TEPIAN Vol. 4 No. 3 (September 2023) p-ISSN 2721-5350 e-ISSN 2721-5369
doi.org/10.51967/tepian.v4i3.2880

Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan

Hendra Saputra *
Computer Engineering, Muhammadiyah University of East Kalimantan, Samarinda, 75124, Indonesia
hs048@umkt.ac.id
**Corresponding author*

Sayekti Harits Suryawan
Computer Engineering, Muhammadiyah University of East Kalimantan, Samarinda, 75124, Indonesia
shs500@umkt.ac.id

Faldi
Computer Engineering, Muhammadiyah University of East Kalimantan, Samarinda, 75124, Indonesia
fal146@umkt.ac.id

Bulan Suci Cahayawati
Computer Engineering, Muhammadiyah University of East Kalimantan, Samarinda, 75124, Indonesia
2011102441094@umkt.ac.id

Ririn Wahyuni
Computer Engineering, UMKT, Muhammadiyah University of East Kalimantan, 75124, Indonesia
2011102441049@umkt.ac.id

Submitted: 2023-07-18; Accepted: 2023-08-23; Published: 2023-09-01

Abstract— This research aims to evaluate and implement the utilization of JSON Web Token (JWT) to verify the authenticity of letters in the letter system at the University of Muhammadiyah in East Kalimantan (UMKT). The previous method relied solely on QR code signatures, which were susceptible to copying and manipulation, thus posing vulnerabilities in the letter verification process. Therefore, this study used JWT tokens as a more secure and effective verification mechanism. The research involved creating JWT tokens containing important information such as UUID, letter number, subject, content, sender, and recipient. These JWT tokens were inserted into the letters as part of the verification mechanism. The Muhammadiyah University of East Kalimantan letter system was updated to verify JWT tokens by extracting the token from the letter and checking the UUID against the database. The research results demonstrate that utilizing JWT tokens as a method for verifying the authenticity of letters provides advantages in terms of efficiency and accuracy. The letter system, which previously relied solely on QR code signatures, can be enhanced by using JWT tokens. The updated letter system can verify letters' authenticity more reliably and dependably, reducing the risks of manipulation or forgery. The utilization of JWT tokens in the Muhammadiyah University of East Kalimantan letter system offers significant benefits in improving the efficiency of the verification process and enhancing the accuracy of letter identification. In this context, this research provides a safer and more effective solution for ensuring the authenticity of letters, thereby enhancing the security and integrity of the letter management system at Muhammadiyah University of East Kalimantan.

Keywords— Token JWT, Letter Authenticity Verification, Letter System, Efficiency, Accuracy

I. INTRODUCTION

As an essential means of written communication in business activities, letters have transformed digitally, including the advent of E-Letter (electronic letters). E-Letter refers to letters created in digital form, facilitating the creation of incoming, outgoing, disposition, and electronic archiving letters (Nurhayati & Sutrisno, 2020) . Using E-Letter to manage correspondence in companies or institutions provides various benefits, such as cost, time, and space savings (Prihanto & Winarno, 2018). In the current era of digitalization, using E-Letter is crucial to support efficiency and effectiveness in correspondence management.

Furthermore, with E-Letter, letters can be accessed online and easily tracked, facilitating quick and timely delivery and receipt (Syukur et al., 2019). E-Letter also enhances the security and confidentiality of letters through data encryption technology (Prihanto & Winarno, 2018). Therefore, the utilization of E-Letter as a means of managing correspondence brings numerous benefits to companies or institutions in terms of efficiency, effectiveness, and security in the process of letter delivery and archiving.

The Muhammadiyah University of East Kalimantan already has an E-Letter application accessible at my.umkt.ac.id. The application already features a QR code as a method to validate the authenticity of the information in the letter. Although the E-Letter application with QR code offers advantages in simplifying and expediting the letter

the Delivery process, there are certain shortcomings to be considered. According to (Jati & Wijaya, 2018), one drawback of using QR codes in E-Letter applications is the vulnerability of data security. QR codes can be reprinted

Saputra , H., Suryawan , S. H., Faldi , F., Cahayawati , B. S., & Wahyuni , R. (2024). Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan. TEPIAN, 4(3). https://doi.org/10.51967/tepian.v4i3.2880

or scanned by unauthorized parties, leading to unauthorized duplication of letters and potential data manipulation or misuse. Additionally, QR codes lack sufficient authentication mechanisms to prove the authenticity of digital signatures (Wulandari & Novitasari, 2019). Therefore, an additional validation method such as JWT tokens is necessary to ensure the security and validity of letters in the E-Letter application.

JSON Web Token (JWT) is an open industry standard (RFC 7519) that enables securely transmitting encrypted information in JSON (JavaScript Object Notation) format between two parties (JWT.IO, 2015). JWT tokens consist of the header, payload, and signature. The header and payload are encrypted to form a token, while the signature is used to verify the token's authenticity.

In the E-Letter application, JWT tokens can be utilized as an additional validation method to ensure the security and validity of PDF-format letters. Before an E-letter is created as a PDF, a JWT token needs to be generated, including the UUID and information of the E-letter. The JWT token is then embedded into the PDF and sent to the recipient. Therefore, if the authenticity of the PDF needs to be validated in the future, the JWT token embedded within the E-Letter must be retrieved.

II. Literature Review

A. Related Research

Several previous studies related to this research include:

1. The paper "Performance comparison of signed algorithms on JSON Web Token" proposes the best encryption algorithm for JWT. Systems that thrive in the digital era require the ability to operate on multiple platforms, using web services and data exchange in JSON format, with authentication using JSON Web Token (JWT). JWT-based token authentication can solve interoperability issues, and in this research, the HMAC algorithm exhibits excellent performance in token generation time, token size, and data transfer speed (Gunawan & Rahmatulloh, 2019).
2. The paper "Security Implications for JSON Web Token Used in MERN Stack for Developing E-Commerce Web Application" discusses implementing authentication and authorization techniques using JSON Web Token (JWT) for role-based web services. The research seeks to produce a more secure JWT token by selecting appropriate secret keys, reducing storage, and generating less predictable keys (Mahindrakar & Pujeri, 2020).
3. "This research discusses the performance of JWT RSA-512 implemented in SOAP and RESTful web services. JWT serves as an authentication mechanism in web services, and in this study, a performance analysis was conducted to compare SOAP and RESTful. The test results show that the speed of the JWT RSA-512 token in the RESTful process is superior by 24.69% compared to SOAP, while the speed of JWT RSA-512 token authentication in RESTful is superior by 11.64% compared to SOAP. Additionally, the size of the JWT RSA-512 token generated in RESTful is only 1.25% superior to SOAP (Rahmatullo et al., 2019).
4. Implementation of RESTful with JWT for Booking Goods at Primajaya Multisindo" discusses the request of PT Primajaya Multisindo, which requires a system that can integrate data to be centralized and easily accessed. To fulfill this request, the tester implemented a web service equipped with JSON Web Token (JWT) authentication as the authentication process for RESTful to enhance data security. The result of the implementation is that the web service at PT Primajaya Multisindo can be accessed on multiple platforms, both web-based and mobile, and the system's security is improved by implementing JSON Web Token (JWT) for user authentication during login (Priyatna & Waluyo, 2022)
5. "Implementation of Security Features with JSON Web Token and Geo-tagging Feature in Training From Home Web Service Application" discusses the implementation of JSON Web Token (JWT) security feature and the development of a geo-tagging feature in a web service application to support the check-in the process from various locations. The researcher conducted experimental testing by implementing the security method using JSON Web Token (JWT) and improving information accuracy using the geo-tagging feature in the web service application. The testing process involved several stages: literature study, requirement analysis, system implementation, and evaluation. The results of the testing successfully implemented JSON Web Token (JWT) in the web service application, using tokens as a form of user authentication to access the web service. The tokens have a time limit of 24 hours, and if the username and password are entered incorrectly, access tokens are not granted. Additionally, if an incorrect token is entered, access to the application is denied. The evaluation process of the geo-tagging feature using the Google Maps method achieved an accuracy rate of 90.9%. It can be concluded that the Android-based web service application built provides accurate check-in position accuracy for the Training From Home program activities (Dirjen et al., 2017).
6. Implementation of Token-Based Method as Authentication Mechanism in IoT Middleware" discusses the development aimed at restricting unauthorized node communication with the middleware. The development involves adding a JSON Web Token (JWT) authentication mechanism, chosen for its compact size, allowing it to be sent through URLs, queries, or headers.

Saputra , H., Suryawan , S. H., Faldi , F., Cahayawati , B. S., & Wahyuni , R. (2024). Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan. TEPIAN, 4(3). https://doi.org/10.51967/tepian.v4i3.2880

The implementation process includes adding the authentication mechanism to the middleware, comprising web service and auth module implementation, as well as publisher and subscriber implementation. The testing process involves authentication without a token, authentication using a valid token, authentication using an expired token, data validity testing, and performance testing. The development successfully implements authentication in the IoT middleware by applying the authentication mechanism to each integrated gateway with the auth module responsible for the authentication process. With the authentication in place, the time required for nodes to establish a connection through publish and subscribe actions can be improved (Chamim Pratama et al., 2019).

7. Implementation of Constrained Application Protocol (CoAP) in Semantic IoT Web Service" discusses testing methods to address the limitations of sensor nodes in receiving diverse communications and the constraints of resource-constrained sensor nodes. The research uses JSON Web Token (JWT) authentication and authorization design methods. The testing results indicate the functional aspect, showing that the semantic IoT web service can receive data in the form of JSON, images, and videos through the CoAP communication protocol (Putra et al., 2019).
8. "Implementation of JWT (JSON Web Token) as Authentication Mechanism for MQTT Protocol on NodeMCU Devices" discusses testing by implementing JSON Web Token (JWT) as an authentication mechanism for the MQTT protocol on NodeMCU devices. The testing is conducted in three stages: username and password validation, token expiration testing, and token generation time testing. Through these tests, the research discovers varying token generation times influenced by the server's response to publisher requests. This indicates that the implemented JSON Web Token (JWT) can validate the username and password sent by the publisher and authenticate expired tokens by displaying an error message, requiring the publisher to request a new token (Warda et al., 2018).
9. Development of Gateway to Connect IoT (Internet of Things) Network and Blockchain Network" discusses the development of a gateway that connects IoT devices (sensor nodes) and a blockchain network. The development considers three main features: the gateway's ability to receive data from sensor nodes, submit data to the blockchain, and restrict access to the blockchain network. Access restrictions are implemented by validating the gateway, allowing only valid gateways to send data to the blockchain. The access restriction mechanism is designed by implementing JSON Web Token (JWT) for authentication. The research successfully implements the authentication mechanism, enabling the system to differentiate between valid and invalid gateways. The success rate in five tests and the average processing time is 0.52ms. The performance achieved is adapted to the specific IoT environment (Nurfaizi et al., 2019).
10. Developing the E-Letter Application Model as an Effort to Enhance Records Management Competency discusses implementing E-Letter applications based on archival principles in handling correspondence within an organization. The study's findings indicate that consistent use of this application can positively impact the effectiveness and efficiency of paper and information utilization within the organization. The importance of adhering to the discipline of archival science in managing electronic correspondence is also highlighted. However, the research points out that there still needs to be more utilization of archival principles in E-Letter applications. Therefore, the development of an E-Letter application model based on records management theory is expected to enhance its benefits for the organization (Susanti et al., 2017).
11. evaluates the use of the E-Letter application as a system for managing active dynamic records at the Archives and Library Office of Central Java Province. The study employs a descriptive research method with a case study approach, and the results indicate that the E-Letter application is successfully used as a tool for managing active dynamic records based on the web and by the standards of the National Archives of the Republic of Indonesia. The application facilitates the process of managing letters, distributing records, storing, and depreciating records, and it can be accessed online through the Internet. Despite some drawbacks, such as the limited smoothness of application access due to the lack of server development, the majority of employees in the office have been able to accept and understand the application of the E-Letter application effectively (Tarigan & Jumino, 2018).
12. Effectiveness of Digital Correspondence System (E-Letter) at the Communication and Informatics Office of Surabaya City focuses on the effectiveness of the digital correspondence system (E-Letter) at the Communication and Informatics Office of Surabaya City. Based on data analysis, the research findings show that the implementation of E-Letter in the office has been highly effective. The effectiveness evaluation was based on accountability, objectives, data security, fairness/non-discriminatory practices, and transparency, with all variables showing

Saputra , H., Suryawan , S. H., Faldi , F., Cahayawati , B. S., & Wahyuni , R. (2024). Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan. TEPIAN, 4(3). https://doi.org/10.51967/tepian.v4i3.2880

satisfactory scores. These results provide evidence that the use of the E-Letter application has successfully improved the efficiency and quality of handling letters and records at the Communication and Informatics Office of Surabaya City (Sibarani & Fanida, 2016).

13. Implementation of the E-Letter Application in the Department of Population and Civil Registration of Surabaya City: This study focuses on utilizing the E-Letter application in the Department of Population and Civil Registration of Surabaya City to support digital-based bureaucracy. The research uses a qualitative method with a descriptive approach, conducting in-depth interviews with staff, civil servants, and superiors alongside field observations and documentation. The results indicate that implementing the E-Letter application in the department has been highly influential, aiding the smoothness of internal bureaucracy and administrative management. However, some challenges have been encountered, such as internal issues related to the E-Letter server and external factors, including the impact of the Covid-19 pandemic on workforce availability and efficiency. In response to these challenges, the Department of Population and Civil Registration has taken measures such as developing new servers, implementing server backups, and conducting archiving training. Despite the obstacles, the research shows positive results in successfully implementing the E-Letter policy (Farhansyah et al., 2022).
14. In the research titled "Authentication system for e-certificate by using RSA's digital signature," the paper proposes using RSA's digital signature on e-certificates to prevent counterfeiting. Only the participant's name in the e-certificate is signed, and the verification process involves comparing both the e-certificate, the participant's name, and the decrypted signed text. The experimental results demonstrate the effectiveness of the proposed method in protecting e-certificates from unauthorized counterfeiting (Somsuk & Thakong, 2020)

The above literature studies mainly utilize JWT as an authentication method for login purposes only. However, the E-Letter application is developed as a website, making its usage more efficient. However, security needs to be adequately addressed, and safeguarding the documents within the website application requires the implementation of JWT tokens. The utilization of JWT is significant, as it provides a long and random string that allows data to be verified by multiple parties, making it more than just an authentication method. JWT can be employed to ensure the data within it remains secure. In this research, JWT will be utilized to validate the documents' authenticity and ownership.

B. Theoretical Basis

1) Django

Django is a web framework used to build websites and web applications quickly and easily (Holovaty & Kaplan-Moss, 2009). It is developed using the Python programming language and designed to enhance the productivity of web developers by providing a wide range of built-in features and capabilities for data management, security, and presentation.

Django boasts powerful and comprehensive features, including Object-Relational Mapping (ORM) for connecting applications to databases, a routing system for directing HTTP requests to the appropriate functions, a templating system for creating dynamic web views, and much more (Mezzina, 2016). The framework also has a robust security system and integrates well with Python.

Large companies and startups widely use Django to build large-scale websites and web applications, including Instagram, Pinterest, and Mozilla (Mezzina, 2016). It has a large and active community, resulting in many additional modules and available support. The E-Letter application uses the Django framework, enabling faster and more secure development.

2) JWT

When a user successfully authenticates with the server, JWT generates a token that is stored in the user's local storage or browser cookies (Al-Zoubi, 2018). This JWT token contains information about the user, such as the username, profile data, and other relevant details, excluding the password. It is important to note that passwords and sensitive credentials should not be included in the payload of the JWT. The payload of the JWT is accessible to anyone, so it is crucial to avoid including sensitive information that should remain Confidential. An example of the JWT structure can be seen in Picture 1.

Picture 1. JWT Structure

in picture 1 consists of 3 parts, namely:

1. Header

The header typically consists of two parts: the token type, JWT, and the signing algorithm used, such as HMAC SHA256 or RSA.

Saputra , H., Suryawan , S. H., Faldi , F., Cahayawati , B. S., & Wahyuni , R. (2024). Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan. TEPIAN, 4(3). https://doi.org/10.51967/tepian.v4i3.2880

2. Payload
   As the information or data, we want to send. In authentication or authorization implementations, this data typically consists of unique user-related information, such as email, ID/UUID, and authorization-related data, like roles. This data serves as identification for the sender of the token.
3. Verify Signature
   The result of hashing or combining the encoded Header and Payload is then appended with a secret code to create the Signature. This Signature is crucial for verifying that the Header and Payload in the token have not been altered from their original values, as it is relatively easy to create fake or tampered Header and Payload. The Signature itself cannot be tampered with because it is a hash, a one-way function that cannot be reversed. Even if we know the hashing algorithm used, we still require the secret key, which is only known by the application creator. The three structures mentioned above are combined and encoded into a random and lengthy Token string. The advantage of this mechanism is that even a slight modification in the Header or Payload will render the Signature invalid. This is crucial in ensuring the integrity of the letter's content remains intact.

III. METHODOLOGY

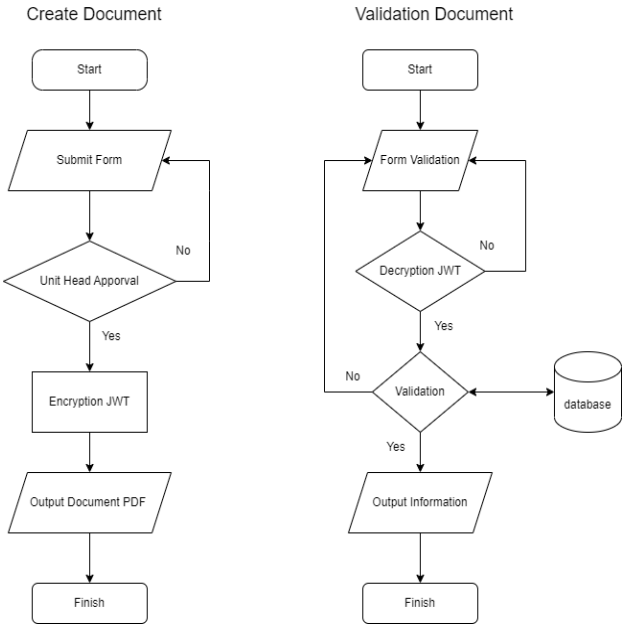
A. *Framework Django*

In implementing this method, the researcher chose to use the Python programming language and the Django framework because they have already been utilized in the existing letter application at Muhammadiyah University of East Kalimantan and facilitate integration with the existing environment. Python is a popular, straightforward programming language with extensive library support, while Django is a robust framework that provides convenience in developing web applications.

B. *Flowchart*

In picture 2, there are two separate flows depicted. The first flow is the document creation process initiated by filling out the letter creation form in my.umkt.ac.id application. If the head of the unit approves the document creation, a JWT token will be generated. The JWT payload consists of a UUID and the encrypted content of the letter, encrypted together with the secret from the Django application, resulting in the JWT token.

The second flow shows the validation form, an upload form for a PDF document. The uploaded PDF will be decrypted using the secret from the Django application. The document proceeds to the validation stage if it can be successfully decrypted. If not, it returns to the Upload Document form page. In the validation stage, the UUID is extracted from the decrypted JWT token and used to search the database. If the UUID is found in the database and matches the content of the JWT token, it displays the valid document information. Otherwise, it returns to the Upload Document form page and displays a message indicating the document is invalid.



Picture 2. Document Builder Flow with JWT

C. *JWT Architecture In Letters*

In the creation of the JWT token, the focus will be on the payload, secret key, and verify signature, which can be explained as follows:

1. Payload
   The payload is where the information we want to include in the JWT token resides. In this letter architecture, the information to be stored includes the UUID, letter number, subject, letter content, sender, and recipient. This information will be stored in JSON format.

2. Secret Key
   The secret key is a randomly generated string, typically a piece of information the application creator has hashed. In this case, the secret key consists of the current time, a secret value, and the UUID of the letter, all hashed using the SHA256 algorithm. An example of creating a secret key using Python can be seen in Picture 3.

```
now = datetime.datetime.now()
sekarang = now.strftime("%d/%m/%Y %H:%M:%S")
secret = 'keamanan lebih dari segalanya'
uuid = 'fd82f7e4-685e-424c-a014-ad332dc37a3f2033'
secret_key = hashlib.sha256("{}{}{}".format(sekarang, secret, uuid). \
             encode('utf-8')).hexdigest()
```

Picture 3. The process of creating a secret key

3. Verify Signature
   The Verify Signature results from hashing or combining the encoded Header (HMAC, SHA256, or RSA) and Payload and then appending the secret code. This Signature is used to verify that both the Header and Payload within

Saputra , H., Suryawan , S. H., Faldi , F., Cahayawati , B. S., & Wahyuni , R. (2024). Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan. TEPIAN, 4(3). https://doi.org/10.51967/tepian.v4i3.2880

the token have not been altered from their original values. It ensures the token's integrity and confirms that it has not been tampered with during transmission. An example of entering a verified signature into a pdf using Python can be seen in Picture 4.

```
encoded_jwt = jwt.encode(data_payload, secret_key, algorithm="HS256")
hash_kode = BytesIO(('%'+encoded_jwt).encode("utf-8"))
output.write(hash_kode.getvalue())

response = HttpResponse(output.getvalue(), content_type='application/pdf')
response['Content-Disposition'] = 'attachment; filename='+'nomor surat'+'.pdf'
return response
```

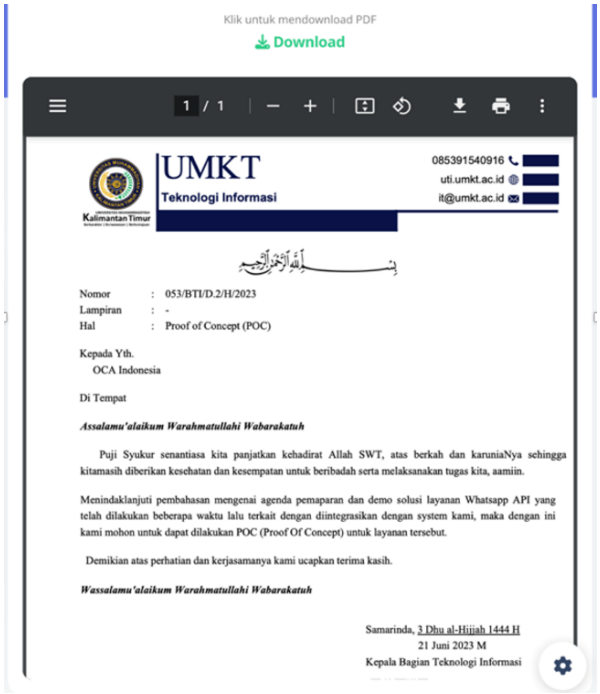
Picture 4. Generation of JWT tokens and inserting them into pdf.

In picture 4, the data payload, secret key, and HS256 algorithm will be encoded. The encoded result will be included simultaneously when rendering the letter in PDF format.

IV. Result And Discussion

A. Letter Creation

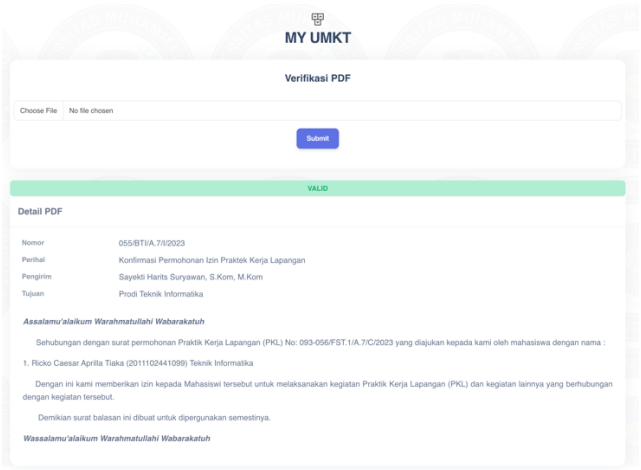
On the letter menu at the address https://my.umkt.ac.id/managemen-surat/, we have added an innovative feature called "letter rendering through an iframe," allowing you to view the letter's appearance via Picture 5. Within the iframe, there is already a JWT token embedded. As a result, when downloading the letter in PDF format, the relevant JWT token is automatically included in the PDF file. This feature ensures better security and authentication in managing the letters.



Picture 5. Render letter data in the form of an iframe PDF.

B. Letter Verification

In our letter application, we have added a verification feature that can be seen in Picture 6. When a downloaded PDF letter file is uploaded to the verification menu, the system will perform PDF extraction and retrieve the JWT token. The JWT token will be decoded, and the UUID inside the JWT will be extracted and compared against the database. If the UUID is found in the database, then the entire payload will be matched with the data. If they match, the verification system will indicate it as VALID and display the information from the letter's content, as shown in Picture 6. If the UUID is not found or the payload does not match, the verification system will indicate it as NOT VALID, which can be seen as shown in Picture 7.



Picture 6. The letter verification page has been successfully found in the database.

Picture 7. The letter verification page could not be found in the database.

C. System Testing

Testing the mail management application will use the Blackbox method because this method is in the functional specifications of the software (Purnia, D & Rahmatullah, 2019). Testing is done by running all existing functions one by one. Then it is seen whether the results are what was designed and expected by the application. The IT admin carries out application testing. The results of testing a web-based payroll application can be seen in Table 1.

In the system trials that have been carried out, such as writing a letter with a letter rendering feature in the form of a pdf iframe, it succeeded in creating and inserting a JWT token into the iframe. When verifying the pdf letter, the system can extract the JWT token so that uuid verification can be carried out into the database. From the results of this trial, research on the use of JWT tokens as verification of the authenticity of this letter can be applied to the existing mail management system at Muhammadiyah University of East Kalimantan.

Saputra , H., Suryawan , S. H., Faldi , F., Cahayawati , B. S., & Wahyuni , R. (2024). Utilization of JWT Tokens as an Authenticity Validation Method for Correspondence at Muhammadiyah University of East Kalimantan. TEPIAN, 4(3). https://doi.org/10.51967/tepian.v4i3.2880

Table 1. System Test

#	Testing Scenario	Results	Trial Date
1	Generation of JWT Tokens when letters are downloaded in pdf format	succeed	13/07/2023
2	Upload Documents that have a JWT Token (valid)	succeed	14/07/2023
3	Upload a letter that does not have a JWT token (not valid)	succeed	14/07/2023

Overall, these testing results reflect the successful implementation of functionalities related to generating, inserting, and verifying JWT tokens in the context of document management. This success instils confidence that the system can effectively respond to various usage scenarios, ensuring the authenticity of letters and efficient document management.

V. CONCLUSIONS

JWT tokens as an alternative method for verifying the authenticity of letters in the letter system at Muhammadiyah University of East Kalimantan offers advantages in terms of efficiency and accuracy. Therefore, incorporating JWT tokens as a means of verifying the authenticity of letters within the letter system at Muhammadiyah University of East Kalimantan can provide significant benefits in improving the efficiency of the verification process and enhancing the accuracy of letter identification. Previously, the letter system relied solely on QR code signatures. However, with JWT token verification, the letter system can become preferable to manual letter creation.

REFERENCES

Al-Zoubi, A. . . (2018). Best Practices for JSON Web Token," International Journal of Advanced Computer Science and Applications. *International Journal of Advanced Computer Science and Applications*, *9*. https://doi.org/10.14569

Chamim Pratama, A., Sakti Pramukantoro, E., & Basuki, A. (2019). *Penerapan Metode Token-Based sebagai Mekanisme Autentikasi pada IoT Middleware* (Vol. 3, Issue 10). http://j-ptiik.ub.ac.id

Dirjen, S. K., Riset, P., Pengembangan, D., Dikti, R., Hibsy, A., & Wibowo, A. (2017). Terakreditasi SINTA Peringkat 2. *Masa Berlaku Mulai*, *1*(3), 618–626.

Farhansyah, M. N., Irianto, H., & Fahmi, A. (2022). Implementasi Aplikasi E-Surat di Dinas Kependudukan dan Pencatatan Sipil Kota Surabaya. *Intelektual Administrasi Publik Dan Ilmu Komunikasi*, *9*(1), 41–53.

Gunawan, R., & Rahmatulloh, A. (2019). JSON Web Token (JWT) untuk Authentication pada Interoperabilitas Arsitektur berbasis RESTful Web Service. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *5*(1), 74. https://doi.org/10.26418/jp.v5i1.27232

Holovaty, A., & Kaplan-Moss, J. (2009). The Definitive Guide to Django: Web Development Done Right. *Apress*.

Jati, D. P., & Wijaya, A. R. (2018). Aplikasi E-Surat Berbasis QR Code di Kecamatan Denpasar Utara. *Jurnal Mantik*, *2*(1), 28–33.

JWT.IO. (2015). *JSON Web Token (JWT)*. https://tools.ietf.org/html/rfc7519.

Mahindrakar, P., & Pujeri, U. (2020). Security Implications for Json web Token Used in MERN Stack for Developing E-Commerce Web Application. *International Journal of Engineering and Advanced Technology (IJEAT)*, *10*(1), 2249–8958.

Mezzina, P. (2016). Learning Django Web Development. *Packt Publishing*.

Nurfaizi, M. C., Bhawiyuga, A., & Amron, K. (2019). *Pengembangan Gateway untuk Menghubungkan Jaringan IoT (Internet Of Things) Dan Jaringan Blockchain*. *3*(12), 10949–10958.

Nurhayati, N., & Sutrisno, A. (2020). Implementation of Electronic Document Management System in Electronic Mail as Supporting Technology in the Administration of Regional Apparatus. *International Journal of Applied Engineering Research*, *15*(8), 1675–1679.

Prihanto, A. A., & Winarno, A. (2018). Implementation of E-Surat in Improving Efficiency and Effectiveness of Electronic Document Management System. *IOP Conference Series: Materials Science and Engineering*, *324*(1), 012010.

Priyatna, R., & Waluyo, S. (2022). IMPLEMENTASI RESTFUL DENGAN JWT UNTUK BOOKING BARANG DI PRIMAJAYA MULTISINDO. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*.

Purnia, D, S., & Rahmatullah, S. (2019). Penerapan Metode Waterfall dalam Perancangan Sistem Informasi Aplikasi Bantuan Sosial Berbasis Android. *Seminar Nasional Sains Dan Teknologi 2019*, 1–7.

Putra, M. R., Sakti Pramukantoro, E., & Bakhtiar, F. A. (2019). Kata kunci: Syntactical Interoperability, Resource Constrained, Semantic IoT Web Service. In *Constrained Application Protocol* (Vol. 3, Issue 5). CoAP. http://j-ptiik.ub.ac.id

Rahmatullo, A., Aldya, A., & Arifin, M. . (2019). Stateless Authentication with JSON Web Tokens using RSA-512 Algorithm. *Jurnal INFOTEL*.

Sibarani, T. D. F., & Fanida, E. H. (2016). Efektivitas Sistem Tata Persuratan Digital (e-Surat) di Dinas Komunikasi dan Informatika Kota Surabaya. *Ilmu Administrasi Negara*.

Somsuk, K., & Thakong, M. (2020). Authentication

system for e-certificate by using RSA's digital signature. *Telkomnika (Telecommunication Computing Electronics and Control)*, *18*(6), 2948–2955. https://doi.org/10.12928/TELKOMNIKA.v18i6.17278

Susanti, T., Sholikhah, F., & Mareta, M. (2017). Pengembangan Model Aplikasi E-Surat sebagai Upaya Peningkatan Kompetensi Bidang Manajemen Rekod. *Jurnal Gadjah Mada*.

Syukur, R., Sutarno, S., & Arum, S. (2019). Development of Electronic Document Management System for Archival Documents at Regional Public Hospitals. *Journal of Physics: Conference Series*, *1339*(1).

Tarigan, A., & Jumino. (2018). Pemanfaatan Aplikasi E-Surat dalam Mendukung Pengelolaan Arsip Dinamis Aktif di Dinas Kearsipan dan Perpustakaan Provinsi Jawa Tengah. *Program Studi Ilmu Perpustakaan*.

Warda, A., Putra, P., Bhawiyuga, A., & Data, M. (2018). *Implementasi Autentikasi JSON Web Token (JWT) Sebagai Mekanisme Autentikasi Protokol MQTT Pada Perangkat NodeMCU* (Vol. 2, Issue 2). http://j-ptiik.ub.ac.id

Wulandari, D. R., & Novitasari, A. (2019). Implementasi JSON Web Token (JWT) pada Sistem Informasi Kepegawaian Berbasis Web. *Jurnal Teknologi Dan Sistem Komputer*, *7*(2), 109–114. https://doi.org/10.14710