Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2026, IX (4): 6726 – 6731 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

IMPLEMENTASI ALGORITMA SHA-256 DAN ONE TIME TOKEN UNTUK KEAMANAN DATA PEMILIHAN OSIS

Ogy Kevinta Surbakti [1], Emerson P. Malau [2], Andy Paul Harianja [3], Paska Marto Hasugian [4]
Universitas Katolik Santo Thomas, Medan
e-mail: [1]ogykevinta@gmail.com, [2]malauemerson@gmail.com,[3]apharianja@gmail.com, [4]paskahmarto86@gmail.com

Abstract: *Electronic voting (e-voting) systems used for student council (OSIS) elections commonly rely only on username and password authentication, which remains vulnerable to credential misuse and unauthorized access. This study aims to implement the SHA-256 hashing algorithm together with a One Time Token (OTT) mechanism to strengthen data security in a web-based OSIS chairperson election application at SMA RK Deli Murni Bandar Baru. The Research and Development method with a Waterfall model was used, consisting of literature study, data collection through observation, interviews, and documentation, security mechanism design, system implementation using PHP, MySQL, and Gmail SMTP, and evaluation using Black Box Testing. After logging in with a student ID and password, the system generates a random twelve-character token, sends it to the student's registered Gmail account, and stores only its SHA-256 hash together with an expiration time and usage status. Testing results show that the hashing process consistently produces a 64-character hexadecimal value, identical inputs yield identical hashes, different inputs yield different hashes, and manual calculation matches the program output. The verification mechanism successfully rejects tokens that are incorrect, expired, or already used, and the double-voting prevention feature works as intended. These findings indicate that combining SHA-256 with a One Time Token strengthens authentication and preserves the integrity of the voting process.*

Keyword: *SHA-256; one time token; e-voting; authentication; data security*

Abstrak: Sistem pemilihan elektronik (e-voting) untuk pemilihan pengurus Organisasi Siswa Intra Sekolah (OSIS) umumnya hanya menggunakan autentikasi berbasis Nomor Induk Siswa dan kata sandi sehingga masih rentan terhadap penyalahgunaan kredensial dan akses tidak sah. Penelitian ini bertujuan mengimplementasikan algoritma SHA-256 bersama dengan mekanisme One Time Token (OTT) untuk meningkatkan keamanan data pada aplikasi pemilihan Ketua OSIS berbasis web di SMA RK Deli Murni Bandar Baru. Metode yang digunakan adalah Research and Development dengan model Waterfall, meliputi studi literatur, pengumpulan data melalui observasi, wawancara, dan dokumentasi, perancangan mekanisme keamanan, implementasi sistem menggunakan PHP, MySQL, dan Gmail SMTP, serta evaluasi menggunakan Black Box Testing. Setelah siswa login menggunakan NIS dan kata sandi, sistem membangkitkan token acak sepanjang dua belas karakter, mengirimkannya ke akun Gmail siswa yang terdaftar, dan hanya menyimpan nilai hash SHA-256 beserta batas waktu dan status penggunaannya. Hasil pengujian menunjukkan bahwa proses hashing secara konsisten menghasilkan nilai 64 karakter heksadesimal, masukan yang sama menghasilkan hash yang sama, masukan yang berbeda menghasilkan hash yang berbeda, serta perhitungan manual sesuai dengan keluaran program. Mekanisme verifikasi berhasil menolak token yang salah, kedaluwarsa, maupun telah digunakan, dan fitur pencegahan double voting berjalan sesuai rancangan. Temuan ini menunjukkan bahwa kombinasi SHA-256 dan One Time Token memperkuat autentikasi serta menjaga integritas proses pemilihan.

Kata kunci: SHA-256; token sekali pakai; e-voting; autentikasi; keamanan data

PENDAHULUAN

Pemanfaatan teknologi informasi di lingkungan pendidikan terus berkembang, tidak terkecuali dalam kegiatan organisasi kesiswaan seperti pemilihan pengurus Organisasi Siswa Intra Sekolah (OSIS). Pemilihan OSIS merupakan sarana pembelajaran demokrasi bagi siswa sehingga proses pemungutan suara perlu berlangsung secara efektif sekaligus menjamin bahwa hak pilih hanya digunakan oleh siswa yang berhak dan hanya satu kali. Prinsip tersebut sejalan dengan karakteristik electronic voting (e-voting) yang menekankan kelayakan pemilih, keunikan suara, serta integritas hasil pemungutan suara.

Digitalisasi pemilihan OSIS telah banyak dikembangkan pada penelitian sebelumnya. Kurniawan (2023) merancang aplikasi e-voting berbasis mobile dengan model Waterfall untuk mempercepat proses pemungutan dan rekapitulasi suara, namun belum menerapkan lapisan autentikasi tambahan selain kata sandi. Chairul Rizal dkk. (2024) mengembangkan sistem e-voting berbasis web dengan metode prototype yang berhasil meningkatkan efektivitas pemungutan suara, tetapi juga belum mengintegrasikan mekanisme autentikasi dua tahap. Rahman dan Herlambang (2024) menerapkan metode Rapid Application Development pada sistem e-voting pemilihan Ketua OSIS, dengan fokus utama pada percepatan proses pengembangan sistem dibandingkan pengamanan data. Pada sisi keamanan token, Tatang Nugraha (2025) menerapkan hashing SHA-256 untuk mengamankan data pada sistem e-voting multi-kategori, sedangkan Arisandi dkk. (2025) menggunakan kombinasi TOTP dan SHA-512 untuk autentikasi dua faktor pada pemilihan presiden mahasiswa. Pendekatan yang lebih kompleks diusulkan oleh Laia dan Barmawi (2024) melalui penerapan post-quantum cryptography pada sistem e-voting berbasis blockchain, meskipun tingkat kompleksitas implementasinya kurang sesuai diterapkan pada lingkup pemilihan OSIS di sekolah menengah.

Berdasarkan kajian tersebut, masih terdapat celah penelitian (research gap), yaitu belum banyak ditemukan penelitian yang secara khusus mengintegrasikan autentikasi bertingkat menggunakan Nomor Induk Siswa (NIS) dan kata sandi, dilanjutkan dengan One Time Token (OTT) yang dikirim melalui surat elektronik, serta mengamankan token tersebut menggunakan algoritma hashing sebelum disimpan ke dalam basis data pada konteks pemilihan OSIS di sekolah menengah. Padahal, apabila autentikasi hanya mengandalkan NIS dan kata sandi, akun berisiko digunakan oleh pihak lain apabila kredensial tersebut diketahui atau bocor, sehingga dapat memengaruhi keabsahan hasil pemilihan (OWASP Foundation, 2025).

One Time Token (OTT) merupakan token autentikasi yang dibangkitkan secara acak dan hanya berlaku untuk satu kali penggunaan dalam periode waktu tertentu sehingga risiko serangan replay dan penyalahgunaan kredensial dapat dikurangi. Agar token tidak tersimpan dalam bentuk teks asli apabila basis data diakses oleh pihak yang tidak berwenang, token perlu diproses terlebih dahulu menggunakan fungsi hash kriptografis. Secure Hash Algorithm 256-bit (SHA-256) merupakan salah satu fungsi hash yang direkomendasikan sebagai standar keamanan informasi karena menghasilkan nilai keluaran sepanjang 256 bit yang bersifat satu arah dan tahan terhadap kolisi (National Institute of Standards and Technology, 2015).

Berdasarkan uraian tersebut, penelitian ini mengimplementasikan algoritma SHA-256 dan mekanisme One Time Token untuk mengamankan data pada aplikasi pemilihan pengurus OSIS berbasis web di SMA RK Deli Murni Bandar Baru. Setelah siswa melakukan autentikasi awal menggunakan NIS dan kata sandi, sistem membangkitkan One Time Token secara acak dan mengirimkannya melalui akun Gmail siswa yang terdaftar. Token tersebut

disimpan dalam bentuk nilai hash SHA-256, memiliki batas waktu penggunaan (token_expired_at), serta status penggunaan (token_used_at) untuk mencegah penggunaan ulang. Penelitian ini bertujuan untuk mengimplementasikan SHA-256 dalam mengamankan token autentikasi, menerapkan mekanisme One Time Token berbasis Gmail sebagai lapisan autentikasi tambahan, menerapkan validasi token berdasarkan token_hash, token_expired_at, dan token_used_at, serta menguji efektivitas mekanisme tersebut dalam mencegah double voting pada proses pemilihan Ketua OSIS.

METODE

Metode Penelitian ini menggunakan pendekatan Research and Development (R&D) dengan model pengembangan perangkat lunak Waterfall karena tahapannya terstruktur dan sesuai dengan proses pembangunan aplikasi e-voting berbasis web. Tahapan penelitian meliputi studi literatur, pengumpulan data, perancangan dan implementasi mekanisme keamanan, implementasi sistem, serta pengujian.

Studi literatur dilakukan dengan mengkaji buku, jurnal nasional dan internasional, serta standar keamanan informasi yang berkaitan dengan electronic voting, autentikasi berlapis, One Time Token, dan algoritma SHA-256, termasuk standar Secure Hash Standard FIPS 180-4 (National Institute of Standards and Technology, 2015) dan praktik autentikasi menurut Authentication Cheat Sheet (OWASP Foundation, 2025). Pengumpulan data dilakukan melalui observasi langsung terhadap proses pemilihan Ketua OSIS yang masih dilakukan secara konvensional di SMA RK Deli Murni Bandar Baru, wawancara dengan pembina OSIS dan panitia pemilihan, serta dokumentasi data siswa dan prosedur pemilihan yang berjalan.

Berdasarkan hasil studi literatur dan pengumpulan data, dirancang mekanisme autentikasi dua tahap. Tahap pertama, siswa melakukan login menggunakan Nomor Induk Siswa (NIS) dan kata sandi yang telah terdaftar. Tahap kedua, setelah autentikasi awal berhasil dan periode pemilihan berada dalam status aktif, sistem membangkitkan One Time Token menggunakan fungsi random_bytes() sebagai pembangkit bilangan acak yang aman secara kriptografis. Token direpresentasikan dalam 12 karakter heksadesimal sehingga memiliki ruang kemungkinan sebesar 16^{12} atau setara 2^{48} kombinasi, dan tidak dibentuk berdasarkan data identitas siswa. Sebelum disimpan ke dalam basis data, token diproses menggunakan algoritma SHA-256 sehingga hanya nilai hash (token_hash) yang tersimpan, sedangkan token asli dikirimkan ke akun Gmail siswa melalui protokol SMTP menggunakan pustaka PHPMailer. Setiap token diberi atribut token_expired_at untuk membatasi masa berlaku dan token_used_at untuk mencatat status penggunaan, sehingga token yang telah digunakan atau kedaluwarsa tidak dapat digunakan kembali. Setelah proses pemungutan suara selesai, status siswa diperbarui menjadi “Sudah Memilih” untuk mencegah double voting.

Implementasi sistem dilakukan menggunakan bahasa pemrograman PHP, basis data MySQL, serta lingkungan pengembangan XAMPP dan Visual Studio Code. Pengujian sistem dilakukan menggunakan metode Black Box Testing, yaitu pengujian yang berfokus pada kesesuaian antara masukan dan keluaran sistem tanpa memeriksa struktur kode program. Pengujian mencakup proses login, konsistensi hasil hashing SHA-256, verifikasi One Time Token, pengujian replay token, pengujian pencegahan double voting, serta validasi hasil hashing manual terhadap hasil hashing program

HASIL DAN PEMBAHASAN

Hasil pengujian menunjukkan bahwa proses autentikasi bertingkat

berjalan sesuai dengan rancangan. Pada pengujian halaman login, sistem berhasil menerima kombinasi NIS dan kata sandi yang valid, menolak kata sandi yang salah, menampilkan pesan kesalahan untuk NIS yang tidak terdaftar, serta meminta pengguna melengkapi data apabila kolom login dikosongkan.

Pengujian kriptografi SHA-256 dilakukan untuk memastikan konsistensi proses hashing token. Hasil pengujian menunjukkan bahwa token yang diproses menghasilkan nilai hash sepanjang 64 karakter heksadesimal, token yang sama menghasilkan nilai hash yang sama, sedangkan token yang berbeda menghasilkan nilai hash yang berbeda. Basis data hanya menyimpan nilai token_hash dan tidak menyimpan token dalam bentuk plaintext. Validasi lebih lanjut dilakukan dengan membandingkan hasil perhitungan SHA-256 secara manual dan hasil implementasi program menggunakan masukan yang sama. Kedua metode menghasilkan nilai hash 64 karakter yang identik, yang menunjukkan bahwa implementasi algoritma pada program telah sesuai dengan spesifikasi SHA-256.

Pengujian verifikasi One Time Token menunjukkan bahwa sistem memberikan akses ke halaman voting hanya apabila hash token yang dimasukkan cocok dengan token_hash, token belum melewati token_expired_at, dan token_used_at masih kosong. Token yang salah, kedaluwarsa, atau kosong ditolak oleh sistem. Pengujian replay token juga menunjukkan bahwa token yang telah digunakan tidak dapat digunakan kembali karena sistem membaca nilai token_used_at yang telah terisi. Pada pengujian double voting, siswa yang belum memilih dapat memberikan suara, sedangkan siswa dengan status “Sudah Memilih” ditolak ketika mencoba memberikan suara kembali maupun mengakses ulang halaman voting.

Tabel 1 Rekapitulasi Hasil Pengujian Sistem

No	Mekanisme	Pengujian	Hasil
1	SHA-256	Hashing token	Berhasil
2	token_ hash	Penyimpanan hash	Berhasil
3	Validasi token	Token benar	Berhasil
4	Validasi token	Token salah	Ditolak
5	token_ expired_at	Token kedaluwarsa	Ditolak
6	token_ used_at	Token telah digunakan	Ditolak
7	OTT	Penggunaan Satu kali	Berhasil
8	Replay token	Token lama digunakan kembali	Ditolak
9	Double voting	Percobaan voting kedua	Ditolak
10	SHA-256	Perhitungan manual vs program	Identik

Secara keseluruhan, hasil pengujian pada Tabel 1 menunjukkan bahwa integrasi algoritma SHA-256 dan mekanisme One Time Token mampu meningkatkan keamanan proses autentikasi pada aplikasi e-voting OSIS. Berbeda dengan penelitian Kurniawan (2023) dan Chairul Rizal dkk. (2024) yang berfokus pada efektivitas proses pemungutan suara tanpa autentikasi tambahan, penelitian ini menambahkan lapisan verifikasi kedua berupa OTT yang dikirim melalui Gmail sehingga kepemilikan akun saja tidak cukup untuk memperoleh akses ke halaman voting. Dibandingkan dengan penelitian Tatang Nugraha (2025) yang menerapkan SHA-256 tanpa autentikasi dua tahap berbasis token sekali pakai, penelitian ini mengintegrasikan hashing SHA-256 dengan validasi token_expired_at dan token_used_at sehingga token tidak hanya diamankan pada saat penyimpanan, tetapi juga dibatasi berdasarkan masa berlaku dan status penggunaannya. Penelitian ini juga menghadirkan mekanisme yang relatif lebih sederhana dibandingkan pendekatan post-quantum cryptography

pada penelitian Laia dan Barmawi (2024) sehingga lebih sesuai diterapkan pada skala pemilihan OSIS di sekolah menengah tanpa mengurangi tingkat keamanan autentikasi secara signifikan.

Penerapan token dengan panjang 12 karakter heksadesimal yang dibangkitkan menggunakan fungsi pembangkit bilangan acak kriptografis menghasilkan ruang kemungkinan sebesar 2^{48} kombinasi, sehingga upaya penebakan token secara acak menjadi tidak praktis dilakukan dalam rentang waktu berlaku token yang terbatas. Kombinasi antara keacakan token, pembatasan masa berlaku, status penggunaan satu kali, serta penyimpanan token dalam bentuk hash SHA-256 memberikan lapisan pertahanan berlapis (defense in depth) yang sejalan dengan prinsip praktik terbaik autentikasi menurut OWASP Foundation (2025). Dengan demikian, hasil penelitian ini menunjukkan bahwa mekanisme keamanan yang diusulkan dapat diterapkan pada sistem e-voting berskala sekolah tanpa memerlukan infrastruktur maupun kompleksitas implementasi yang tinggi.

SIMPULAN

Berdasarkan hasil implementasi dan pengujian, algoritma SHA-256 dan mekanisme One Time Token berhasil diterapkan untuk mengamankan proses autentikasi pada aplikasi pemilihan pengurus OSIS berbasis web di SMA RK Deli Murni Bandar Baru. Token autentikasi yang dibangkitkan secara acak tidak disimpan dalam bentuk teks asli, melainkan diproses menggunakan SHA-256 sehingga hanya nilai hash sepanjang 64 karakter heksadesimal yang tersimpan pada basis data, dan hasil pengujian menunjukkan bahwa proses hashing tersebut konsisten serta identik dengan perhitungan manual. Mekanisme validasi berdasarkan token_hash, token_expired_at, dan token_used_at terbukti mampu menolak token yang salah, telah kedaluwarsa, maupun telah digunakan sebelumnya, sehingga token hanya dapat dimanfaatkan satu kali dalam batas waktu tertentu. Kombinasi mekanisme tersebut juga berhasil mendukung pencegahan double voting karena status siswa yang telah memberikan suara secara otomatis ditolak ketika mencoba mengakses kembali halaman pemungutan suara. Dengan demikian, penelitian ini memberikan kontribusi berupa mekanisme autentikasi dua tahap yang relatif sederhana namun tetap memenuhi prinsip keamanan yang memadai untuk diterapkan pada sistem e-voting berskala sekolah, sekaligus mendukung terselenggaranya prinsip satu pemilih satu suara dalam proses pemilihan Ketua OSIS.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Teknik Informatika dan Fakultas Ilmu Komputer Universitas Katolik Santo Thomas Medan atas dukungan yang diberikan, serta kepada pihak SMA RK Deli Murni Bandar Baru atas izin dan bantuan selama proses pengumpulan data penelitian ini.

DAFTAR PUSTAKA

Arisandi, D., Hartati, S., & Vrabora, G. (2025). Otentikasi dua faktor menggunakan TOTP dengan SHA-512 untuk sistem pemilihan presiden mahasiswa. Explorer, 5(1), 14–25. https://doi.org/10.47065/explorer.v5i1.1782

Chairul Rizal, Purwanti, J., Nabilla, P., Hartika, C., & Latipah. (2024). Rancang bangun sistem informasi e-voting untuk pemilihan ketua OSIS menggunakan metode prototype berbasis web. Bulletin of Computer Science Research, 4(2), 170–180. https://doi.org/10.47065/bulletincsr.v4i2.332

Kurniawan, A. (2023). Perancangan aplikasi e-voting pada pemilihan

ketua OSIS berbasis mobile. Jurnal Ilmiah Informatika dan Ilmu Komputer (JIMA-ILKOM), 2(1), 26–31. https://doi.org/10.58602/jima-ilkom.v2i1.15

Laia, S., & Barmawi, A. M. (2024). Strengthening the authentication mechanism of blockchain-based e-voting system using post-quantum cryptography. JOIN (Jurnal Online Informatika), 9(1), 159–168. https://doi.org/10.15575/join.v9i1.1305

Laudon, K. C., & Laudon, J. P. (2020). Management information systems: Managing the digital firm (16th ed.). Pearson.

National Institute of Standards and Technology. (2015). Secure hash standard (FIPS PUB 180-4). https://doi.org/10.6028/NIST.FIPS.1

OWASP Foundation. (2025). Authentication cheat sheet. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

Rahman, M., & Herlambang, T. S. (2024). Penerapan metode RAD dalam rancang bangun sistem e-voting pemilihan ketua OSIS SMK Tritech Medan. IT (Informatic Technique) Journal, 12(2), 13–23.

Tatang Nugraha. (2025). Pembuatan e-voting dengan model multi vote berdasarkan kategori menggunakan hashing SHA-256. Bridge: Jurnal Publikasi Sistem Informasi dan Telekomunikasi, 3(3), 102–116. https://doi.org/10.62951/bridge.v3i3.538