

## Sistem Manajemen Konten Berbasis Web Pada Portal Berita TV Menggunakan Metode One-Time Password (OTP) sebagai Pengamanan Login Admin

Rifda Arifah Ashari<sup>\*1</sup>, Bambang Agus Herlambang<sup>2</sup>

<sup>1</sup>Informatika, Universitas PGRI Semarang, Semarang, [rifdaarifahashari26@gmail.com](mailto:rifdaarifahashari26@gmail.com)

<sup>2</sup>Informatika, Universitas PGRI Semarang, Semarang, [bambangherlambang@upgris.ac.id](mailto:bambangherlambang@upgris.ac.id)

### Abstract.

Data security on administrator accounts in system development is a very crucial aspect. The application of data security serves to protect systems, networks and programs from many cyber threats. The impact of a cyberattack can be in the form of illegal access taking, alteration, and destruction of sensitive information in a system. The INTV news portal's administrative panel is currently still implementing static passwords as data security. This method is less secure for securing the INTV news portal administration system. So there is a need to increase the security layer, or the implementation of Multi Factor Authentication (MFA), in this case the INTV news portal administration page implements the One-Time Password (OTP) feature. The system development method applied to the INTV news portal is the prototyping method using PHPNative and MySQL databases. The system generates OTPs in the form of 6-digit numbers automatically via WhatsApp using the Fonnte API and via Email with the SMTP-based PHPMailer library. Bcrypt is used to secure the storage of user passwords in the database. The test results show that the OTP is sent in 1-3 seconds via WhatsApp and 3-5 seconds via Email, with a validity period of 5 minutes after it is sent. With this OTP feature, the security of the INTV news portal administration page has been proven to be improved against various cyber threats, without disrupting the efficiency of the public relations team's work.

**Keywords:** One-Time Password, App Security, Website News, Multi-Factor Authentication.

### Abstrak

Keamanan data pada akun administrator dalam pengembangan sistem merupakan aspek yang sangat krusial. Penerapan keamanan data berfungsi untuk melindungi sistem, jaringan dan program dari banyaknya ancaman siber. Dampak dari serangan siber bisa berupa pengambilan akses secara ilegal, perubahan hingga penghancuran informasi sensitif dalam sebuah sistem. Panel administrasi portal berita INTV saat ini masih menerapkan kata sandi statis sebagai pengamanan data. Metode seperti ini kurang aman untuk pengamanan sistem administrasi portal berita INTV. Sehingga perlu adanya peningkatan lapisan keamanan, atau penerapan *Multi Factor Authentication* (MFA), dalam hal ini halaman administrasi portal berita INTV mengimplementasikan fitur *One-Time Password* (OTP). Metode pengembangan sistem yang diterapkan pada portal berita INTV ini yaitu metode *prototyping* dengan memanfaatkan *PHPNative* dan basis data *MySQL*. Sistem menghasilkan OTP berupa 6 digit angka secara otomatis melalui *WhatsApp* menggunakan *API Fonnte* serta melalui Email dengan *library PHPMailer* berbasis *SMTP*. *Bcrypt* digunakan untuk mengamankan penyimpanan password pengguna di database. Hasil uji coba menunjukkan OTP terkirim dalam 1-3 detik melalui *WhatsApp* dan 3-5 detik via Email, dengan masa berlaku 5 menit setelah dikirim. Dengan adanya fitur OTP ini, keamanan halaman administrasi portal berita INTV terbukti meningkat terhadap berbagai ancaman siber, tanpa mengganggu efisiensi kerja tim kehumasan.

**Kata Kunci:** *One-Time Password*, Keamanan aplikasi, Website Berita, *Multi-Factor Authentication*.

## 1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi saat ini telah membawa transformasi pada berbagai sektor, tidak terkecuali pada industri media massa [1]. Media sosial dan platform digital saat ini telah merambah ke bidang jurnalistik, produk jurnalistik yang dulunya berupa surat kabar kini telah berpindah menjadi portal berita online yang dapat diakses real-time, kapan saja dan dimana saja [2]. Saluran berita kini ikut beradaptasi dengan mengembangkan sistem manajemen konten berbasis web agar tetap relevan dalam menyalurkan berbagai informasi secara cepat dan terpercaya [3]. Di balik kemudahan dan efisiensi yang ditawarkan terdapat ancaman pada aspek keamanan sistem. Portal berita seringkali menjadi sasaran kejahatan dari pihak-pihak yang tidak bertanggung jawab, mulai dari peretasan akun, modifikasi konten secara ilegal (defacing), hingga pencurian data-data sensitif [4]. Sebuah kebocoran data bisa mengakibatkan kerugian finansial, kerusakan reputasi, hingga tindakan kriminal. Titik paling krusial dari sebuah sistem yaitu terdapat pada panel administrasi (login admin) [3]. Oleh karena itu pentingnya peningkatan pengamanan login admin, karena apabila akses untuk login admin dapat dengan mudah ditembus maka seluruh informasi dan data yang ada di dalamnya bisa disalahgunakan atau bahkan dirusak oleh pihak yang tidak berwenang [5]. Disinilah autentikasi memainkan peran penting dalam melindungi akses ke sistem [6].

Proses pengamanan data saat ini hanya mengandalkan kata sandi statis (single-factor authentication) di mana metode ini dianggap tidak cukup efektif. Kata sandi memiliki kerentanan terhadap berbagai macam serangan siber seperti *brute force*, *keylogging*, maupun *social engineering*. Seringkali pengguna menyimpan kata sandi pada browser yang dapat memperburuk kondisi keamanan, terutama ketika website tersebut digunakan pada perangkat yang bukan milik pribadi [7]. Maka dari itu, dibutuhkan metode keamanan berlapis yang disebut dengan *Multi-Factor Authentication* (MFA) [8]. Dengan peningkatan keamanan ini pengguna diwajibkan memberikan dua atau lebih bukti verifikasi untuk memperoleh akses ke akun. Metode MFA yang di gunakan terbatas pada *Two-Factor Authentication* (2FA) yang menggabungkan faktor pengetahuan (*password*) dan faktor kepemilikan (*One-Time Password*) yaitu password yang sifatnya sementara dan hanya dapat digunakan sekali saja dan dibatasi oleh waktu yang relative singkat [9].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang antarmuka (UI/UX), membangun *Content Management System* (CMS) fungsional dan peningkatan keamanan akun admin pada portal berita INTV di Perusahaan Penyedia Solusi IT. Sistem ini mengimplementasikan metode OTP 6-digit numerik dengan masa berlaku terbatas (30 detik hingga 5 menit) yang dikirimkan secara *real-time* via WhatsApp (menggunakan API Fonnte) dan Email (menggunakan SMTP PHPMailer). OTP merupakan sebuah kode yang digunakan hanya sekali untuk otentikasi pengguna dalam sebuah sesi [10]. Kode OTP diperoleh berdasarkan kinerja mesin atau *machine-generated*, sehingga kode yang dihasilkan bersifat rahasia, tidak ada yang dapat mengetahuinya selain penerima kode dari perangkat yang digunakannya [11]. Penggunaan layanan *Fonnte* yang memiliki response cepat, serta sejalan dengan studi yang mampu meningkatkan ketahanan sistem terhadap akses tidak sah [12]. Keamanan diperkuat di sisi basis data melalui algoritma hashing Bcrypt untuk menjamin integritas kredensial dan keandalan sistem dari risiko pengambilalihan akun secara ilegal. Harapannya, implementasi dari CMS Portal Berita INTV yang di lengkapi dengan sistem keamanan berlapis (2FA) berbasis OTP dan enkripsi Bcrypt ini dapat menjadi solusi teknologi yang mampu melindungi data-data berita di perusahaan. Selain untuk meningkatkan standar keamanan siber dari risiko pengambilalihan akun secara ilegal, sistem ini juga diharapkan mampu mempermudah dan mengoptimalkan efisiensi dan produktivitas kerja dalam mengelola publikasi digital secara dinamis, mandiri, dan terpercaya.

## 2. Metode

### 2.1 Metode Penelitian



Gambar 4 Metode Penelitian

#### 1. Observasi

Tahap awal dilakukan dengan mengamati langsung mekanisme *Content Management System* (CMS) dan sistem keamanan login admin pada portal berita TV yang sudah ada sebelumnya. Berdasarkan pengamatan, sistem lama masih bersifat sangat sederhana dan rentan karena hanya menggunakan metode autentikasi tunggal (*Single authentication* berupa *username* dan *password* biasa), sehingga rawan terhadap ancaman peretasan oleh pihak yang tidak berwenang.

#### 2. Wawancara

Proses wawancara dilakukan bersama admin pembuat dan pengelola *website* TV berita. Hasil wawancara menunjukkan adanya keluhan terkait keterbatasan fitur pengelolaan konten, tampilan antar muka yang kurang menarik, serta kekhawatiran yang tinggi terhadap kerentanan keamanan data dikarenakan lemahnya sistem autentikasi yang ada saat ini.

#### 3. Studi Pustaka

Pengumpulan pustaka dilakukan dengan mengkaji berbagai literatur ilmiah berupa artikel, jurnal, dan buku teks terkait tema penelitian. Referensi yang dikumpulkan difokuskan pada teori *Content Management Sistem* (CMS), keamanan website, *Multi-Factor Authentication* (MFA), mekanisme *One-Time Password* (OTP), serta penerapan algoritma *hashing* menggunakan *Bcrypt* untuk mengamankan penyimpanan data kredensial.

#### 4. Pengembangan Sistem

Sistem CMS portal berita TV ini dikembangkan menggunakan metode *prototyping*. Pendekatan rekayasa perangkat lunak ini dipilih untuk mempermudah visualisasi sistem yang akan dioperasikan oleh pengguna sebelum diimplementasikan secara penuh. Penjelasan detail mengenai tahapan *prototyping* dijabarkan pada sub-bab berikutnya.

#### 5. Penyusunan laporan

Setelah melalui proses analisis data hasil observasi, wawancara, serta pengujian fungsionalitas sistem login admin, langkah selanjutnya adalah menyusun laporan penelitian. Pada tahap ini, diuraikan pula bagaimana sistem keamanan login diintegrasikan dengan layanan pihak ketiga, seperti API Fonnte (untuk pengiriman OTP via WhatsApp) dan PHPMailer (untuk pengiriman OTP via Email).

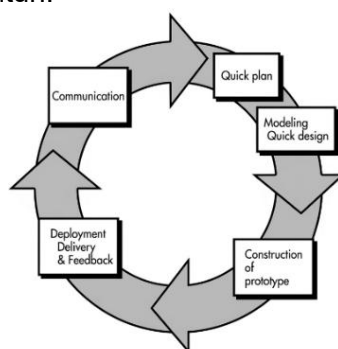
**6. Diseminasi Hasil**

Target luaran yang dicapai dari penelitian ini meliputi:

- Terlaksananya sosialisasi sistem login admin berbasis OTP melalui presentasi kepada pihak pengelola portal berita.
- Dipublikasikannya hasil penelitian mengenai implementasi OTP dan pengaruhnya terhadap peningkatan keamanan portal berita TV dalam bentuk laporan, artikel ilmiah seminar, atau media publikasi lainnya.
- Tersebarnya informasi mengenai efektivitas penggunaan OTP sebagai mekanisme keamanan tambahan bagi sistem portal berita.

**2.2 Metode Pengembangan Sistem (Prototyping)**

Metode *prototyping* merupakan salah satu model pengembangan sistem yang bersifat iteratif dan evolusioner [13]. Paradigma ini sangat efektif digunakan jika pengembang belum mendapatkan informasi yang detail mengenai input, proses, dan kebutuhan output yang diinginkan oleh pengguna secara utuh.



Gambar 5 Prototyping Model

Berdasarkan alur kerja pada gambar di atas, tahapan metode *prototype* terdiri dari:

1. Communication, yaitu tahap awal di mana pengembang bertemu dengan pemangku kepentingan untuk mendefinisikan objektif keseluruhan perangkat lunak, mengidentifikasi kebutuhan yang diketahui dan area di mana definisi eksplorasi lebih lanjut diperlukan.
2. Quick Plan, yaitu perencanaan cepat yang difokuskan pada penyajian aspek-aspek perangkat lunak yang akan terlihat oleh pengguna (misalnya format *input* OTP dan tata letak dashboard berita)
3. Modeling Quick Design, yaitu pembuatan model desain cepat yang memberikan gambaran kasar tentang arsitektur perangkat lunak, fokus pada representasi antarmuka pengguna.
4. Construction of Prototype, yaitu pembuatan purwarupa (sistem sementara) yang akan dievaluasi oleh pengguna. Dalam proyek ini, purwarupa mencakup simulasi alur *login* admin dengan pengiriman kode OTP.
5. Deployment, Delivery & Feedback, yaitu tahap di mana purwarupa dipresentasikan kepada pengguna untuk mendapatkan umpan balik (*feedback*). Jika pengguna merasa alur keamanan atau manajemen konten belum sesuai, maka proses akan kembali ke tahap awal hingga mencapai kesepakatan final.

**3. Hasil dan Pembahasan****3.1 Hasil**

Bagian ini menyajikan hasil konkret dari sistem manajemen konten (CMS) berbasis web pada portal beritaTV menggunakan metode *One-Time Password* pengamanan login admin yang telah berhasil dibangun. Penjelasan meliputi proses implementasi sistem serta analisis terhadap efektivitas dan dampaknya kepada perusahaan penyedia solusi IT. Hasil pengembangan Sistem Manajemen Konten (CMS) berbasis web pada portal berita TV dengan pengamanan login admin menggunakan metode *One-Time Password* (OTP) ini diperoleh melalui tiga tahap utama, yaitu analisis kebutuhan, desain sistem, dan implementasi sistem.

## 1. Analisis Kebutuhan Sistem

Tahap ini merinci spesifikasi kebutuhan yang harus dipenuhi oleh sistem, yang dibagi menjadi kebutuhan fungsional dan kebutuhan non-fungsional.

Tabel 4 Analisis Kebutuhan Sistem

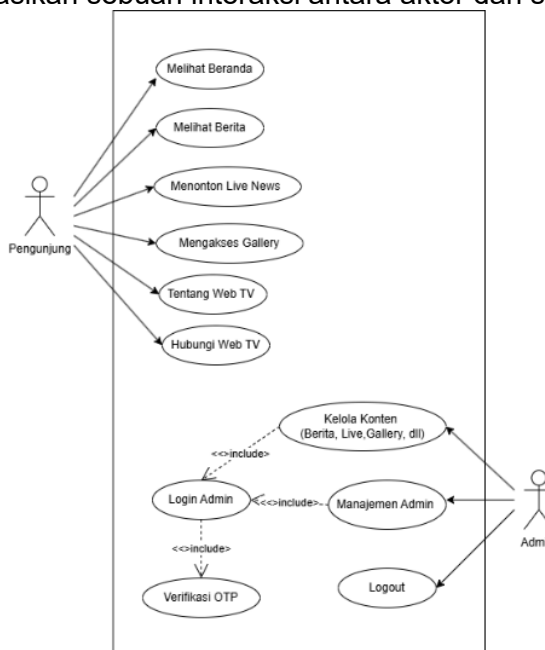
| Jenis Kebutuhan              | Deskripsi                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kebutuhan Fungsionalitas     | <ul style="list-style-type: none"> <li>• Sistem harus dapat menampilkan berita dalam kategori yang rapi.</li> <li>• Sistem wajib meminta verifikasi kedua (OTP) setelah admin memasukkan kata sandi yang benar.</li> <li>• Sistem harus bisa mengirimkan kode OTP secara otomatis ke WhatsApp atau Email admin.</li> <li>• Sistem harus menolak akses jika kode OTP yang dimasukkan salah atau sudah kadaluwarsa.</li> </ul> |
| Kebutuhan Non-Fungsionalitas | <ul style="list-style-type: none"> <li>• Semua data sensitif (password dan OTP) harus disimpan dalam bentuk <i>hash</i> menggunakan <i>Bcrypt</i>.</li> <li>• Tampilan <i>dashboard</i> admin harus mudah dipahami meskipun fiturnya telah ditambah.</li> </ul>                                                                                                                                                              |

## 2. Desain Sistem

Rancangan arsitektur dan visualisasi fungsionalitas sistem dikembangkan menggunakan pemodelan diagram UML (*Unified Modeling Language*) dan rancangan antarmuka berupa *wireframe*.

## a. Use Case Diagram

Use Case Diagram merupakan gambaran dari fungsionalitas yang diharapkan dari sebuah sistem, dan mempresentasikan sebuah interaksi antara aktor dan sistem [14].



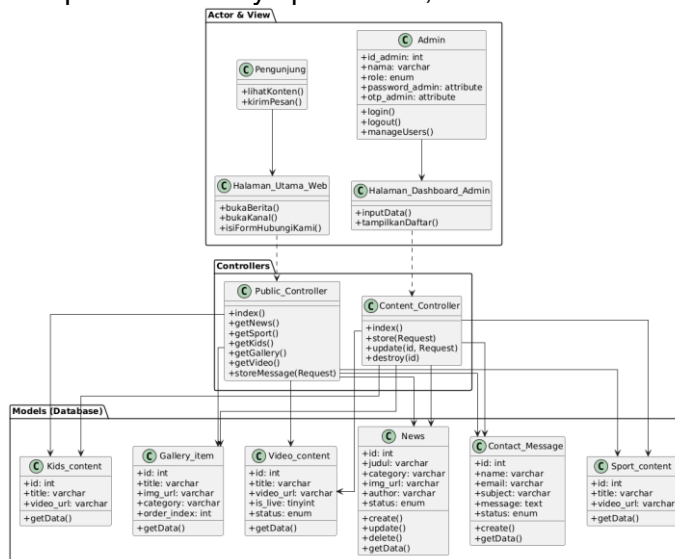
Gambar 6 Use Case Diagram INTV

Use Case diagram pada Gambar 3 memperlihatkan bagaimana aktor Pengunjung (aktor pertama) memiliki akses terbatas pada fitur publik tanpa memerlukan proses login, meliputi fungsi melihat beranda, melihat berita, menonton Live News, mengakses galeri, melihat informasi profil TV, serta mengirimkan pesan pada menu Hubungi Web TV. Sementara aktor Admin (aktor kedua) memiliki akses untuk masuk ke dashboard admin melalui proses login yang mewajibkan tahap verifikasi kode *One-Time Password* (OTP).



## b. Class Diagram

Class Diagram merupakan gambaran struktur dan deskripsi dari class, package, dan objek yang saling berhubungan seperti diantaranya pewarisan, asosiasi dan lainnya [15].

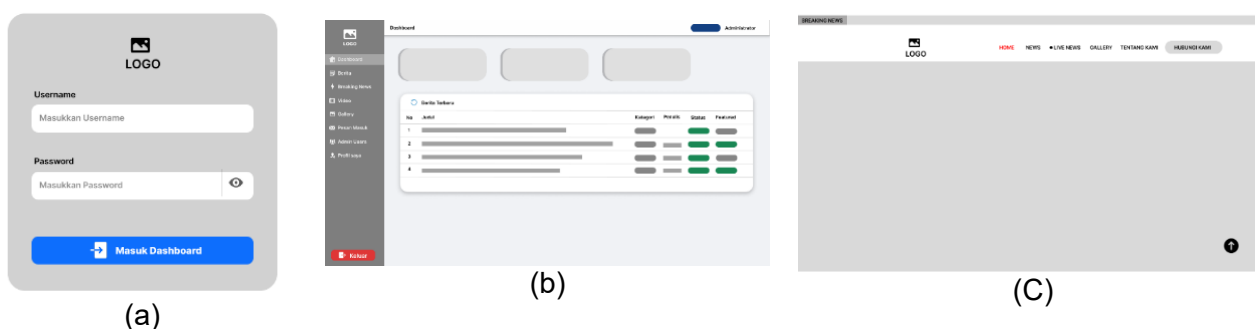


Gambar 7 Class Diagram

Class diagram pada gambar 4 menggambarkan struktur statis dan hubungan antar komponen di dalam sistem yang dirancang menggunakan pola arsitektur *Model-View-Controller* (MVC). Setiap class pada diagram ini mempunyai atribut yang menunjukkan data ataupun karakteristik yang dimilikinya, serta tindakan yang dapat dijalankan oleh kelas tersebut.

## c. Wireframe Antarmuka

Sebelum diimplementasikan ke dalam baris kode program, rancangan struktur visual halaman masuk admin didesain melalui bentuk *wireframe* minimalis seperti yang ditunjukkan pada Gambar 5.

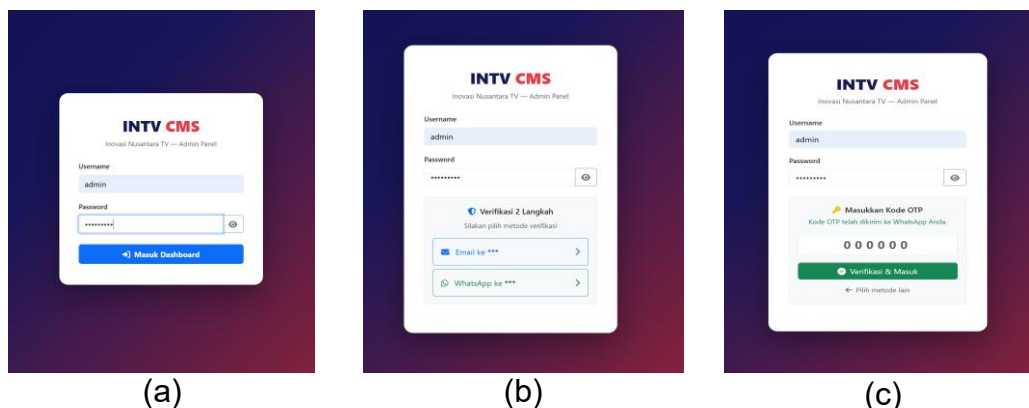


Gambar 5. Wireframe Antarmuka

- Halaman login admin pada gambar (a) berfungsi sebagai pintu gerbang utama sebelum pengguna masuk ke dalam panel kendali (*dashboard*). Halaman ini menyediakan kolom input kredensial untuk memverifikasi hak akses administratif, yang kemudian akan langsung terintegrasi dengan sistem keamanan lapis kedua berupa verifikasi kode OTP.
- Halaman Dashboard admin pada gambar (b) ini berupa tampilan dashboard admin khusus bagi admin yang telah berhasil melewati tahap autentikasi login dan verifikasi OTP. Melalui halaman dashboard ini, admin memiliki otoritas penuh untuk melakukan pengelolaan data berita secara dinamis.

- Halaman home pada gambar (c) ini berupa tampilan utama website portal berita TV. Berbeda dengan halaman administrasi, halaman home ini dirancang agar dapat diakses secara terbuka oleh pengunjung umum kapan saja tanpa perlu melakukan proses login terlebih dahulu.

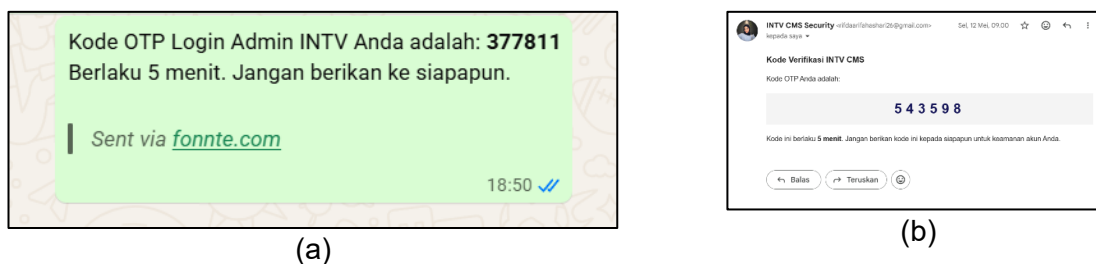
### 3. Implementasi Sistem



Gambar 6 Proses Login Admin

Alur proses login admin pada Gambar 6 menunjukkan tahapan yang harus dilewati oleh aktor admin untuk mengakses dashboard, yaitu melalui tahapan autentikasi awal dan verifikasi kode *One-Time Password* (OTP).

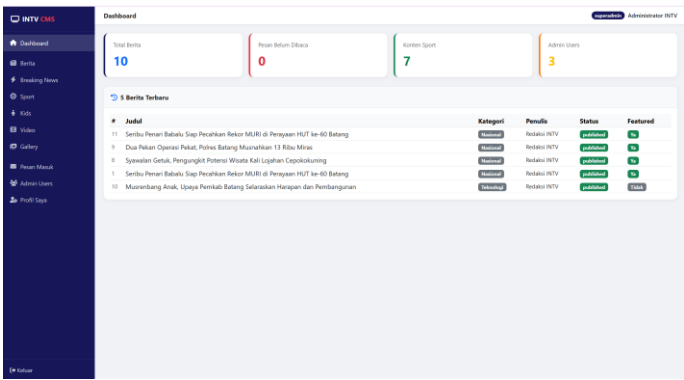
- Pada gambar (a) ini pengguna diminta memasukkan username dan password yang valid.
- Setelah username dan password pada langkah pertama dinyatakan benar selanjutnya pada gambar (b) pengguna diminta memilih metode pengiriman OTP baik melalui WhatsApp ataupun Email.
- Setelah memilih metode pengiriman, selanjutnya pada gambar (c) sistem menampilkan form pengisian OTP untuk bisa mengakses dashboard admin.



Gambar 7 Input OTP

Gambar 7 menyajikan dokumentasi perolehan kode *One-Time Password* (OTP) yang diterima oleh admin. Pesan verifikasi ini dikirimkan secara otomatis oleh sistem segera setelah admin menentukan jalur transmisi pada halaman autentikasi sebelumnya. Log transmisi tersebut terbagi menjadi dua saluran komunikasi utama, yaitu pesan teks masuk melalui aplikasi WhatsApp dan surat elektronik melalui kotak masuk Email.

- Gambar (a) merupakan gambar pesan instan OTP yang di kirimkan melalui WhatsApp dengan waktu response pengiriman berkisar antara 1 hingga 3 detik, disertai informasi batas validasi penggunaan kode sebelum kadaluwarsa.
- Gambar (b) merupakan tampilan pesan instan OTP yang dikirimkan melalui Email dengan waktu estimasi yang dibutuhkan berkisar antara 3 hingga 5 detik yang hangus secara otomatis dalam durasi 5 menit.



Gambar 8 Halaman Dashboard

Halaman dashboard pada Gambar 8 berfungsi sebagai pusat kendali administratif untuk manajemen konten berita TV. Melalui antarmuka ini, admin memiliki akses penuh untuk melakukan operasi CRUD (*Create, Read, Update, Delete*), yang meliputi penambahan, pengubahan, dan penghapusan berbagai kategori konten publikasi secara dinamis.

3 . 2 Pembahasan

Implementasi sistem keamanan lapis kedua berupa *Multi-Factor Authentication* (MFA) berbasis *One-Time Password* (OTP) pada CMS Portal Berita INTV membawa perubahan signifikan terhadap perlindungan panel administratif. Mekanisme login konvensional yang awalnya bersifat tunggal (*single authentication*) dan bergantung pada kata sandi statis telah ditingkatkan menjadi ekosistem autentikasi yang dinamis dan adaptif [16]. Integrasi komponen arsitektur sistem pada Gambar 4 menjabarkan koordinasi yang terstruktur antara lapisan *Controller* dan basis data (*Models*). Ketika admin melakukan proses login awal melalui antarmuka pada Gambar 6, kata sandi statis yang dimasukkan langsung dicocokkan dengan rekaman pada tabel Admin. Peningkatan keamanan mendasar di sisi basis data diwujudkan melalui penggunaan algoritma *hashing* Bcrypt [17]. Algoritma Bcrypt memiliki keunggulan komparatif dibanding algoritma *fixed-length* tradisional seperti MD5 [18], [19]. Keberadaan fitur *salt* otomatis dan sifatnya yang adaptif (*work factor*) membuat data kredensial di dalam database sangat tangguh dari ancaman serangan berbasis *rainbow table* maupun *offline brute-force*. Setelah enkripsi utama tervalidasi, sistem tidak langsung memberikan hak akses melainkan mengalihkan pengguna ke halaman verifikasi dua langkah (Gambar 6 (b)). Penggunaan dua jalur alternatif, yaitu pesan instan WhatsApp melalui gerbang API Fonnte (Gambar 7 (a)) dan surat elektronik melalui SMTP PHPMailer (Gambar 7 (b)), memberikan fleksibilitas fungsionalitas bagi admin. Berdasarkan hasil uji coba operasional, sistem berhasil memvalidasi hak akses admin secara *real-time*. Efisiensi performa pengiriman data kuantitatif dari kedua jalur transmisi tersebut dijabarkan pada tabel berikut:

| Tabel 5 Efisiensi Pengguna |                            |                          |                     |
|----------------------------|----------------------------|--------------------------|---------------------|
| Jalur Transmisi OTP        | Rata-Rata Waktu Pengiriman | Durasi Batas Kadaluwarsa | Status Keberhasilan |
| API Fonnte (WhatsaApp)     | 1 hingga 3 detik           | 5 menit (300 detik)      | 100% Sukses         |
| PHPMailer (Email)          | 3 hingga 5 detik           | 5 menit (300 detik)      | 100% Sukses         |

Data di atas menunjukkan bahwa pengiriman kode verifikasi 6-digit numerik melalui API Fonnte memiliki respons yang lebih cepat (1–3 detik) dibandingkan dengan jalur SMTP PHPMailer (3–5 detik). Hal ini mengonfirmasi studi terdahulu oleh Manik dkk. (2025) yang



menyatakan bahwa integrasi WhatsApp OTP via Fonnte menyajikan respons yang cepat serta andal untuk mencegah akses tidak sah [12], [20].

Dari aspek manajemen risiko, penetapan durasi kedaluwarsa kode OTP selama 5 menit (Gambar 7 (a) dan (b)) bertindak sebagai baris pertahanan perimeter temporal. Jendela waktu yang singkat ini memastikan bahwa jika kode dicegat oleh pihak ketiga, kode tersebut akan hangus dan tidak dapat dieksploitasi kembali.

Temuan dalam penelitian ini berhasil menjawab tujuan awal yang diuraikan pada pendahuluan. Portal berita INTV kini memiliki perlindungan penuh dari potensi pengambilalihan akun ilegal (*account takeover*), modifikasi konten tidak sah (*defacing*), dan kebocoran informasi internal. Keterbaruan (*novelty*) dari sistem ini terletak pada fleksibilitas *multi-channel* OTP (WhatsApp dan Email) yang berjalan di atas PHP Native, sehingga komputasi sistem menjadi lebih ringan tanpa mereduksi efisiensi operasional kehumasan perusahaan. Namun demikian, keterbatasan sistem ini adalah ketergantungan penuh terhadap stabilitas koneksi internet lokal di area operasional TV serta ketersediaan kuota kupon layanan pada server pihak ketiga (Fonnte API).

#### **4. Kesimpulan**

Berdasarkan hasil rancang bangun, implementasi, dan pengujian yang telah dilaksanakan pada CMS Portal Berita INTV, maka dapat ditarik kesimpulan strategis yaitu penelitian ini telah berhasil memodernisasi sekaligus mengamankan panel administrasi publikasi digital portal berita INTV melalui penerapan *Multi-Factor Authentication* (MFA) berlapis berbasis *One-Time Password* (OTP) dan enkripsi basis data menggunakan algoritma Bcrypt.

Implementasi opsi dual-transmisi kode verifikasi memberikan hasil kinerja yang responsif dan bernilai keberhasilan 100%, dengan rata-rata waktu pengiriman via WhatsApp API Fonnte selama 1 hingga 3 detik dan via SMTP PHPMailer selama 3 hingga 5 detik, serta diproteksi oleh batas kedaluwarsa kode maksimal selama 5 menit.

Penerapan sistem baru ini terbukti efektif mengeliminasi kerentanan kata sandi statis dari ancaman siber pengambilalihan akun secara ilegal, sekaligus berhasil mengoptimalkan efisiensi dan produktivitas kerja kehumasan dalam mengelola konten berita secara mandiri dan dinamis. Diharapkan pada penelitian selanjutnya dapat mengembangkan metode autentikasi yang lebih aman, efisien dan ramah pengguna.

#### **5. Referensi**

- [1] H. Gilang Setyo Nugroho, "Rancang Bangun Portal Berita Berbasis Multimedia Dengan Waterfall," *Journal Computer Science*, vol. 1, no. 2, 2022.
- [2] S. Winda Kustiawan, A. Dwi Kinanti, M. Hafizh Rafi, R. Nadiyah Siregar, K. Tariq Sitorus, and U. Islam Negeri Sumatera Utara, "SEJARAH PERKEMBANGAN JURNALISTIK," 2025. [Online]. Available: <https://ejournals.com/ojs/index.php/>
- [3] M. Mustamin, ) Mahdar, ) Abdul, and S. Menungsa, "TRANSFORMASI MEDIA CETAK KE MEDIA DIGITAL (STUDI PADA HARIAN RAKYAT SULTRA)," Hal, 2025. [Online]. Available: <https://jurnal.unusultra.ac.id/index.php/jisdik>
- [4] D. Nur Diana, M. Amin, and M. Zeinudin, "ANALISIS KRIMINOLOGIS DEFACING DALAM BENTUK CYBER CRIME," 2023.
- [5] Mochamad Ramdani, "Pentingnya Kesadaran Mengenai Keamanan Data dan Cara untuk Menjaga Keamanan Data," Kementrian Keuangan.
- [6] F. Maulana, Y. Hendra, P. Sakinah, Y. Septi Eirlangga, and A. Qurrata Ayun, "Efektivitas dan Kelemahan Autentikasi Berbasis Web Menggunakan One-Time Password (OTP) dalam Mencegah Akses Tidak Sah," vol. 12, no. 3, 2025.
- [7] A. Azkiya *et al.*, "Analisis Sistem Autentikasi Dua Faktor (2FA) Dan Efektivitasnya Dalam Meningkatkan Keamanan Akses," 2026.
- [8] S. Eko Prasetyo and A. Mindy, "Implementasi Multi-Factor Authentication Pada Aplikasi Berbasis Website dan Pengembangan Company Profile PT Raflesia Berjaya Properti,"

- Jurnal Pengabdian Masyarakat Indonesia*, vol. 1, no. 6, pp. 86–93, 2024, doi: 10.62017/jpmi.
- [9] W. A. A. Azhar, “Sistem Keamanan pada Halaman Login menggunakan One Time Password,” Nov. 2020.
- [10] I. H. Cahyadi, M. A. Hidayatullah, and S. N. Ramdan, “PERANCANGAN SISTEM OTENTIKASI BERBASIS ONE TIME PASSWORS (OTP) DENGAN ALGORITMA RSA SEBAGAI METODE AUTENTIKASI: IMPLEMENTASI MENGGUNAKAN BAHASA PEMROGRAMAN PHYTON.”
- [11] “Apa itu Kode OTP, Fungsi, Jenis dan Perbedaannya dengan PIN,” BankMas.
- [12] A. R. Manik, D. Kiswanto, M. B. Akbar, and J. Purba, “Academic Portal with MFA (WhatsApp OTP via Fonnte), Role-Based Access Control, and Logging System for Network Monitoring,” *Jurnal Ilmiah Sistem Informasi*, vol. 4, no. 3, pp. 674–687, Nov. 2025, doi: 10.51903/qwz6pt87.
- [13] “Mengetahui Metode Prototype Kelebihan Dan Kekurangan.”
- [14] S. W. Ramdany, S. Aulia Kaidar, B. Aguchino, C. Amelia, A. Putri, and R. Anggie, “Penerapan UML Class Diagram dalam Perancangan Sistem Informasi Perpustakaan Berbasis Web.”
- [15] W. A. A. Azhar, “Apa itu UML? Beserta Pengertian dan Contohnya,” Dicoding.
- [16] A. Azkiya *et al.*, “Analisis Sistem Autentikasi Dua Faktor (2FA) Dan Efektivitasnya Dalam Meningkatkan Keamanan Akses,” 2026.
- [17] D. S. M. T. J. A. Q. K. Khairunnisak Nur Isnainia1, “Teknik Bcrypt Hashing Password,” Jan. 2025.
- [18] F. Raihan, R. Renaldy, H. R. Putra, and K. Kunci, “SISTEM KEAMANAN DATA WEB LAYANAN KESEHATAN DENGAN METODE MULTI FACTOR AUTHENTICATION (MFA) DAN ALGORITMA HASHING MD5,” *Science And Engineering National Seminar*, vol. 9, no. 9, 2024.
- [19] G. Husni Editya and S. Mulyati, “APLIKASI MOBILE ONE TIME PASSWORD MENGGUNAKAN ALGORITMA MD5 DAN SHA1 UNTUK MENINGKATKAN KEAMANAN WEBSITE,” 2018.
- [20] M. Naufal, “IMPLEMENTASI KEAMANAN LOGIN DENGAN METODE ONE TIME PASSWORD (OTP) MENGGUNAKAN FUNGSI HASH ALGORITMA SHA-512,” 2018.