Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2026, IX (4): 5958 – 5962 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

IMPLEMENTASI TWO-FACTOR AUTHENTICATION PADA SISTEM INFORMASI KEUANGAN KAMPUNG BERBASIS WEB

Irvandi Reinal Ambui[1], Desmin Tuwohingide[2], Alfrianus Papuas[3], Miske Silangen[4]
Politeknik Negeri Nusa Utara, Sulawesi Utara
e-mail: [1]irvandiambui@gmail.com

Abstract: *Information security plays a crucial role in protecting the village (kampung) financial information system that manages budgeting, funding sources, planning, and reporting. Authentication mechanisms relying solely on usernames and passwords remain vulnerable to credential theft and unauthorized access. This study aims to implement Two-Factor Authentication (2FA) using Google Authenticator in a web-based Kampung Financial Information System. The system was developed using the Waterfall software development methodology. The system is integrated with a two-step verification procedure, specifically requiring that any financial data to be published to the public must first be verified by the kampung authority, namely the Head of the Kampung (Kepala Kampung). Functional testing was conducted using the Black Box Testing method to evaluate authentication and authorization features. The results indicate that the application of 2FA significantly minimizes the risk of unauthorized access and ensures data integrity before publication without reducing system usability.*

Keyword: *google authenticator; role-based access control; sistem informasi keuangan desa; two-factor authentication; website.*

Abstrak: Keamanan sistem informasi memegang peranan krusial dalam melindungi sistem informasi keuangan kampung yang mengelola penganggaran, sumber dana, perencanaan, hingga pelaporan. Autentikasi yang hanya mengandalkan kombinasi username dan password sangat rentan terhadap pencurian kredensial dan akses tidak sah. Penelitian ini bertujuan mengimplementasikan Two-Factor Authentication (2FA) menggunakan Google Authenticator ke dalam Sistem Informasi Keuangan Kampung berbasis web. Sistem dikembangkan menggunakan metode Waterfall. Sistem terintegrasi dengan prosedur alur verifikasi dua tahap, di mana secara spesifik setiap data keuangan yang akan dipublikasikan kepada masyarakat wajib diverifikasi terlebih dahulu oleh otoritas kampung, yaitu Kepala Kampung. Pengujian dilakukan menggunakan metode Black Box Testing terhadap fungsionalitas autentikasi dan otorisasi. Hasil penelitian menunjukkan penerapan 2FA secara signifikan meminimalisir risiko akses tidak sah dan menjamin integritas data sebelum publikasi tanpa mengurangi kemudahan penggunaan.

Kata kunci: google authenticator; role-based access control; sistem informasi keuangan desa; two-factor authentication; website.

PENDAHULUAN

Pemanfaatan sistem informasi berbasis web memberikan kemudahan krusial dalam mengelola administrasi pemerintahan kampung, khususnya tata kelola keuangan yang mencakup pendataan sumber dana, pengesahan anggaran (APBKam), hingga penerbitan laporan keuangan (Fauzi & Suwanda 2022). Penerapan e-government di tingkat kampung ini secara signifikan mendorong tingkat transparansi kinerja. Namun, di sisi lain, digitalisasi ini memunculkan tantangan baru terkait keamanan siber (Kusuma & Ayu 2020; Nugroho & Ratnasari 2021). Sistem ini menyimpan data-data keuangan yang sensitif dan memiliki risiko hukum jika termanipulasi, sehingga memerlukan perlindungan

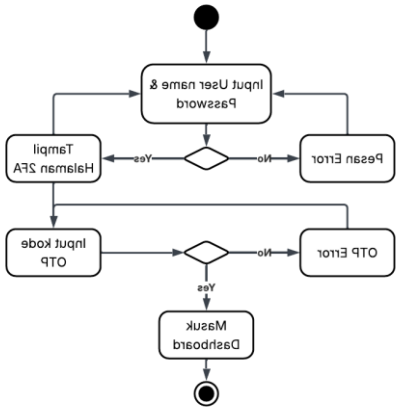
ekstra.

Pada banyak sistem saat ini, proses autentikasi administrator masih mengandalkan kombinasi username dan password sebagai metode verifikasi tunggal (Single-Factor Authentication). Mekanisme dasar ini terbukti memiliki berbagai kelemahan mendasar karena sangat rentan terhadap pencurian kredensial, serangan brute force, maupun manipulasi informasi oleh pihak tidak berwenang (Anwar & Setiawan 2022; Putra & Ramadhan 2020). Untuk menutupi celah keamanan tersebut, diperlukan mekanisme verifikasi tambahan yang mengikat identitas pengguna dengan perangkat fisik yang dimilikinya. Solusi yang diimplementasikan dalam penelitian ini adalah prosedur verifikasi dua tahap atau Two-Factor Authentication (2FA), yang mengombinasikan kata sandi statis dengan One-Time Password (OTP) yang bersifat dinamis (Irawan & Putra 2019). Sistem ini memanfaatkan Google Authenticator yang menghasilkan OTP berbasis algoritma Time-Based One-Time Password (TOTP) (Hidayat & Wibowo 2021; Rahman & Hartono 2020). Selain penguatan di sektor autentikasi, sistem ini juga mengikat otorisasi pengguna melalui penerapan Role-Based Access Control (RBAC) (Hakim & Mulyanto 2019). Integrasi antara 2FA dan RBAC ini secara khusus difokuskan pada pengamanan alur persetujuan (verifikasi berjenjang), untuk memastikan bahwa setiap rincian data keuangan kampung harus terlebih dahulu diverifikasi oleh otoritas tertinggi (Kepala Kampung) sebelum diizinkan terpublikasi kepada masyarakat luas (Santoso & Yulianto 2020; Ningsih & Pratama 2021).

METODE

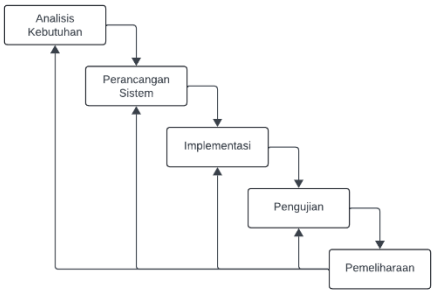
Penelitian ini menggunakan metode pengembangan perangkat lunak Waterfall yang sistematis, meliputi tahapan analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan (Prasetyo & Astuti 2022; Iqbal & Pratama 2020). Hasil analisis kebutuhan di Kantor Kampung Taloarane menunjukkan urgensi mekanisme verifikasi dua tahap (2FA) untuk mengatasi kelemahan autentikasi konvensional dan mengamankan alur publikasi data.

Pada tahap perancangan, hak akses pengguna dipetakan secara kaku menggunakan konsep RBAC menjadi Super Admin, Bendahara, Sekretaris Kampung, dan Kepala Kampung (Syah & Pahlavi 2021). Dirancang pula mekanisme verifikasi dua tahap yang mengamankan dua pintu utama: pintu masuk aplikasi (login) dan pintu persetujuan data. Validasi kredensial awal (kata sandi) wajib dilanjutkan dengan verifikasi OTP dari Google Authenticator sebelum pengguna dapat mengakses area administratif (dashboard). Alur keamanan ini digambarkan dalam Activity Diagram berikut:



Gambar 1 Activity Diagram Login 2FA.

Tahapan pengembangan perangkat lunak secara keseluruhan diilustrasikan pada gambar di bawah ini:

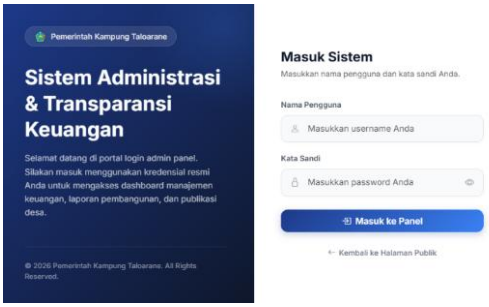


Gambar 2 Tahapan Metode Waterfall

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2026, IX (4): 5958 – 5962 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

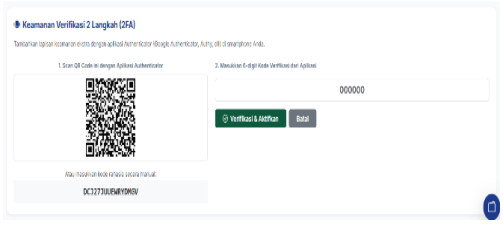
HASIL DAN PEMBAHASAN

Halaman login merupakan gerbang utama autentikasi. Pengguna memasukkan username dan password yang kemudian diverifikasi dengan data terenkripsi di dalam database. Apabila kredensial tahap pertama ini berhasil, sistem akan menahan akses menuju dashboard dan mengarahkan pengguna ke halaman verifikasi 2FA.



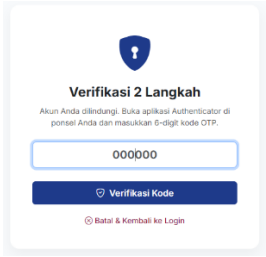
Gambar 3 Halaman Login

Implementasi keamanan ekstra ini memanfaatkan Google Authenticator berbasis algoritma TOTP. Sebelum fitur dapat digunakan, administrator administrator harus meregistrasi secret key dengan memindai QR Code yang di-generate oleh sistem seperti pada Gambar 4.



Gambar 4 QR Code Google Authenticator

Setelah registrasi berhasil, aplikasi seluler akan menghasilkan 6 digit kode OTP yang otomatis berubah setiap 30 detik. Pengguna wajib memasukkan kode tersebut pada halaman verifikasi. Jika kode valid, akses diberikan. Namun, jika kode salah atau sudah melewati batas waktu (kedaluwarsa), sistem secara tegas menolak login dan meminta kode baru (Gambar 5). Lapisan ini menjamin akun tetap terlindungi meski password utama berhasil diketahui pihak lain.

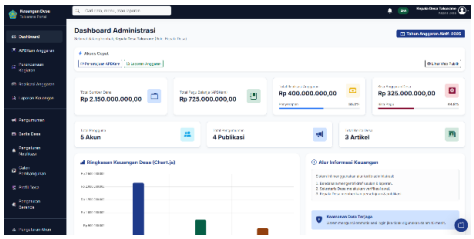


Gambar 5 Halaman Input OTP

Sistem menerapkan hierarki pembagian peran yang ketat (RBAC) untuk mengatur hak akses pengguna sesuai dengan peran masing-masing. Penerapan 2FA dalam sistem ini bukan sekadar mengamankan pintu masuk (login), melainkan dititikberatkan pada alur persetujuan sebelum data keuangan kampung dipublikasikan. Empat jenis pengguna yang diterapkan pada sistem terdiri atas Super Admin, Bendahara, Sekretaris Kampung, dan Kepala Kampung.

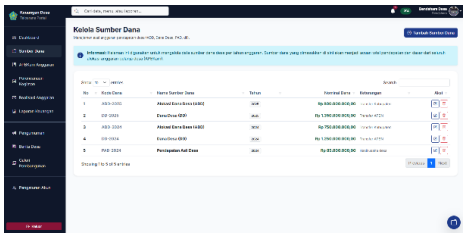
Pengujian dilakukan menggunakan metode Black Box Testing yang difokuskan pada uji fungsional fitur autentikasi, batas waktu kedaluwarsa OTP, dan otorisasi pengguna dalam memverifikasi data (Jaya (2018). Hasil pengujian membuktikan proses persetujuan dan login mutlak tidak dapat diselesaikan tanpa kode OTP yang valid, membuktikan mekanisme 2FA jauh lebih kuat dibanding password saja tanpa mengorbankan kenyamanan sistem.

Otoritas dan batasan hak akses dari masing-masing peran tersebut diterapkan pada antarmuka sistem yang berbeda-beda. Tampilan antarmuka untuk Kepala Kampung dapat dilihat pada Gambar 6, sedangkan halaman utama untuk Bendahara, Super Admin, dan Sekretaris Kampung disajikan secara berturut-turut pada Gambar 7, Gambar 8, dan Gambar 9.

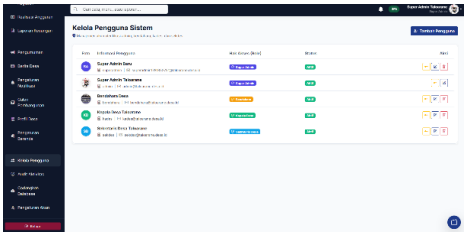


Gambar 6 Halaman Kepala Desa

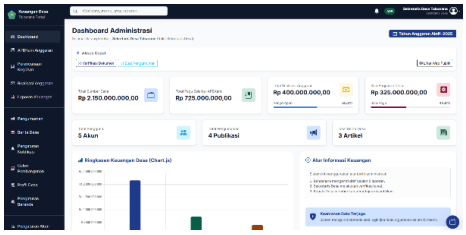
Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2026, IX (4): 5958 – 5962 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



Gambar 7 Halaman Bendahara.



Gambar 8 Halaman Super Admin



Gambar 9 Halaman Sekretaris Desa

SIMPULAN

Penelitian ini berhasil mengimplementasikan Two-Factor Authenticator (2FA) menggunakan Google Authenticator pada Sistem Informasi Keuangan Kampung berbasis web sebagai mekanisme keamanan tambahan. Penerapan autentikasi dua faktor mewajibkan pengguna memasukkan One-Time Password (OTP) dinamis setelah memverifikasi username dan password. Terintegrasi dengan mekanisme Role-Based Access Control (RBAC), sistem ini mampu secara efektif membatasi akses sesuai kewenangan dan memblokir risiko akses tidak sah. Implementasi 2FA (verifikasi dua tahap) ini sangat membantu dalam meningkatkan keamanan informasi dan meminimalisir kesalahan data (khususnya data keuangan) yang ter-publish. Hasil Black Box Testing mengonfirmasi bahwa seluruh skenario autentikasi dan verifikasi berjenjang berjalan optimal tanpa mengurangi kemudahan penggunaan aplikasi.

DAFTAR PUSTAKA

Anwar, K., & Setiawan, D. (2022). Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking. *Jurnal Media Informatika Budidarma*, *6*(1), 101–110.

Fauzi, R. A., & Suwanda, H. (2022). Sistem Informasi Manajemen Hibah Internal Berbasis Web Menggunakan Adaptasi Metode Research and Development. *Jurnal SMARTCOMP*, *11*(1), 55–63.

Hakim, L., & Mulyanto, E. (2019). Desain dan Implementasi Hak Akses Bertingkat Menggunakan Role-Based Access Control pada Aplikasi Web. *Jurnal Informatika Terpadu*, *5*(2), 88–96.

Hidayat, R., & Wibowo, S. (2021). Implementasi Keamanan Sistem Informasi Menggunakan Two-Factor Authentication (2FA) Berbasis Algoritma Time-Based One-Time Password (TOTP). *Jurnal Teknik Informatika Dan Sistem Informasi (JATISI)*, *8*(3), 1120–1135.

Iqbal, M., & Pratama, F. (2020). Penerapan Metode Waterfall Pada Pengembangan Sistem Informasi Berbasis Web. *Jurnal Teknik Informatika (JUTIF)*, *1*(2), 71–78.

Irawan, D., & Putra, M. Y. (2019). Analisis Keamanan Login System dengan Menggunakan Mekanisme One-Time Password (OTP). *Jurnal Sistem Informasi Dan Komputer (JUSIKOM)*, *5*(1), 77–85.

Jaya, T. S. (2018). Pengujian Aplikasi dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung). *Jurnal Informatika: Jurnal Pengembangan IT*, *3*(1), 45–48. https://doi.org/10.30591/jpit.v3i1.647

Kusuma, H., & Ayu, T. (2020). Aplikasi

Sistem Informasi Keuangan Desa Berbasis Web. *Jurnal Sistem Informasi Dan Teknologi (Sisfotek)*, *4*(2), 115–124.

Ningsih, S., & Pratama, A. (2021). Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning. *Jurnal Sains Teknologi Dan Sistem Informasi (SATESI)*, *1*(2), 34–42.

Nugroho, W., & Ratnasari, D. (2021). Penerapan Sistem Keuangan Desa Dalam Pengelolaan Keuangan Desa. *Jurnal Akuntansi Dan Keuangan Desa*, *2*(1), 40–49.

Prasetyo, B., & Astuti, A. (2022). Pengaruh Sistem Informasi Keuangan Desa (SISKEUDES) Terhadap Kinerja Kepala Desa. *Indonesian Journal on Information System (IJIS)*, *7*(1), 10–18.

Putra, A., & Ramadhan, S. (2020). Penyedia Pengamanan Login Pada Sistem Informasi Menggunakan Timed Based One Time Password. *Jurnal Informatika JTINFO*, *5*(1), 22–30.

Rahman, F., & Hartono, B. (2020). Penerapan Google Authenticator Sebagai Lapisan Keamanan Tambahan Pada Aplikasi Berbasis Web. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(2), 245–251.

Santoso, T., & Yulianto, B. (2020). Role-Based Access Control (RBAC) untuk Sistem Otorisasi Terpusat Berbasis Web. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(2), 110–118.

Syah, M. H., & Pahlavi, R. (2021). Enhancing Network Security in Web Applications with Role-Based Access Control. *Journal of Information Systems and Informatics*, *3*(3), 305–315