INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 6 Tahun 2023 Page 5279-5292
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Penerapan JSON Web Token sebagai Strategi Pengamanan Data pada Aplikasi MultiMasjid

Unggul Budi Astowo[1✉], Ari Sujarwo[2]
Teknik Informatika, Universitas Islam Indonesia
Email: Unggulbudiatowo@gmail.com[1✉]

Abstrak

Banyak perubahan telah terjadi dalam sistem pengelolaan masjid karena kemajuan teknologi informasi. Penggunaan aplikasi berbasis mobile menjadi solusi yang tepat untuk membantu takmir mengelola masjid dengan lebih baik. Namun, pengelolaan data jamaah yang bersifat privat menimbulkan risiko kebocoran dan penyalahgunaan data. Oleh karena itu, peningkatan keamanan data menjadi prioritas dalam merancang aplikasi pengelolaan masjid. Tujuan dari penelitian ini adalah untuk merencanakan dan menerapkan JSON Web Token (JWT) pada aplikasi Multimasjid menggunakan algoritma hash SHA-512 untuk meningkatkan keamanan otorisasi dan autentikasi pengguna. Metode waterfall adalah model pengembangan perangkat lunak yang digunakan. Hasil penelitian menunjukkan bahwa implementasi JWT dan SHA-512 dapat menjamin keamanan data, mencegah akses yang tidak sah, serta memberikan respons yang cepat dalam autentikasi dan otorisasi pengguna. Disimpulkan bahwa perencanaan implementasi JWT dan SHA-512 dapat meningkatkan keamanan aplikasi Multimasjid.

Kata Kunci: *Aplikasi Multimasjid, JSON Web Token, Keamanan Data*

Abstract

Many changes have occurred in the mosque management system due to the advancement of information technology. The use of mobile-based applications is the right solution to help takmir manage mosques better. However, the management of private congregation data poses the risk of data leakage and misuse. Therefore, data security improvement is a priority in designing mosque management applications. The purpose of this study is to plan and implement JSON Web Token (JWT) on the Multimasjid application using the SHA-512 hash algorithm to improve user authorization and authentication security. The waterfall method is the software development model used. The results of the study show that the implementation of JWT and SHA-512 can guarantee data security, prevent unauthorized access, and provide fast responses in user authentication and authorization. It is concluded that the planning of implementing JWT and SHA-512 can improve the security of the Multimasjid application.

Keyword*: Data Security, JSON Web Token, Mutimasjid Application*

PENDAHULUAN

Di era modern saat ini, kemajuan teknologi telah membawa perubahan signifikan dalam pengelolaan masjid. Dengan perkembangan teknologi informasi dan komunikasi, penggunaan teknologi menjadi penting untuk mengatasi berbagai masalah yang dihadapi pengelolaan masjid. Pendidikan abad 21 menuntut kita untuk melek terhadap perkembangan teknologi, menggunakan teknologi informasi dan komunikasi secara bijaksana, berpikir kritis, serta menganggap teknologi informasi sebagai media literasi modern (Dedy et al., 2021). Oleh karena itu, pengelolaan masjid harus beradaptasi dengan kemajuan teknologi ini untuk memberikan layanan yang lebih baik kepada jamaah dan masyarakat sekitar serta meningkatkan efisiensi dalam menjalankan berbagai kegiatan di masjid, sehingga keberadaan masjid dapat berfungsi dengan baik dan memberi manfaat bagi masyarakat sekitarnya melalui manajemen masjid yang baik(Qadaruddin et al., 2016).

Dalam rangka meningkatkan efisiensi pengelolaan masjid, perancangan aplikasi berbasis mobile menjadi solusi yang tepat untuk membantu para takmir dalam mengelola masjid dengan lebih baik. Pengelolaan masjid tidak lepas dari kebutuhan pengelolaan data pribadi. Data pribadi harus dilindungi karena merupakan hak privasi setiap orang. Data pribadi jamaah yang disimpan dan dikelola oleh pengurus masjid perlu mendapatkan perhatian khusus terkait perlindungan privasi dan keamanan informasi. Hal ini sesuai dengan Undang-Undang Nomor 27 Tahun 2022 yang menjadi landasan hukum utama di Indonesia tentang perlindungan data pribadi. Undang-undang ini mengharuskan semua pengolahan data pribadi menghormati hak privasi individu sebagaimana diatur dalam Pasal 16 E ayat (2). Pasal ini menegaskan bahwa pengolahan data pribadi harus melindungi data

dari akses, pengungkapan, manipulasi, penyalahgunaan, kerusakan, atau penghapusan data yang tidak sah. Jika terjadi kebocoran data, maka dapat dikenakan sanksi pidana sesuai dengan pasal yang berlaku. Hal ini sejalan dengan tujuan untuk memberikan perlindungan data yang optimal. Oleh karena itu, diperlukan sistem informasi yang didesain dengan tingkat keamanan yang sangat tinggi (Riyadi & Toto Tohir Suriaatmadja, 2023).

Dalam pengembangan sebuah sistem, keamanan data merupakan masalah utama yang perlu diatasi. Kehadiran informasi sensitif, seperti data pribadi pengguna, jadwal, dan catatan terkait pendanaan, menuntut perlindungan yang kuat dari akses yang tidak sah. Keamanan data dan privasi pengguna semakin penting karena semakin banyak data dan informasi yang diproses dan disimpan dalam aplikasi masjid.

Oleh sebab itu, keamanan data menjadi salah satu prioritas utama dalam merancang sebuah aplikasi pengelolaan masjid. Dengan semakin banyaknya data yang dikumpulkan dan diakses, perlindungan data dan privasi pengguna menjadi hal yang kritis. Solusi yang diusulkan untuk meningkatkan keamanan data pada sistem pengelolaan masjid yaitu dengan mengaplikasikan enkripsi pada tabel *database* aplikasi dan melakukan pengamanan otorisasi pengguna menggunakan JSON Web Token.

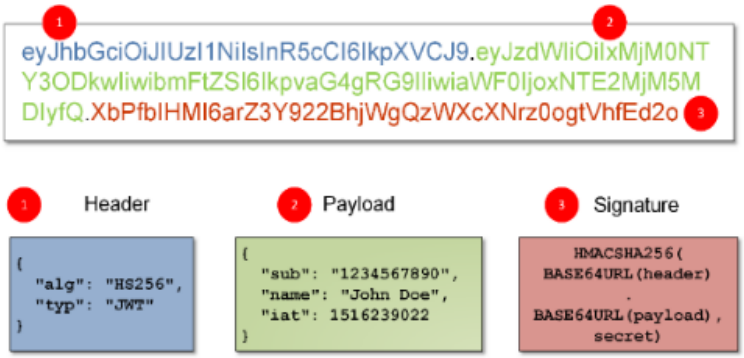
Enkripsi merupakan prosedur untuk mengubah informasi asli menjadi bentuk yang tak terbaca atau tak terlihat, dengan cara mengacak atau menguraikan data informasi tersebut. Sementara itu, dekripsi adalah kebalikan dari enkripsi, yaitu prosedur untuk mengembalikan informasi yang telah diacak ke bentuk karakter aslinya yang dapat terbaca dan terlihat (Prayudi & Halik, 2005). Istilah enkripsi (*encryption*) secara etimologis berasal dari bahasa Yunani *kryptos* yang memiliki arti rahasia atau tersembunyi (Rahmadi & Yunita, 2020). Tujuan dari enkripsi adalah agar isi dan makna data aslinya menjadi tidak dapat dimengerti atau tidak bermakna jika dibaca tanpa melalui proses dekripsi terlebih dahulu dengan kunci yang tepat. Dengan demikian, enkripsi bertujuan untuk menjaga kerahasiaan, keaslian, keutuhan, dan ketersediaan data penting dengan cara mengamankannya dalam wujud data sandi yang hanya dapat diakses oleh pihak-pihak berwenang saja.

Menerapkan teknik enkripsi di dalam database yang menyimpan data sensitif jamaah sangatlah penting untuk melindungi kerahasiaan dan mencegah penyalahgunaan data. Jika data jamaah yang bersifat privat ini disimpan tanpa enkripsi, maka apabila database berhasil diakses oleh pihak yang tidak bertanggung jawab, data jamaah dapat dicuri dan disalahgunakan untuk tindak kejahatan seperti pencurian identitas atau penipuan. Penggunaan enkripsi kuat pada database jamaah diperlukan agar data pribadi tersimpan aman dan terjaga kerahasiaannya meskipun database berhasil disusupi. Enkripsi database adalah cara efektif melindungi privasi jamaah serta mencegah dampak negatif dari

pencurian atau kebocoran data.

Selain enkripsi sebagai keamanan data pada database, menerapkan keamanan data juga penting dilakukan pada proses otorisasi pengguna dengan memanfaatkan JSON Web Token (JWT). JWT merupakan sebuah token yang berisi informasi yang digunakan untuk proses otentikasi dan pertukaran informasi (Painem & Soetanto, 2020). Pada umumnya JWT digunakan pada proses otorisasi karena token JWT dapat digunakan untuk melakukan otentikasi dan otorisasi pengguna dengan aman karena JWT menyimpan klaim atau informasi pengguna di dalam payload-nya yang telah ditandatangani secara digital. Salah satu komponen penting dalam arsitektur JWT adalah algoritma HMAC SHA-512, yang digunakan untuk mengenkripsi token saat melakukan proses autentikasi (Setiawan & Purnamasari, 2020). Algoritma ini merupakan salah satu algoritma enkripsi yang paling unggul dan efisien, terutama jika diimplementasikan pada arsitektur 64-bit (Rahmatulloh et al., 2018). Algoritma ini dapat meningkatkan kecepatan dan ukuran data pada keamanan REST, yang merupakan gaya arsitektur untuk membuat layanan web yang ringan dan fleksibel. Dalam proses otorisasi dan otentikasi, JWT digunakan secara luas. Mereka memungkinkan komunikasi data yang aman antara berbagai pihak, seperti server dan klien, setelah pengguna melakukan otentikasi. Aplikasi dapat memverifikasi identitas pengguna dan memberikan izin akses yang sesuai dengan informasi yang terenkripsi dalam token JWT. Dengan demikian, integritas dan otentikasi informasi dalam JWT dapat terjamin sehingga dapat mencegah penyamaran identitas maupun manipulasi data oleh pihak yang tidak berwenang.

JWT adalah token dalam format string yang sangat ringkas dan mengandung informasi independen. Token ini digunakan untuk sistem otentikasi dan pertukaran informasi antarsistem (Kelvin, 2019). Dengan JSON yang mengimplementasikan JWT, aplikasi dapat memverifikasi identitas pengguna dengan mengirimkan token dari klien ke server sebagai bukti autentikasi. Selanjutnya, server akan memverifikasi token tersebut dan memberikan akses ke sumber daya yang diminta jika token tersebut valid. JWT memiliki tiga komponen yang dibedakan oleh titik (“.”), yaitu header, payload, dan signature, seperti yang ditunjukkan pada gambar berikut (Mahindrakar & Pujeri, 2020).



Gambar 1. Konsep JWT

Algoritma hash SHA-512 yang akan diimplementasikan merupakan fungsi hash satu arah yang dibuat oleh Badan Keamanan Nasional (NSA) Amerika Serikat dan dipublikasikan sebagai Standar Pengolahan Informasi Federal (FIPS) oleh Lembaga Standar dan Teknologi Nasional (NIST) pada tahun 1993. SHA-512 merupakan bagian dari keluarga algoritma SHA-2, bersama dengan SHA-224, SHA-256, dan SHA-384 (Ipdal, 2021). Penggunaan algoritma hash SHA-512 akan meningkatkan keamanan dan melindungi data serta informasi pengguna dari akses yang tidak sah dan potensi kebocoran data.

Makalah ini akan berfokus menjelaskan rencana penerapan JWT dengan menggunakan algoritma hash SHA-512 pada aplikasi Multimasjid. Pembahasan lebih detail mengenai langkah-langkah dan strategi yang akan diterapkan dalam perencanaan implementasi ini akan dijabarkan pada bagian-bagian berikutnya.

METODE PENELITIAN

Subjek & Objek Penelitian

Subjek penelitian adalah komponen utama yang menjadi fokus pembahasan dalam sebuah penelitian. Subjek bisa berupa kelompok, individu, benda, topik, atau bidang ilmu yang diteliti. Sementara objek penelitian adalah perilaku atau fenomena yang terjadi pada subjek penelitian dan diobservasi selama penelitian. Subjek dan objek penelitian sangat menentukan desain penelitian, karena mempengaruhi perumusan masalah, batasan penelitian, tujuan, manfaat, dan metodologi yang digunakan. Pemilihan subjek dan objek yang tepat merupakan dasar penting dalam merancang dan melaksanakan sebuah penelitian. Subjek dari penelitian ini difokuskan pada JSON Web, sedangkan objek pada penelitian ini adalah implementasi JSON Web Token sebagai pilihan keamanan data pada aplikasi Multimasjid.

Sumber Data

Sumber data yang memadai sangat penting dalam proses penelitian, tanpa sumber data penelitian tidak dapat berkembang. Karena itu, menggunakan metode pengumpulan data yang sesuai dengan kebutuhan akan sangat mendukung peneliti untuk mencapai hasil yang diinginkan dari penelitian yang dilakukan. Dalam penelitian ini, data dikumpulkan dari sumber data primer yang didapatkan langsung dari asalnya dan sumber data sekunder yang didapatkan dari sumber yang sudah ada sebelumnya.

Data primer dalam penelitian ini diperoleh dengan metode observasi, yaitu cara pengumpulan data di mana peneliti melihat dan menelusuri subjek penelitian secara langsung untuk mendapatkan data dan fakta-fakta yang diperlukan untuk mendukung dan memperkuat hasil penelitian. Data primer yang dihasilkan dari observasi antara lain berupa data mengenai pengelola masjid (takmir) dan data jamaah masjid. Selain itu, Penelitian ini juga memanfaatkan data sekunder yang berasal dari studi literatur yaitu teknik pengumpulan data melalui berbagai referensi literatur terkait topik penelitian dari berbagai sumber terpercaya dan bereputasi baik. Melalui studi pustaka, peneliti berupaya mengumpulkan data dari beragam referensi yang berhubungan dan relevan dengan isu atau permasalahan yang sedang diteliti untuk memperkaya substansi penelitian.

Indikator Keberhasilan

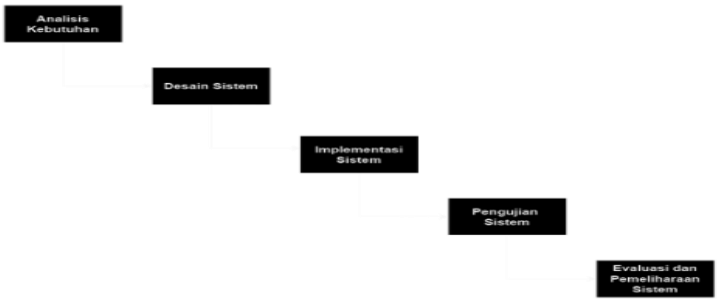
Indikator keberhasilan merupakan hal yang dapat menunjukkan tercapainya tujuan dalam sebuah penelitian. Keberhasilan suatu penelitian ditentukan oleh terpenuhi atau tidaknya tujuan yang sudah ditetapkan sebelumnya. Adapun indikator keberhasilan pada penelitian ini adalah terjadinya proses otentikasi dan otorisasi dengan aman. Setiap permintaan mengakses data pada sistem harus melalui proses otentikasi dan otorisasi dengan memverifikasi JWT (JSON Web Token) yang dikirimkan pengguna. JWT tersebut harus valid dan ditandatangani dengan benar untuk membuktikan identitas pengguna yang mengakses. Ketika pengguna berhasil login, mereka akan mendapatkan token JWT. Token JWT ini selanjutnya digunakan untuk otentikasi pada setiap permintaan akses data, sehingga pengguna hanya dapat melihat dan menginput data jika permintaan tersebut menyertakan token JWT yang valid. Sebaliknya, permintaan tanpa token JWT yang valid akan ditolak dan pengguna tidak akan dapat mengakses data.

Metode Penelitian

Agar tujuan penelitian dapat tercapai, diperlukan serangkaian proses dalam menjalankan penelitian tersebut. Proses-proses sistematis ini disebut dengan metode penelitian. Metode penelitian menjadi penting karena menunjukkan tahapan-tahapan yang harus dilakukan selama penelitian berlangsung. Dengan mengikuti metode penelitian yang

tepat, peneliti dapat melakukan penelitian secara terstruktur sehingga tujuan akhir penelitian dapat tercapai.

Dalam penelitian ini, metodologi yang digunakan mengacu pada metode waterfall yang terdiri dari lima tahapan utama, yaitu: (1) Analisis Kebutuhan untuk mendefinisikan fitur dan fungsionalitas sistem berdasarkan kebutuhan user; (2) Desain Sistem untuk membuat perancangan arsitektur dan detail teknis sistem; (3) Implementasi Sistem untuk menerjemahkan desain ke dalam kode-kode program; (4) Pengujian Sistem baik secara unit maupun terintegrasi untuk memastikan sistem berjalan sesuai kebutuhan; dan (5) Evaluasi dan Pemeliharaan untuk mengevaluasi kinerja sistem setelah digunakan dan melakukan pemeliharaan jika dibutuhkan. Penulis memilih model waterfall karena sifatnya yang berurutan dan sistematis, dimana setiap tahapan harus diselesaikan terlebih dahulu secara penuh sebelum dapat melanjutkan ke tahapan berikutnya. Konsep berurutan ini mudah untuk dipahami dan diimplementasikan. Gambaran umum dari alur model waterfall dapat dilihat pada diagram di bawah ini:



Gambar 2. Metode Waterfall

Analisis Kebutuhan Sistem

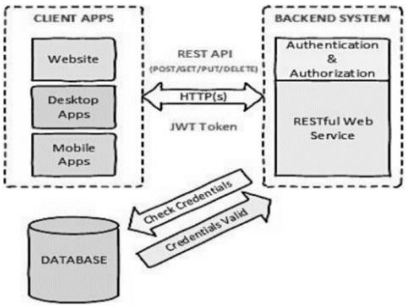
Analisis kebutuhan sistem dilakukan untuk pemecahan masalah yang terjadi pada sistem menjadi beberapa bagian agar mudah dipahami dalam mengidentifikasi masalah. Tahap ini memiliki peran untuk merencanakan struktur yang akan dikembangkan sesuai dengan permasalahan yang terjadi. Perencanaan implementasi penggunaan JSON Web Token dimulai dengan memahami semua kebutuhan sistem seperti informasi arsitekstur, database, alur proses bisnis BPMN, dokumentasi API, dan kebutuhan fungsional sistem.

Desain Sistem

Setelah mengumpulkan data-data yang dibutuhkan sebagai persyaratan untuk perancangan sistem, tahap selanjutnya adalah membuat desain sistem secara keseluruhan. Pada tahap perancangan ini, beberapa diagram dan rancangan akan dibuat guna menggambarkan detail dari sistem yang akan dibangun, seperti diagram kasus penggunaan (use case) untuk mengetahui fungsionalitas yang ada, diagram aktivitas (activity diagram) untuk menggambarkan workflow/alur kerja sistem, antarmuka sistem, serta rancangan basis

data untuk mendefinisikan struktur penyimpanan data yang diperlukan. Hasil dari tahap perancangan desain sistem ini nantinya akan digunakan sebagai acuan dalam pengembangan dan implementasi sistem.

Implementasi Sistem



Gambar 3. Implementasi JWT pada Arsitektur Aplikasi MultiMasjid

Gambar tersebut menunjukkan sistem backend yang mengurus proses autentikasi dan otorisasi dalam RESTful Web Service. Server akan mengirim token JWT sebagai kunci untuk mengakses sumber daya di server setelah login sukses. REST API ini bisa diakses oleh berbagai macam klien, seperti web, desktop, dan mobile. Beberapa langkah yang direkomendasikan dalam mekanisme ini adalah:

1. Pengguna adalah klien berbasis mobile.
2. Pengguna melakukan login, dan kredensialnya akan dikirim ke API.
3. Untuk mengakses fitur pengelolaan jamaah masjid, pengguna harus memiliki token yang valid. Jika token tidak ada atau sudah habis masa berlakunya, sistem akan menolak permintaan pengguna.
4. Backend system akan melakukan otentikasi pengguna sebelum memungkinkan aksi tertentu.
5. Database akan memeriksa kredensial yang diberikan.
6. Token JWT akan dikembalikan ke klien jika kredensial sesuai.

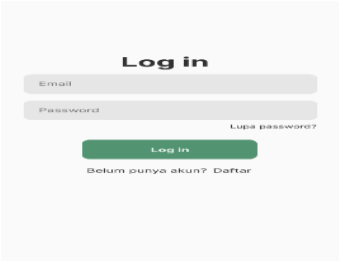
Setelah memastikan token masih valid, langkah berikutnya adalah mengecek apakah token memiliki otorisasi untuk mengakses sumber daya yang diinginkan pengguna. Jika ya, maka layanan web akan memberikan sumber daya yang dibutuhkan.

HASIL DAN PEMBAHASAN

Pada tahap ini, akan menyampaikan hasil dan pembahasan dari penelitian yang telah dilakukan secara mendalam. Pembahasan akan mencakup hasil yang kami peroleh dari pelaksanaan implementasi yang telah dilakukan, serta berbagai pengujian yang telah dijalankan untuk menguji kinerja dan kehandalan sistem yang telah dibangun.

Perancangan Aplikasi

Dalam tahap awal penelitian ini, kami merancang aplikasi dengan membuat gambaran umum tentang bagaimana sistem akan berjalan dan tampilan utama aplikasi. Aplikasi ini akan memiliki beberapa menu yang memungkinkan pengguna untuk melihat, mengedit, dan menghapus data. Gambar di bawah ini adalah desain halaman login, sebagaimana yang ditunjukkan dalam gambar 4



Gambar 4. Rancangan Halaman Login Aplikasi

Tampilan rancangan pada dashboard pengguna ketika mengakses aplikasi ini mirip dengan contoh yang terlihat pada gambar 5

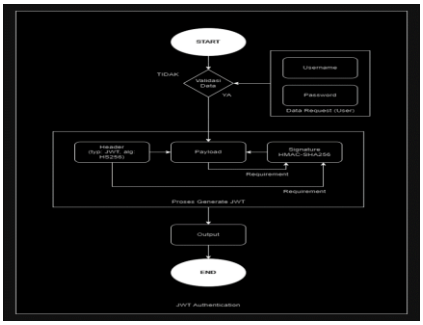
Gambar 5. Rancangan Halaman Utama Aplikasi

Implementasi JSON Token (JWT) pada Authentication User

Setelah perancangan selesai, langkah selanjutnya adalah mengimplementasikannya menggunakan bahasa pemrograman JavaScript. Tahapan diawali dengan pembuatan halaman login untuk mengautentikasi pengguna dengan menerapkan JSON Web Token (JWT) menggunakan algoritma SHA-512.

Penulisan Function JWT pada Authentication User

Pada tahap ini, fungsi JSON Web Token (JWT) ditulis pada aplikasi dengan menerapkan algoritma SHA-512. Alur proses dari aplikasi digambarkan dalam sebuah flowchart sebagai berikut.



Gambar 6. Flowchart Authentication JWT

Gambar 6 menampilkan alur flowchart aplikasi yang menjelaskan bagaimana sistem melakukan pemeriksaan apakah pengguna memiliki token atau tidak. Jika pengguna tidak memiliki token, sistem akan mengarahkannya ke halaman login, dan setelah pengguna memasukkan kredensial yang valid, token akan diberikan. Jika kredensial tidak valid, pengguna akan dikembalikan ke halaman login. Setelah mendapatkan token, pengguna akan menggunakannya untuk melakukan permintaan data. Jika token yang dimiliki pengguna valid, sistem akan mengirimkan permintaan data yang diminta oleh pengguna.

Kemudian, langkah-langkah yang telah dirancang akan diterapkan dalam bahasa pemrograman seperti yang ditunjukkan berikut. Implementasi ini akan mencakup penulisan kode menggunakan bahasa pemrograman, seperti JavaScript, untuk mengikuti langkah-langkah yang ada dalam flowchart. Proses implementasi ini meliputi pendaftaran dan login pengguna kedalam aplikasi, manipulasi token, pengelolaan sesi pengguna, serta verifikasi dan otentikasi dalam aplikasi.

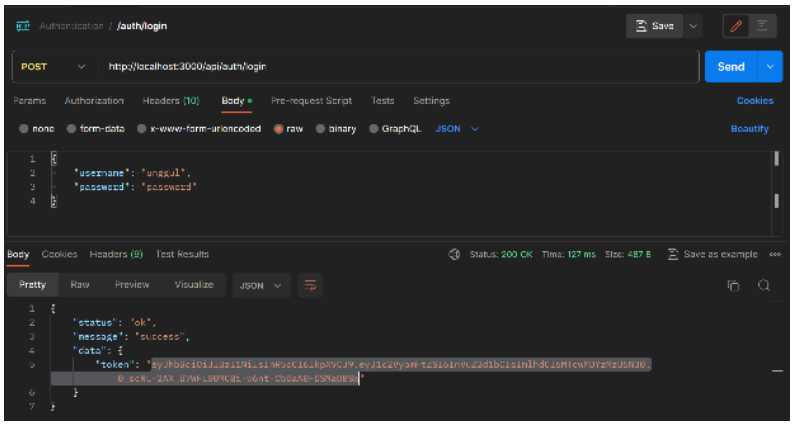
```
router.post("/register",
async(req,res)=>{
   let user = await User.findOne({email : req.body.email});
   if (user)
   return res.send("User with given email is existing!");

 user= new User({
   fullname: req.body.fullname,
   email: req.body.email,

password: await bcrypt.hash(req.body.password, 10),


})
const savedUser = await user.save();
const response = new Response.Success (false, null,
savedUser)
res.send(200).json(response);
}
)
//Login
router.post("/login",
async(req,res)=> {
   const user = await User.findOne({email:req.body.email});
   if (user)
   {
      if(bcrypt.compare(req.body.password, user.password))
      {
         res.send(
            {
               _id:user._id,
               fullname:user.fullname,
               email:user.email,
               password:user.password,
               token:generateLogToken(user),
            }
         )
      }
   }
});

// Penerapan JWT
const jwt = require ("jsonwebtoken")
 const generateLogToken = (user)=>{
   return jwt.sign(
      {
         _id:user._id,
         fullname:user.fullname,
         email:user.email,
      },
      process.env.JWT_PASS || 'tes123',
      {
         expiresIn:'10d',
      }

   );
};

module.exports = generateLogToken;

// Validasi token
router.post('/', verifyToken, async (req, res) => {
  try {


 const newJamaah = await Jamaah.create({

      nama: req.body.nama,
      alamat: req.body.alamat,
      noTelp: req.body.noTelp
    });

    res.status(200).json({
      error: false,
      message: 'Data Jamaah berhasil disimpan',
      data: newJamaah
    });
  } catch (error) {

   console.log(error)
    res.status(500).json({
      error: true,
      message: error.message
    });
  }
});

module.exports = router;
```

Gambar 7. Implementasi Function JWT pada Backend

Gambar 3.4 menunjukkan penulisan fungsi JSON Web Token pada REST API Web Service. Source code ini berperan sebagai proses pembuatan dan login pengguna serta mekanisme autentikasi dan otorisasi pengguna dalam aplikasi yang mengimplementasikan JSON Web Token dengan algoritma SHA-512. Pengguna diminta untuk memasukkan kredensial yang mereka miliki, dan jika kredensial tersebut sesuai dengan yang ada di database, pengguna akan diberikan token yang nantinya digunakan untuk mengakses aplikasi.

Pengujian Authentication Users

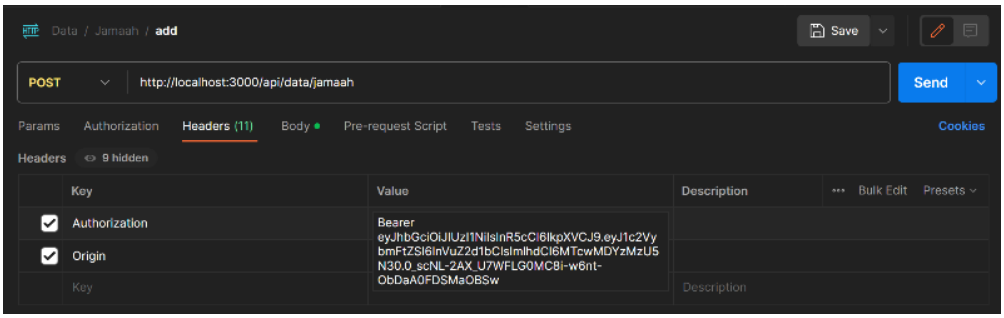
Pada tahap ini, validitas token JSON Web Token yang dihasilkan dari proses otentikasi login dengan menggunakan algoritma SHA-512 akan diperiksa. Pengujian dilakukan dengan menggunakan Postman sebagai klien REST API untuk menguji coba REST API yang telah dibuat. Pengujian dilakukan dengan memasukkan informasi yang benar, seperti nama pengguna dan kata sandi, untuk menghasilkan token yang nantinya akan digunakan dalam permintaan data selanjutnya.



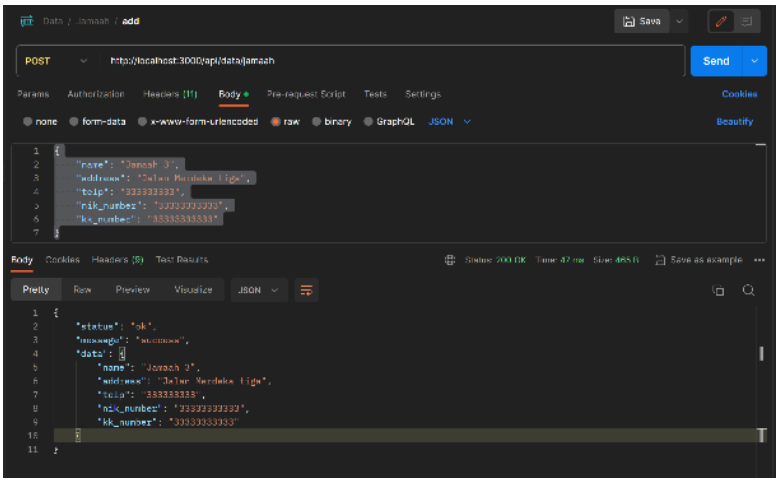
Gambar 8. Authentication User dengan JSON Web Token

Dari hasil gambar 3.5, terlihat bahwa telah dilakukan proses login yang menghasilkan token sebagai kunci untuk mendapatkan akses dalam permintaan data selanjutnya. Setiap token memiliki nilai yang berbeda karena setiap token menyimpan data pengguna dan hak akses yang unik.

Setelah melakukan pengujian proses otentikasi login, dilakukan proses pengujian dengan melakukan request POST ke endpoint /jamaah dengan menyertakan JSON Web Token (JWT) yang valid di Authorization header menggunakan format Bearer token. Token JWT digunakan untuk otentikasi dan otorisasi akses ke endpoint tersebut. Request menyertakan data jamaah masjid baru pada request body.



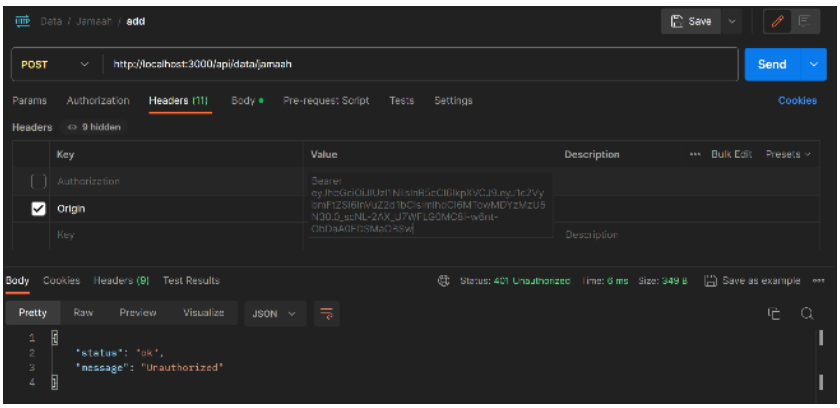
Gambar 9. Token JWT untuk melakukan Request Post



Gambar 10. Hasil Request POST Penambahan Jamaah Baru Menggunakan Token Valid

Pada gambar diatas server mengembalikan response code 200 OK dan data jamaah yang telah berhasil disimpan di database. Hal ini menunjukkan bahwa request yang menyertakan JWT token valid berhasil melalui proses otentikasi dan otorisasi, sehingga dapat mengakses endpoint serta menyimpan data jamaah baru.

Selanjutnya, dilakukan pengujian dengan melakukan request POST ke endpoint /jamaah tanpa menyertakan JWT pada Authorization header. Server mengembalikan response 401 Unauthorized dan pesan error 'No token provided'. Hal ini sesuai requirement bahwa setiap request ke endpoint /jamaah harus melampirkan JWT token yang valid untuk autentikasi dan otorisasi. Request tanpa token valid akan ditolak dan tidak dapat mengakses endpoint maupun menyimpan data.



Gambar 11. Status JSON Web Token Tidak Valid

SIMPULAN

Perencanaan implementasi JSON Web Token (JWT) dengan algoritma hash SHA-512 dalam aplikasi Multimasjid menggunakan arsitektur RESTful Web Service bertujuan untuk meningkatkan keamanan otorisasi dan autentikasi aplikasi. Dengan mengimplementasikan JWT, aplikasi dapat memverifikasi identitas pengguna melalui token yang dikirim dari klien ke server sebagai bukti autentikasi. Algoritma hash SHA-512 yang digunakan akan meningkatkan keamanan data dan melindungi informasi pengguna dari akses yang tidak sah. Dalam uji coba, implementasi JWT dengan SHA-512 memberikan hasil yang optimal dalam hal kecepatan dan respons dari server, menjamin bahwa sumber daya aplikasi dapat diakses dengan aman dan sesuai hak akses pengguna.

DAFTAR PUSTAKA

A. Rahmatulloh, H. Sulastri, and R. Nugroho, "Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512," 2018.

A. Setiawan and A. I. Purnamasari, "Implementasi JSON Web Token Berbasis Algoritma SHA-512 untuk Otentikasi Aplikasi BatikKita," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 6, pp. 1036-, Dec. 2020, doi: 10.29207/resti.v4i6.2533.

G. A. Riyadi and Toto Tohir Suriaatmadja, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Bandung Conference Series: Law Studies*, vol. 3, no. 1, Jan. 2023, doi: 10.29313/bcsls.v3i1.4945.

G. Dedy *et al.*, "Paradigma Pendidikan Abab 21 Di Masa Pandemi Covid-19 (Tantangan Dan Solusi)," 2021.

Kelvin, "Simulasi E-Voting Pemilu Untuk Penyandang Tuna Netra Menggunakan Google Cloud Speech Berbasis Raspberry Pi (Uji Coba Yayasan Peduli Kesejahteraan Tuna Netra) Program Studi Teknik Informatika," 2019, [Online]. Available: http://repository.uinjkt.ac.id/dspace/handle/123456789/48647

M. Ipdal, "Analisa Metode SHA-512 Untuk Tanda Tangan Digital Pada File Video," 2021. doi: https://doi.org/10.47065/jimat.v1i1.87.

P. Mahindrakar and U. Pujeri, "Security Implications for Json web Token Used in MERN Stack for Developing E Commerce Web Application," *Int J Eng Adv Technol*, vol. 10, no. 1, pp. 39–45, Oct. 2020, doi: 10.35940/ijeat.A1663.1010120.

P. Painem and H. Soetanto, "Sistem Presensi Pegawai Berbasis Web Service Menggunakan Metode Restfull Dengan Keamanan JWT Dan Algoritma Haversine," *Fountain of Informatics Journal*, vol. 5, no. 3, p. 6, Nov. 2020, doi: 10.21111/fij.v5i3.4906.

P. Rahmadi and H. Yunita, "Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi," *Jurnal Cendikia*, vol. 19, no. 1, Apr. 2020, [Online]. Available: https://jurnal.dcc.ac.id/index.php/JC/article/view/331

Q. Qadaruddin, A. Nurkidam, and F. Firman, "Peran Dakwah Masjid dalam Peningkatan Kualitas Hidup Masyarakat," *Ilmu Dakwah: Academic Journal for Homiletic Studies*, vol. 10, pp. 222–239, Dec. 2016, doi: 10.15575/idajhs.v10i2.1078.

Y. Prayudi and I. Halik, "Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data," vol. 0, Jan. 2005.