BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Single Sign-On (SSO) merupakan sebuah mekanisme autentikasi yang memungkinkan pengguna mengakses berbagai layanan digital dengan hanya sekali login. Di lingkungan kampus, SSO kerap diterapkan untuk mempermudah mahasiswa dalam mengakses layanan seperti sistem pembelajaran, perpustakaan digital, dan portal akademik. Dari kemudahan ini juga menyebabkan tantangan terkait kesadaran keamanan. Mengingat data dan informasi pribadi mahasiswa yang tersimpan di dalamnya sangat rentan terhadap ancaman siber.

Mahasiswa sebagai pengguna utama teknologi SSO di universitas sering kali kurang memahami risiko keamanan yang melekat pada sistem ini. Kurangnya pengetahuan tentang ancaman potensial seperti *phishing* dan kelemahan kata sandi yang umum, dapat membuat mahasiswa lebih rentan terhadap serangan siber. Penelitian menunjukkan bahwa kesadaran keamanan yang rendah, ditambah dengan kebiasaan buruk seperti menggunakan kata sandi yang sama di berbagai platform atau tidak melakukan *log out* setelah selesai menggunakan layanan, meningkatkan risiko kebocoran data.

Oleh karena itu, meningkatkan kesadaran keamanan siber pada mahasiswa sangat penting untuk melindungi integritas dan privasi data dalam sistem SSO universitas. Langkah-langkah edukatif seperti seminar keamanan siber, pelatihan mengenai praktik autentikasi yang aman, serta pengenalan terhadap potensi ancaman siber dapat menjadi upaya preventif yang efektif. Dengan demikian, diharapkan mahasiswa tidak hanya memahami pentingnya menjaga keamanan data pribadi mereka, tetapi juga mampu mengambil langkah-langkah untuk melindungi diri mereka dari ancaman siber. Kesadaran ini juga akan berkontribusi pada keamanan keseluruhan infrastruktur digital universitas yang dapat menciptakan lingkungan belajar yang lebih aman dan terpercaya.

1.2 Latar Belakang Penelitian

Teknologi informasi telah memberikan dampak signifikan di berbagai sektor, termasuk pendidikan, seiring dengan pesatnya perkembangan

penggunaannya di berbagai bidang (Melgis et al., 2024). Kesadaran keamanan informasi atau *Information Security Awareness* (ISA) adalah kumpulan keterampilan yang memungkinkan pengguna untuk mengurangi risiko serangan rekayasa sosial dengan efektif (Solomon et al., 2022). Dalam konteks penggunaan sistem digital, persepsi keamanan terbukti memiliki pengaruh penting terhadap kepercayaan pengguna terhadap platform. Siagian et al. (2022) menjelaskan bahwa semakin tinggi tingkat *perceived security*, maka semakin besar pula kepercayaan (*trust*) pengguna dalam menggunakan suatu layanan digital. Kepercayaan ini kemudian mendorong terbentuknya niat perilaku (*behavioral intention*) dalam menggunakan sistem secara konsisten dan aman. Meskipun penelitian mereka berfokus pada platform pembayaran digital, konsep ini sangat relevan dengan sistem autentikasi kampus seperti *Single Sign-On* (SSO), di mana persepsi keamanan dan kemudahan penggunaan turut membentuk sikap mahasiswa terhadap keamanan informasi pribadi mereka.

Penguatan persepsi keamanan dan pemahaman teknis perlu menjadi bagian penting dalam edukasi keamanan siber di lingkungan perguruan tinggi. Dalam serangan siber, penyerang memanfaatkan perilaku manusia, bukan celah pada sistem. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN, 2024), insiden kebocoran kredensial akun mahasiswa meningkat sebesar 25% dalam satu tahun terakhir. Hasil survei awal terhadap 50 mahasiswa menunjukkan bahwa 60% responden belum memahami risiko penggunaan kata sandi yang sama di berbagai layanan, termasuk SSO. Mengukur kesadaran keamanan informasi pengguna serta mengidentifikasi siapa saja yang rentan terhadap serangan ini menjadi hal yang penting dalam menilai risiko keamanan siber. Meskipun teknologi keamanan semakin canggih, kelemahan utama sering kali terletak pada faktor manusia, yang seringkali menjadi pintu masuk bagi serangan siber. Di sisi lain, meningkatnya kebutuhan untuk menjaga kesadaran keamanan informasi menjadi semakin mendesak, terutama di tengah bertambahnya jumlah layanan berbasis internet yang mengharuskan pengguna mengelola banyak akun. Kondisi ini menciptakan tantangan besar bagi pengguna, karena pengguna harus mengelola semakin banyak pasangan nama pengguna dan kata sandi. Sementara itu, semakin banyaknya layanan ini justru menambah risiko keamanan yang lebih tinggi. Pengguna sering kali merasa kesulitan untuk menjaga keamanan setiap akun dengan tingkat proteksi yang memadai yang pada akhirnya menjadi lebih memperburuk situasi di mana

pengguna yang kurang terlatih dalam kesadaran keamanan informasi lebih mudah menjadi sasaran serangan siber.

Kondisi ini semakin terasa urgensinya ketika melihat contoh kasus nyata seperti kebocoran data yang terjadi pada Januari 2021. Ketika lebih dari 125 ribu data mahasiswa Universitas Diponegoro (Undip) di Jawa Tengah dilaporkan bocor dan ditawarkan secara gratis di forum jual beli data alam sistem, terutama di institusi pendidikan tinggi yang memiliki banyak pengguna dengan akses data sensitif (Aditya Putra Perdana, 2021). Kasus kebocoran data ini menggambarkan secara jelas perlunya peningkatan sistem keamanan informasi dan kesadaran akan risiko yang lebih besar, terutama dalam menghadapi serangan yang memanfaatkan kelalaian manusia dan kelemahan dalam pengelolaan akun dan kata sandi.

Di era digital saat ini, sistem autentikasi berbasis *Single Sign-On* (SSO) telah menjadi komponen vital dalam manajemen akses di lingkungan pendidikan tinggi. *Single Sign-On* (SSO) telah muncul sebagai solusi untuk mengatasi tantangan autentikasi, memberikan pengguna kemampuan untuk masuk ke dalam jaringan sekali saja dan dapat mengakses berbagai aplikasi tanpa perlu melakukan autentikasi ulang di dalam jaringan (James et al., 2020). Implementasi SSO di universitas membantu mengintegrasikan berbagai layanan akademik seperti sistem pembelajaran daring, perpustakaan digital, dan portal akademik dalam satu platform terintegrasi. Pada akhirnya, seberapa kuat kata sandi yang digunakan dalam SSO, autentikasi ini tetap berbasis satu faktor yang hanya mengandalkan apa yang pengguna ketahui. Hal ini menimbulkan tantangan keamanan, karena satu kata sandi yang kuat sekalipun rentan jika hanya mengandalkan satu bentuk autentikasi (Pratama et al., 2022).

Diharapkan temuan dalam penelitian ini dapat menjadi landasan untuk pengembangan kebijakan edukatif mengenai keamanan informasi di kalangan mahasiswa, khususnya dalam penggunaan akun *Single Sign-On* (SSO). Dengan meningkatnya kesadaran ini, diharapkan mahasiswa lebih memahami pentingnya perlindungan data pribadi dan menjadi lebih waspada dalam aktivitas digital mereka. Penelitian ini juga diharapkan dapat memberikan wawasan lebih dalam mengenai hubungan antara kekhawatiran privasi, tingkat familiaritas terhadap SSO, dan faktor demografi dengan kesadaran keamanan informasi. Pada kenyataannya, kesadaran ini sangat penting di era digital yang rentan terhadap berbagai ancaman

siber. Berdasarkan latar belakang tersebut, penulis melakukan penelitian dengan judul "Hubungan antara *Privacy Concern*, Familiaritas SSO, Demografi, *Big Five Personality* dan Literasi Digital terhadap Kesadaran Keamanan Informasi pada Penggunaan Akun SSO di Kalangan Mahasiswa".

1.3 Perumusan Masalah

Sehingga, berdasarkan latar belakang yang telah di paparkan, Rumusan masalah yang didapat yaitu sebagai berikut:

1. Bagaimana *Gender* (jenis kelamin) memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
2. Bagaimana *Age* (umur) memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
3. Bagaimana *Academic Role* (peran akademik) memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
4. Bagaimana Familiaritas *Single Sign On* (SSO) memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
5. Bagaimana *Privacy Concern* memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
6. Bagaimana *Extraversion* memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
7. Bagaimana *Agreebelness* memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
8. Bagaimana *Conscientiousness* memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
9. Bagaimana *Emotional Stability* memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?
10. Bagaimana *Openess* memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?

11. Bagaimana Literasi Digital memengaruhi kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO)?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, penelitian ini bertujuan untuk:

1. Untuk mengetahui dan menganalisis pengaruh *Gender* (jenis kelamin) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
2. Untuk mengetahui dan menganalisis pengaruh *Age* (umur) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
3. Untuk mengetahui dan menganalisis pengaruh *Academic Role* (peran akademik) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
4. Untuk mengetahui dan menganalisis pengaruh *Familiaritas Single Sign-On* (SSO) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
5. Untuk mengetahui dan menganalisis pengaruh *Privacy Concern* (kekhawatiran) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
6. Untuk mengetahui dan menganalisis pengaruh *Extraversion* (kepribadian ekstrovert) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On (SSO)*.
7. Untuk mengetahui dan menganalisis pengaruh *Agrebelness* (keramahan) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
8. Untuk mengetahui dan menganalisis pengaruh *Conscientiousness* (kedisiplinan) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).

9. Untuk mengetahui dan menganalisis pengaruh *Emotional Stability* (ketenangan emosi) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
10. Untuk mengetahui dan menganalisis pengaruh *Openess* (sifat terbuka) terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).
11. Untuk mengetahui dan menganalisis pengaruh Literasi Digital terhadap kesadaran mahasiswa terhadap keamanan penggunaan sistem *Single Sign-On* (SSO).

1.5 Manfaat Penelitian

1.5.1 Manfaat Teoritis

Penelitian ini memberikan kontribusi dalam memperkaya kajian teoritis terkait kesadaran keamanan informasi, khususnya dalam konteks penggunaan sistem *Single Sign-On* (SSO) di lingkungan pendidikan tinggi. Dengan memanfaatkan berbagai variabel seperti kekhawatiran privasi, familiaritas dengan SSO, demografi, kepribadian *Big Five*, dan literasi digital, penelitian ini memperkuat pemahaman mengenai faktor-faktor yang memengaruhi kesadaran keamanan siber. Penelitian ini memberikan kontribusi dengan menguji peran gender sebagai variabel kontrol, sehingga dapat memberikan gambaran lebih akurat mengenai hubungan variabel independen dengan kesadaran keamanan akun SSO. Hasilnya diharapkan dapat menjadi dasar bagi pengembangan teori dan model yang lebih komprehensif terkait keamanan informasi di era digital.

1.5.2 Manfaat Praktis

Penelitian ini memberikan panduan bagi institusi pendidikan tinggi dalam merancang strategi untuk meningkatkan kesadaran keamanan informasi di kalangan mahasiswa. Dengan memahami hubungan antara variabel-variabel yang diteliti, institusi dapat mengembangkan kebijakan dan program edukasi, seperti pelatihan keamanan siber yang disesuaikan dengan tingkat literasi digital dan demografi.

mengidentifikasi dan memitigasi risiko keamanan berdasarkan pola perilaku pengguna, sehingga menciptakan ekosistem digital yang lebih aman dan anda

1.6 Sistematika Penulisan Tugas Akhir

Sistematika penulisan tugas akhir ini terdiri dari lima bab yang setiap bagiannya memiliki peran tersendiri, sebagai berikut:

a. BAB I PENDAHULUAN

Bab ini memberikan gambaran umum secara singkat dan jelas mengenai isi penelitian. Bagian ini mencakup deskripsi tentang Gambaran Umum Objek Penelitian, Latar Belakang Penelitian, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, serta Sistematika Penulisan Tugas Akhir.

b. BAB II TINJAUAN PUSTAKA

Bab ini berisi berbagai teori yang relevan, mulai dari konsep umum hingga khusus, serta mencakup hasil penelitian sebelumnya. Selain itu, bab ini juga memuat kerangka pemikiran penelitian yang dapat dilengkapi dengan hipotesis, apabila diperlukan.

c. BAB III METODE PENELITIAN

Bab ini menjelaskan pendekatan, metode, dan teknik yang digunakan untuk pengumpulan dan analisis data dalam menjawab pertanyaan penelitian. Isi bab ini meliputi jenis penelitian, operasionalisasi variabel, populasi dan sampel (jika menggunakan pendekatan kuantitatif), metode pengumpulan data, uji validitas dan reliabilitas, serta teknik analisis data yang diterapkan.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian serta pembahasannya secara sistematis sesuai dengan rumusan masalah dan tujuan penelitian. Bagian awal memaparkan hasil penelitian, sementara bagian selanjutnya membahas dan menganalisis hasil tersebut. Pembahasan dimulai dengan analisis data, dilanjutkan dengan interpretasi, dan diakhiri dengan kesimpulan. Selain itu, pembahasan sebaiknya mencakup perbandingan dengan penelitian terdahulu atau teori yang mendukung.

e. BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang merangkum jawaban atas pertanyaan penelitian, diikuti oleh saran yang relevan berdasarkan temuan penelitian. Saran yang disampaikan sebaiknya langsung terkait dengan hasil penelitian dan manfaat yang dihasilkan.