Rancang Bangun Website Pengamanan Database *E-Voting* dengan Menerapkan Algoritma *Rivest Shamir Adleman* (RSA)

Danis Setiawan[1)], Andrianingsih[2)], Gatot Soepriyono[3)]

[1)2)3)] Program Studi Informatika, Universitas Nasional
[*)]Correspondence Author: danissetiawan2019@student.unas.ac.id, Jakarta, Indonesia
DOI: https://doi.org/10.37012/jtik.v9i2.1687

Abstrak

Algoritma *Rivest Shamir Adleman* (RSA) dapat diterapkan pada sistem pemungutan suara elektronik untuk mengenkripsi informasi pemilih dan hasil pemilu sehingga hanya orang yang berwenang yang dapat mengaksesnya. Ini dapat membantu menjaga kerahasiaan informasi pemilih dan mencegah manipulasi data pemilu. Metode Agile baik untuk proyek yang membutuhkan fleksibilitas dan kemampuan menyesuaikan diri dengan perubahan. Untuk menggunakan kriptografi algoritma kunci asimetris RSA, ada tiga langkah utama yang dilakukan, yaitu pembangkitan kunci dan operasi enkripsi dan dekripsi. Karena algoritma ini termasuk algoritma asimetris yang menggunakan kunci enkripsi dan kunci dekripsi, data yang dikirim antara pengguna dan server dienkripsi dengan kunci publik dan kunci privat, sehingga hanya dapat didekripsi dengan kunci yang disimpan oleh pengguna sendiri di server. Salah satu metode pengujian keamanan yang dikenal sebagai pengujian *brute force* bertujuan untuk mencoba semua kombinasi password atau kunci enkripsi yang mungkin untuk mendapatkan akses yang tidak sah. Pengujian yang melibatkan alat seperti OWASP ZAP dan *BurpSuite* menemukan kerentanan keamanan seperti *SQL injection* dan *Cross-Site Scripting* (XSS). Penelitian ini berhasil mengembangkan situs web E-Voting yang melindungi data dengan menggunakan algoritma RSA. Sistem ini memungkinkan pemilih untuk melakukan pemilihan elektronik dengan aman dan efektif. Website evoting harus dipantau secara teratur untuk mencegah serangan keamanan yang dapat merusak kerahasiaan dan integritas data pemilih.

Kata Kunci: Algoritma RSA, Metode Agile, Pengujian BurpSuite dan OWASP ZAP, Keamanan Data

Abstract

Rivest Shamir Adleman's Algorithm (RSA) can be applied to electronic voting systems to encrypt voter information and election results so that only authorized people can access them. This can help keep voter information confidential and prevent manipulation of election data. Agile methods are good for projects that require flexibility and the ability to adapt to change. To use the RSA asymmetric key algorithm cryptography, there are three main steps carried out, namely key generation and encryption and decryption operations. Because this algorithm is an asymmetric algorithm that uses an encryption key and a decryption key, data sent between the user and the server is encrypted with a public key and a private key, so that it can only be decrypted with the key stored by the user himself on the server. One of the security testing methods known as brute force testing aims to try all possible combinations of passwords or encryption keys to gain unauthorized access. Testing involving tools such as OWASP ZAP and BurpSuite discovered security vulnerabilities such as SQL injection and Cross-Site Scripting (XSS). This research succeeded in developing an E-Voting website that protects data using the RSA algorithm. This system allows voters to conduct electronic voting safely and effectively. Voting websites must be monitored regularly to prevent security attacks that could damage the confidentiality and integrity of voter data.

Keywords: *RSA Algorithm, Agile Method, BurpSuite and OWASP ZAP Testing, Data Security*

PENDAHULUAN

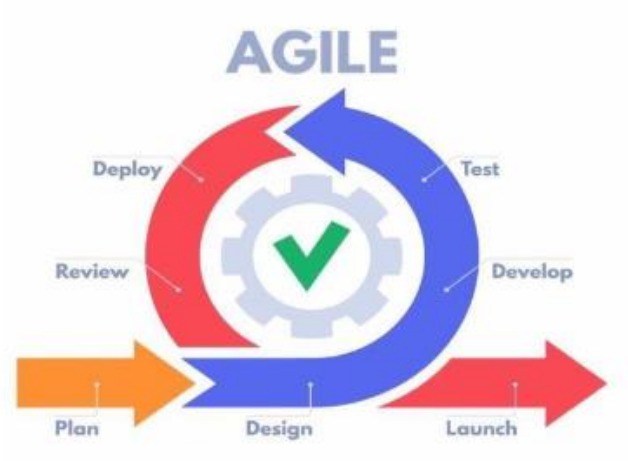
Perkembangan teknologi yang pesat terjadi di berbagai bidang dan kehidupan, seperti transportasi, komunikasi, kesehatan, pendidikan dan bidang lainnya dimana masyarakat semakin membutuhkan teknologi untuk mempermudah kehidupannya (Sitorus & Antonieta DC, 2022). Misalnya sistem pengambilan keputusan yang dapat mendukung pengambilan keputusan sehingga masalah dapat diselesaikan sesuai dengan maksud dan tujuan (Nabilah & Amrozi, 2019). Dalam perusahaan atau organisasi, sistem informasi dituntut untuk menghasilkan informasi yang cepat dan akurat.

Pemungutan suara elektronik (*e-voting*) secara umum dipahami sebagai penggunaan teknologi informasi dalam pemungutan suara, khususnya pemungutan suara elektronik, untuk mengurangi biaya pemilihan dan mempercepat pengumpulan data. Hal ini penting terutama untuk kegiatan mediasi yang biasanya masih dilakukan secara manual, baik dalam skala terkecil maupun terbesar. Dengan voting online, diharapkan anggota organisasi dapat mengakses dan memilih calon ketua dimanapun tanpa harus datang langsung ke tempat pemungutan suara (Siahaan & Irmada, 2021). Berdasarkan hal tersebut maka tujuan dari penelitian ini adalah untuk membantu pemangku kepentingan dalam mengambil keputusan secara cepat dan percaya diri dengan menggunakan metode identifikasi pengguna (Zulkiawan et al., 2020).

Enkripsi terdiri dari 2 (dua) bagian penting yaitu enkripsi dan dekripsi. Enkripsi adalah proses pencampuran pesan asli ke dalam pesan lain yang tidak dapat diuraikan seperti pesan aslinya. Meskipun deskripsi itu sendiri berarti bahwa pesan terenkripsi diubah menjadi pesan aslinya (Murdowo, 2017). Algoritma enkripsi RSA merupakan algoritma asimetris dimana kunci yang digunakan untuk enkripsi disebut kunci publik dan kunci yang digunakan untuk dekripsi disebut kunci privat. Menggunakan algoritma RSA cukup aman karena sulit menghitung bilangan besar sebagai faktor prima. Semakin tinggi angka prima, semakin aman dan baik keamanan data dan informasi. Keamanan merupakan faktor penting dalam sistem pemilu. Metode cadangan dibuat untuk memastikan keamanan data dalam database. Salah satu kemungkinannya adalah dengan menggunakan enkripsi, karena nilai yang disimpan dalam database terenkripsi berbeda dengan nilai dalam database (Kasus et al., 2021).

METODE

Agile development merupakan metode pengembangan perangkat lunak jangka pendek. *Agile development* adalah metode pengembangan yang gesit untuk pengambilan keputusan yang cepat dan akurat, yang menawarkan peluang bagus untuk memproses perubahan sesuai kebutuhan pengguna (Putri et al., 2022). Namun, metode ini juga membutuhkan komitmen yang kuat dari tim pengembangan sistem dan pengguna untuk berkolaborasi dan berkomunikasi secara efektif untuk mencapai hasil yang diinginkan. Di bawah ini adalah gambar yang menjelaskan langkah-langkah metodologi *Agile*:

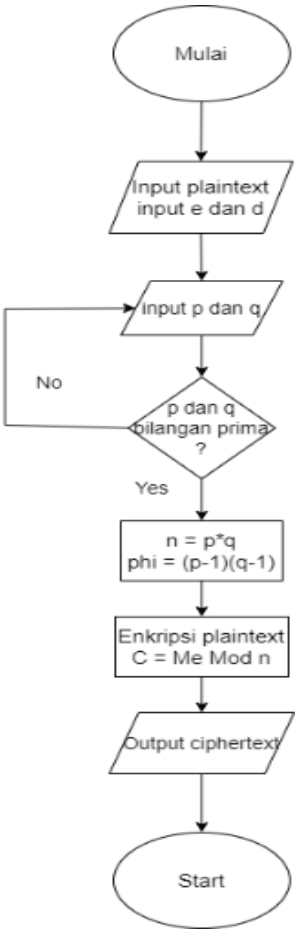


Gambar 1. *Agile Development* (Pristiwanti et al., 2022)

- Desain: Desain sistem berdasarkan kebutuhan yang diidentifikasi. Desain arsitektur sistem, desain basis data, dan desain antarmuka pengguna. Perlu dipertimbangkan penggunaan algoritma RSA untuk keamanan data.
- Perkembangan: Setiap sprint mengembangkan fitur penerapan yang menggunakan algoritma Laravel, MySQL, dan RSA untuk mengenkripsi dan mendeskripsi data sensitif.
- Pengujian: Melakukan pengujian sistem secara menyeluruh untuk memastikan bahwa sistem pemungutan suara berfungsi dengan baik dan memenuhi semua persyaratan yang telah ditentukan.
- Penerapan: Implementasi sistem terintegrasi dengan infrastruktur yang diperlukan seperti web server dan database untuk melakukan pengaturan yang diperlukan termasuk pengaturan akses pengguna.

- Penilaian dan pasca penilaian: Setelah peluncuran produk, tim pengembangan sistem meninjau proses pengembangan sistem yang telah selesai untuk mengidentifikasi kesalahan dan kekurangan serta melakukan perbaikan untuk sprint berikutnya.
- Pengulangan: Proses pengembangan sistem diulangi di setiap sprint hingga proyek selesai.

Proses aplikasi kriptografi algoritma kunci asimetris RSA memiliki proses utama yang terdiri dari pembangkit kunci, operasi enkripsi dan operasi dekripsi. Kunci enkripsi disimpan secara tidak rahasia dan tersedia untuk umum (disebut kunci publik), sedangkan kunci dekripsi bersifat publik (disebut kunci privat) (Hartama et al., 2022). Ada banyak algoritma enkripsi yang tersedia dan terdiri dari dua jenis: *simetris*, yang hanya menggunakan satu kunci rahasia, dan *asimetris* (algoritma kunci publik), yang menggunakan sepasang kunci publik dan rahasia (Sulaiman & Vebu, 2018).

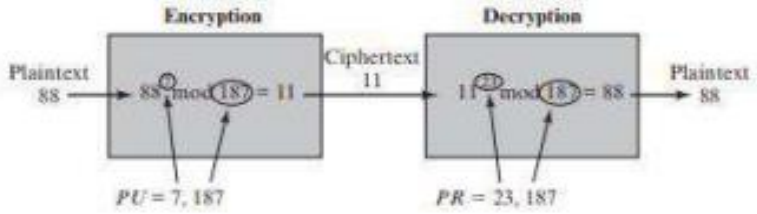


Gambar 2. Proses Pembangkitan Kunci

Pembangkitan kunci melakukan pemfaktoran angka besar ke nilai faktor-faktor prima yang sangat kompleks. Berikut terdapat langkah-langkah untuk pembangkitan kunci RSA:

1. Tentukan bilangan prima $p\ dan\ q$; kedua bilangan prima $p\ dan\ q$, bisa dihasilkan secara random dan ditentukan oleh penerima. Nilai p tidak sama dengan q (p $\neq$ q).
2. Hitung nilai $n = p\ x\ q$; nilai ini diizinkan diketahui oleh publik.
3. Hitung $\mathcal{P}(n) = (p-1)(q-1)$; bilangan ini adalah rahasia.
4. Pilih kunci publik integer e; dengan syarat e wajib memiliki relatif prima terhadap $\mathcal{P}(n)$.
5. Bangkitkan kunci rahasia d; serta persamaan dirumuskan $d = e^{-1} (\text{mod } \mathcal{P}(\text{n}))$.
6. Hasil pembangkitan kunci sebagai berikut:
   - Kunci publik: $PU = \{e, n\}$
   - Kunci rahasia: $PR = \{d, n\}$

Untuk melakukan enkripsi diperlukan nilai kunci publik, nilai modular, dan pesan. Fungsi enkripsi memiliki masukan plaintext sebagai sebuah byte array (M) dan sebuah kunci publik (PU). Sedangkan dekripsi mengubah *ciphertext* dari hasil enkripsi menjadi *plaintext* untuk mendapatkan informasi awal. Proses operasi enkripsi dan operasi dekripsi algoritma RSA ditunjukkan pada gambar 3.



Gambar 3. Enkripsi dan Dekripsi Algoritma RSA (Stallings, 2017)

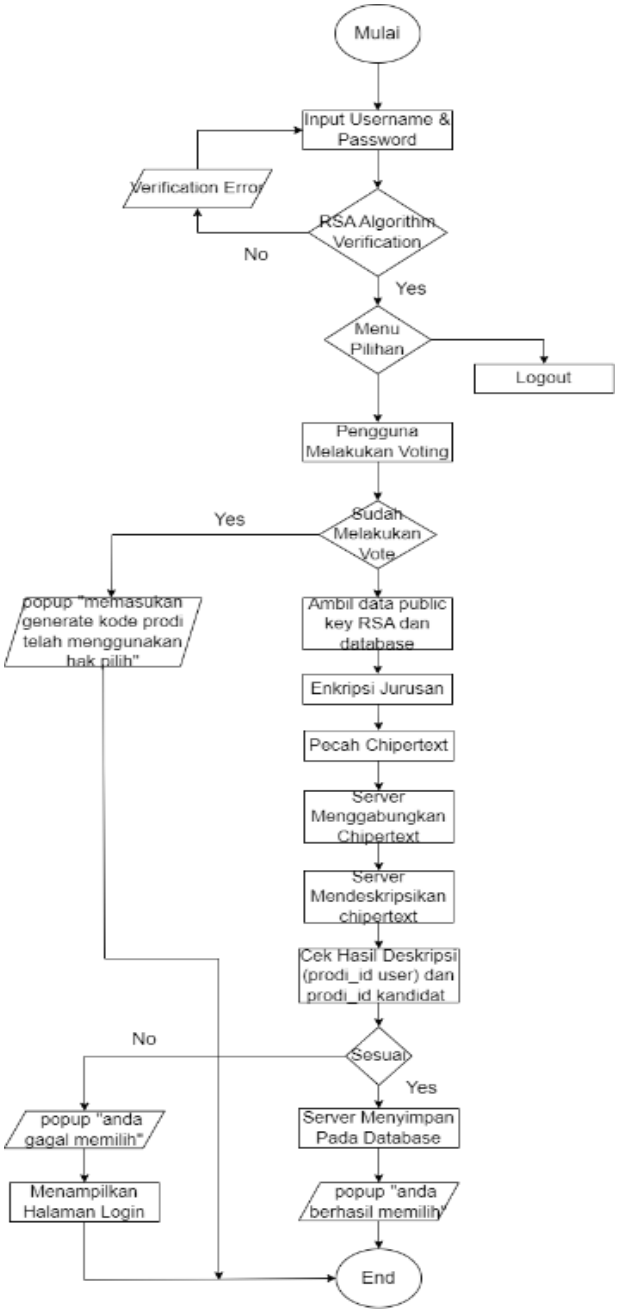
Setelah menyiapkan hal yang diperlukan proses enkripsi dan dekripsi memerlukan rumus untuk menghasilkan output. Selanjutnya tahapan proses yang dilakukan.

Rumus Enkripsi: $C = M^{\text{e}}\ mod$ (1)

Rumus Deskripsi: $M = C^{\text{d}}\ mod\ n = (M^{\text{e}})^{\text{d}} mod\ n = M^{\text{ed}} mod\ n$ (2)

Langkah-langkah proses enkripsi dan dekripsi:

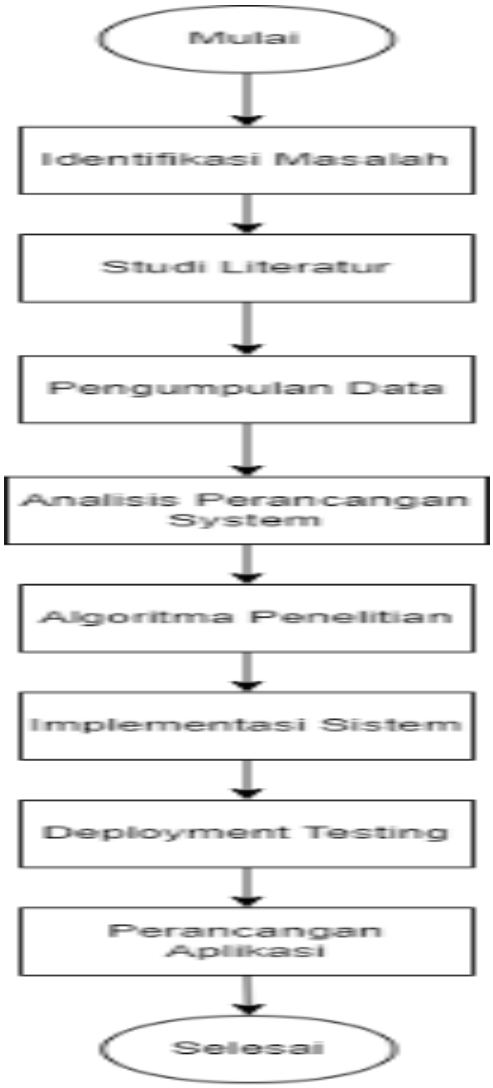
1. Masukkan pesan *plaintext* (M) untuk dienkripsi atau pesan *ciphertext* (C) untuk didekripsi.
2. Masukkan kunci publik (PU) untuk operasi enkripsi, kunci rahasia (PR) untuk dekripsi.
3. Lakukan proses perhitungan enkripsi dan deskripsi.
4. Hasil dari enkripsi adalah pesan *ciphertext* (C) dan dekripsi adalah pesan *plaintext* (M).



Gambar 4. Algoritma Penelitian RSA Pemilihan Calon Ketua

HASIL DAN PEMBAHASAN

Pada penelitian ini akan dilakukan beberapa tahapan tahapan penelitian. Adapun tahapan yang dilakukan pada penelitian ini dapat dilihat pada gambar 4 dibawah ini.



Gambar 5. Tahap-tahap Penelitian

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Wawancara

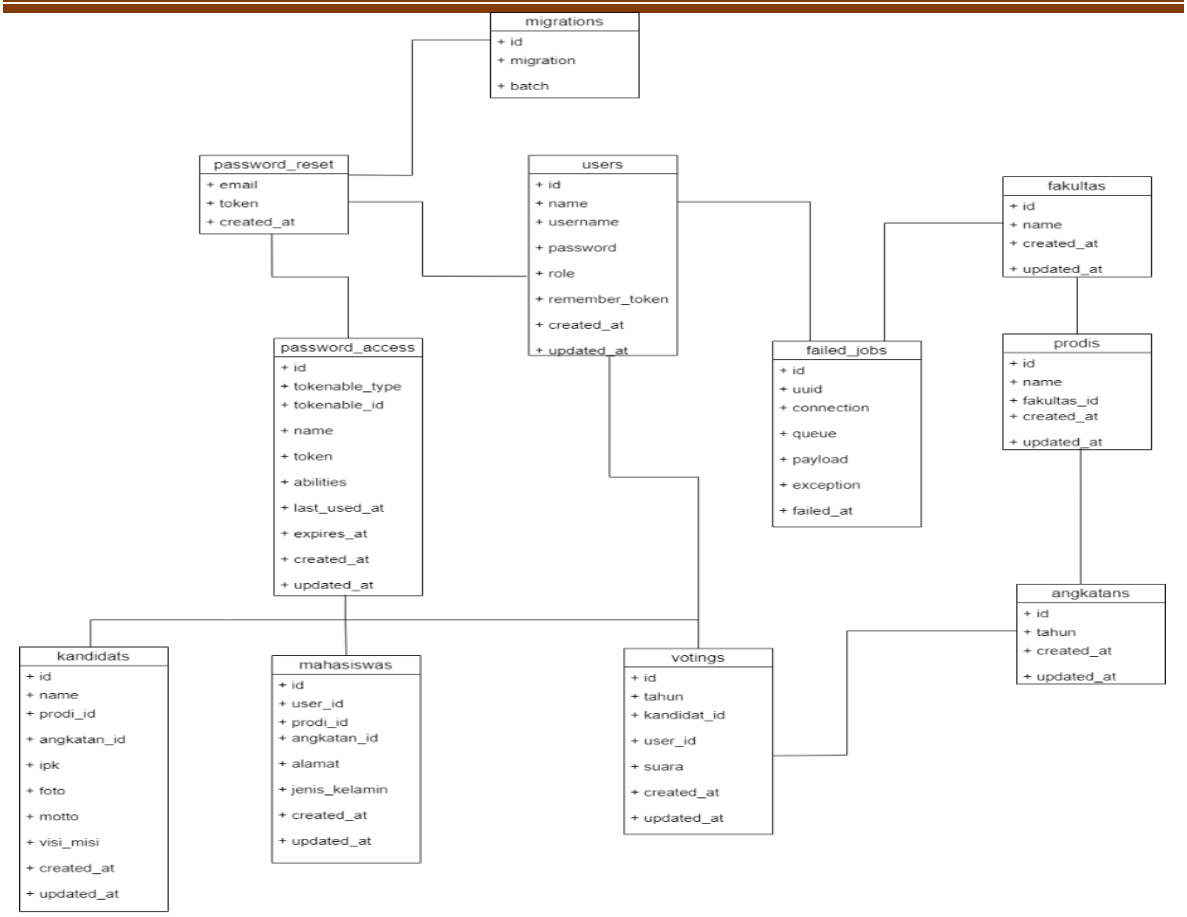
   Metode pengumpulan data ini dilakukan melalui wawancara langsung antara individu yang mengumpulkan data dan sumber data.

2. Studi literatur

Metode pengumpulan data ini melibatkan membaca buku dan majalah untuk mendapatkan informasi yang diperlukan. Peneliti memutuskan untuk melakukan penelitian literatur dengan mengumpulkan buku-buku dan referensi jurnal tentang perancangan sistem pemungutan suara elektronik berbasis web sebagai bahan referensi untuk penelitian ini.

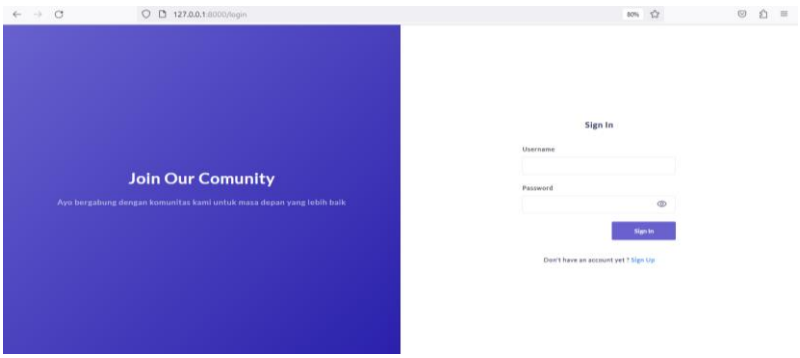
Pada sistem ini post-modelling fungsional dilakukan dengan menggunakan diagram *use case*. Diagram *use case* adalah diagram yang memodelkan perilaku sistem. Setiap diagram *use case* memiliki aktor, *use case* dan *class diagram* (Syarif & Nugraha, 2020).

Gambar 6. *Use Case* Admin dan User



Gambar 7. *Class Diagram* Pemilihan Calon Ketua

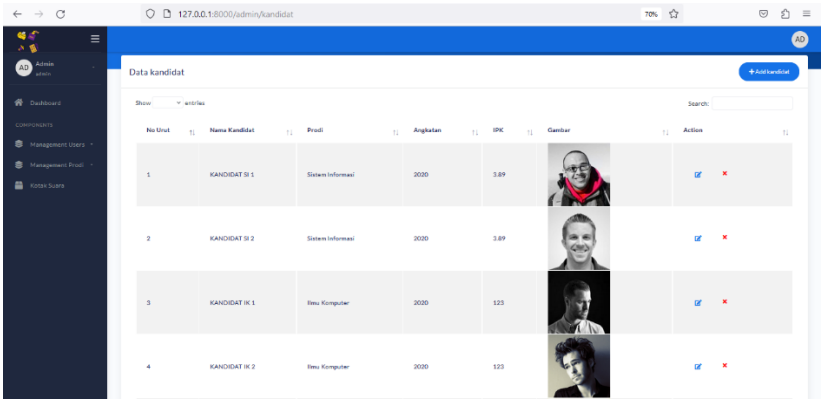
Implementasi sistem voting ini menggunakan bahasa pemrograman Laravel dan MySQL sebagai penyimpanan databasenya. Menggunakan algoritma RSA, data yang dikirim antara pengguna dan server dienkripsi dengan kunci publik yang hanya dapat didekripsi dengan kunci privat yang disimpan di server.



Gambar 8. Halaman Login Administrator

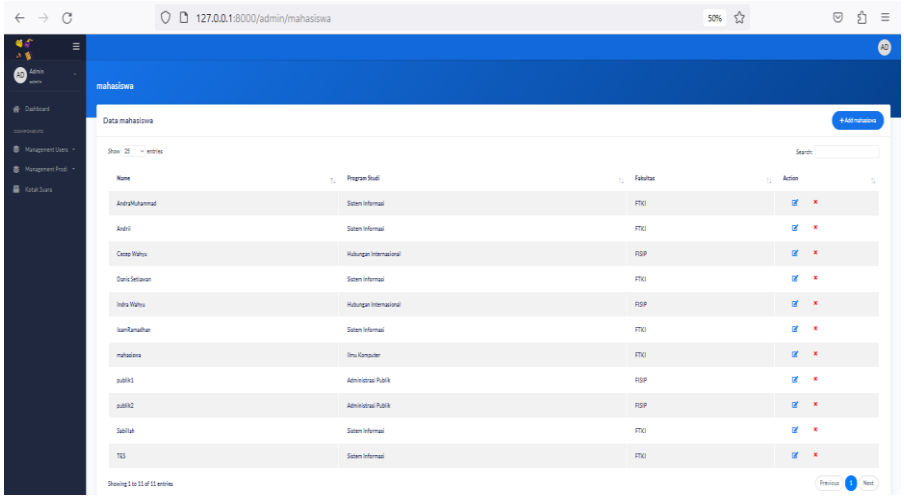
Metode pengamanan sistem pemungutan suara ini mengeksploitasi otentikasi pengguna, sebuah metode untuk mengidentifikasi dan memverifikasi keaslian administrator yang masuk sebelum pemungutan suara, menggunakan fitur *middleware* dari kerangka kerja Laravel yang digunakan untuk menetapkan hak akses.

Halaman informasi kandidat yang memungkinkan administrator untuk melihat, menambah, mengedit, dan menghapus informasi kandidat. Perlu untuk mengimplementasikan fitur keamanan yang memadai dan menyertakan validasi data sebelum menyimpan atau mengedit di database.



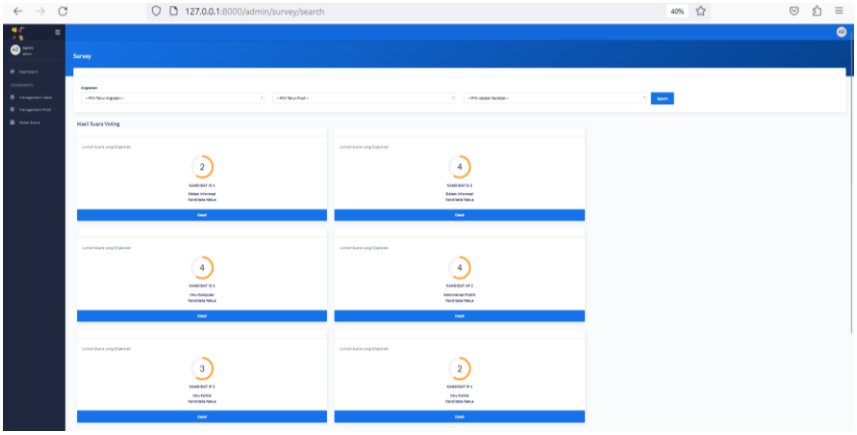
Gambar 9. Menu Informasi Kandidat

Ketika seorang pemilih mendaftar dalam sistem pemungutan suara elektronik, informasi pribadi seperti nama, jenis kelamin, prodi_id, angkatan_id dan alamat akan dikumpulkan dan dimasukkan ke dalam daftar dan digunakan untuk mengenkripsi data pemilih dengan kunci publik RSA sebelum data dikirim ke server.



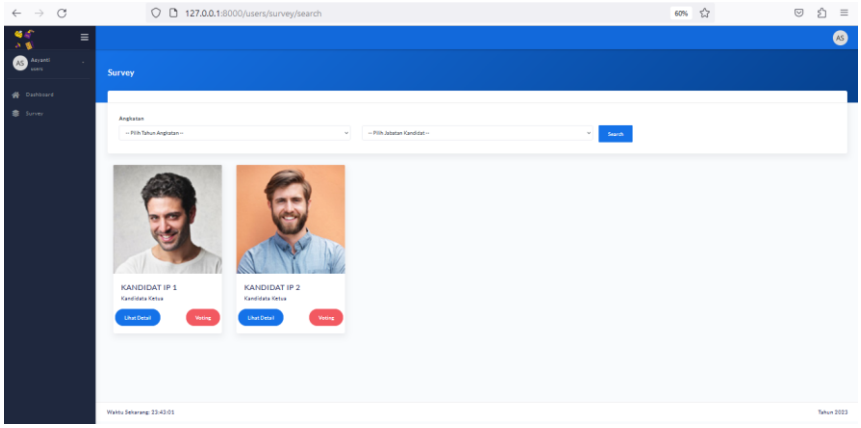
Gambar 10. Halaman Informasi Pemilih

Penerapan algoritma RSA menggunakan Laravel dan MySQL, sisi administrasi sistem pemungutan suara menggunakan metode enkripsi RSA untuk menjamin keamanan informasi pemilih dan hasil pemilu. Halaman ini digunakan untuk melakukan berbagai tugas administratif terkait dengan proses pemilihan, seperti mengelola data angkatan, prodi, jabatan, serta memantau dan mengawasi jalannya proses pemilihan.



Gambar 11. Halaman Admin Pemungutan Suara

Pengguna dapat memilih kandidat dari daftar yang disediakan. Keputusan pemilih disimpan dan dienkripsi dengan aman menggunakan algoritme RSA.



Gambar 12. Halaman Vote Pengguna

Tahapan pengujian OWASP ZAP (*Zed Attack Proxy*) terdiri dari beberapa langkah, termasuk persiapan, menjalankan pengujian, melakukan analisis hasil, dan melakukan perbaikan keamanan. OWASP ZAP juga dapat menghasilkan laporan keamanan yang berisi hasil pengujian, termasuk temuan kerentanan, peringkat risiko, dan saran untuk perbaikan.

OWASP ZAP digunakan untuk menemukan keterangan Anti-CSRF dan Comment saat melakukan pengujian. OWASP ZAP digunakan sebagai alat pengujian keamanan untuk menemukan potensi kerentanan pada aplikasi web, termasuk kerentanan terhadap serangan CSRF dan Comment Injection Anti CSRF (*Cross-Site Request Forgery*) mekanisme keamanan yang digunakan dalam aplikasi web, termasuk Website Evoting, untuk melindungi dari serangan CSRF.

Melakukan pemindaian otomatis pada semua halaman web evoting yang terkait dengan data pemilih menggunakan fitur pemindaian aktif OWASP ZAP. Active Scan akan mengirimkan permintaan GET ke server dan menganalisis tanggapannya untuk mencari kerentanan keamanan yang mungkin. Setelah Active Scan selesai, hasilnya diperiksa untuk memastikan apakah permintaan yang dilakukan memiliki status GET 200 OK.

Hasil pengujian menunjukkan bahwa tags AntiCSRF dipasang pada halaman data pemilih admin untuk melindunginya dari serangan CSRF. Dengan kerentanan keamanan tingkat keparahan sedang, perlindungan AntiCSRF merupakan langkah positif untuk mencegah serangan CSRF.

Ada proses di mana mesin secara otomatis menavigasi halaman web untuk menemukan halaman dan fungsi yang ada. Setelah pemindaian selesai, OWASP ZAP akan menganalisis hasilnya dan mencari potensi kerentanan keamanan di situs web atau aplikasi yang diuji. Ini termasuk fungsionalitas untuk melihat hasil pemilihan, mengubah status pemilih, atau melakukan tindakan lain yang terkait dengan proses pemungutan suara. Setelah mengidentifikasi fungsionalitas yang relevan, digunakan OWASP ZAP untuk melakukan pengujian keamanan.

Masalah telah diselesaikan dengan meningkatkan keamanan melalui mekanisme enkripsi RSA dan mencegah CSRF pada komponen tersembunyi. Penggunaan enkripsi RSA pada formulir dan kata sandi, serta pencegahan CSRF melalui elemen tersembunyi, telah meningkatkan keamanan halaman pemungutan suara pengurus. Data pemungutan suara admin aman karena semua masalah keamanan telah ditangani dengan baik.

Software Burpsuite digunakan untuk pengujian *Brute force*. Untuk memulai, harus ditentukan jenis serangan yang akan dilakukan; dalam kasus ini, itu adalah serangan sniper, yang berarti serangan tunggal terus menerus. Selanjutnya dicatat proses selama pemilihan dengan mengumpulkan data penghentian pemilih. Pengujian alat BurpSuite menggunakan

teknik *payload position* pada pemungutan suara admin di website e-voting yang menggunakan algoritma RSA telah membantu menemukan masalah keamanan yang mungkin dan menunjukkan integritas sistem pemungutan suara.

Karena proses enkripsi *brute force* pada *ciphertext* yang dihasilkannya tidak sesuai dengan identitas calon pada database, pengujian *brute force* dilakukan selama kurang lebih 3 jam 42 menit dan menghasilkan 660 percobaan. Waktu pengujian ini sama dengan waktu sesi setiap pemilih. Oleh karena itu, dapat dengan yakin dikatakan bahwa sistem ini sangat aman dengan tingkat keamanan 85%.

KESIMPULAN DAN REKOMENDASI

Penelitian "Rancang Bangun Website Pengamanan Database *E-Voting* dengan Menerapkan Algoritma *RSA*" menghasilkan beberapa hal kesimpulan berikut:

1. Implementasi Sistem E-Voting: Penelitian ini berhasil mengembangkan situs web E-Voting yang melindungi data dengan menggunakan algoritma RSA. Sistem ini memungkinkan pemilih untuk melakukan pemilihan elektronik dengan aman dan efektif.
2. Kerentanan keamanan seperti *SQL injection* dan *Cross-Site Scripting* (XSS) ditemukan setelah melakukan pengujian dengan alat seperti OWASP ZAP dan *BurpSuite*.

Rekomendasi berikut dapat dilakukan untuk meningkatkan kualitas dan keamanan sistem E-Voting:

1. Pengujian Keamanan Lanjutan: Pastikan sistem diuji secara menyeluruh, termasuk pengujian penetrasi, untuk mencegah serangan dan gangguan keamanan.
2. Pemantauan Keamanan: Website evoting harus dipantau secara teratur untuk mencegah serangan keamanan yang dapat merusak integritas dan kerahasiaan data pemilih. Sistem pemantauan keamanan yang canggih dapat membantu menemukan serangan dan mencegah serangan.
3. Edukasi Pengguna: Beri pemilih instruksi dan informasi yang jelas tentang cara menggunakan sistem E-Voting agar proses pemilihan berjalan lancar dan pemilih dapat menggunakan sistem dengan mudah.

REFERENSI

Dairi, MSD, & Asih, MS (2023). Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan. Jurnal Ilmu Komputer dan …, jurnal.unity-academy.sch.id, https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/44

Hartama, D., Kirana, I. O., & Gunawan, I. (2022). Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab . Simalungun. 2(1), 57–66.

Hasibuan, MR (2022). Implementasi Algoritma Quicksort Untuk Pembangkitan Kunci Algoitma RSA Pada Pengamanan Data Audio. Journal of Informatics, Electrical and Electronics …, djournals.com, https://djournals.com/jieee/article/view/392

Indriani, U, Alfina, O, & Syahputri, N (2022). Penerapan Algoritma RSA Dalam Keamanan File Ms Word. Journal of Machine Learning …, journal.fkpt.org, https://journal.fkpt.org/index.php/malda/article/download/301/197

Kasus, S., Presiden, P., & Stmik, M. (2021). Implementasi Kriptografi Dalam Pengamanan Database E-Voting Menggunakan Algoritma RSA Dan Base64 Berbasis Progresive Web Apps. E-Jurnal JUSITI (Jurnal Sistem Informasi Dan Teknologi Informasi), 10(1), 30–40. https://doi.org/10.36774/jusiti.v10i1.818

Murdowo, S. (2017). Mengenal Lebih Dekat Kriptografi Klasik Vigenere Chipper Menggunakan Visual Basic Net. *Jurnal Infokam*, 65–73.

Nabilah, A., & Amrozi, Y. (2019). Jurnal Teknologi Sistem Informasi dan Aplikasi Rancang Bangun E-Voting Berbasis Web pada Organisasi Karang Taruna Kelurahan Kedurus. Jurnal Teknologi Sistem Informasi Dan Aplikasi, 2(3), 105–109. http://openjournal.unpam.ac.id/index.php/JTSI

Pristiwanti, D., Badriah, B., Hiadayat, S., & Ratna Sari Dewi. (2022). Jurnal Pendidikan dan Konseling Pengertian Pendidikan. Jurnal Pendidikan Dan Konseling Volume 4 Nomor 6 Tahun 2022, 4(11), 1707–1715.

Putri, A. M., Novianti, E., Wulandari, S., Ansyari, M. F., Rezky, M., & Hamzah, M. L. (2022). Perancangan Sistem Informasi E-Voting Untuk Pemilihan Ketua OSIS Menggunakan Agile Method. Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB), 25–31.

Saputra, MW, Sapitri, A, & Putri, MA (2023). Penerapan Kriptosistem Hybrid Untuk Mengenkripsi Pesan Menggunakan Algoritma RSA Cipher. JOCITIS-Journal Science …, jurnal.ittc.web.id, https://jurnal.ittc.web.id/index.php/jct/article/view/29

Siahaan, A. T., & Irmada, H. N. (2021). Aplikasi Sistem e-Voting Ketua Umum UPN Band Veteran Jakarta Berbasis Website. Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer Dan Aplikasinya, 2(2), 742–751.

Sitorus, M., & Antonieta DC, C. (2022). Perancangan Sistem Pemilihan Ketua Bem (Badan Eksekutif Mahasiswa) Berbasis E-Voting Dengan Metode Crud Sebagai Digitalisasi Organisasi Di Bri Institute. Infotech: Journal of Technology Information, 7(2), 125–132. https://doi.org/10.37365/jti.v7i2.122

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice 7th Global Edition.

Sulaiman, R., & Vebu, M. (2018). Peningkatan Keamanan Pesan Berbasis Android Menggunakan Algoritma Kriptografi RSA. Jurnal Sisfokom (Sistem Informasi Dan Komputer), 7(2), 116–120. https://doi.org/10.32736/sisfokom.v7i2.574

Susanto, AE (2023). Keamanan Pesan Teks Dengan Metode Enkripsi Dan Dekripsi Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Android. Jurnal Teknologi Pintar, teknologipintar.org, http://teknologipintar.org/index.php/teknologipintar/article/view/347

Syarif, M., & Nugraha, W. (2020). Pemodelan Diagram UML Sistem Pembayaran Tunai Pada Transaksi E-Commerce. Jurnal Teknik Informatika Kaputama (JTIK), 4(1), 70 halaman. http://jurnal.kaputama.ac.id/index.php/JTIK/article/view/240

Zulkiawan, A., Dengen, N., Puspitasari, N., & Aksenta, A. (2020). Penerapan Metode User Authentication Pada Sistem Monitoring, E-Voting, dan Evaluasi PEMIRA. Jurnal Rekayasa Teknologi Informasi (JURTI), 4(2), 172. https://doi.org/10.30872/jurti.v4i2.5821