BAB II
DASAR TEORI DAN KAJIAN PUSTAKA

2.1 Tinjauan Pustaka

Berikut ini adalah beberapa tinjauan pustaka yang dilakukan oleh sebagian peneliti-peneliti sebelumnya. Penelitian oleh Herdiantoro et al pada tahun 2023 menyoroti pentingnya keamanan dalam penggunaan website di era industri 4.0. Penelitian ini berfokus pada penerapan teknologi keamanan untuk melindungi akun administrator dari serangan siber, khususnya melalui metode Two-Factor Authentication (2FA) dan kebijakan firewall. Hasilnya menunjukkan bahwa 2FA dan firewall memberikan lapisan perlindungan tambahan terhadap upaya pencurian akun, dengan 2FA mengharuskan verifikasi tambahan melalui email atau telepon, serta firewall yang membatasi akses hanya pada alamat IP tertentu.

Kemudian penelitian Heriyanto et al pada tahun 2022 menunjukkan bahwa penerapan Two-Factor Authentication (2FA) menggunakan One-Time Password (OTP) dan autentikasi melalui aplikasi Telegram secara signifikan dapat mengurangi risiko akses tidak sah ke sistem informasi akademik. Metode ini menambah lapisan keamanan dengan memerlukan dua langkah verifikasi, sehingga menyulitkan pihak yang tidak berwenang untuk mengakses data. Implementasi ini tidak hanya meningkatkan keamanan dari perspektif pengguna dan penyedia sistem, tetapi juga menjadi langkah penting dalam menghadapi ancaman keamanan digital yang semakin kompleks.

Penelitian selanjutnya oleh Andrian et al pada tahun 2023 menunjukkan bahwa penerapan 2FA berbasis TOTP dalam sistem informasi pendidikan di SDN Cimahi Mandiri 1 efektif dalam melindungi data sensitif dari akses tidak sah. Fokus penelitian adalah penggunaan OTP sebagai metode autentikasi untuk memastikan hanya pengguna sah yang dapat mengakses data siswa. Penerapan 2FA ini meningkatkan keamanan sistem dan memperkuat kepercayaan pengguna terhadap platform. Selain itu, penelitian ini menggarisbawahi pentingnya lapisan tambahan

keamanan dalam sistem informasi pendidikan untuk mengurangi risiko pelanggaran data.

Selain itu penelitian yang dilakukan oleh Anwar Fauzi et al pada tahun 2024 menilai peningkatan keamanan data rekam medis di rumah sakit dengan mengusulkan penerapan Multi-Factor Authentication (MFA) untuk melindungi informasi sensitif. Penelitian menunjukkan bahwa sistem keamanan yang bergantung pada autentikasi email dan kata sandi saja rentan terhadap pencurian data. MFA yang diterapkan menggunakan kata sandi, pertanyaan pribadi, dan kode TOTP, secara signifikan meningkatkan keamanan sistem dan mengurangi risiko akses tidak sah. Meskipun ada masalah dengan kesesuaian kode TOTP, MFA dianggap langkah penting untuk melindungi privasi data pasien. Penelitian ini menekankan pentingnya implementasi MFA untuk menghadapi tantangan keamanan modern dan menjaga integritas serta kerahasiaan data rekam medis.

Selanjutnya penelitian yang dilakukan oleh Aprilia et al pada tahun 2024 berfokus pada pengaruh Two Factor Authentication (2FA) dalam mencegah pencurian data di media sosial, terutama di kalangan Gen-Z yang sering kurang sadar akan pentingnya keamanan data. Menggunakan metode kualitatif dengan data dari penelitian terdahulu, penelitian ini menemukan bahwa 2FA secara signifikan meningkatkan perlindungan terhadap ancaman siber dan menekankan pentingnya peningkatan kewaspadaan masyarakat terhadap kejahatan cybercrime. Selain itu, penelitian ini juga menyoroti bahwa penggunaan teknologi keamanan seperti 2FA tidak hanya berfungsi sebagai pengaman, tetapi juga sebagai sarana edukasi bagi pengguna media sosial dalam memahami dan menghadapi risiko yang ditimbulkan oleh kejahatan siber di era digital.

Pada penelitian Morin pada tahun 2024 menggunakan objek penelitian berupa Website Lembaga Pelatihan, sedangkan penelitian sebelumnya menggunakan objek seperti Autentikasi Untuk Aplikasi Android dan Website, Sistem Keamanan Kode One Time Password (OTP) Pada Informasi Nilai Sekolah, Halaman Administrator Website, dan Sistem Informasi Akademik. Metode keamanan yang digunakan adalah OTP email, berbeda dengan penelitian Setiawan et al yang menggunakan

TOTP Android, QR *Code,* dan *Secret-Key Website.* Kemudian, berbeda dengan penelitian oleh Andrian *et al* yang menggunakan metode OTP Whatsapp, sedangkan Herdiantoro *et al* memakai Firewal *whitelist* dan OTP SMS, serta berbeda dengan OTP Telegram yang digunakan dalam penelitian Yusuf Heriyanto *et al.*

Tabel 2.1 Perbandingan Penelitian Sebelumnya

Nama, Tahun	Objek Penelitian	Tools	Metode Keamanan	Keterangan
Setiawan et al., (2020)	Autentikasi Untuk Aplikasi Android dan Website	PHP, MySQL, Java	2FA TOTP aplikasi Android, Quick Response Code (QR Code) atau Secret key website	Sebagian besar pengguna menganggap sistem ini sangat efektif dalam meningkatkan keamanan, mengindikasikan bahwa penerapan 2FA berbasis TOTP merupakan solusi yang kuat untuk mengatasi masalah keamanan dalam akses informasi melalui internet.
Andrian et al., (2023)	Sistem Keamanan Kode One Time Password (OTP) Pada Informasi Nilai Sekolah	PHP, MySQL	2FA OTP Whatsapp	Penerapan sistem keamanan menggunakan kode OTP efektif dalam meningkatkan perlindungan terhadap informasi nilai sekolah.
Herdiantoro*, et al.*, (2023)	Halaman Administrator Website	PHP, MySQL	2FA Firewall, OTP Email, OTP SMS	Kombinasi 2FA dan firewall policies dapat mengurangi risiko akses tidak sah.
Yusuf Heriyanto et al., (2022)	Sistem Informasi Akademik	PHP, MySQL,	2FA OTP, Telegram.	Sistem mampu memberikan keamanan akses baik dari sisi pengguna karena metode 2FA menerapkan strategi OTP dan otentikasi perhitungan selain metode password untuk mengakses sistem informasi akademik.

Tabel 2.1 Perbandingan Penelitian Lanjutan

Nama, Tahun	Objek Penelitian	Tools	Metode Keamanan	Keterangan
Fauzi et al., (2023)	Sistem Informasi Rekam Medis Rumah Sakit	PHP, MySQL, Google Autenticator	Personal Security Question, Auth Token, TOTP email	Menjadikan sistem informasi rekam medis Rumah Sakit menjadi lebih aman dan mengurangi risiko diakses oleh pihak yang tidak berwenang.
Morin (2024)	Website Lembaga Pelatihan	PHP, MySQL	2FA OTP email	Meningkatkan keamanan akses pengguna dengan memberikan lapisan perlindungan tambahan dan mengurangi risiko akses tidak sah serta melindungi data sensitif.

2.2 Dasar Teori

2.2.1 Implementasi

Menurut Mulyadi (2015), implementasi adalah tindakan yang dilakukan untuk mencapai tujuan yang telah ditetapkan dalam suatu keputusan. Tindakan ini berusaha untuk mengubah keputusan tersebut menjadi pola-pola operasional dan mencapai perubahan yang signifikan atau kecil sesuai dengan perubahan yang telah diputuskan sebelumnya. Pada dasarnya, implementasi juga berarti mencari tahu apa yang seharusnya terjadi setelah program dijalankan.

2.2.2 Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) adalah metode autentikasi yang memerlukan dua bentuk verifikasi identitas sebelum akses diberikan. Proses

pemeriksaan identitas untuk memastikan bahwa identitas tersebut asli untuk masuk ke dalam sistem dikenal sebagai autentikasi atau otentikasi (Saputra, 2021). Ada beberapa cara untuk melakukan otentikasi*: something you know*, yaitu menggunakan sesuatu yang kita ketahui, seperti kata sandi dan password; *something you have*, yaitu menggunakan sesuatu yang unik, seperti kartu SIM telepon; atau *something you are*, yaitu menggunakan sidik jari, retina mata, atau detektor wajah. Proses otentikasi pada aplikasi yang sensitif, seperti transaksi keuangan, penilaian, dan aplikasi penting lainnya

Manfaat 2FA mencakup peningkatan keamanan secara signifikan karena meskipun satu faktor (seperti password) telah dikompromikan, pengguna yang tidak memiliki faktor kedua (seperti kode OTP dari ponsel) tidak akan bisa mengakses akun. Bonneau et al. (2012) menunjukkan bahwa penerapan 2FA mengurangi risiko serangan phishing dan pencurian identitas.

2.2.2 OTP (*One Time Password*)

One Time Password (OTP) atau kode sandi sekali pakai adalah salah satu teknik paling umum untuk meningkatkan otentikasi yaitu sebagai 2FA. Ini adalah string alfanumerik atau numerik sekali pakai yang dihasilkan secara otomatis (Wigmore, 2018). Kode yang dihasilkan tidak dapat digunakan kembali karena bersifat sementara, sehingga tidak rentan terhadap serangan berulang. Artinya, penggunaan duplikat OTP menjadi tidak valid jika disadap oleh *malware* atau ditemukan oleh seseorang yang mengawasi kita.

Kata sandi statis dapat digunakan sendiri, bersamaan dengan OTP, atau sebagai tambahan OTP. Kata sandi sekali pakai terdiri dari dua bagian besar:

HOTP (OTP berbasis HMAC) dan TOTP (OTP berbasis waktu). Kode OTP terdiri dari kombinasi nomor rahasia unik yang ditentukan secara acak dan biasanya digunakan untuk transaksi online atau pendaftaran akun karena dianggap lebih aman untuk keamanan dan kata sandi terus diubah.

2.2.3 Website

Website adalah sebuah platform yang digunakan sebagai media untuk memasarkan produk, menyampaikan informasi, dan mempresentasikan citra perusahaan(Fariadi, 2022). Menurut Mastan (2019), berdasarkan tujuannya, website dapat dibagi menjadi beberapa jenis, yaitu personal website, corporate website, portal website, dan forum website. Setiap jenis website dirancang sesuai dengan tujuannya: personal website untuk kebutuhan pribadi, corporate website untuk mendukung kebutuhan perusahaan, portal website untuk layanan seperti berita, email, dan jasa, serta forum website untuk media diskusi.

2.2.4 Lembaga Pelatihan

Menurut *Susilo (2017)*, lembaga pelatihan berperan penting dalam pengembangan sumber daya manusia, terutama dalam mempersiapkan tenaga kerja yang kompeten dan siap bersaing di dunia industri. Lembaga pelatihan juga sering bekerja sama dengan perusahaan atau organisasi untuk menyesuaikan program pelatihan dengan kebutuhan spesifik industri tertentu.

Selain itu, *Nugroho (2018)* menyatakan bahwa lembaga pelatihan memiliki tugas utama dalam memberikan layanan pendidikan dan pelatihan yang berfokus pada peningkatan keahlian praktis, yang berbeda dengan pendidikan formal yang lebih menekankan pada teori. Lembaga ini juga memiliki peran dalam meningkatkan employability atau kemampuan seseorang untuk mendapatkan pekerjaan melalui program-program yang disesuaikan dengan tuntutan pasar.

2.2.5. PHP

PHP, singkatan dari Hypertext Preprocessor, adalah bahasa pemrograman script yang digunakan dalam server yang umumnya digunakan untuk membuat aplikasi web dinamis (Winanjar *et al* 2021). PHP memiliki banyak sekali pustaka bawaan yang menyediakan fungsi-fungsi untuk memanipulasi data, salah satunya adalah PHPMailer. PHPMailer adalah pustaka kode yang memungkinkan pengiriman email dengan mudah dan aman melalui kode PHP dari server web. PHPMailer memungkinkan kita mengakses SMTP, IMAP, dan POPMail dari server penyedia email untuk digunakan pada sistem yang memakai bahasa pemrograman PHP. PHPMailer memberikan fleksibilitas untuk mengirim dan membaca pesan dalam suatu sistem informasi, sehingga kita dapat mengimplementasikan fungsi klien email pada sistem tersebut, memungkinkan sistem tersebut untuk mengirimkan email melalui server SMTP. PHPMailer memberikan kebebasan untuk mengirim dan membaca pesan pada sistem informasi,

memungkinkan kita menerapkan fungsi email client pada sistem tersebut. Dengan demikian, sistem tersebut dapat mengirim email melalui server SMTP pada sistem informasi yang dibuat. (M. Sudana et al, 2019).

PHP adalah bahasa pemrograman server-side, atau diproses di server. PHP adalah bahasa pemrograman universal yang digunakan untuk menangani pembuatan dan pengembangan website, dan fungsi utamanya adalah untuk melakukan pengolahan data pada database. Data yang berasal dari sebuah website akan dimasukkan ke database, diubah, dihapus, dan ditampilkan pada website yang diatur oleh PHP (Resman *et al* 2021). PHP, juga dikenal sebagai Preprocessor Hypertext, adalah Bahasa pemrograman yang digunakan untuk menerjemahkan basis kode program menjadi kode mesin yang dapat dimengerti oleh komputer yang bersifat server-side dan ditambahkan ke HTML (Hari Utami, 2022).