah sampel survei sebanyak 10.000 responden yang berasal dari 514 kabupaten/kota dan 34 provinsi Indonesia. Responden merupakan WNI dengan kriteria umur antara 13 sampai 70 tahun dan sudah mengakses internet selama 3 bulan terakhir sebelum Bulan Oktober 2021. Hasil surveinya menyatakan bahwa 53,6% responden mempunyai tingkat perlindungan privasi yang rendah. Sedangkan responden yang mempunyai tingkat privasi yang tinggi sekitar 46,4%. Berikutnya ada jurnal dari Revilia & Irwansyah pada tahun 2020 berfokus pada kalangan milenial berusia antara 26 hingga 33 tahun, mencakup individu yang berkarier di sektor publik maupun swasta. Sebagian besar partisipan diketahui telah memiliki pengalaman menggunakan media sosial selama lebih dari satu dekade. Dalam hal pemahaman terhadap konsep keamanan digital, sebagian besar responden menunjukkan tingkat pengenalan yang tinggi terhadap sejumlah istilah penting. Sebanyak 90% memahami istilah *spam* dan *hacker*, disusul 81,8% yang mengenali konsep *identity theft*, virus, serta *malware*. Sementara itu, 63,6% responden familiar dengan istilah *spyware* dan penipuan daring, sedangkan hanya 54,5% yang mengetahui istilah *phishing* dan *worm*. Sebagian besar responden pernah mengalami berbagai bentuk kerentanan digital. Ancaman *spamming* dialami oleh 63,6% peserta, diikuti oleh gangguan pemeliharaan sistem yang berdampak pada 54,5% responden. Sebanyak 36,4% melaporkan masalah keamanan situs *web* dan akses tidak sah terhadap akun pribadi, sementara 27,3% menghadapi serangan *malware*. Kasus pencurian identitas tercatat pada 18,2% responden, dan hanya 9,1% yang menyatakan tidak pernah mengalami bentuk ancaman siber apa pun. Dapat diasumsikan bahwa lamanya pengguna berinternet selama bertahun-tahun, tidak menjamin pengguna aman dari ancaman yang mengganggu keamanan maupun privasi mereka.

Beragam metode digunakan oleh sejumlah peretas untuk memperoleh informasi terkait *username* dan kata sandi dari suatu akun. Jenis akun yang menjadi sasaran dapat mencakup akun media sosial, surat elektronik, permainan daring, maupun bentuk akun digital lainnya. Cara yang digunakan oleh peretas untuk mengetahui informasi *password* akun yang akan digali disebut dengan *password sniffing*. *Password sniffing* adalah suatu teknik mengendus kata sandi (*password*) menggunakan bantuan piranti lunak untuk menggali informasi hingga

mengambil detail informasi dari *remote login* seperti *username* dan *password* (Suhendra et al., 2008). Berbagai informasi yang diakses dan dikelola pengguna saat berinternet juga rentan terhadap beberapa tindakan pencurian data melalui berbagai serangan. Selain *sniffing* ada juga yang menggunakan teknik serangan lain, misalnya *phishing*. Serangan *phishing* sering sekali digunakan untuk memalsukan sebuah sistem tertentu serta mempunyai tampilan yang hampir mirip atau menyerupai sistem informasi asli. Tujuan pelaku kejahatan internet membuat *phishing* adalah mencari kesalahan pengguna entah itu lalai maupun tidak teliti dengan apa yang diakses. Informasi yang diterima dari pengguna tersebut dimanfaatkan untuk keuntungan pribadi si pelaku kejahatan internet. Melalui penerapan teknik rekayasa sosial, pelaku kejahatan siber dapat memanipulasi korban agar bersedia memberikan berbagai informasi pribadi, sehingga data tersebut akhirnya jatuh ke tangan pelaku. (Fitriyansyah & Hazri, 2020). Dilansir PrivyId yang mengutip data milik Polri (Kepolisian Republik Indonesia) pada Bulan Januari-September 2020 sebanyak 2259 laporan terkait kasus kejahatan berinternet, di mana pencurian data/identitas hanya sebanyak 39 kasus dan masih tergolong sedikit jika dibandingkan dengan konten provokasi (1.048 kasus), penipuan online (649 kasus), pornografi (208 kasus), Akses ilegal (138 kasus), dan manipulasi data (71 kasus). Adapun laporan dari perusahaan keamanan digital *SurfShark*, yang mencatat Indonesia berada di peringkat ke 3 (di bawah Rusia dan Perancis) dengan jumlah kebocoran data terbanyak. Ada 12,74 juta data akun yang bocor di Indonesia selama kuartal III tahun 2022. Menurut laporan UpGuard, terkait 6 penyebab umum kebocoran data di tahun 2021 disebabkan oleh kesalahan pengaturan piranti lunak, kesalahan pengguna (*social engineering*), kata sandi berulang, pencurian data sensitif, kerentanan piranti lunak, dan penggunaan sandi bawaan.

Terkait sandi, pengguna bisa menggunakan kombinasi dari huruf, angka, dan karakter yang sudah pasti bisa diingat dengan mudah. Pengguna juga manusia yang terkadang bisa melakukan kesalahan sewaktu-waktu, baik secara sadar maupun tidak sadar, seperti menggunakan kombinasi *password* yang umum diketahui orang-orang banyak. Hal ini berpotensi menyebabkan *password* mudah dipecahkan menggunakan alat (*tools*) pemecah *password* oleh pihak yang tidak

berwenang ketika berhasil menyerang *server* melalui celah injeksi dengan memanfaatkan kelemahan di *database* (Fitriyansyah & Hazri, 2020; Mardiansyah et al., 2021). Dengan mempertimbangkan potensi ancaman terhadap keamanan sistem, autentikasi berbasis *login* statis seperti penggunaan nama pengguna (*username*) dan kata sandi (*password*) yang jarang diperbarui memerlukan perlindungan tambahan guna memastikan bahwa hanya individu yang berwenang yang dapat mengakses akun tersebut. Salah satu pendekatan yang disarankan untuk meningkatkan keamanan proses *login* adalah dengan penerapan *One Time Password* (OTP) sebagai lapisan autentikasi tambahan. Dilansir InvestorId pada tahun 2022 yang mengutip data penelitian perusahaan Kaspersky. Disebutkan sebanyak 67% pengguna aplikasi perbankan berbasis digital di Indonesia lebih memilih untuk menerapkan OTP sebagai keamanan 2 faktornya. Di luar Indonesia, implementasi OTP juga menjadi fokus penting dalam kebijakan keamanan digital di berbagai negara Asia Tenggara. Tingkat penerapan tercatat mencapai 66% di Malaysia, 75% di Filipina, 63% di Thailand, 74% di Vietnam, serta 65% di Singapura. Berdasarkan studi berjudul *Mapping a Secure Path for the Future of Digital Payments in APAC* yang dilakukan oleh Kaspersky, mayoritas partisipan mengakui pentingnya penerapan autentikasi dua faktor (2FA), dengan tingkat dukungan sebesar 57%. Selain itu, fitur keamanan berbasis biometrik, seperti sidik jari dan pengenalan wajah, juga mendapat perhatian tinggi, dengan persentase sebesar 56%. Sekitar 40% responden juga mengharapkan agar Kaspersky secara otomatis dapat mendeteksi dan mencegah aksi penipuan daring dengan mengandalkan analisis terhadap *log* transfer pengguna. Sementara itu, lebih dari 28% responden menilai bahwa penerapan tokenisasi yang dibentuk melalui proses algoritmik mampu memperkuat perlindungan data sensitif serta meningkatkan tingkat keamanan aplikasi perbankan dan transaksi elektronik. Melalui penelitian Kaspersky, mereka menemukan 58% responden bergegas menggunakan dompet elektronik yang sudah tercantum fitur biometrik, dan keamanan dua lapis (2FA) salah satunya adalah OTP.

OTP merupakan metode autentikasi yang menggunakan kunci kriptografi sementara dan akan kedaluwarsa dalam jangka waktu tertentu (Yahya & Amini,

2018). OTP mengirimkan pesan autentikasi melalui berbagai saluran komunikasi secara simultan, dengan tujuan meningkatkan kerahasiaan dan menjaga identitas pengguna tetap aman. Pengamanan autentikasi OTP pada umumnya memanfaatkan algoritma acak. Hal ini dilakukan agar autentikasi OTP tidak dapat diprediksi dikemudian hari. Tanggapan permintaan autentikasi dapat dikirim melalui saluran yang terhubung ke pengguna secara langsung, misalnya melalui aplikasi pesan instan yang mampu menyampaikan pesan untuk mempermudah kode autentikasi agar sampai ke pemilik (pengguna) sebenarnya. Setelah autentikasi sampai ke pengguna sesungguhnya, pengguna bisa menyelesaikan proses autentikasi dengan menanggapi pesan atau memasukkan kode yang diterima dari aplikasi pesan instan lalu meneruskannya ke *Web*. Adapun aplikasi pesan instan yang bisa dimanfaatkan dalam penerimaan kode OTP seperti: SMS, *Email*, Whatsapp, Telegram, dan lain-lain (Santoso, 2013). Ketidakmampuan *single factor authentication* (SFA) dalam menjaga keamanan akun pengguna, dapat memicu timbulnya kebutuhan autentikasi lebih dari satu faktor (2FA) (Fitriyansyah & Hazri, 2020; Mardiansyah et al., 2021). *Two Factor Authentication* (2FA) merupakan mekanisme verifikasi berlapis yang mengharuskan pengguna untuk melewati dua tahapan identifikasi, guna meningkatkan tingkat keamanan terhadap identitas digital mereka. (Fitriyansyah & Hazri, 2020) dan *Single Factor Authentication* (SFA) merupakan mekanisme autentikasi yang memverifikasi identitas pengguna melalui pencocokan data antara kombinasi nama pengguna dan kata sandi dengan informasi yang tersimpan di dalam basis data. Proses ini bertujuan untuk menentukan apakah pengguna tersebut memiliki hak akses terhadap sistem yang dimaksud. (Mardiansyah et al., 2021).

Universitas Pendidikan Ganesha (Undiksha) merupakan institusi pendidikan tinggi yang berlokasi di Jalan Udayana No. 11, Singaraja, Kabupaten Buleleng, Bali. Untuk mendukung kelancaran aktivitas kampus secara daring, Undiksha menerapkan Sistem Informasi Akademik (SIAK), yaitu perangkat lunak yang dirancang untuk menyajikan data serta mengatur alur administrasi yang berkaitan dengan kegiatan akademik. Penggunaan sistem ini diharapkan mampu membantu pengelolaan administrasi secara terstruktur dan memungkinkan akses informasi

secara *real-time*. (Santoso et al., 2013). Sistem informasi milik Undiksha tersebut memiliki ekosistem berbasis *web app* dan *mobile app*. Pada penelitian ini, ruang lingkup peneliti hanya berfokus pada ekosistem *web app* (aplikasi *website*) saja. Selama ini akses masuk ke SIAK Undiksha sudah menggunakan teknologi SSO, namun untuk pengamanannya masih menggunakan metode *Single Factor Authentication* (1FA), dan akan bisa masuk hanya dengan mencocokkan identitas *email* dan *password* sesuai dengan yang terdaftar pada *database*. Dari wawancara yang dilakukan peneliti kepada pihak UPT TIK Undiksha. Peneliti mendapatkan laporan dari narasumber yang menyatakan bahwa sistem kepegawaian memiliki isu pengguna, di mana pengguna yang tidak berwenang memaksa masuk ke sistem bertujuan untuk mengubah data, mengunggah berkas yang tidak sesuai (mencurigakan), dan menyerang akses masuk (*login*). Sebanyak kurang dari 10 kasus sudah terindikasi, dan berpotensi melebar ke sistem lainnya apabila dibiarkan, karena pada dasarnya sistem milik Undiksha sudah terhubung dan terintegrasi melalui SSO.

Sebagai langkah untuk mengamankan portal masuk *website* Undiksha, maka diperlukan sebuah metode pengaman tambahan 2 faktor (2FA), salah satu yang populer adalah OTP. Sistem OTP ini dioperasikan menggunakan algoritma *Secure Hash Algorithm* 512 (SHA-512), yang termasuk dalam kelompok algoritma *hash* SHA-2. SHA-2 dikembangkan sebagai penyempurnaan terhadap kelemahan matematis yang ditemukan pada pendahulunya, yakni SHA-1 (Yahya & Amini, 2018). Media yang akan digunakan sebagai penerima kode OTP dalam penelitian kali ini adalah *bot* dari aplikasi pesan instan Telegram. Aplikasi pesan instan Telegram mempunyai grup pengembang yang responsif dan aktif. Kita dapat menemukan grup tersebut di pelbagai tempat seperti forum diskusi, grup Telegram, saluran khusus, dan layanan pengembang lainnya. Pada grup / saluran tersebut, pengembang bisa bertanya, berbagi ilmu, berbagi pengalaman, dan membantu anggota satu sama lain. Dalam hal ini, berlaku juga untuk pengembangan *bot*. Telegram juga menyediakan akses resmi untuk pengembang termasuk contoh kode, API yang kuat, dan dokumentasi yang komprehensif. Perkembangan komunitas Telegram dapat dilihat langsung melalui portal moderasi yang aksesnya sudah transparan, platform tersebut bisa menjadi opsi

yang inovatif karena telah mendorong banyak pengembang untuk berkontribusi di dalam ekosistemnya termasuk membangun *bot* yang menarik dan bermanfaat. Terlebih aplikasi pesan instan Telegram memiliki jumlah pengguna yang semakin bertambah, dan *platform*-nya mampu berjalan pada perangkat yang berbeda (*multiplatform*). Dilansir dari media DataIndonesia yang mengutip sumber dari *blog* Telegram dan "*We are Social*" pada tahun 2022. Jumlah pengguna aktif bulanan aplikasi pesan instan Telegram *region* global sudah mencapai 700 juta pengguna pada perhitungan Juni tahun 2022. Jumlah tersebut sudah mengalami peningkatan sebanyak 40% dibandingkan perhitungan tahun sebelumnya (2021) yang berjumlah sekitar 500 juta pengguna. Ditinjau berdasarkan demografinya dari mayoritas pengguna, sekitar 12% pengguna pesan instan Telegram masih berumur 16 tahun keatas. Berdasarkan laporan *We Are Social* edisi Juli 2022, sekitar 42,3% pengguna Telegram merupakan perempuan, sebagaimana ditentukan melalui analisis demografis platform tersebut.

Penelitian sejenis yang mendukung penelitian ini antara lain penelitian yang dilakukan oleh Kusumaningsih, D (2021), dengan hasil penelitian menunjukkan bahwa penerapan OTP mampu memberikan perlindungan terhadap akun Admin dari upaya manipulasi atau kecurangan yang berkaitan dengan sistem penghargaan karyawan (*reward*) di lingkungan PT. Telekomunikasi Indonesia Divisi Enterprise Service Jakarta Pusat. Penelitian lain juga dilakukan oleh Yahya, N. I., & Amini, S. (2018), dengan hasil penelitian bahwa analisa, perancangan, serta implementasi yang dilakukan terbukti mampu meningkatkan keamanan hak akses pengguna (*user*) dalam mengatasi permasalahan *login* di SMK Cyber Media. Dalam penelitian ini masih terdapat kekurangan secara teknis, sehingga perlu peningkatan lagi pada pengembangan berikutnya. Selain itu, penelitian sejenis dilakukan oleh Setiawan & Purwanto (2018), dengan hasil penelitian bahwa kode OTP ampuh dalam meningkatkan keamanan akses pemilik akun dalam mengatasi permasalahan pada Badan Kepegawaian dan Pengembangan SDM Kita Tangerang, Banten. Dalam penelitian ini masih terdapat kekurangan pada layanan SMS dikarenakan sangat tidak efektif dan boros.

Merujuk pada pemaparan permasalahan yang telah diuraikan, peneliti terdorong untuk merancang dan mengembangkan solusi teknologi keamanan

sistem dengan fokus pada penerapan metode OTP (*One-Time Password*) dalam portal *login Single Sign-On* (SSO), menggunakan algoritma SHA-512 sebagai pendekatan kriptografi. Studi ini diimplementasikan pada Universitas Pendidikan Ganesha sebagai lokasi penelitian. Hasil survei awal terkait implementasi OTP pada SSO milik Undiksha (**Lampiran 01**.) menunjukkan 44% memilih sangat setuju, 35% memilih setuju, 18% memilih netral, 2,5% memilih tidak setuju, dan sisanya 0,5% memilih sangat tidak setuju. Data responden tersebut diambil peneliti dengan jumlah sampel sebanyak 20 orang.

1.2 Identifikasi Masalah

1. Kurangnya lapisan keamanan tambahan: Dalam beberapa kasus, penggunaan autentikasi tingkat pertama (1FA/SFA) mungkin belum cukup untuk melindungi akses data yang bersifat sensitif seiring berkembangnya zaman. Untuk mencari tahu permasalahan ini, tentunya membutuhkan solusi dengan menerapkan autentikasi multifaktor (MFA/2FA) didukung *hash* yang kuat sebagai alternatif dalam melindungi keamanan akun dari pihak yang tidak berwenang.
2. Adanya isu keamanan pada sistem informasi: Pengguna yang tidak berwenang ingin melakukan pengubahan data, mengunggah berkas yang mencurigakan, dan menyerang akses masuk (*login*).

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, penulis merumuskan permasalahan utama dalam penelitian ini sebagai berikut:

1. Bagaimana rancangan dan implementasi *One Time Password* pada portal *login* SSO (ekosistem *website*) Universitas Pendidikan Ganesha dengan menggunakan algoritma *hash* SHA-512?
2. Bagaimana respon pengguna terhadap kemudahan yang diberikan setelah OTP pada portal *login* SSO (berbasis *website*) diimplementasikan?

1.4 Tujuan Penelitian

Merujuk pada rumusan masalah yang telah disampaikan sebelumnya, penelitian ini bertujuan untuk mencapai sejumlah capaian utama sebagai berikut:

1. Mengetahui proses dari perancangan dan implementasi OTP pada portal *login* SSO Undiksha menggunakan algoritma *hash* SHA-512 dengan baik.
2. Mengukur tingkat kemudahan yang dirasakan pengguna saat penerapan tambahan OTP sebagai opsi untuk mengamankan akses masuk (*login*) pada portal SSO Undiksha.

1.5 Batasan Masalah Penelitian

1. Sampel terbatas: Penelitian ini hanya menangkap beberapa mahasiswa sebagai sampel, sehingga hasil yang diperoleh tidak mencerminkan pengalaman pegawai, dosen, atau staf akademik yang juga menggunakan sistem SSO Undiksha. Meskipun mereka ikut terlibat dalam ekosistem universitas, penelitian difokuskan pada mahasiswa, karena mereka merupakan salah satu *role* dengan pengguna terbanyak (mayoritas) jika dibandingkan dengan *role* lainnya seperti: dosen, staf akademik, atau pegawai. Jika suatu sistem autentikasi tidak efisien bagi mahasiswa, maka akan berdampak pada kelancaran akses akademik, mulai dari login ke portal universitas hingga akses materi perkuliahan.
2. Data pendukung yang terbatas: Data terkait hasil survei / penelitian dari tahun sebelumnya sampai yang terbaru, dengan tujuan untuk menguatkan urgensi penelitian, berpotensi masih belum cukup.
3. OTP sangat bergantung pada perangkat seperti smartphone dan token yang bisa rusak, dicuri, atau hilang. Selain itu, kesalahan pengguna saat memasukkan OTP bisa mengurangi keefektifannya.
4. Penggunaan OTP bisa dipengaruhi oleh kebiasaan dan preferensi setiap pengguna, faktor ini mungkin tidak sepenuhnya dikontrol dalam penelitian. Sehingga hasilnya dipengaruhi oleh variasi pengguna dalam menggunakan OTP.
5. Tidak ada sistem yang sempurna. Meskipun OTP dianggap metode keamanan yang kuat, peneliti mungkin menemukan kekurangan saat mengimplementasikan.
6. Sistem *login* OTP menggunakan Telegram tidak langsung diintegrasikan pada sistem yang telah lama berjalan, karena berpotensi mengganggu kinerja sistem tersebut, serta sistem tersebut memiliki basis pengguna yang tidak

sedikit. Jadi *login* OTP pada SSO masih terbatas pada fitur prototipe. Untuk pengujian fitur tersebut, dilakukan secara terpisah.

1.6 Manfaat Hasil Penelitian

Penelitian ini diharapkan memberikan sejumlah manfaat, baik secara teoritis maupun praktis, antara lain:

1. Dari sisi teoritis, hasil penelitian ini diharapkan dapat berkontribusi sebagai sumber rujukan alternatif dalam rancangan dan implementasi keamanan *One Time Password* berbasis 2FA sebagai solusi pengamanan portal *login* SSO untuk mengakses Sistem Informasi Akademik dan Kepegawaian.
2. Dari sisi praktis peneliti, hasilnya diharapkan dapat memperluas pemahaman dan wawasan dalam bidang keamanan sistem, khususnya terkait implementasi OTP berbasis algoritma SHA-512 dan pemanfaatan Telegram *bot* dalam autentikasi pengguna. Dari sisi praktis Undiksha, hasilnya diharapkan dapat membantu meningkatkan keamanan pengguna di lingkungan Universitas Pendidikan Ganesha, baik dalam mengoperasikan sistem informasi maupun menggunakannya untuk keperluan administrasi.


UNIVERSITAS PENDIDIKAN GANESHA
UNDIKSHA