

Pemanfaatan *One-Time Password* dan Algoritma *Advanced Encryption Standard* dalam Sistem Login Internet Kampus

Angga Eko Bayu Arieska¹, Fransiska Sisilia Mukti^{2✉}

^{1,2} Teknik Informatika, Fakultas Teknologi dan Desain, Institut Teknologi dan Bisnis Asia Malang, Indonesia

Informasi Artikel

Riwayat Artikel

Diserahkan : 03-08-2023

Direvisi : 14-08-2023

Diterima : 17-08-2023

Kata Kunci:

AES, keamanan jaringan,
login internet, OTP

Keywords :

AES, internet login,
network security, OTP

ABSTRAK

Tingginya kebutuhan informasi melalui internet masyarakat modern kerap dihadapkan pada permasalahan mengenai keamanan informasi. Mudah-mudahan data diperoleh melalui internet sepatutnya diimbangi dengan jaminan kerahasiaan data dari orang-orang yang tidak berkepentingan. Proses autentikasi menjadi salah satu tahapan yang penting untuk dilakukan dalam memverifikasi kepemilikan akses pengguna terhadap sebuah data. Berbeda dengan jaringan *wireless* yang umumnya menggunakan mekanisme *static password*, jaringan kabel justru tidak menawarkan adanya proses autentikasi di dalamnya. Hal ini dapat menjadi celah bagi para penjahat siber untuk mengambil data secara ilegal atau merusak tatanan sistem. Untuk itu, menambahkan mekanisme autentikasi dalam penggunaan internet di area kampus dianggap penting untuk dilakukan. Penelitian ini secara khusus menggabungkan mekanisme OTP untuk proses autentikasi dan algoritma AES untuk pengamanan data autentikasi pada sistem login internet kampus. Hasil penelitian menunjukkan bahwa integrasi metode OTP dan algoritma AES mampu menjaga integritas dan kerahasiaan informasi login pengguna, serta memberikan akses internet secara tepat guna hanya bagi pengguna yang memiliki kredensial.

ABSTRACT

The high need for information via the internet, modern society is often faced with problems regarding information security. The ease of obtaining data via the internet should be balanced with guarantees of data confidentiality from unauthorized persons. The authentication process is one of the important steps to be carried out in verifying ownership of user access to data. In contrast to wireless networks which generally use a static password mechanism, wired networks do not offer an authentication process in them. This can be a loophole for cybercriminals to retrieve data illegally or damage the system. For this reason, adding an authentication mechanism for using the internet in the campus area is considered important. This research specifically combines the OTP mechanism for the authentication process and the AES algorithm for securing authentication data on campus internet login systems. The results of the study show that the integration of the OTP method and the AES algorithm is able to maintain the integrity and confidentiality of user login information, and provide effective internet access only for users who have credentials.

Corresponding Author :

Fransiska Sisilia Mukti

Teknik Informatika, Fakultas Teknologi dan Desain, Institut Teknologi dan Bisnis Asia Malang

Jl. Soekarno Hatta - Rembuku No.1 A, Malang

Email: ms.frans@asia.ac.id

PENDAHULUAN

Teknologi informasi dan komunikasi menjadi infrastruktur penting yang tidak terpisahkan dalam kehidupan masyarakat modern saat ini, karena berperan utama dalam menyediakan fasilitas komunikasi dan pertukaran informasi (Zhan & Ye, 2020). Tingginya lalu lintas data yang terjadi harus diimbangi dengan adanya penyediaan prosedur keamanan yang mumpuni untuk menjaga keutuhan dan kerahasiaan data yang ada. Setiap pengguna perlu melakukan verifikasi identitas sebelum diberikan akses terhadap sebuah data atau informasi (Oluwakemi Christiana et al., 2019), proses ini didefinisikan sebagai autentikasi (Taqwim et al., 2021).

Autentikasi menjadi salah satu isu krusial dalam sistem keamanan informasi. Beragam penelitian telah dikembangkan untuk menghasilkan metode autentikasi yang paling efektif dan aman (Styugin, 2019). Saat ini, metode autentikasi yang banyak dikenal diklasifikasikan ke dalam tiga klaster, yaitu token, *biometric* dan *knowledge-based system*. Autentikasi berbasis token menggunakan perangkat keras seperti *smart card* atau *key card*, sementara autentikasi berbasis *biometric* menggunakan panca indera manusia untuk mengaktifkannya, seperti suara, sidik jari, wajah, retina, dan sebagainya. Meskipun dinilai memiliki tingkat keamanan yang baik, namun pengaplikasian kedua metode autentikasi ini membutuhkan biaya yang besar untuk pengembangannya. Sesuai dengan namanya, metode autentikasi berbasis *knowledge-based system* menggunakan pengetahuan pengguna dalam proses verifikasi, seperti kata sandi dalam bentuk grafis (gambar atau pola) ataupun teks. Kata sandi berbentuk teks dibedakan menjadi statis dan dinamis, dimana sandi statis umumnya terdiri dari 6 ataupun 8 digit karakter yang ditentukan oleh pengguna (Oluwakemi Christiana et al., 2019).

Konsep autentikasi berbasis password statis menjadi metode autentikasi yang paling sederhana namun paling banyak diimplementasikan dalam berbagai sistem informasi. Mekanisme ini memiliki tingkat keamanan yang rendah dan rentan terhadap serangan maupun kebocoran kata sandi (Imamah, 2018). Selain itu, *static password* juga rentan terhadap *human error* seperti lupa password atau konten password yang terlalu mudah ditebak oleh *hacker* berdasarkan data pribadi pengguna (Styugin, 2019). Keterbatasan ini menuntut adanya pengembangan autentikasi berbasis *dynamic password*, salah satunya adalah *One time Password* (OTP). Sistem akan menghasilkan serangkaian *password* acak yang hanya dapat digunakan sekali dalam periode waktu tertentu (Oluwakemi Christiana et al., 2019).

Untuk memperkuat keamanan dalam proses autentikasi, metode OTP kerap dikombinasikan dengan algoritma kriptografi. Kriptografi meningkatkan keamanan informasi melalui proses *authentication*, *non-repudiation* dan *confidentiality* (Kelana et al., 2021). Mengingat informasi pengguna untuk proses autentikasi bersifat sensitif dan rahasia, maka diperlukan peran algoritma kriptografi dalam menyandikan data melalui proses enkripsi dan dekripsi. *Advanced Encryption Standard* (AES) merupakan salah satu algoritma kriptografi yang bersifat *symmetric*, yaitu penggunaan kunci yang sama untuk proses enkripsi dan dekripsinya (Riyan Andriyanto et al., 2022).

Beragam penelitian dilakukan untuk mengetahui performansi algoritma AES dalam melakukan pengamanan informasi. Anwar dkk melakukan perbandingan kinerja antara algoritma AES dan RSA dalam melakukan pengamanan data, dan didapatkan hasil bahwa algoritma AES memiliki rata-rata 236 kali lebih cepat pada proses enkripsi dan 2,5 kali lebih cepat pada proses dekripsi dibandingkan dengan algoritma RSA (Anwar et al., 2018). Performansi algoritma AES juga diuji melalui penelitian yang dilakukan oleh Kurniawan dkk dengan membandingkannya dengan algoritma Blowfish. Didapatkan hasil bahwa algoritma AES memiliki selisih kecepatan sebesar 0,015 ms untuk enkripsi dan 0,04 ms untuk dekripsi, lebih cepat dibandingkan algoritma Blowfish (Kurniawan et al., 2021).

Proses autentikasi untuk login internet pada umumnya menggunakan mekanisme *static password*, yaitu dengan cara menghubungkan perangkat ke jaringan yang diinginkan (memilih *Service Set Identifier* / SSID dari jaringan *wireless*) kemudian memasukkan *password* secara manual. Sementara jika ingin terhubung dengan jaringan kabel, maka pengguna cukup menghubungkan

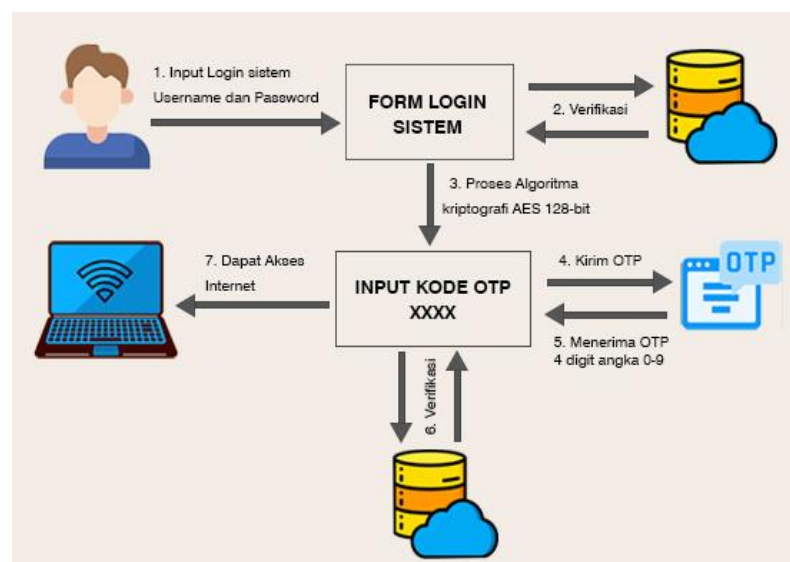
perangkat dengan kabel yang sudah disediakan oleh pihak penyedia jasa layanan internet di kampus tersebut. Biasanya, tidak ada autentikasi secara khusus yang dilakukan oleh pengguna jika terhubung jaringan secara kabel.

Jika dilihat dari sudut pandang keamanan pengguna, maka mekanisme koneksi ke jaringan kabel lebih rentan mengalami pengaksesan data secara ilegal karena tidak adanya proses autentikasi yang harus dilakukan. Demikian pula untuk jaringan *wireless*, pengguna dapat dengan bebas mengakses internet hanya dengan memiliki informasi *password*. Hal ini dapat menjadi celah bagi para penjahat siber untuk mengambil data secara ilegal atau merusak sistem dalam kampus. Untuk itu, autentikasi pada sistem login internet kampus menjadi sebuah proses penting yang perlu dilakukan dalam rangka menjaga keamanan data pengguna.

Penelitian ini secara khusus menggabungkan mekanisme OTP untuk proses autentikasi dan algoritma AES untuk pengamanan data autentikasi pada sistem login internet kampus. Integrasi metode OTP dan algoritma AES diharapkan mampu menjaga integritas dan kerahasiaan informasi login pengguna, serta memberikan akses internet secara tepat guna hanya bagi pengguna yang memiliki kredensial terhadap akses internet kampus.

METODE PENELITIAN

Penelitian ini dilakukan secara komprehensif dengan menggabungkan antara metode eksplorasi, eksperimental, serta implementasi pada studi kasus. Tahapan penelitian dimulai dengan fase konseptual, dimana dilakukan proses identifikasi dan visualisasi topologi jaringan pada studi kasus, termasuk di dalamnya tipe pengguna yang ada. Selanjutnya, proses perancangan terhadap parameter-parameter penelitian, seperti data sampel dan skenario pengujian. Fase ketiga yang dilakukan adalah fase empiric, yaitu proses pengambilan data berdasarkan scenario yang telah ditetapkan. Hasil dari fase empiric selanjutnya dilakukan analisis dan evaluasi untuka mendapatkan hasil penelitian. Keseluruhan tahapan penelitian ditutup dengan fase diseminasi, yaitu implementasi hasil penelitian pada studi kasus (Susdyastama Putra et al., 2020).



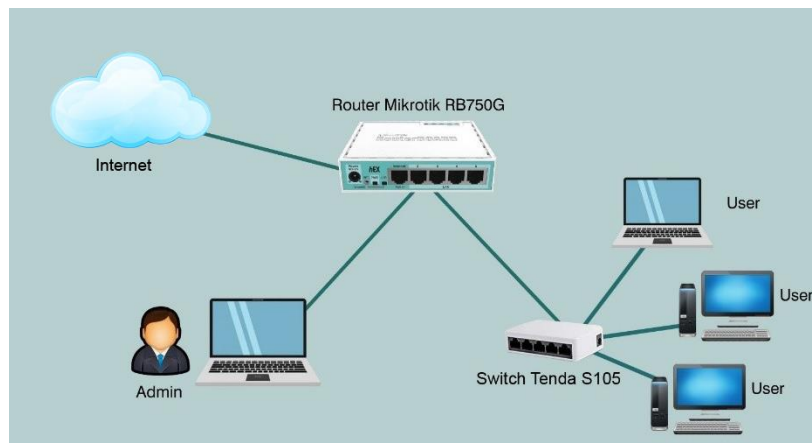
Gambar 1. Blok Diagram Proses Autentikasi Login Internet

Gambaran Umum Sistem

Mekanisme sistem login internet kampus yang diusulkan melalui penelitian ini mengadopsi mekanisme *two-factor authentication* (2FA), yaitu menggabungkan antara mekanisme *knowledge-based system* (verifikasi kata sandi) dan *security token* (verifikasi kode OTP) (Kaur et al., 2022). Mekanisme OTP dikerjakan oleh sistem dengan cara membangkitkan kode TP dari data

pengguna yang meliputi *username*, *password* dan alamat *e-mail*, dengan menggunakan algoritma *hash SHA-256* pada kurun waktu tertentu (Prayogo & Rony, 2018). Pada waktu bersamaan, sistem juga melakukan enkripsi terhadap *password* pengguna dengan menggunakan algoritma AES. Kombinasi kerja keduanya membuat proses autentikasi lebih aman dilakukan oleh pengguna yang akan mengakses internet.

Setiap pengguna yang akan mengakses internet diharuskan untuk memiliki akun terlebih dahulu yang didaftarkan melalui portal yang telah disediakan. Data yang dibutuhkan dalam proses registrasi akun meliputi data *username*, *password*, nomor HP, alamat tempat tinggal serta alamat *e-mail*. Proses registrasi akan divalidasi oleh pihak admin terlebih dahulu sebelum akun dapat digunakan. Setelah terverifikasi, pengguna dapat masuk ke dalam halaman login dengan memasukkan identitas *username* dan *password*. Sistem akan memverifikasi kredensial akun terlebih dahulu ke dalam *database*, dan jika data yang dimasukkan sudah benar, maka pengguna akan diminta untuk memasukkan kode OTP yang dikirimkan sistem melalui *e-mail*. Jika kode valid, maka pengguna akan diarahkan ke halaman utama kampus dan mendapatkan akses internet. Namun jika kode tidak valid, maka pengguna akan diberi peringatan bahwa kode salah dan tidak memiliki akses internet. Gambaran umum dari sistem yang dibangun ditunjukkan melalui Gambar 1.



Gambar 2. Topologi Pengujian Sistem

Skenario Pengujian

Penelitian ini menggunakan sampel pengujian pengguna internet di lingkungan Institut Asia Malang (dosen, mahasiswa dan karyawan). Institut Asia Malang menyediakan akses internet dalam dua tipe, yaitu jaringan kabel dan nirkabel. Jaringan kabel digunakan pada lingkungan laboratorium dan administrasi, dengan jumlah perangkat mencapai 250 perangkat, sedangkan untuk jaringan nirkabel menggunakan akun HotSpot yang telah dikonfigurasi melalui Router MikroTik dengan memanfaatkan fitur CapsMan. Sebagai sampel pengujian, penelitian ini menggunakan pengguna jaringan kabel untuk lingkungan laboratorium dan administrasi, dengan topologi yang terlihat pada Gambar 2. Prosedur pengujian sistem dikategorikan menjadi 2 tahapan yang diuraikan sebagai berikut.

1. Pengujian validasi kode OTP: prosedur pengujian yang dilakukan untuk mengetahui keberhasilan mekanisme OTP dalam melakukan proses autentikasi pengguna. Proses pengujian dilakukan mulai dari kesesuaian kode, jumlah masukan kode, hingga batas waktu penggunaan kode.
2. Pengujian algoritma AES: prosedur pengujian yang dilakukan untuk mengetahui keberhasilan sistem dalam mengenkripsikan data *password* pengguna menggunakan

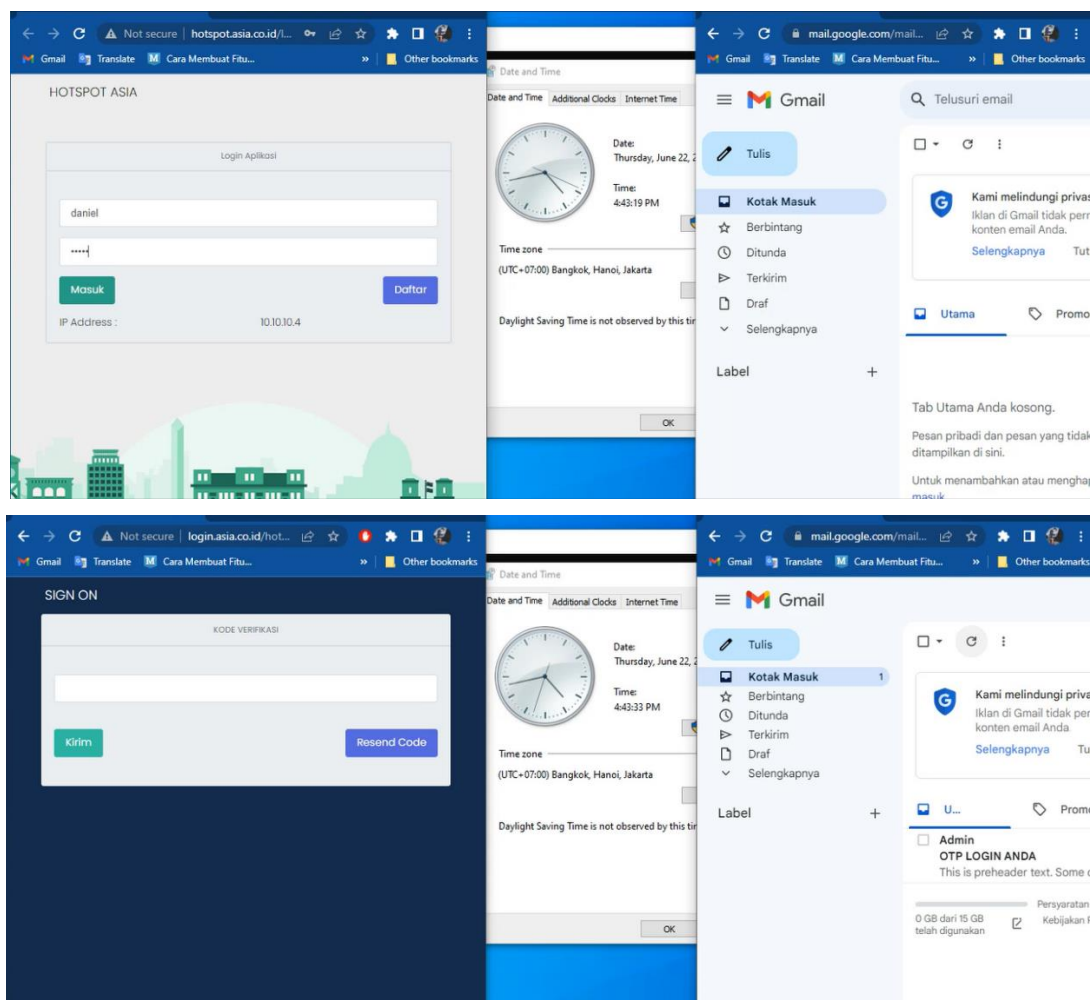
algoritma AES. Pengujian dilengkapi dengan prosedur dekripsi untuk mengetahui apakah data sesuai dengan data awal.

3. Pengujian akses internet: prosedur pengujian yang dilakukan untuk mengetahui keberhasilan sistem dalam memberikan akses internet bagi pengguna yang terverifikasi ataupun tidak. Pengujian ini bertujuan untuk mengevaluasi tingkat kesesuaian sistem dalam membatasi akses pengguna.

HASIL DAN PEMBAHASAN

Pengujian Validasi Kode OTP

Pengujian pertama dilakukan dengan meminta pengguna untuk melakukan proses autentikasi pada portal yang disediakan pada tiga perangkat yang berbeda. Pengamatan dilakukan dengan cara menghitung selisih waktu yang dibutuhkan oleh sistem untuk mengirimkan kode OTP ke *e-mail* pengguna setelah melakukan proses *login* dengan memasukkan *username* dan *password*, sebagaimana yang terlihat pada Gambar 3.



Gambar 3. Pengujian Selisih Waktu Penerimaan Kode OTP

Sebagaimana yang terlihat pada Gambar 3, terdapat selisih waktu antara pengiriman kode melalui sistem dengan penerimaan kode OTP melalui *e-mail* pengguna. Adanya selisih waktu dipengaruhi oleh banyak faktor, seperti kecepatan sistem dalam membangkitkan algoritma SHA-256 untuk mengirimkan kode serta tingkat kecepatan internet dari perangkat pengguna untuk

membuka *e-mail*. Tabel 1 menunjukkan rekapitulasi hasil pengujian sistem terhadap sampel 10 pengguna di Institut Asia Malang. Didapatkan hasil bahwa kecepatan penerimaan kode OTP berada di rentang waktu 9 – 14 detik dengan nilai rata-rata waktu secara keseluruhan sebesar 11,6 detik. Hasil ini dapat memiliki perbedaan waktu apabila dilakukan pengujian pada perangkat yang berbeda, sehingga dapat disimpulkan bahwa selain kestabilan koneksi internet pengguna, proses kecepatan penerimaan OTP juga dipengaruhi oleh jenis perangkat yang digunakan oleh pengguna.

Tabel 1. Pengujian Selisih Waktu Penerimaan Kode OTP

Pengguna	Perangkat 1	Perangkat 2	Perangkat 3
Pengguna 1	14 detik	12 detik	11 detik
Pengguna 2	11 detik	10 detik	10 detik
Pengguna 3	14 detik	13 detik	10 detik
Pengguna 4	13 detik	12 detik	11 detik
Pengguna 5	12 detik	10 detik	12 detik
Pengguna 6	12 detik	12 detik	10 detik
Pengguna 7	11 detik	13 detik	10 detik
Pengguna 8	13 detik	11 detik	9 detik
Pengguna 9	14 detik	12 detik	13 detik
Pengguna 10	13 detik	11 detik	12 detik
Rata-rata Waktu	12,6 detik	11,6 detik	10,8 detik

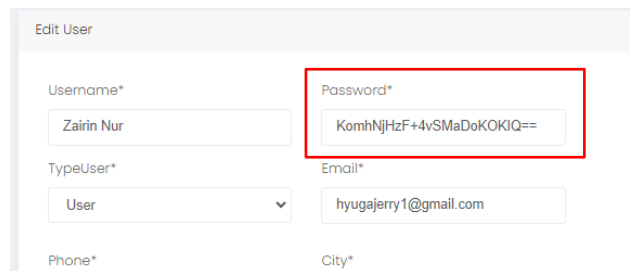
Sesuai dengan namanya, OTP berupa serangkaian karakter atau angka hanya berlaku untuk satu kali sesi autentikasi dengan masa hidup kata sandi sekitar 180 detik. Mekanisme ini diberlakukan untuk meningkatkan sistem keamanan data yang bersifat sensitif (Balilo et al., 2017). Untuk mengevaluasi kevalidan kata sandi OTP, dilakukan prosedur pengujian kode OTP berdasarkan masa berlaku sandi, baik dari segi jumlah penggunaan maupun masa hidup kode. Pengujian dilakukan secara berulang dari pengguna yang berbeda dalam dua studi kasus, yaitu kasus 1: masukan kode OTP secara berulang pada perangkat yang berbeda; kasus 2: penggunaan kode OTP melewati masa hidup kata sandi (menit ke-4 dari pengiriman kode OTP). Hasil pengujian menunjukkan bahwa sistem berhasil memverifikasi kode OTP sesuai dengan fungsionalnya, sebagaimana yang terlihat pada Gambar 4.

Gambar 4. Pengujian Validasi Kode OTP Berdasarkan Masa Berlaku Kode

Pengujian Algoritma AES

Pemanfaatan algoritma AES pada sistem login internet kampus ditujukan agar proses autentikasi yang dilakukan oleh pengguna lebih terjaga kerahasiaannya. Variasi panjang kunci yang digunakan oleh algoritma AES memegang peranan penting dalam melakukan proses enkripsi dan dekripsi (Musliyana et al., 2016). Secara khusus, penelitian ini mengadopsi algoritma AES

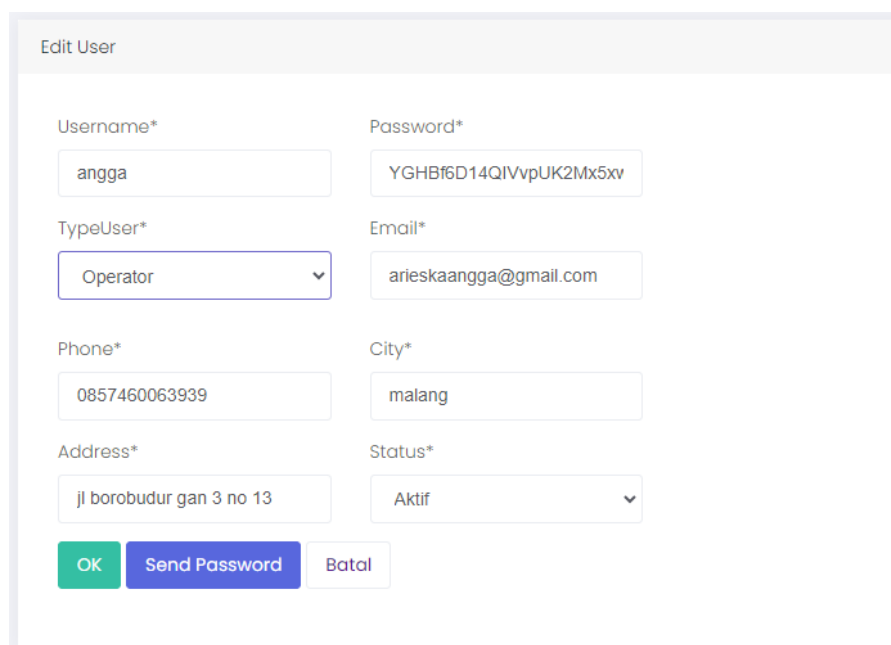
untuk mengubah data *password* pengguna (*plaintext*) ke dalam serangkaian karakter acak (*ciphertext*) hasil dari pembangkitan kunci dinamis, sebagaimana yang terlihat pada Gambar 5.



The screenshot shows a web form titled "Edit User". It contains several input fields: "Username*" with the value "Zairin Nur", "TypeUser*" with a dropdown menu showing "User", "Phone*", and "City*". The "Password*" field is highlighted with a red rectangle and contains the encrypted value "KornhNjHzF+4vSMaDoKOKIQ==". The "Email*" field contains "hyugajerry1@gmail.com".

Gambar 5. Penerapan Algoritma AES untuk Data Password Pengguna

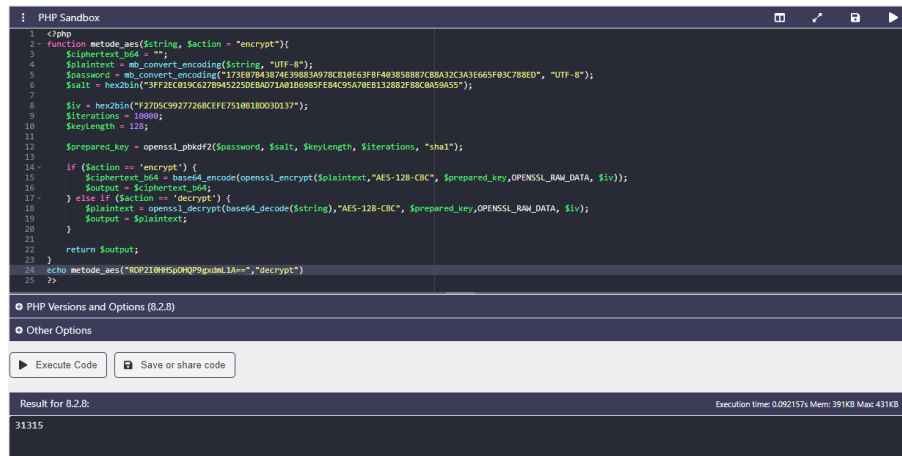
Hasil enkripsi dari algoritma AES ini dapat terlihat langsung pada tampilan *dashboard* pengguna maupun pada *database* operator. Pengguna tidak dapat melihat secara langsung *password* yang digunakan dalam sistem, demikian pula operator. Jika didapati kasus bahwa pengguna lupa terhadap *password* yang dibuat, maka pengguna dapat melakukan *request lupa password* kepada operator. Proses pengiriman *password* akan dilakukan *by sistem* (tombol *Send Password*), yaitu operator mengirimkan hasil dekripsi *password* kepada pengguna tanpa mengetahui *plaintext password* (lihat Gambar 6). Keseluruhan proses enkripsi dan dekripsi yang dibangun melalui sistem ini membuat kerahasiaan data menjadi lebih baik, karena data tidak dapat terbaca dengan mudah.



The screenshot shows a web form titled "Edit User". It contains several input fields: "Username*" with the value "angga", "TypeUser*" with a dropdown menu showing "Operator", "Phone*" with the value "0857460063939", "Address*" with the value "jl borobudur gan 3 no 13", "City*" with the value "malang", and "Status*" with a dropdown menu showing "Aktif". The "Password*" field contains the encrypted value "YGHbF6D14QIVvpUK2Mx5xv". At the bottom of the form, there are three buttons: "OK", "Send Password", and "Batal".

Gambar 6. Konfirmasi Lupa Password Pengguna oleh Operator

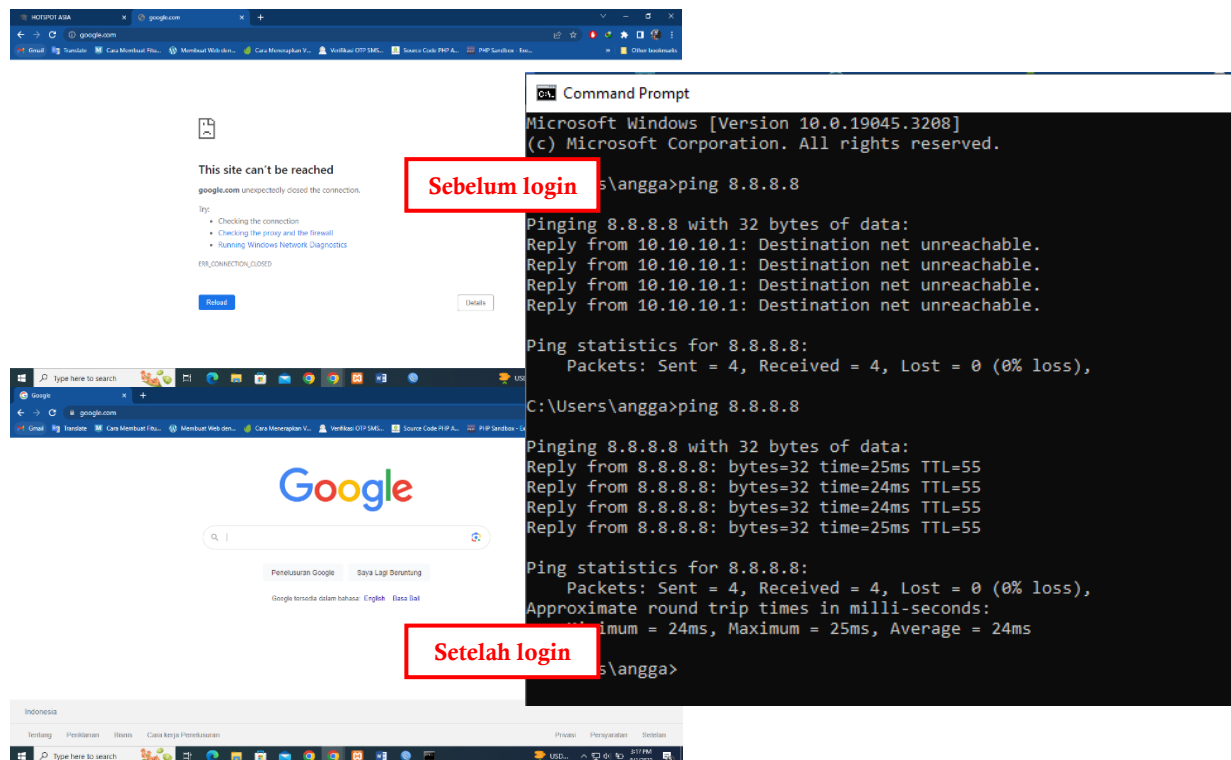
Untuk mengetahui kesesuaian penggunaan algoritma AES dalam proses enkripsi dan dekripsi data *password* pengguna, serangkaian pengujian dilakukan secara berulang dengan cara memasukkan *ciphertext password* pengguna ke dalam <https://onlinephp.io/>. Validasi telah dilakukan pada sampel pengguna dan didapatkan hasil dekripsi *plaintext* berhasil dilakukan dan menghasilkan data asli yang sesuai (lihat Gambar 7). Hasil pengujian menunjukkan bahwa sekalipun *ciphertext* yang dihasilkan berbeda-beda (tergantung pada pembangkit kunci dinamis), namun proses dekripsi yang dilakukan oleh sistem mampu mengembalikan informasi sesuai dengan data aslinya.



Gambar 7. Verifikasi Hasil Enkripsi – Dekripsi Password Menggunakan Algoritma AES

Pengujian Akses Internet Pengguna

Sebagaimana tujuan awal, sistem yang dibangun bertujuan untuk membatasi akses internet bagi pengguna. Hanya mereka yang terdaftar ke dalam sistem dan sudah divalidasi oleh operator, serta berhasil melewati proses autentikasi dengan tepat yang akan memiliki akses untuk terhubung ke internet. Pengujian dilakukan untuk mengevaluasi keberhasilan sistem dalam menjalankan tugasnya sesuai dengan tujuan pembuatan sistem. Pengujian dilakukan pada dua jenis pengguna, yaitu pengguna terdaftar dan pengguna tidak terdaftar. Hasil pengujian pada Gambar 8 menunjukkan bahwa sistem berhasil mengidentifikasi jenis pengguna dan memberikan akses internet kepada pengguna sesuai dengan kapasitasnya masing-masing.



Gambar 8. Validasi Pengguna untuk Sistem Autentikasi Internet Kampus

KESIMPULAN DAN SARAN

Kesimpulan

Internet dipandang sebagai salah satu pintu terdekat bagi masyarakat era digital saat ini dalam mengakses informasi dan komunikasi. Namun, kemudahan akses yang ditawarkan ini justru dimanfaatkan pula oleh orang-orang yang tidak bertanggungjawab untuk masuk secara ilegal dan merusak tatanan sistem. Oleh karena itu, keamanan masih menjadi isu krusial yang masih terus diupayakan oleh banyak pihak dalam rangka menjaga kerahasiaan data atau informasi. Beragam penelitian telah dikembangkan untuk menghasilkan sistem keamanan yang paling efektif dan terpercaya, salah satunya adalah autentikasi.

Penelitian ini mengusung konsep autentikasi ganda 2FA untuk sistem login internet kampus dengan mengintegrasikan metode OTP (*token-based*) dan algoritma AES (*knowledge-based*). Mekanisme OTP dikerjakan oleh sistem dengan cara membangkitkan kode TP dari data pengguna yang meliputi *username*, *password* dan alamat *e-mail*, dengan menggunakan algoritma hash SHA-256 pada kurun waktu tertentu. Pada waktu bersamaan, sistem juga melakukan enkripsi terhadap *password* pengguna dengan menggunakan algoritma AES. Kombinasi kerja keduanya membuat proses autentikasi lebih aman dilakukan oleh pengguna yang akan mengakses internet.

Hasil penelitian menunjukkan bahwa mekanisme OTP dalam proses autentikasi melalui e-mail memberikan keamanan yang lebih baik dibandingkan mekanisme *static password* karena OTP hanya berlaku untuk satu kali sesi autentikasi dengan masa hidup kode tidak lebih dari 180 detik. Algoritma AES juga bekerja bersamaan dengan proses OTP dengan melakukan enkripsi pada masukan data *password* pengguna. Sistem akan tetap menyimpan data dalam bentuk kode enkripsi, baik pada *dashboard* pengguna, operator hingga *database*. Keseluruhan proses enkripsi dan dekripsi yang dibangun melalui sistem ini membuat kerahasiaan data menjadi lebih baik, karena data tidak dapat terbaca dengan mudah. Pada akhirnya, hanya pengguna yang terverifikasi yang memiliki akses untuk menggunakan internet. Dengan demikian, penggunaan internet di lingkungan kampus menjadi aman dan tepat guna.

Saran

Pemanfaatan mekanisme autentikasi baiknya dilakukan secara terintegrasi untuk jaringan kabel maupun nirkabel. Lebih lanjut, mekanisme ini dapat dikembangkan untuk sistem *single sign-on* kampus. Perlu dilakukan komparasi dengan algoritma enkripsi lainnya yang memiliki panjang bit yang lebih bervariasi, untuk meningkatkan kompleksitas hasil enkripsi.

UCAPAN TERIMA KASIH

Terimakasih ditujukan kepada tim Unit Pelaksana Teknis (UPT) Jaringan dan Komputer Institut Asia Malang yang telah memberikan dukungan data dan infrastruktur perangkat selama proses keberlangsungan penelitian ini.

REFERENSI

- Anwar, N., Abduh, M., & Santosa, N. B. (2018). Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 2(3), 783–791. <http://jurnal.iaii.or.id>
- Balilo, B. B., Gerardo, B. D., Medina, R. P., & Byun, Y. (2017). An Improved OTP Grid Authentication Scheme Email-Based using Middle-Square for Disaster Management System. *International Journal of Grid and Distributed Computing*, 10(11), 43–56. <https://doi.org/10.14257/ijgdc.2017.10.11.05>

- Imamah. (2018). One Time Password (OTP) Based on Advanced Encrypted Standard (AES) and Linear Congruential Generator(LCG). *Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, 391–394.
- Kaur, S., Kaur, G., & Shabaz, M. (2022). A Secure Two-Factor Authentication Framework in Cloud Computing. *Security and Communication Networks*, 2022. <https://doi.org/10.1155/2022/7540891>
- Kelana, O. H., Lucky, P., Irawan, T., & Halim, P. M. (2021). Implementasi One Time Password dengan Metode Advanced Encryption Standard. *Prosiding Seminar Nasional Sistem Informasi Dan Teknik Informatika*, 36–53.
- Kurniawan, D. E., Iqbal, M., Friadi, J., Hidayat, F., & Permatasari, R. D. (2021). Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance. *Journal of Physics: Conference Series*, 1783(1). <https://doi.org/10.1088/1742-6596/1783/1/012041>
- Musliyana, Z., Arif, T. Y., & Munadi, R. (2016). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. *Jurnal Rekayasa ElektriKa*, 12(1), 21–29. <https://doi.org/10.17529/jre.v12i1.2896>
- Oluwakemi Christiana, A., Noah Oluwatobi, A., Ayomide Victory, G., & Roseline Oluwaseun, O. (2019). A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme. *Journal of Physics: Conference Series*, 1299(1). <https://doi.org/10.1088/1742-6596/1299/1/012059>
- Prayogo, A., & Rony, M. A. (2018). Implementasi One Time Password pada Sistem Login dengan Algoritma SHA-256 dan DES pada Aplikasi EO Blucampus Berbasis Client Server. *SKANIKA*, 1(2), 146–152.
- Riyan Andriyanto, M., Sukmasetya, P., & Penulis Korespondensi, E. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of Computer System and Informatics (JoSYC)*, 4(1), 179–187. <https://doi.org/10.47065/josyc.v4i1.2451>
- Styugin, M. (2019). Dynamic key password authentication. In *Int. J. Security and Networks* (Vol. 14, Issue 2). <http://dkauth.com>.
- Susdyastama Putra, Y., Indriastuti, M. T., & Mukti, S. (2020). Optimalisasi Nilai Throughput Jaringan Laboratorium Menggunakan Metode Hierarchical Token Bucket (Studi Kasus: STMIK Asia Malang). *Jurnal Ilmiah NERO*, 5(2), 83–90.
- Taqwim, M. A., Kusyanti, A., & Siregar, R. A. (2021). Implementasi Algoritme Speck Untuk Enkripsi One-Time Password Pada Two-Factor Authentication. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 5(7), 3103–3111. <http://j-ptiik.ub.ac.id>
- Zhan, W., & Ye, X. (2020). Research on Dynamic Identity Authentication Mechanism Based on Digital Signature. *Journal of Physics: Conference Series*, 1693(1). <https://doi.org/10.1088/1742-6596/1693/1/012009>