

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai sektor, termasuk sektor perbankan, salah satunya melalui layanan *mobile banking* yang memungkinkan nasabah melakukan transaksi secara cepat dan efisien melalui perangkat digital. Kemudahan, kecepatan, dan fleksibilitas yang ditawarkan oleh layanan *mobile banking* menjadi salah satu faktor yang mendorong meningkatnya penggunaan layanan tersebut oleh masyarakat dalam melakukan transaksi keuangan secara digital [1]. Salah satu bank yang menyediakan layanan *mobile banking* di Indonesia adalah Bank Central Asia (BCA). Berdasarkan laporan kuartal pertama tahun 2025, jumlah pengguna aktif *mobile banking* BCA mencapai sekitar 33,4 juta pengguna [2]. Hal ini menunjukkan bahwa layanan *mobile banking* BCA telah menjadi bagian penting dalam aktivitas transaksi keuangan masyarakat.

Namun, di balik kemudahan tersebut, penggunaan layanan *mobile banking* juga diiringi dengan meningkatnya risiko keamanan informasi. Berbagai bentuk kejahatan siber seperti *phishing*, *social engineering*, *malware*, dan pencurian data pribadi semakin sering terjadi dan menargetkan pengguna layanan perbankan. Berdasarkan laporan Indonesia Anti-Scam Center (IASC) yang dikoordinasikan oleh Otoritas Jasa Keuangan (OJK), hingga tahun 2025 tercatat 373.129 laporan penipuan digital dengan total kerugian mencapai Rp 8,2 triliun [3]. Salah satu kasus yang terjadi pada nasabah BCA melalui modus SMS *phishing* menggunakan teknologi *Fake BTS*, sehingga pelaku dapat mengirim SMS seolah-olah berasal dari bank dan mengarahkan korban ke tautan palsu untuk mencuri data perbankan, seperti *user ID*, *password*, PIN, maupun kode OTP yang dapat digunakan untuk mengakses layanan *mobile banking* secara tidak sah [4]. Selain itu, kasus hilangnya saldo nasabah akibat dugaan *phishing* juga terjadi pada nasabah Bank Sumut di Sumatera Utara. Berdasarkan hasil investigasi internal, pihak bank menyatakan tidak ditemukan pelanggaran sistem keamanan, namun terdapat indikasi bahwa nasabah menjadi korban *phishing* atau penipuan digital [5]. Kondisi tersebut menunjukkan bahwa ancaman keamanan pada layanan *mobile banking* tidak hanya berasal dari aspek teknologi, tetapi juga berkaitan dengan tingkat kewaspadaan dan kesadaran pengguna dalam menjaga keamanan informasi pribadi dan aktivitas transaksi digital.

Selain terjadi secara nasional, ancaman kejahatan *mobile banking* juga telah menjadi perhatian dalam konteks daerah. Penelitian berjudul "Analisis Pidana terhadap Penipuan dan Penggelapan Dana melalui *M-Banking* di Kota Medan" menunjukkan bahwa tindak penipuan dan penggelapan dana melalui layanan *mobile banking* juga ditemukan dalam konteks Kota Medan. Meskipun data spesifik jumlah korban pengguna *mobile banking* BCA di Kota Medan belum dipublikasikan secara resmi, keberadaan penelitian tersebut menunjukkan bahwa ancaman keamanan *mobile banking* relevan dengan kondisi masyarakat di Kota Medan. Kondisi ini memperlihatkan bahwa faktor manusia menjadi salah satu penyebab utama terjadinya insiden keamanan informasi akibat kurangnya kesadaran pengguna dalam menjaga data dan aktivitas transaksi digital [6]. Berdasarkan kondisi tersebut, penelitian ini secara khusus memilih pengguna *mobile banking* BCA di Kota Medan sebagai objek penelitian. Pemilihan *mobile banking* BCA dilakukan untuk memberikan konteks layanan yang spesifik dalam pengukuran kesadaran keamanan informasi, sehingga responden memiliki konteks penggunaan *mobile banking* yang sama dalam memberikan penilaian. Pembatasan pada Kota Medan tidak dimaksudkan untuk menunjukkan bahwa ancaman keamanan *mobile banking* hanya terjadi di wilayah tersebut, tetapi untuk memfokuskan analisis kesadaran keamanan informasi pada pengguna *mobile banking* BCA dalam populasi yang ditetapkan dalam penelitian.

Dalam konteks keamanan informasi, faktor manusia sering dianggap sebagai salah satu elemen yang paling menentukan dalam keberhasilan penerapan keamanan sistem informasi, karena banyak insiden keamanan terjadi akibat kesalahan atau kelalaian pengguna dalam menjaga keamanan informasi. Oleh karena itu, penting untuk mengukur tingkat *Information Security Awareness* (ISA) pengguna *mobile banking* guna mengetahui sejauh mana pengguna memahami, menyikapi dan menerapkan praktik keamanan informasi dalam aktivitas transaksi digital. Penelitian ini menggunakan instrumen *Human Aspects of Information Security Questionnaire* (HAIS-Q) untuk mengukur tingkat kesadaran keamanan informasi pengguna berdasarkan dimensi *Knowledge*, *Attitude*, dan *Behavior* (KAB) pada sembilan fokus area keamanan informasi. Selain itu, penelitian ini juga menggunakan metode *Analytical Hierarchy Process* (AHP) untuk menentukan bobot prioritas setiap fokus area keamanan informasi karena setiap fokus area memiliki tingkat kepentingan yang berbeda dalam konteks *mobile banking* [7-10].

Sejumlah penelitian terdahulu telah menggunakan HAIS-Q untuk mengukur tingkat kesadaran keamanan informasi pada berbagai objek penelitian, termasuk pengguna *mobile banking*. Beberapa penelitian juga telah menerapkan metode AHP untuk menentukan bobot

prioritas fokus area keamanan informasi [11-15]. Namun, penelitian pada pengguna *mobile banking* umumnya masih berfokus pada pengukuran tingkat kesadaran keamanan informasi tanpa mengintegrasikan hasil *awareness* dengan bobot prioritas setiap fokus area keamanan informasi [16-19]. Oleh karena itu, penelitian ini mengintegrasikan hasil pengukuran HAIS-Q dan pembobotan AHP menggunakan pendekatan *Weighted Sum Model* (WSM) untuk menghasilkan nilai kesadaran keamanan informasi yang lebih representatif karena telah mempertimbangkan tingkat prioritas setiap fokus area keamanan informasi. Dengan demikian penelitian ini diharapkan dapat memberikan gambaran tingkat kesadaran keamanan informasi pengguna *mobile banking* di Kota Medan secara lebih komprehensif berdasarkan tingkat prioritas setiap fokus area keamanan informasi [20]. Berdasarkan gap penelitian tersebut, penelitian ini dilakukan dengan judul **“Analisis Kesadaran Keamanan Informasi Pengguna M-BCA di Kota Medan Menggunakan HAIS-Q dan AHP”**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat kesadaran keamanan informasi pengguna layanan *mobile banking* BCA di Kota Medan berdasarkan dimensi *Knowledge, Attitude, dan Behavior* (KAB) yang ditinjau dari sembilan fokus area keamanan informasi menggunakan instrumen HAIS-Q?
2. Bagaimana urutan bobot prioritas dari sembilan fokus area keamanan informasi pada pengguna *mobile banking* berdasarkan metode *Analytical Hierarchy Process* (AHP)?
3. Bagaimana hasil akhir tingkat kesadaran keamanan informasi pengguna *mobile banking* BCA di Kota Medan dengan mengintegrasikan skor ISA dan bobot prioritas menggunakan pendekatan *Weighted Sum Model* (WSM)?

1.3 Tujuan

Berdasarkan rumusan masalah di atas, penelitian ini memiliki tujuan adalah sebagai berikut:

1. Untuk menganalisis tingkat kesadaran keamanan informasi pengguna layanan *mobile banking* BCA di Kota Medan berdasarkan dimensi *Knowledge, Attitude, dan Behavior* (KAB) yang ditinjau dari sembilan fokus area keamanan informasi menggunakan instrumen HAIS-Q.

2. Untuk menentukan urutan bobot prioritas dari sembilan fokus area keamanan informasi dalam penggunaan *mobile banking* menggunakan metode *Analytical Hierarchy Process* (AHP).
3. Untuk menganalisis indeks kesadaran keamanan informasi pengguna *mobile banking* dengan mengintegrasikan skor ISA dan bobot prioritas melalui pendekatan *Weighted Sum Model* (WSM).

1.4 Manfaat

Berdasarkan tujuan di atas, manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Secara teoritis, penelitian ini berkontribusi dalam validasi dan penerapan *framework Information Security Awareness* (ISA), memberikan model empiris mengenai interaksi dimensi *Knowledge*, *Attitude*, dan *Behavior* dalam konteks spesifik layanan *mobile banking* BCA pada populasi di Kota Medan.
2. Secara analitis, penelitian ini memberikan pendekatan evaluasi yang lebih presisi melalui penggunaan *Weighted Sum Model* (WSM). Dengan menggabungkan skor ISA dan bobot prioritas fokus area keamanan informasi, penelitian ini mampu mengidentifikasi area kerentanan kritis secara lebih akurat dibandingkan metode rata-rata sederhana, sehingga memberikan metodologi referensi bagi penelitian keamanan informasi selanjutnya.
3. Secara praktis, penelitian ini memberikan gambaran objektif mengenai profil kesadaran keamanan informasi masyarakat Kota Medan dalam bertransaksi digital. Data ini dapat digunakan oleh pemerintah daerah atau lembaga terkait sebagai dasar dalam merancang program literasi keamanan digital yang tepat sasaran.
4. Bagi pihak perbankan, khususnya Bank Central Asia Tbk., hasil penelitian ini dapat menjadi evaluasi strategis untuk memetakan fokus area yang memerlukan penguatan edukasi. Dengan mengetahui area yang memiliki bobot urgensi tinggi namun skor ISA rendah, pihak bank dapat menyusun strategi sosialisasi yang lebih efektif untuk meminimalkan risiko insiden keamanan akibat faktor kelalaian manusia (*human error*).

1.5 Ruang Lingkup

Ruang lingkup penelitian ini adalah sebagai berikut:

1. Subjek dan lokasi penelitian adalah penduduk Kota Medan yang merupakan pengguna aktif layanan *mobile banking* BCA.

2. Penentuan responden dalam penelitian ini menggunakan teknik *purposive sampling*, yaitu pemilihan sampel berdasarkan kriteria tertentu. Adapun kriteria responden dalam penelitian ini adalah penduduk Kota Medan yang merupakan pengguna aktif layanan *mobile banking* BCA yang telah melakukan transaksi minimal satu kali dalam tiga bulan terakhir. Jumlah responden dalam penelitian ini ditentukan menggunakan rumus Lemeshow karena jumlah populasi pengguna *mobile banking* BCA di Kota Medan tidak diketahui secara pasti.
3. Penelitian ini dilakukan dengan pendekatan kuantitatif menggunakan instrumen *Human Aspects of Information Security Questionnaire* (HAIS-Q).
4. Pengumpulan data dilakukan melalui penyebaran kuesioner secara online kepada mahasiswa dan masyarakat umum. Pengumpulan data juga diperoleh melalui berbagai sumber seperti jurnal, buku, laporan penelitian, dan publikasi resmi yang mendukung penelitian.
5. Data yang diperoleh akan diolah berdasarkan dimensi *Knowledge*, *Attitude*, dan *Behavior* untuk memperoleh skor tingkat kesadaran keamanan informasi pengguna *mobile banking* BCA berdasarkan sembilan fokus area. Perhitungan dilakukan dengan menjumlahkan skor jawaban responden tiap fokus area, kemudian menghitung nilai rata-rata untuk memperoleh skor tingkat kesadaran keamanan informasi tiap fokus area. Untuk menentukan bobot prioritas fokus area keamanan informasi, menggunakan metode AHP melalui penyusunan hierarki, perbandingan berpasangan, perhitungan bobot prioritas, serta pengujian konsistensi hasil penilaian. Penilaian perbandingan berpasangan pada metode AHP dilakukan oleh empat *experts*, yaitu dua dosen spesialisasi di bidang keamanan informasi dan keamanan siber, serta dua staf BTI Universitas Mikroskil yang memiliki pengalaman operasional dalam mengelola infrastruktur TI. Hasil akhir penelitian diperoleh dengan menggabungkan skor ISA dari instrumen HAIS-Q dengan bobot prioritas dari metode AHP menggunakan pendekatan *Weighted Sum Model* (WSM).