

Implementasi Tanda Tangan Digital menggunakan ECDSA (Studi Kasus: Jurnal Tipe File pdf)

Nabilah Arwa^{*1}, Aminudin², Sofyan Arifianto³

^{1,2,3}Universitas Muhammadiyah Malang

nabilaharwa@webmail.umm.ac.id^{*1}, aminudin2008@umm.ac.id², sofyan.arifianto@gmail.com³

Abstrak

Perkembangan teknologi membuat hampir seluruh pembuatan dokumen dilakukan secara digital. Dokumen digital yang bersifat rahasia akan sulit jika terdapat modifikasi oleh orang yang tidak bertanggung jawab. Oleh karena itu dibuatlah suatu skema tanda tangan untuk dokumen digital yaitu tanda tangan digital. Tanda tangan digital pada dasarnya berfungsi sebagai alat otentikasi untuk menjamin keaslian dokumen tersebut serta menghindari adanya penyangkalan. Tanda tangan digital dapat menjamin beberapa aspek keamanan, yaitu *authenticity*, *integrity* dan *non-repudiation*. Tanda tangan digital dapat menggunakan Algoritma Elliptic Curve Digital Signature (ECDSA) yang merupakan gabungan dari Elliptic Curve Cryptography (ECC) dan Digital Signature Standard (DSS). Penelitian ini melakukan implementasi tanda tangan digital menggunakan Algoritma ECDSA pada file jurnal tipe pdf. Hasil penelitian ialah tanda tangan digital ini dapat menjamin *authenticity*, *integrity*, dan *non-repudiation* pada file jurnal tipe pdf tersebut.

Kata Kunci: Tanda Tangan Digital, Algoritma ECDSA, Authenticity, Integrity, Non-repudiation

Abstract

Technological developments have made almost all document creation done digitally. Confidential digital documents will be difficult if there is modification by irresponsible people. Therefore, a signature scheme was made for digital documents, namely digital signatures. The digital signature basically functions as an authentication tool to ensure the authenticity of the document and avoid denial. Digital signatures can guarantee several aspects of security, namely *authenticity*, *integrity* and *non-repudiation*. Digital signatures can use the Elliptic Curve Digital Signature (ECDSA) Algorithm, which is a combination of Elliptic Curve Cryptography (ECC) and Digital Signature Standard (DSS). This study implements a digital signature using the ECDSA algorithm in a pdf type journal file. The result of the research is that this digital signature can guarantee *authenticity*, *integrity*, and *non-repudiation* in the pdf type journal file.

Keywords: Digital Signature, ECDSA Algorithm, Authenticity, Integrity, Non-repudiation

1. Pendahuluan

Perkembangan teknologi membuat hampir seluruh pembuatan dokumen dilakukan secara digital. Dokumen digital yang bersifat rahasia akan sulit jika terdapat modifikasi oleh orang yang tidak bertanggung jawab. Maka dibuatlah skema tanda tangan untuk dokumen digital yang disebut tanda tangan digital[1]. Tanda tangan digital pada dasarnya berfungsi sebagai alat otentikasi untuk menjamin keaslian dokumen tersebut serta menghindari adanya penyangkalan. Tanda tangan digital dapat menjamin beberapa aspek keamanan, yaitu *authenticity*, *integrity* dan *non-repudiation*. *Authenticity* menjelaskan siapa yang membuat dokumen tersebut. *Integrity* yaitu tidak terdapat perubahan dari dokumen setelah tanda tangan digital dilakukan. *Non-repudiation* ialah pembuat dokumen tidak bisa menyangkal di kemudian hari, bahwa ia tidak pernah membuat dokumen tersebut [2]. Dokumen yang terdapat tanda tangan digital akan sangat rentan terhadap pemalsuan yang dilakukan oleh pihak yang tidak bertanggung jawab.

Tanda tangan digital dapat diimplementasikan dengan 2 cara, yaitu enkripsi pesan dan menggunakan fungsi hash[3]. Proses enkripsi pesan dapat dilakukan menggunakan algoritma kunci publik. Algoritma kunci publik menggunakan dua pasang kunci, yaitu kunci rahasia (*private*) dan kunci publik. Kunci rahasia (*private*) hanya diketahui oleh pemiliknya, sedangkan kunci publik dapat disebarluaskan. Pembangkitan kedua kunci dapat dilakukan menggunakan beberapa algoritma kunci publik, seperti *Digital Signature Algorithm* (DSA), *Rivest Shamir Adleman* (RSA),

Elliptic Curve Digital Signature Algorithm (ECDSA). Fungsi hash digunakan untuk memastikan integritas data yang dikirim dan *authentication* pesan[2]. Contoh dari beberapa fungsi hash, yaitu SHA-1, SHA-2, MD5, Keccak dan lain-lain.

Penelitian yang dilakukan oleh Kusuma dan Darmaji (2014), melakukan implementasi tanda tangan digital dan perbandingan dari segi performa dan segi keamanan menggunakan DSA dan ECDSA pada file berekstensi txt. Hasil yang didapat bahwa dari segi performa kedua algoritma hampir sama saat dijalankan, namun dari segi keamanan ECDSA lebih baik daripada DSA[1]. Rahman (2017) dalam penelitiannya, melakukan implementasi tanda tangan digital menggunakan ECDSA dan Keccak. Hasil yang didapat ialah terdapat fitur tambahan berupa penyimpanan menggunakan tanda tangan digital pada teks editor yang telah dibuat dalam penelitian [2]. Penelitian Sutarno (2016), melakukan implementasi tanda tangan digital menggunakan ECDSA pada sistem *upload* file berukuran besar berekstensi mp4. Pengujiannya berhasil dalam otentikasi pengirim dan integritas file[3].

Hampir sama dengan penelitian sebelumnya, penelitian Sutrisna (2016) melakukan implementasi tanda tangan digital menggunakan ECDSA pada sistem *upload* file, namun file yang digunakan hanya file berukuran kecil, seperti file gambar berekstensi jpg. Hasil yang didapat dari penelitian ialah proses *authentication* dan *integrity* file dapat diterapkan, serta serangan yang dapat dihadapi pada saat *upload* file[4]. Berbeda dengan penelitian-penelitian sebelumnya, Hutasuhut, Effendi dan Situmorang (2019) dalam penelitiannya, melakukan implementasi menggunakan RSA dan MD5 pada sistem *upload* file dengan beberapa tipe ekstensi, seperti docx, xlsx, txt, rar, mp3, pdf dan mp4. Hasil dari penelitian ialah menjamin keamanan pada keaslian suatu file, karena sedikit saja terdapat perubahan pada file akan berpengaruh pada tanda tangan digital yang telah dibentuk[5].

Penelitian Prabowo dan Afrianto (2017) melakukan implementasi tanda tangan digital menggunakan RSA pada file berekstensi pdf. Hasil dari penelitian didapatkan bahwa tanda tangan digital memberikan layanan keamanan terhadap otentikasi file[6]. Sedyono dan Setiawan (2015) dalam penelitiannya, melakukan implementasi tanda tangan digital menggunakan RSA dan SHA-512 pada file berekstensi pdf. Hasil yang didapat ialah keaslian data terjamin dan dapat mendeteksi perubahan pada suatu file[7]. Penelitian yang dilakukan oleh Rezanisa (2016), melakukan implementasi tanda tangan digital menggunakan RSA dan Keccak pada file teks. Hasil dari penelitian didapatkan bahwa pembentukan waktu pembentukan tanda tangan digital relatif singkat, serta tercapainya tujuan tanda tangan digital yang menjamin keamanan pada beberapa aspek, yaitu *integrity*, *authenticity*, dan *non-repudiation*[8].

Perbedaan penelitian yang akan dilakukan dari penelitian sebelumnya ialah implementasi tanda tangan digital menggunakan Algoritma ECDSA pada file berekstensi pdf yaitu jurnal. Algoritma ECDSA merupakan algoritma tanda tangan digital yang menggunakan analogi kurva ellips, yang mana kekuatan per bit kunci algoritma ini lebih kuat jika dibandingkan dengan algoritma biasa. Pentingnya dilakukan penelitian ini ialah untuk menghindari adanya duplikasi dan modifikasi pada file jurnal tersebut serta menjamin penulis merupakan penulis yang sebenarnya, sehingga penulis melakukan penelitian yang berjudul Implementasi Tanda Tangan Digital menggunakan ECDSA (Studi Kasus: Jurnal Tipe File pdf). Penulis akan membuat sistem *upload* jurnal dengan menyisipkan tanda tangan digital di dalamnya. Penelitian terhadap tanda tangan digital ini diharapkan dapat menjamin *authenticity*, *integrity*, dan *non-repudiation* suatu data.

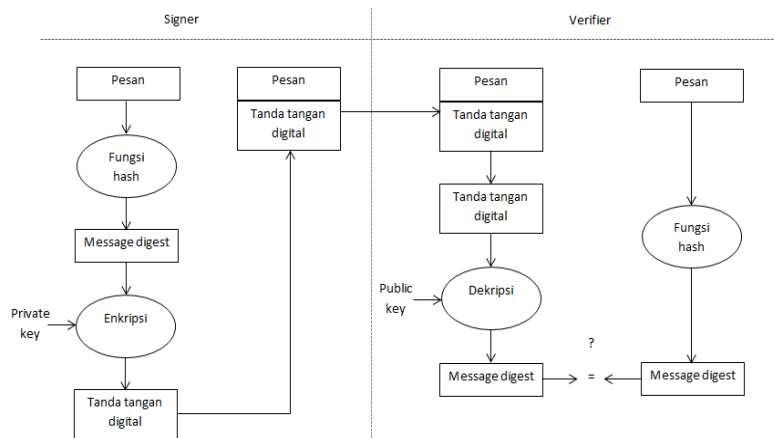
2. Metode Penelitian

2.1 Tanda Tangan Digital

Dokumen cetak kini banyak beralih menjadi dokumen digital seiring berkembangnya zaman. Setiap dokumen cetak pasti memiliki tanda tangan sebagai bukti disahkannya dokumen tersebut. Namun, tanda tangan pada dokumen cetak sebagai bukti otentikasi kini bisa saja diduplikasi oleh pihak yang tidak bertanggung jawab. Sama halnya dengan dokumen cetak yang memiliki tanda tangan, dokumen digital juga memiliki tanda tangan yang disebut dengan tanda tangan digital. Tanda tangan digital merupakan salah satu cabang ilmu kriptografi yang di dalamnya memiliki nilai kriptografis yang bergantung pada isi dokumen yang dikirimkan.

Tanda tangan digital memungkinkan penerima untuk memastikan pesan yang dikirimkan berasal dari pengirim yang bersangkutan, sehingga pengirim tidak bisa menyangkal telah mengirim pesan tersebut [3]. Tanda tangan digital terdapat 3 proses utama yaitu: pembangkitan kunci, pemberian tanda tangan digital dan verifikasi keabsahan tanda tangan

digital tersebut[9]. Selain itu, tanda tangan digital juga memberikan beberapa aspek keamanan, seperti kerahasiaan (*confidentiality*), integritas (*integrity*), otentikasi (*authentication*), dan anti-penyangkalan (*non-repudiation*). Dalam pengimplementasian tanda tangan digital seperti pada Gambar 1, algoritma yang sering digunakan ialah algoritma kunci publik.



Gambar 1. Proses Tanda Tangan Digital

2.2 Algoritma Kunci Publik

Algoritma kunci publik atau algoritma asimetri merupakan algoritma yang membangkitkan dua kunci yang berbeda saat proses enkripsi dan dekripsi. Kunci yang digunakan untuk enkripsi tidak rahasia, sehingga dinamakan juga kunci publik (*public key*), sedangkan kunci yang digunakan untuk dekripsi rahasia, sehingga dinamakan kunci privat (*private key*)[6]. Saat enkripsi dilakukan, pengirim menggunakan kunci publik yang dimiliki oleh penerima. Kemudian hanya penerima pesan yang dapat melakukan dekripsi pesan menggunakan kunci rahasia miliknya. Algoritma kunci publik mempunyai beberapa contoh, seperti *Rivest Shamir Adleman* (RSA), *Diffie-Hellman*, *EIGamal*, *ECC* dan lain sebagainya.

Aplikasi kriptografi kunci-publik dapat dibagi menjadi 3 kategori[10]:

1. Kerahasiaan data

Contoh algoritma yang dapat digunakan seperti RSA, Knapsack, Rabin, *EIGamal*, *Elliptic Curve Cryptography* (ECC).

2. Tanda tangan digital

Contoh algoritma yang dapat digunakan seperti RSA, *Digital Signature Algorithm* (DSA), *ECC*, dan *EIGamal*.

3. Pertukaran kunci (*key exchange*)

Contoh algoritma yang dapat digunakan seperti RSA dan *Diffie-Hellman*.

Penelitian yang akan dilakukan berfokus pada pengaplikasian tanda tangan digital. Selain dari yang telah disebutkan di atas, aplikasi tanda tangan digital dapat menggunakan *Elliptic Curve Digital Signature* (ECDSA) yang merupakan gabungan dari *Elliptic Curve Cryptography* (ECC) dan *Digital Signature Standard* (DSS).

2.3 Fungsi Hash

Fungsi hash adalah fungsi apapun yang dapat digunakan untuk memetakan data dengan ukuran acak ke data dengan ukuran tetap[2]. Fungsi hash memiliki algoritma yang iterative dan searah, yang dapat memproses pesan yang diberikan untuk menghasilkan representasi yang lebih pendek yang disebut *message digest*[11]. Fungsi hash biasa digunakan untuk *integrity* data dan *authentication* pesan. Terdapat beberapa contoh fungsi hash, yaitu MD-5, SHA-1, SHA-2, SHA-3 (Keccak) dan lain sebagainya.

Dalam ECDSA, DSA menggunakan Algoritma *Elliptic Curve Cryptography* (ECC), sementara fungsi hash menggunakan SHA-1[3]. *Secure Hash Algorithm 1* atau SHA-1 menerima masukan berupa string dengan ukuran maksimum 2^{64} bit. Setiap string, SHA-1 akan menghasilkan keluaran sebesar 160 bit dari string tersebut yang disebut *message digest*[12]. Langkah-langkah pembuatan *message digest* pada SHA-1 adalah sebagai berikut[10]:

1. Penambahan bit-bit pengganjal.
Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) yang kongruen dengan 448 modulo 512.
2. Penambahan nilai panjang pesan semula.
Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula.
3. Inisialisasi penyangga (*buffer*) MD.
SHA membutuhkan 5 buah penyangga (*buffer*) yang masing-masing panjangnya 32 bit, kelima penyangga ini menampung hasil antara dan hasil akhir.
4. Pengolahan pesan dalam blok berukuran 512 bit.
Pesan yang telah dibagi menjadi L blok yang masing-masing memiliki panjang 512 bit yang akan diproses bersama dengan penyangga *message digest* menjadi keluaran 128 bit.

2.4 Algoritma ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) adalah salah satu algoritma yang diterapkan dalam pembuatan tanda tangan digital yang menggunakan analogi kurva elips[13]. ECDSA merupakan algoritma yang termasuk dalam *Digital Signature Standard* (DSS). Algoritma pada DSS terdiri dari dua komponen, yaitu algoritma tanda tangan digital (*Digital Signature Algorithm* atau DSA) dan fungsi hash standar (*Secure Hash Algorithm* atau SHA). Dalam ECDSA, DSA menggunakan Algoritma *Elliptic Curve Cryptography*, sementara fungsi hash menggunakan SHA-1[3]. ECDSA mencakup analogi kurva *ellips* pada DSA. Kurva *ellips* yang digunakan disini adalah kurva *ellips* yang berada di bidang datar yang berhingga dan dibagi atas 2 bagian, yaitu[13]:

- a. Kurva elips yang berada di F_p
- b. Kurva elips yang berada di F_{2^m}

Penelitian ini menggunakan kurva *ellips* yang berada di F_p . Bidang terbatas F_p merupakan sebuah bidang yang beranggotakan bilangan integer $\{0,1,\dots,p-1\}$, dan p merupakan bilangan prima, setiap perhitungan dikalkulasikan dengan modulo p agar hasilnya tetap berada dalam daerah F_p . Anggota dari bidang terbatas F_p biasa disebut dengan nilai parameter kurva *ellips* pada bidang F_p . Nilai parameter yang telah ditentukan akan digunakan pada saat implementasi Algoritma ECDSA.

Implementasi tanda tangan digital menggunakan Algoritma ECDSA memiliki 3 tahapan, yaitu pembangkitan kunci, pemberian tanda tangan digital, dan verifikasi tanda tangan digital. Keuntungan penggunaan ECDSA salah satunya ialah kekuatan per bit kunci algoritma yang menggunakan kurva *ellips* lebih kuat secara substansial daripada algoritma biasa[13]. Proses tanda tangan digital menggunakan Algoritma ECDSA[9] adalah sebagai berikut:

a. **Key Generation (Pembangkitan Kunci)**

Setelah menentukan nilai parameter kurva, akan dilakukan proses pembangkitan kunci. Pembangkitan kunci dilakukan untuk mendapatkan 2 pasang kunci, yaitu kunci publik dan kunci rahasia (*private*). Kunci publik bersifat umum yang dapat dibagikan kepada orang banyak, sedangkan kunci rahasia (*private*) bersifat rahasia yang hanya dapat diketahui oleh orang yang berwenang.

b. **Signing (Pemberian Tanda Tangan)**

Setelah pembangkitan kunci, maka langkah selanjutnya ialah pemberian tanda tangan digital. Tanda tangan digital dibuat menggunakan hasil hash dan kunci *private* yang telah dibangkitkan. Tanda tangan digital yang telah dibuat akan disisipkan pada file yang akan dikirim.

c. **Verifying (Verifikasi Tanda Tangan Digital)**

Tahap verifikasi dilakukan untuk memeriksa valid atau tidaknya tanda tangan digital yang telah dibuat pada saat pengiriman file. Jika tanda tangan tidak sesuai, maka dapat dipastikan file telah dimodifikasi atau diakses oleh orang yang tidak berwenang.

2.5 Penggunaan Library

Library merupakan suatu fungsi yang dibuat untuk mempermudah programmer dalam membuat sebuah aplikasi[14]. *Library* juga dapat diartikan sebagai suatu kode program yang di dalamnya berisikan variabel, konstanta, tipe data, *object*, dan fungsi-fungsi yang telah ditulis oleh seseorang atau sekelompok orang, sehingga orang lain dapat menggunakannya atau menambahkannya dalam program yang mereka buat. *Library* biasanya terdapat dalam beberapa

bahasa pemrograman, seperti C+, Java, PHP, dan bahasa pemrograman lainnya. Pada implementasi yang akan dilakukan menggunakan bahasa pemrograman PHP. Bahasa pemrograman PHP biasanya diimplementasikan dalam sebuah *framework*. *Framework* adalah suatu struktur konseptual dasar yang digunakan untuk memecahkan atau menangani suatu masalah kompleks[15]. Banyak keuntungan dari menggunakan *framework*. Salah satunya ialah memberikan struktur yang baik dalam program yang dibuat karena *framework* memiliki library atau fungsi yang bisa langsung digunakan[16]. Contoh *framework* yang sering digunakan ialah *framework laravel* yang berbasis PHP bersifat *open source*.

Pada penelitian yang akan dilakukan, implementasi menggunakan *library* pada *framework laravel*. *Library* yang digunakan adalah *library* ECDSA-PHP yang bersifat *open source*. *Library* ini dibuat oleh Starkbank yang memuat kode program dari Algoritma ECDSA. Starkbank membuat *library* ini untuk sistem dasar Algoritma ECDSA. *Library* ini juga banyak digunakan oleh beberapa pengguna lainnya untuk beberapa sistem, seperti *website monitoring*, absensi, transaksi via *email*, dan lain sebagainya. Pada penelitian ini, *library* digunakan untuk sistem *upload* jurnal menggunakan tanda tangan digital yang implementasinya menggunakan Algoritma ECDSA.

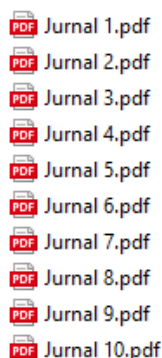
3. Hasil Penelitian dan Pembahasan

Pada tahapan ini peneliti melakukan pengujian pada sistem yang telah di implementasikan yang berbasis web. Pengujian dilakukan dengan beberapa tahap yaitu sebagai berikut:

3.1 Pengujian Sistem

3.1.1 Siapkan 10 Jurnal

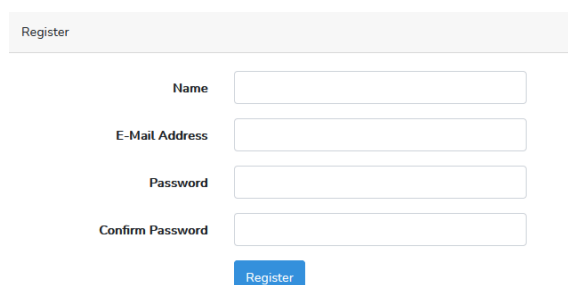
10 jurnal akan di-upload ke sistem. Jurnal memiliki tipe data pdf, seperti yang ditunjukkan pada Gambar 2.



Gambar 2. 10 Jurnal yang akan di-upload

3.1.2 Buat akun untuk sistem upload jurnal

User harus membuat akun terlebih dahulu agar bisa menggunakan sistem. Membuat akun dengan mengisi beberapa data seperti pada Gambar 3. Jika user telah memiliki akun, user dapat langsung login dengan memasukkan email dan password, seperti pada Gambar 4.

A registration form titled 'Register' with a light gray background. It contains four input fields: 'Name', 'E-Mail Address', 'Password', and 'Confirm Password'. Below the fields is a blue button with the text 'Register' in white.

Gambar 3. Halaman register

Gambar 4. Halaman login

3.1.3 Upload 10 Jurnal ke Sistem

User telah berhasil upload 10 jurnal ke sistem, yang ditunjukkan pada Gambar 5.

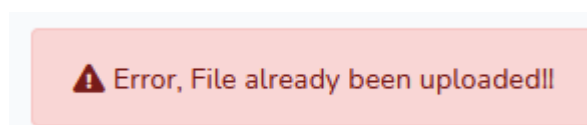
No.	Journal Uploader	Journal Title	Action
1	icha	Jurnal 1	Check Detail Download
2	icha	Jurnal 2	Check Detail Download
3	icha	Jurnal 3	Check Detail Download
4	icha	Jurnal 4	Check Detail Download
5	Nabilah	Jurnal 5	Check Detail Download
6	Nabilah	Jurnal 6	Check Detail Download
7	Nabilah	Jurnal 7	Check Detail Download
8	Nabilah	Jurnal 8	Check Detail Download
9	Nabilah	Jurnal 9	Check Detail Download
10	Nabilah	Jurnal 10	Check Detail Download

Gambar 5. Jurnal berhasil di-upload

3.1.4 Abstract setiap jurnal yang di-upload akan di hash dan dijadikan id

- a. Jika Abstract jurnal sama, jurnal tidak bisa di-upload

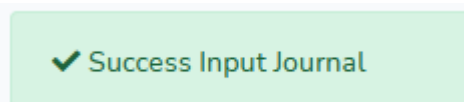
Jika jurnal tidak berhasil di-upload akan tampil pesan error seperti pada Gambar 6.



Gambar 6. Pesan error jurnal tidak berhasil di-upload

- b. Jika Abstract jurnal berbeda, jurnal berhasil di-upload

Jika jurnal berhasil di-upload akan tampil pesan sukses seperti pada Gambar 7.



Gambar 7. Pesan sukses jurnal berhasil di-upload

3.1.5 Jurnal yang berhasil di-upload telah memiliki tanda tangan digital di dalamnya yang dapat dilihat pada tombol "Detail"

Tanda tangan digital telah meliputi hash, pembangkitan kunci dan penandatanganannya. Jurnal yang di-upload telah disisipkan tanda tangan digital di dalamnya. Detail dari hash dan tanda tanganada setiap jurnal dapat dilihat pada tombol "Detail". Gambar 8 menunjukkan detail dari jurnal 1.

Journal Title	Jurnal 1
Abstract	The rapid growth of social media does not make Twitter left by its users. Twitter is one of the social media that allows user to interact each other, share information, or even to express feelings and opinions, including in expressing film opinions. Comments or Tweets about movies that exist on Twitter can be used as an evaluation in watching movies and increasing film production. To figure it out, sentiment analysis can be used to classify into negative or positive sentiments. In Tweets contain many languages used in the form of non-standard languages such as slang, word-outs, and misspellings. Therefore it takes special handling on Twitter comments. In this research used non-standard word dictionary and Levenshtein Distance normalization to improve non-standard word to standard word by classification Naive Bayes. Based on the result of the test, the highest accuracy, precision, recall, and f-measure value are 98.33%, 96.77%, 100%, and 98.36%.
Hash Abstract	072f2fb13e693466534f9d56f18a135f546f1d96
Signature	MEQClFxpPoyfCM2SNew2N3sozzhJBtKe7cq1qTJB9Zcs6wuZAiB305eL2IHBlN7xbEUg9KDHppy0Z4FeznFMrGkhnAYotw==

Gambar 8. Detail jurnal 1

3.1.6 Hasil pembangkitan kunci (kunci publik dan kunci private) dari upload jurnal dapat dilihat pada tombol “Check” dengan input password saat buat akun terlebih dahulu

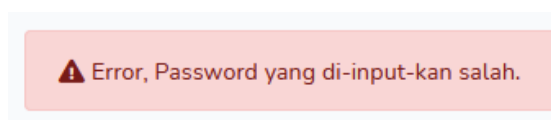
- a. Jika password benar, hasil pembangkitan kunci akan ditampilkan
Password yang digunakan ialah password saat melakukan register atau login. Gambar 9 menampilkan kunci publik dan kunci private jurnal 1.

Public Key MFYwEAYHKoZlZj0CAQYFK4EEAAoDQgAE3eFsq/TQ
//Gj3EIQPzj1wmxFxXbq9Szrfi7NLjF8jcdJKfPTCjAnq1EvEwwM8h
GEj6ylAVE2hqXMCjndB3hOMQ==

Private Key public/pemfile/private/privateKey-19.pem

Gambar 9. Hasil pembangkitan kunci jurnal 1

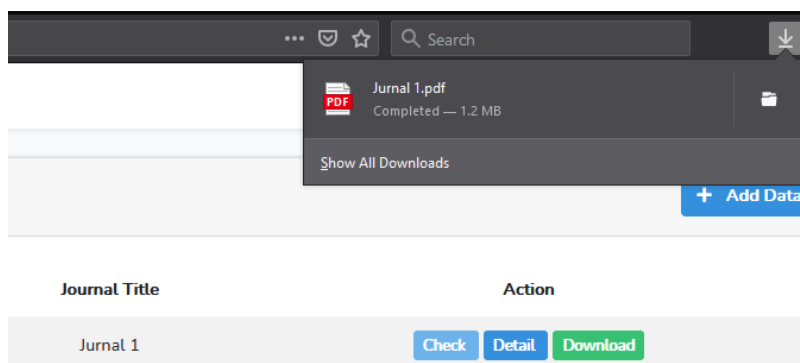
- b. Jika password salah, akan tampil pesan error
Pesan error ditunjukkan pada Gambar 10.



Gambar 10. Pesan error

3.1.7 Jurnal yang telah di-upload dapat di-download

Jurnal yang telah di-upload ke sistem dapat di-download, seperti yang ditunjukkan pada Gambar 11.



Gambar 11. Jurnal berhasil di-download

3.2 Hasil Analisa berdasarkan Pengujian

3.2.1 Analisa Integrity

Pengujian integrity dilakukan untuk membuktikan keaslian suatu file dengan pembuatan tanda tangan digital dan verifikasi tanda tangan digital tersebut. Tanda tangan digital yang dihasilkan akan berbeda pada setiap jurnalnya. Analisa dapat dilakukan sebagai berikut:

1. User meng-upload jurnal asli dengan judul jurnal 3, yang memiliki detail seperti pada Gambar 12

Journal Title	Jurnal 3
Abstract	Infectious disease is a problem in health that requires antimicrobials or antibiotics. Acute Respiratory Infection (ARI) is a disease of the respiratory tract caused by bacteria that attacks one part of the respiratory tract from the nose to the alveoli. ARI disease consists of two, namely non-pneumonia ARI or better known as influenza. Treatment of non-pneumonia ARI at the age of under five is sufficient by providing traditional medicine and no need for antibiotic treatment. This disease is susceptible to attacking children and toddlers because of their lower immune system. ARI pneumonia in toddlers is characterized by symptoms of coughing and / or difficulty breathing, such as rapid breathing, inward pulling of the chest or a picture of the thorax. Meanwhile, non-pneumonia ARI in toddlers is characterized by coughing symptoms but does not experience rapid breathing and there is no inward pulling of the lower chest wall. Inappropriate antibiotic drug administration still occurs. The use of antibiotics in each health center has an indicator of errors in prescribing antibiotics by $\leq 20\%$. In handling this case, the classification of pneumonia and non-pneumonia ARIs in toddlers and children can be done. This study uses the SVM (Support Vector Machine) algorithm to classify pneumonia and non- pneumonia ARIs. The dataset used was 271 data consisting of 135 non-pneumonia data and 136 pneumonia data. The proposed model gets the best results on linear kernels with outlier cleaning process and feature selection using PCA of 96%. Based on the results of the proposed SVM model test, it is effective to classify ARI non-pneumonia and pneumonia.
Hash Abstract	7c89a0e355c134f433b35e7c8e4fd43c6201ec8
Signature	MEYCIQDQ70JITkYt6A0fg6w/61Phd1k8g33KMgyHz5myAmfQIhAKv6vikNV0hevzJjeulOrdKAha1NI4Kh/FjCwRyups2P

Gambar 12. Detail Jurnal Asli

2. User meng-upload jurnal modifikasi dengan judul jurnal 4, yang memiliki detail sebagai berikut:

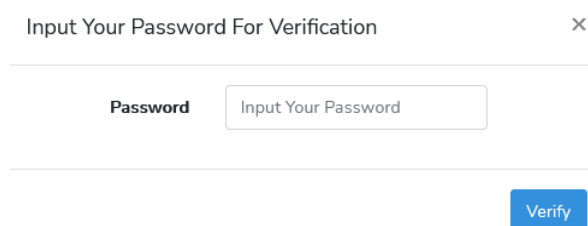
Journal Title	Jurnal 4
Abstract	Infectious disease is a problem in health that requires antimicrobials or antibiotics. Acute Respiratory Infection (ARI) is a disease of the respiratory tract caused by bacteria that attacks one part of the respiratory tract from the nose to the alveoli. ARI disease consists of two, namely non-pneumonia ARI or better known as influenza. Treatment of non-pneumonia ARI at the age of under five is sufficient by providing traditional medicine and no need for antibiotic treatment. This disease is susceptible to attacking children and toddlers because of their lower immune system. ARI pneumonia in toddlers is characterized by symptoms of coughing and / or difficulty breathing, such as rapid breathing, inward pulling of the chest or a picture of the thorax. Meanwhile, non-pneumonia ARI in toddlers is characterized by coughing symptoms but does not experience rapid breathing and there is no inward pulling of the lower chest wall. Inappropriate antibiotic drug administration still occurs. The use of antibiotics in each health center has an indicator of errors in prescribing antibiotics by $\leq 20\%$. In handling this case, the classification of pneumonia and non-pneumonia ARIs in toddlers and children can be done. This study uses the SVM (Support Vector Machine) algorithm to classify pneumonia and non- pneumonia ARIs. The dataset used was 271 data consisting of 135 non-pneumonia data and 136 pneumonia data. The proposed model gets the best results on linear kernels with outlier cleaning process and feature selection using PCA of 96%. Based on the results of the proposed SVM model test, it is effective to classify ARI non-pneumonia and pneumonia.
Hash Abstract	11ba721a79779ff4e0f5a53b4317f6a52e6ca175
Signature	MEQCIH6vk9XwyFUJrfqH1E07+aKT+4aJTh7C80q3GOYAostJAI BIPvcMaP/PQn4CdFQzthLs/mptodEal4DfE76e08B+g==

Gambar 13. Detail Jurnal Modifikasi

Pada dasarnya, jurnal 3 (asli) dan jurnal 4 (modifikasi) merupakan jurnal yang sama. Namun, pada jurnal 4 dilakukan modifikasi pada isi abstract, yaitu dengan menambahkan satu huruf pada awal kalimat. Hasil hash abstract dari jurnal 3, berbeda dengan hasil hash abstract jurnal 4. Hal ini dapat dilihat pada Gambar 12 untuk jurnal 3 dan pada Gambar 13 untuk jurnal 4. Perbedaan hasil hash abstract dapat dijadikan acuan untuk melakukan pengujian integrity untuk memastikan keaslian dari jurnal.

3.2.2 Analisa Authenticity

Pengujian authenticity dilakukan untuk memastikan hanya user yang berwenang dapat melihat hasil pembangkitan kunci. Jurnal yang di-upload memiliki 2 pasang kunci, yaitu kunci publik dan kunci private. Setiap jurnal memiliki kunci publik dan kunci rahasia (private) yang berbeda. Detail dari hasil pembangkitan kunci dapat dilihat pada button "Check", yang hanya dapat dilihat oleh user yang melakukan upload jurnal dengan memasukkan password seperti pada Gambar 14. Detail dari pembangkitan kunci akan ditampilkan jika password yang dimasukkan benar seperti pada Gambar 9. Pesan error akan muncul jika user salah memasukkan password, hal ini ditunjukkan pada Gambar 10.



Gambar 14. Input password

3.2.3 Analisa Non-repudiation

Pengujian non-repudiation dilakukan untuk memastikan bahwa user yang meng-upload jurnal tidak dapat menyangkalnya. Saat jurnal di-upload, jurnal otomatis telah disisipkan tanda tangan digital di dalamnya, yang mana tanda tangan digital dibuat dengan dibangkitkannya sepasang kunci, yaitu kunci publik dan kunci rahasia (private). Tanda tangan digital yang telah dibuat menggunakan kunci rahasia (private) milik jurnal 1, hanya dapat diverifikasi menggunakan kunci publik milik jurnal 1 itu sendiri. Sehingga dapat dipastikan bahwa user yang telah memiliki sepasang kunci tersebut merupakan user yang telah meng-upload jurnal tersebut ke sistem. Selain itu, nama user yang melakukan upload jurnal ditampilkan saat jurnal telah berhasil di-upload.

4. Kesimpulan

Penelitian yang telah dilakukan didapat beberapa kesimpulan, yaitu sebagai berikut:

1. Algoritma ECDSA dapat diimplementasikan untuk tanda tangan digital pada sistem *upload* file.
2. Algoritma ECDSA memiliki bit yang lebih pendek dibandingkan algoritma kunci publik lainnya saat melakukan enkripsi dan dekripsi pada saat implementasi.
3. Tanda tangan digital menggunakan ECDSA dapat menjamin beberapa aspek keamanan, yaitu *integrity*, *authenticity*, dan *non-repudiation* suatu data.

Referensi

- [1] V. Kusuma, J. Matematika, and F. Matematika, "Elliptic Curve dan Implementasinya pada Algoritma Tanda Tangan Digital," vol. 3, no. 2, pp. 3–6, 2014.
- [2] R. A. Azdy, "Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA," vol. 5, no. 3, pp. 184–191, 2016.
- [3] D. A. Rahman, "Pemanfaatan Tanda Tangan Digital Menggunakan ECDSA dan Keccak pada Teks Editor," Bandung, 2018.
- [4] M. V. Sutarno, "Implementasi ECDSA untuk Verifikasi Berkas Berukuran Besar dengan Menggunakan Merkle Tree," pp. 2–7, 2017.
- [5] R. Y. Sutrina, "Sistem Autentikasi Pengunggahan File dengan Algoritma ECDSA," Bandung, 2016.

- [6] Z. S. Budi K. Hutasuhut, Syahril Efendi, "InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InforTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 3, no. 2, pp. 164–169, 2019.
- [7] I. A. Egi Cahyo Prabowo, "Penerapan Digital Signature dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital," *J. Ilm. Komput. dan Inform.*, vol. 6, no. 2, pp. 83–90, 2017.
- [8] M. S. Ramadhan, P. F. Ariyani, T. Informatika, F. T. Informasi, and U. B. Luhur, *Peningkatan Keamanan Login Website Dengan Implementasi One Time Password Menggunakan Algoritma SHA1 dan MD5 Berbasis Mobile*, vol. 1. 2018.
- [9] L. Refialy, E. Sedyono, and A. Setiawan, "Pengamanan Sertifikat Tanah Digital menggunakan Digital Signature SHA-512 dan RSA," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 3, pp. 229–234, 2015.
- [10] R. Munir, *Kriptografi*. Bandung: Informatika Bandung, 2019.
- [11] P. Sendi *et al.*, "Implementasi Algoritma Ecdsa Untuk Pengamanan E-Mail (Verifikasi Keaslian Pesan)," Surabaya, 2010.
- [12] B. R. P. N, L. M. Citrady, and R. F. Sinaga, "Elliptic Curve Digital Signature Algorithm (ECDSA)," Bandung.
- [13] A. Triwinarko, "Elliptic Curve Digital Signature Algorithm (ECDSA)," Bandung, 2005.
- [14] W. A. Triyanto, "Class Library Untuk Pembuatan Aplikasi Crud Wiwit Agus Triyanto Program Studi Sistem Informasi, Fakultas Teknik, Universitas Muria Kudus Gondangmanis, PO Box 53, Bae, Kudus 59352," *Pros. SNATIF Ke-1*, pp. 349–356, 2014.
- [15] D. Naista, *Codeigniter Vs Laravel Kasus Membuat Website Pencari Kerja*. Yogyakarta: Lokomedia, 2017.
- [16] D. Ambriani, "Rancang Bangun Repository Publikasi Ilmiah Dosen Berbasis Web Menggunakan Framework Laravel," *J. Manaj. Inform.*, vol. 10, no. 1, pp. 58–66, 2020.