

BAB I

PENDAHULUAN

A. Latar Belakang

Internet merupakan sesuatu yang sudah tidak asing lagi bagi kita, bahkan dalam dunia pendidikan. Oleh karena itu pendidikan memerlukan teknologi dapat membantu guru dan siswa lebih mudah dalam proses belajar mengajar, metode lebih efektif, waktu persiapan lebih singkat dan dapat dilakukan dimana saja. Pembelajaran online memenuhi tantangan ini. Seiring dengan berkembangnya Internet di dunia, hampir seluruh kegiatan menerapkan Internet. Dalam dunia pendidikan pembelajaran yang ada sampai dengan merupakan sistem pembelajaran yang menggunakan metode langsung, dimana proses belajar mengajar hanya dapat dilakukan dengan syarat dilakukan pertemuan demonstrasi di dalam kelas. Apabila pertemuan tidak berlangsung maka proses pembelajaran tidak dapat berlangsung secara otomatis. (Sastra, 2017)

Dalam pengembangan *e-learning*, aspek keamanan menjadi sangatlah penting mengingat dimasa sekarang sering sekali terjadi ancaman yang melibatkan dunia siber yang dapat membahayakan pengguna dan juga pemilik sistem. Ancaman siber seperti peretasan, pencurian data pribadi, dan serangan siber lainnya dapat membahayakan integritas dan kerahasiaan informasi atau data dalam platform *e-learning*. Selain itu juga, pelanggaran keamanan dapat mengganggu proses pembelajaran, pengaksesan informasi

dan juga menyebabkan terjadinya penurunan kepercayaan pengguna terhadap platform *e-learning* yang telah dibangun dan dikembangkan.

Didalam *e-learning* terdapat banyak sekali data dan informasi yang sangat penting didalamnya seperti, data para pengguna *e-learning* baik user ataupun *administrator* yang mengatur sistem *e-learning* secara fungsi yang mana jika tidak diamankan data ini dapat dijadikan alat untuk melakukan tindak kejahatan salah satu contohnya *doxing*.

Doxing sendiri adalah sebuah praktik yang dilakukan dengan cara mencari, mengumpulkan, dan menyebarkan informasi pribadi seseorang secara daring dengan tujuan tertentu. *Doxing* dapat mencakup informasi pribadi seperti nama lengkap, alamat tempat tinggal, nomor telepon, alamat email dan lain sebagainya. Setelah informasi pribadi korban terkumpul, pelaku *doxing* biasanya akan menyebarkan informasi tersebut secara luas di internet dengan tujuan untuk mengekspos atau merendahkan reputasi korban. *Doxing* ini juga dapat digunakan untuk melakukan tindakan negatif lainnya seperti penyerangan verbal, pelecehan, penculikan ataupun ancaman.

Dikutip dari jurnal *Indonesian Journal of Education And Computer Science (INDOTECH)* dengan judul “Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman *Cybersecurity*”. Berdasarkan data dari Badan Cyber dan Sandi Negara (BSSN) Indonesia mengalami hampir 190 juta percobaan serangan siber dari Januari hingga Agustus 2020, yang lebih dari

empat kali lipat dari periode yang sama pada tahun sebelumnya, sekitar 39 juta percobaan (Dwi Madya et al., n.d.,2023.). Tentunya hal ini dapat menjadi tolak ukur pentingnya penerapan keamanan data pengguna website khususnya sistem *e-learning* yang mana sistemnya sendiri juga berbasis website.

Dari masalah tersebut, penelitian ini akan membahas topik mengenai perancangan keamanan data dan juga aplikasi dalam pengembangan *e-learning* SDN 01 Manisrejo. Tujuan utama dari penelitian ini adalah untuk mendesain, dan mengimplementasikan sistem keamanan yang efektif dalam *e-learning* guna melindungi data dan informasi *sensitive* yang dimiliki oleh *platform* tersebut. Dengan sistem keamanan yang kuat ini, diharapkan pengguna *e-learning* SDN 01 Manisrejo akan merasa lebih aman dan juga nyaman dalam menggunakan layanan *e-learning* tersebut.

Selain itu, penelitian ini akan mengeksplorasi berbagai metode dan juga teknologi keamanan yang dapat diterapkan dalam pengembangan platform *e-learning*. Hal ini tentunya akan membantu dalam proses pengembangan *e-learning* dan untuk memahami bagaimana mengidentifikasi potensi ancaman keamanan yang dapat terjadi juga merancang solusi yang sesuai guna menghindari ancaman tersebut. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi positif dalam meningkatkan keamanan *platform e-learning* dan mendorong para pengguna *internet* untuk memakai *e-learning* dalam dunia Pendidikan.

Melalui penelitian ini juga, diharapkan dapat tercipta *platform e-learning* yang lebih aman dan nyaman, yang dapat meningkatkan kualitas Pendidikan secara menyeluruh karena mudahnya akses informasi. Selain itu, penelitian ini juga akan memberikan wawasan baru dalam bidang keamanan informasi dan teknologi yang dapat menjadi kontribusi berharga dalam mengatasi tantangan keamanan yang terus berkembang dalam era digital ini.

B. Rumusan Masalah

Dari latar belakang yang telah dirumuskan, diperoleh rumusan masalah sebagai berikut:

1. Berapakah tingkat keamanan yang dimiliki oleh *e-learning* SDN 01 Manisrejo sebelum dilakukan perancangan ini?
2. Apa saja rancangan yang diperlukan guna meningkatkan keamanan *platform e-learning* yang dimiliki oleh SDN 01 Manisrejo?
3. Bagaimana implementasi terkait keamanan aplikasi dan data pada *e-learning* SDN 01 Manisrejo?

C. Batasan Masalah

Adapun batasan dari penelitian ini yaitu:

1. Objek penelitian dilakukan di SDN 01 Manisrejo.
2. Penelitian ini hanya berfokus pada *website e-learning* milik SDN 01 Manisrejo “pecelae.anggariyandisaputra.my.id”.
3. Metode yang akan digunakan pada penelitian ini adalah metode *R&D* dan *Mixed Method*.

4. Fungsi yang akan digunakan dalam *framework NIST* adalah *Protect* yang berfokus pada kategori *Identity Management Authentication and Access Control, Awareness and Training, Data Security, Platform Security, Technology Infrastructure Resilience*.

D. Tujuan Penelitian

Tujuan dari penelitian berdasarkan rumusan dan batasan masalah tersebut yaitu:

1. Mengetahui seberapa jauh tingkat keamanan yang dimiliki oleh platform e-learning milik SDN 01 Manisrejo.
2. Mengetahui rancangan yang akan digunakan dalam platform e-learning SDN 01 Manisrejo.
3. Mengetahui bagaimana mengimplementasikan rancangan keamanan aplikasi dan data untuk *e-learning* milik SDN 01 Manisrejo.