BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Organisator himpunan mahasiswa di Universitas Multimedia Nusantara (UMN) bertugas untuk memberdayakan, memfasilitasi, dan membantu perkembangan mahasiswa, dosen, dan alumni program studi himpunan tersebut (Lampiran 2). Bila organisator yang terpilih tidak mewakili suara mahasiswa yang diwakili, maka permasalahan akan mudah muncul. Oleh karena itu, tingkat partisipasi mahasiswa dalam proses pemungutan suara sangatlah penting. Karena, jika tingkat partisipasi mahasiswa rendah, maka resiko suara mayoritas tidak terdengar akan meningkat [1].

Berdasarkan hasil observasi data pemilu UMN 2021 dari halaman instagram KPU UMN, hanya 26,7% mahasiswa Teknik Komputer, 19% mahasiswa Informatika, 97% mahasiswa Teknik Fisika dan Teknik Elektro, dan 26,9% mahasiswa Sistem Informasi berpartisipasi dalam pemilu ketua dan wakil organisasi himpunan mahasiswa pada tahun 2021. Hal tersebut tentunya sangat tidak ideal. Selain Teknik Fisika dan Teknik Elektro, 3 program studi lain di Fakultas Teknik dan Informatika UMN tidak memiliki ketua dan wakil organisasi himpunan mahasiswa yang dipilih oleh $< 50\%$ mahasiswa dari program studi yang mereka wakilkan.

Smartmatic (2018) menyatakan bahwa adanya sebuah platform voting elektronik (e-voting) yang baik telah berhasil meningkatkan tingkat partisipasi penduduk Estonia dalam pemilu mereka sebanyak 39% untuk pemilu lokal, dan 5% untuk pemilihan anggota parlemen [2]. Toots, dkk (2016) juga setuju bahwa sistem voting elektronik berhasil diterapkan di Estonia, dimana hampir 32% pemberi suara yang umumnya merupakan kaum terpelajar telah menggunakan sarana voting elektronik dibandingkan dengan voting tradisional [3]. Penelitian-penelitian tersebut menunjukkan bahwa keberadaan platform e-voting yang baik telah berhasil meningkatkan tingkat partisipasi masyarakat dalam sebuah pemilu. Selain itu, tingkat partisipasi masyarakat dalam e-voting sudah kompetitif dengan tingkat partisipasi masyarakat dalam voting tradisional, yang berarti sebagian dari masyarakat sudah menerima dan siap mengadopsi sistem e-voting. Terakhir, karena demografi dalam subjek penelitian ini adalah kaum terpelajar yaitu mahasiswa

UMN, kemungkinan mereka untuk mengadopsi sistem e-voting cukup tinggi, seperti pada kasus di Estonia.

Penggunaan Google Form sebagai media voting elektronik di UMN dapat membatasi pengembangan aspek-aspek yang mampu membantu meningkatkan tingkat partisipasi mahasiswa dalam proses demokrasi di UMN. Penelitian yang dilakukan oleh Islam, dkk (2020) menemukan bahwa dalam bidang perbankan, berbagai aspek sebuah halaman web seperti interaktivitas, tampilan, kustomisasi, dan kemudahan penggunaan memiliki dampak positif terhadap keterlibatan pengunjung halaman tersebut. Mereka juga menemukan bahwa tingkat keterlibatan pengunjung memiliki hubungan positif dengan tingkat kepercayaan pelanggan dan tingkat retensi pelanggan [4].

Rismayanti dan Sarah (2021) menemukan bahwa kualitas situs web Traveloka.com, yang terdiri dari fungsionalitas, kemudahan penggunaan, keamanan dan privasi pengguna merupakan salah satu aspek yang dapat mempengaruhi kepercayaan online konsumen kepada situs web secara positif dan signifikan. Kualitas situs web, ditambah dengan kualitas informasi ulasan memberikan kontribusi untuk meningkatkan kepercayaan online sebesar 29,6% [5]. Berdasarkan penelitian-penelitian tersebut, dapat dilihat bahwa dalam bidang manapun, desain, tampilan, kemudahan penggunaan, keamanan, dan privasi merupakan aspek-aspek penting yang akan mendorong seseorang untuk menggunakan sebuah halaman web. Dengan demikian, diharapkan bahwa dengan dibangunnya aplikasi *e-voting* dalam penelitian ini, mahasiswa UMN yang pernah memberikan suaranya melalui aplikasi yang dibangun akan terus menggunakannya dalam pemilu-pemilu selanjutnya. Sehingga retensi pengguna dapat dijaga dan jumlah pemberi suara setiap tahunnya dapat terus meningkat.

Selain batasan desain dan tampilan, penggunaan aplikasi *third-party* seperti Google Form juga berarti menyerahkan aspek keamanan dan privasi kepada pihak di luar Universitas Multimedia Nusantara. Kasus kecurangan seperti yang terjadi di *Berkeley High School* pada Maret 2019 dapat terjadi karena sistem verifikasi identitas yang digunakan untuk Google Form masih kurang kuat [6]. Jika di kemudian hari KPU UMN atau pihak universitas ingin meningkatkan keamanan sistem pemilu yang digunakan, mereka akan kesulitan karena yang memegang kontrol pada sistem tersebut adalah Google, bukan KPU UMN ataupun pihak universitas. Adanya sistem e-voting yang dikelola secara independen akan memungkinkan adanya integrasi dengan sistem SSO UMN yang memiliki informasi akun yang terpisah dari alamat *email* milik mahasiswa, sehingga meningkatkan

keamanan sistem verifikasi yang digunakan. Wawancara yang dilakukan dengan salah satu mahasiswa UMN (Lampiran 3) juga mendukung pendapat bahwa Google Form masih kurang cocok untuk dijadikan sarana melakukan voting. Selain tidak dapat melihat perkembangan voting secara langsung dan suara yang diberikan tidak bersifat rahasia sehingga dapat menyebabkan permasalahan ketika seseorang memberikan suara untuk kandidat yang berbeda dengan lingkaran sosialnya, penambahan fitur baru seperti notifikasi pemberi suara saat waktu voting selesai yang disarankan olehnya akan sulit karena sistem yang digunakan dikontrol oleh Google, bukan pihak universitas ataupun KPU UMN.

Selain aspek verifikasi identitas, sistem e-voting juga perlu memiliki mekanisme untuk menjaga kerahasiaan suara. Dalam hal ini, penggunaan algoritma enkripsi homomorfis parsial memungkinkan kita untuk menjumlahkan data suara yang telah dienkripsi, dan menghitung hasil pemilu tanpa perlu melakukan dekripsi terlebih dahulu. Hal tersebut akan meningkatkan tingkat kerahasiaan suara yang diberikan karena suara yang telah disimpan di database tidak perlu didekripsi terlebih dahulu sebelum proses perhitungan suara dimulai. Algoritma Paillier merupakan salah satu algoritma enkripsi homomorfis parsial yang paling terkenal [7]. Algoritma Paillier dipilih karena algoritma tersebut memiliki 3 kelebihan utama dibandingkan algoritma homomorfis parsial lainnya. Pertama, Algoritma Paillier dibuat pada tahun 1999 [8]. Lebih baru dibandingkan algoritma enkripsi homomorfis terkenal lainnya seperti Rivest–Shamir–Adleman (RSA) (1977 - 1978) , ElGamal (1985), Benaloh (1985), dan Okamoto-Uchiyama (1998) [9] [10] [11] [12] [13]. Hal tersebut memungkinkan Algoritma Paillier untuk mengintegrasikan perkembangan di bidang matematika dan kriptografi untuk menghasilkan algoritma yang lebih modern. Kedua, Algoritma Paillier memiliki sifat homomorfis aditif yang akan menjadi kunci utama dalam proses perhitungan suara. Sedangkan algoritma RSA dan ElGamal hanya memiliki sifat homomorfis multiplikatif. Sehingga tidak dapat digunakan dalam perhitungan suara [14]. Ketiga, Algoritma Paillier memiliki waktu komputasi yang lebih baik dibandingkan dua algoritma homomorfis aditif lainnya, yaitu Okamoto-Uchiyama dan Benaloh [15] [16].

Suwandi, dkk (2018) menerbitkan jurnal pembangunan sistem voting elektronik dengan memanfaatkan sifat homomorfis dari algoritma enkripsi. Penelitian tersebut membandingkan implementasi Algoritma Okamoto-Uchiyama dan Paillier dalam sistem voting elektronik. Setelah menjelaskan cara kerja dari kedua algoritma, penelitian tersebut membahas desain implementasi sistem elektronik dan dilanjutkan pada uji coba implementasi dari masing-masing

algoritma. Hasil penelitian menunjukkan bahwa penggunaan algoritma enkripsi homomorfis dalam sistem voting elektronik dapat memungkinkan perhitungan suara untuk dilakukan dengan tetap menjaga kerahasiaan suara yang diberikan. Selain itu, penelitian tersebut juga menunjukkan bahwa Algoritma Paillier memiliki proses yang lebih cepat, dan menghasilkan hasil enkripsi yang lebih kecil dibandingkan algoritma Okamoto-Uchiyama [15]. Salman (2021) melakukan analisa performa Algoritma Paillier dan Benaloh dalam penerapannya pada pembangunan sistem voting elektronik. Penelitian tersebut memberikan penjelasan dari Algoritma Paillier dan Benaloh, memberikan skema sistem voting elektronik yang dapat dibangun, dan kebutuhan-kebutuhan untuk sistem yang diajukan. Hasil penelitian tersebut menemukan bahwa Algoritma Paillier lebih sederhana dan memiliki efisiensi waktu komputasi yang lebih baik dibandingkan dengan Algoritma Benaloh [16].

Oleh karena itu, penelitian rancang bangun sebuah sistem pemungutan suara yang mudah digunakan baik oleh anggota KPU UMN sebagai panitia, maupun mahasiswa UMN sebagai pemberi suara dalam pemilihan umum organisator di UMN dilakukan. Sistem pemungutan suara tersebut akan dibangun dengan menggunakan algoritma enkripsi Paillier untuk menjaga kerahasiaan dan privasi pemberi suara, dan memastikan proses pemungutan suara berjalan secara jujur dan adil tanpa ada pengaruh dari pihak lain baik dari penyelenggara pemungutan suara, pemberi suara, maupun pihak luar lainnya.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah :

1. Bagaimana cara membangun sistem voting elektronik di UMN dengan menggunakan Algoritma Paillier?
2. Bagaimana penerimaan pengguna terhadap sistem voting elektronik yang telah dibangun dengan menggunakan *Technology Acceptance Model* (TAM)?

1.3 Batasan Permasalahan

Batasan masalah dalam penelitian ini adalah :

1. Aplikasi yang dibangun hanya ditujukan untuk digunakan oleh mahasiswa UMN untuk melakukan pemilihan organisator himpunan mahasiswa di UMN.

2. Jumlah maksimal pemberi suara untuk masing-masing himpunan mahasiswa adalah 9999 mahasiswa.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Membangun sistem voting elektronik di UMN dengan menggunakan Algoritma Paillier.
2. Mengetahui tingkat penerimaan pengguna terhadap sistem voting elektronik yang telah dibangun dengan menggunakan *Technology Acceptance Model* (TAM).

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Untuk peneliti
   (a) Menambah pengetahuan tentang aspek-aspek penting dalam pembangunan sebuah sistem voting elektronik.
   (b) Menambah pengetahuan tentang proses pembangunan sistem aplikasi.
   (c) Menambah pengetahuan tentang berbagai sistem dan algoritma yang digunakan dalam kriptografi.
2. Untuk UMN
   (a) Mendapatkan sarana pemberian suara yang lebih profesional, jelas dan mudah digunakan.
   (b) Mempermudah proses pemberian suara, dan verifikasinya.
   (c) Meningkatkan minat mahasiswa untuk berpartisipasi dalam pemilihan organisator di UMN.
   (d) Meningkatkan kualitas infrastruktur kampus dengan adanya sistem yang lebih profesional tersebut.
3. Untuk Ilmu Pengetahuan
   (a) Menambah ilmu tentang pengembangan sistem voting elektronik dengan menggunakan Algoritma Paillier.

1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab 1 menjelaskan latar belakang dilakukannya penelitian, yaitu kurangnya keamanan sistem pemungutan suara di UMN. Bab 1 juga menjelaskan rumusan dan batasan masalah yang akan dihadapi dalam penelitian ini, serta tujuan dan manfaat penelitian ini.

- Bab 2 LANDASAN TEORI
  Bab 2 menjelaskan landasan teori yang digunakan dalam penelitian ini, yaitu : Algoritma Enkripsi Homomorfis Paillier karya Pascal Paillier, pembangunan sistem e-voting dari penelitian-penelitian terdahulu, serta arsitektur framework model-view-controller yang akan digunakan untuk membangun sistem e-voting dalam penelitian ini.

- Bab 3 METODOLOGI PENELITIAN
  Bab 3 menjelaskan metodologi dan tahapan-tahapan yang dilakukan dalam penelitian ini secara mendetail. Mulai dari identifikasi masalah hingga pembuatan laporan penelitian. Bab ini mengandung banyak gambar dan diagram yang diharapkan dapat membantu menjelaskan sistem yang dibangun dalam penelitian ini.

- Bab 4 HASIL DAN DISKUSI
  Bab 4 mengandung hasil penelitian yang dicapai dan diskusi serta analisis terkait hasil penelitian tersebut. Bab ini akan membahas hasil dari *User Acceptance Test* untuk sistem yang telah dibangun.

- Bab 5 KESIMPULAN DAN SARAN
  Bab 5 berisi simpulan terkait dengan pekerjaan yang telah dilakukan dan dijelaskan pada bab sebelumnya, serta saran untuk penelitian-penelitian terkait yang akan dilakukan di kemudian waktu.