

ALGORITMA MD5 PADA SISTEM INVENTORY DENGAN METODE AGILE

Ridwan A. Yusuf^{*1}, Septi Andryana²

Sistem Informasi Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional
e-mail: ^{*1}ridwana.yusuf2019@student.unas.ac.id , ²septi.andryana@civitas.unas.ac.id

ABSTRAK

Segala aktivitas dalam era digital 5.0 ini tak lepas dari teknologi komunikasi dan informatika. Dengan bantuan internet, segala sesuatu dapat terhubung secara terus-menerus. Berkat kemajuan pesat teknologi informasi dan penyebaran internet secara global, setiap orang dapat menggunakan internet dan mengakses informasi. Namun, hal ini juga membawa dampak negatif terhadap keamanan data dan privasi, di mana data dan privasi bisa dengan mudah dieksploitasi di dunia maya, terutama bagi perusahaan yang memiliki sistem informasi inventaris yang berisi data barang yang bersifat pribadi dan tidak boleh diakses sembarang orang. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan penerapan keamanan data dan privasi digital. Penelitian ini menggunakan algoritma MD5 untuk mengenkripsi data dan Sistem Peringatan Dini yang bertujuan untuk memberikan peringatan jika stok tersedia mendekati batas minimum yang ada.

Kata Kunci : MD5, Inventory System, Algoritma, Agile

ABSTRACT

All activities in the digital 5.0 era cannot be separated from communication and information technology. With the help of the internet, everything can be connected continuously. Thanks to the rapid advancement of information technology and the global spread of the internet, everyone can use the internet and access information. However, this also has a negative impact on data security and privacy, where data and privacy can easily be exploited in cyberspace, especially for companies that have an inventory information system that contains data on items that are personal and cannot be accessed by just anyone. Therefore, this study aims to develop the application of data security and digital privacy. This study uses the MD5 algorithm to encrypt data and an Early Warning System which aims to provide a warning if the available stock is close to the existing minimum limit. Keywords: MD5, Early Warning System, Inventory System.

Keywords: MD5, Inventory System, Algoritma, Agile

1. PENDAHULUAN

Peningkatan pesat dalam teknologi memberikan berbagai manfaat bagi kehidupan manusia dalam berbagai aspek. Teknologi tersebut membantu meningkatkan efisiensi dalam menjalankan tugas-tugas sehari-hari. Dengan adanya kemajuan dalam bidang teknologi informasi, kita dapat menghemat waktu yang lebih banyak, mengurangi penggunaan energi, serta mendapatkan data yang akurat dan presentasi yang lebih baik.[1].

Salah satu metode yang dapat digunakan untuk menjaga keamanan data dari akses yang tidak sah adalah teknik hash MD5. Metode ini menggunakan algoritma hash untuk mengubah data asli menjadi sebuah string karakter yang tidak dapat dipahami oleh pihak yang tidak memiliki kunci dekripsi. Namun, teknik hash MD5 memiliki kelemahan yang terkenal dalam hal keamanan, sehingga diperlukan pendekatan yang lebih aman guna melindungi data dengan lebih baik. [2]

Penelitian ini bertujuan untuk melindungi data yang tersimpan dalam database sistem informasi inventaris stok dengan menggunakan metode MD5. Metode ini dapat mencegah potensi pencurian data yang ada dalam database sistem

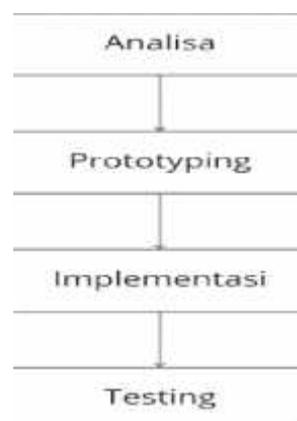
2. METODE PENELITIAN

Dalam penelitian ini dimulai dengan tahap perancangan serta analisis dari permasalahan utama yaitu tentang mengamankan data teks, dalam tahapan analisis mempersiapkan beberapa kebutuhan software dan metode algoritma yang akan diterapkan dalam penelitian. Penulis merencanakan untuk mengimplementasikan metode enkripsi pada aplikasi stok barang berbasis web dan akan berfokus kepada enkripsi data penting seperti nama supplier dan no transaksi barang. Tools yang digunakan untuk mengimplementasikan aplikasi ini adalah php, Laravel sebagai framework mvc untuk mempermudah proses perancangan web dan mysql sebagai database untuk menyimpan data.

Selanjutnya yaitu tahap design prototype, yang dirancang dari tahap analisis kebutuhan wireframe aplikasi dibuat untuk memungkinkan pengguna memasukkan data yang akan dienkripsi dan untuk menentukan konten bentuk apa yang diperlukan saat pengguna melihat data yang di dekripsi.

Tahapan selanjutnya adalah tahap pengujian, pada tahapan ini merupakan tahapan yang utama dari penelitian ini dimana algoritma MD5 akan diuji secara kecepatan dan keamanannya. Pada tahap ini penulis juga melakukan pengujian pada seluruh fitur yang ada dalam aplikasi agar dapat sesuai dengan hasil perencanaan.

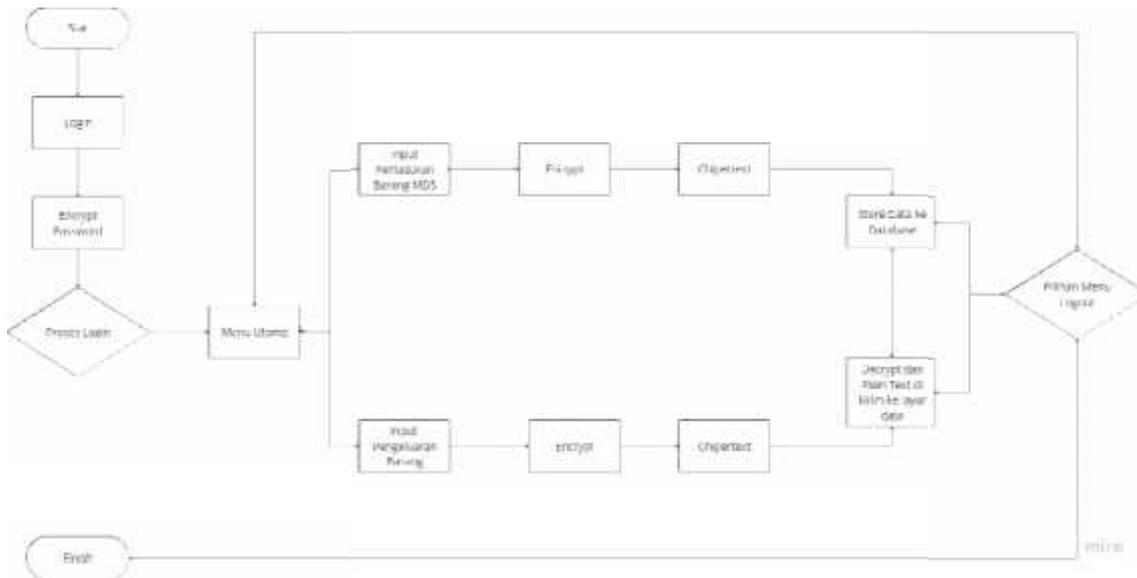
Tahapan terakhir adalah implementasi metode AGILE, setelah itu proses implementasi dan pengujian berpindah ke fase distribusi dan aplikasi dapat berlangsung dalam paradigma AGILE aplikasi dikembangkan untuk beradaptasi dengan teknologi yang ada di masa depan. Data dari seluruh pengujian adalah hasil dari implementasi aplikasi yang telah di deploy.



Gambar 1. Flow Perancangan

3. 1 Rancangan Aplikasi

Pada penelitian ini memberikan output berupa aplikasi berbasis website yang menerapkan keamanan enkripsi dan dekripsi menggunakan MD5. Dimana pada pengimplementasiannya aplikasi ini menerapkan system login dan menu utama sebagai bagian dari navigasi sebelum user menginputkan data dan melihat data yang telah disimpan menggunakan MD5 untuk menguji keamanan serta kecepatannya proses enkripsi dan dekripsi dan memberi peringatan dini pada stok barang jika stok barang <5.

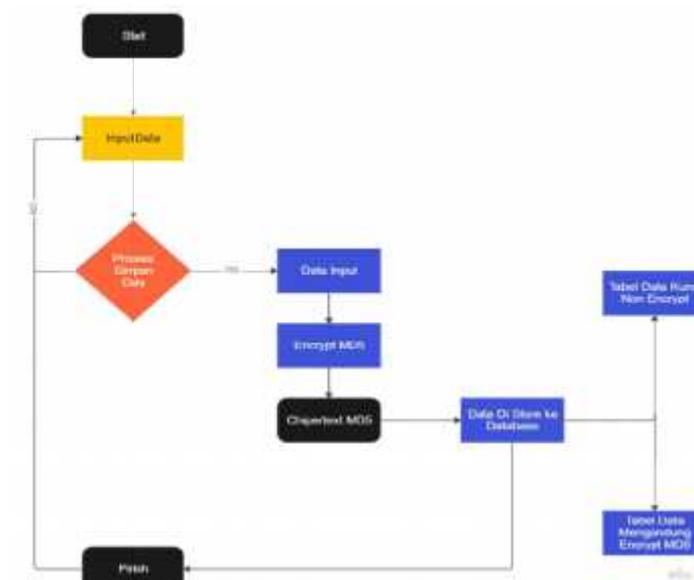


Gambar 2. Flow Aplikasi Inventory System

Pada gambar 3 menunjukkan bahwa keterbaruan dalam penelitian ini ada pada bagian input menu data dan daftar dari data stok pemasukan dan pengeluaran barang, sebagaimana flowchart pada gambar 4. Pengimplementasian dari MD5 dan Early Warning System diuji dan dibandingkan didalam fitur-fitur tersebut.

Implementasi MD5 dan Early Warning System dalam penelitian ini bertujuan untuk mengamankan data No Transaction dan nama Supplier dikarenakan No Transaction mengandung data penting tentang privasi data stok perusahaan. Untuk menjelaskan cara kerja algoritma MD5 dan Early Warning System dalam aplikasi dapat dilihat dalam flowchart. Berikut adalah rancangan system pengamanan data privasi menggunakan MD5 dan Early Warning System pada saat penginputan data yang di enkripsi terlebih dahulu dan pada saat menampilkan data yang di dekripsi pada saat data dalam database diambil.

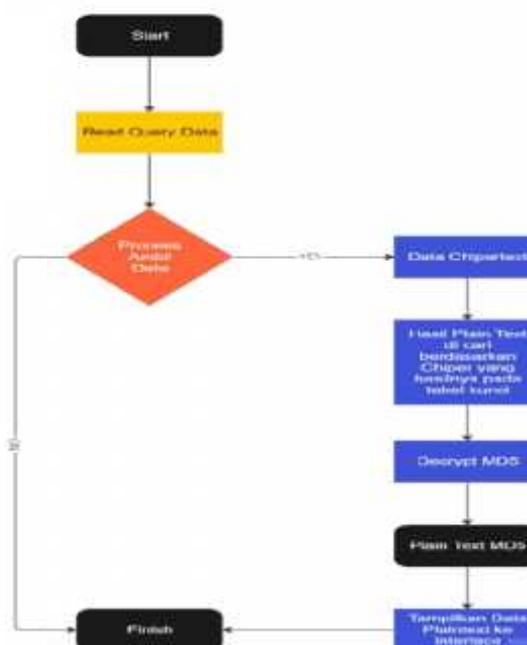
MD 5 ALGORITHM ENCRYPT WORKFLOW



Gambar 3. Flowchart Enkripsi Algoritma MD5

Pada gambar 4 di atas merupakan alur dari enkripsi MD5 dimana data yang akan dienkripsi diacak sepanjang blok-blok yang ada pada MD5 yaitu sebesar 512-bit berulang-ulang.

MD5 ALGORITHM DECRYPT WORKFLOW



Gambar 4. Flowchart Deskripsi MD5

Lalu pada gambar 5 di atas merupakan alur dekripsi MD5 dimana chiphertext tersebut akan dicari didalam tabel yang menghasilkan string yang sama dengan hasil chiphertext tersebut, maka hasil dekripsi akan didapatkan Kembali ke plaintext yang asli dan sesuai.

3. 2 Kebutuhan Sistem

Dalam memenuhi kebutuhan dan mendukung pengembangan sistem aplikasi berbasis website dalam pengimplementasian MD5 dan Triple DES dalam pengamanan data sensitive dari karyawan serta proses enkripsi dan dekripsi untuk mengamankan dan menampilkan didalam interface ada beberapa perangkat yang dapat mendukung agar software ini dapat berjalan baik dan dapat dioperasikan.

Table 1 Spesifikasi Cloud Hosting

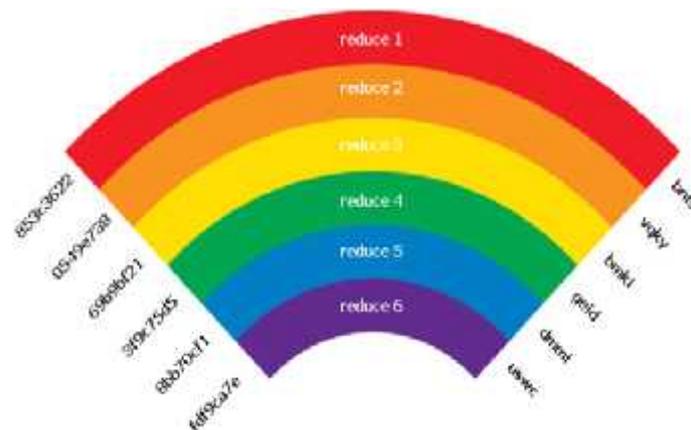
Perangkat	Spesifikasi
Hosting Panel	CPU 0,5 Core, Memory 256 MB, databases Unlimited

Table 2 Software yang dipergunakan

Jenis	Versi / Spesifikasi
Sistem Operasi	Windows 10 Professional 64 bit
Code Editor	Visual Studio Code
Framework	Laravel 8
Bahasa Pemrograman	PHP 8
Database	MYSQL
Database Remote	Navicat
Flowchart Editor	Miro

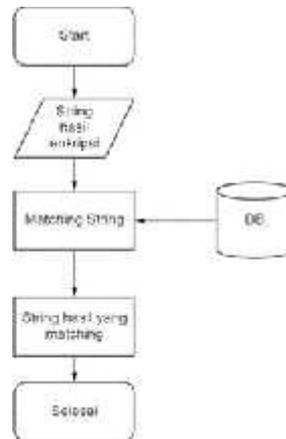
3. 3 Metode Pengujian

Pada penelitian ini menggunakan dua metode pengujian yaitu kecepatan untuk input output data dan cracking text yang terenkripsi dengan menggunakan brute force dan rainbow table sebagai metode pengujian ketahanan dari suatu teks yang terenkripsi.



Gambar 6 Ilustrasi Metode Rainbow Table

Pada gambar 7 disini terdapat ilustrasi dari bagaimana cara atau flow suatu teks terenkripsi itu dapat dipecahkan yaitu dengan menyamakan hasil dari enkripsi yang dilakukan dari suatu dekripsi. Dimana hal itu juga berlaku sebaliknya dimana dekripsi akan menghasilkan enkripsi yang sesuai dengan chiphertext.



Gambar 7 Ilustrasi Brute Force

Pada gambar 7 dapat dilihat flowchart dari pencarian chiphertext terhadap string yang match terhadap hasil plaintext yang didapatkan dari kombinasi chipertext. Brute force juga merupakan sebuah teknik matching pattern atau mencari berbagai kemungkinan chiphertext yang hasil dekripsinya akan sama dengan pattern yang ada pada chiphertext.

3. HASIL DAN PEMBAHASAN

4.1 Interface Aplikasi



Gambar 8 Halaman Login

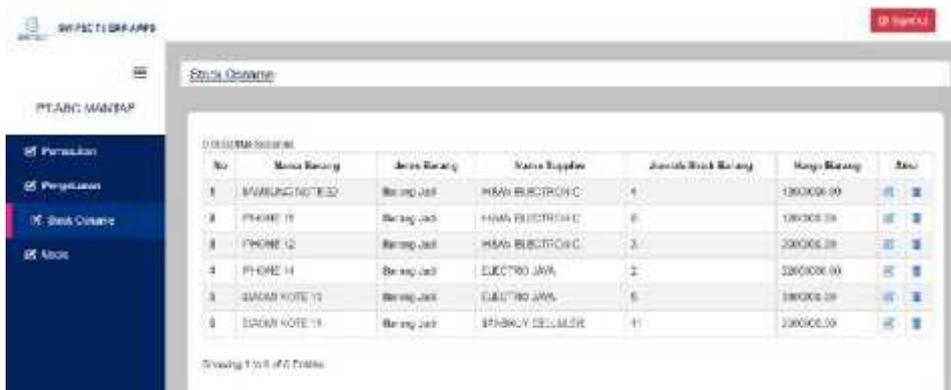
Gambar 8 menunjukkan antarmuka awal untuk halaman login yang digunakan untuk masuk ke dalam aplikasi sistem inventaris. Setelah login berhasil, pengguna akan diarahkan ke

halaman dashboard dalam aplikasi tersebut. Pada halaman login, password dienkripsi menggunakan metode MD5 guna meningkatkan keamanan. Dengan menggunakan enkripsi ini, password sulit dibaca dalam situasi ketika terjadi serangan terhadap basis data. Penelitian sebelumnya juga telah menggunakan menu login dan metode enkripsi yang sama untuk mengamankan password, sehingga password tetap aman dan sulit dibaca oleh pihak ketiga yang berusaha mengakses atau membobol basis data.



Gambar 9 Tampilan Input Barang Masuk

Pada Gambar 9, terdapat Halaman Menu Utama yang merupakan halaman pertama yang muncul setelah masuk ke aplikasi. Halaman ini langsung mengarahkan pengguna ke halaman input pemasukan stok barang.



Gambar 10 Stock Opname

Gambar 10 menunjukkan halaman Stock Opname yang berfungsi untuk menampilkan seluruh stok barang yang tersedia.

Message	Summary	Result 1	Profile	Status			
1	id	notrans	name_brg	jenis_brg	jml_brg	supplier	harga_brg
2	id	notrans	SAMSUNG NOTE 22	Bahan Baku	6	e1a1d68-8f79b1569399ac7	1000000,00
3	id	notrans	SAMSUNG S22	Barang Jadi	15	e1a1d68-8f79b1569399ac7	1500000,00
4	id	notrans	IPHONE 11	Barang Jadi	6	e1a1d68-8f79b1569399ac7	1000000,00
5	id	notrans	IPHONE 12	Barang Jadi	3	e1a1d68-8f79b1569399ac7	1500000,00
6	id	notrans	IPHONE 14	Bahan Baku	2	0643606acc7ead421df87d	2000000,00
7	id	notrans	XIAOMI NOTE 10	Bahan Baku	5	0683606acc7ead421df87d	3000000,00
8	id	notrans	XIAOMI NOTE 11	Bahan Baku	6	42e90daeebe938bbe49333e	2000000,00

Gambar 11 Hasil Enkripsi MD5

Selain dari hasil dari enkripsi gambar 11 diatas untuk mengamankan data menggunakan MD5.

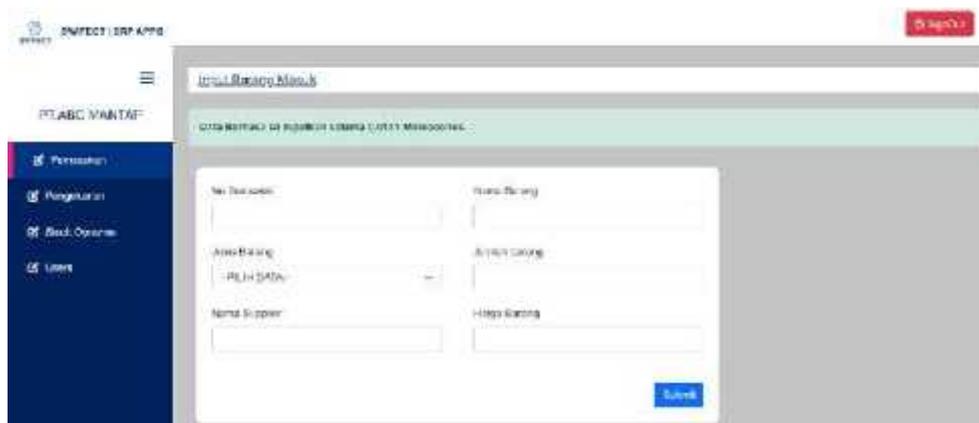
No	No Transaksi	Nama Barang	Jenis Barang	Nama Supplier	Jumlah Barang	Harga Barang	Aksi
1	TR501	IPHONE 11	Barang Jadi	6	IHSAN ELECTRONIC	100000.00	 
2	TR502	IPHONE 12	Barang Jadi	3	IHSAN ELECTRONIC	150000.00	 
3	TR504	XIACMI NOTE 10	Barang Baku	6	ELECTRO JAYA	300000.00	 
4	TR505	XIACMI NOTE 11	Barang Baku	6	SANSKUY CELLULER	200000.00	 
5	TR508	XIACMI NOTE 12	Barang Jadi	10	ELECTRO JAYA	350000.00	 
6	TR507	REDMI 10	Barang Jadi	10	SANSKUY CELLULER	100000.00	 
7	TR508	REDMI 11	Barang Jadi	10	SANSKUY CELLULER	150000.00	 
8	TR52209	REDMI 12	Barang Jadi	10	ELECTRO JAYA	200000.00	 
9	TR522010	REDMI 10 PRO	Barang Jadi	20	SANSKUY CELLULER	200000.00	 
10	TR522011	REDMI 11 PRO	Barang Jadi	10	IHSAN ELECTRONIC	200000.00	 

Gambar 12 Hasil Penampilan Data Yang di Dekripsi Pada Interface Apps

Gambar 12 di atas menampilkan hasil dari antarmuka aplikasi, di mana data ditampilkan dengan jelas dan mudah dibaca agar pengguna dapat memahami informasi yang disajikan. Proses ini melibatkan dekripsi data yang sebelumnya terenkripsi dalam basis data, sehingga dapat ditampilkan kembali dalam bentuk plaintext.

4.2 Pengujian Aplikasi

Dalam aplikasi ini, data penting dari antarmuka yang diinputkan oleh pengguna akan dienkripsi menggunakan MD5. Setelah pengguna berhasil mengirimkan data, proses penginputan akan melibatkan enkripsi data, dan hasil enkripsi (ciphertext) akan dimasukkan ke dalam dua tabel, yaitu tabel form dan tabel data kunci enkripsi. Berikut adalah tampilan antarmuka untuk penginputan data menggunakan MD5:



Gambar 13 Tampilan Date Time Enkripsi MD5

Dalam proses enkripsi data-data sensitif, penulis melakukan pengujian terhadap kecepatan enkripsi data No Transaksi dan Supplier menggunakan algoritma MD5. Berikut adalah hasil pengujian yang mendapatkan waktu sebagai berikut:

Table 3 Data Plain Text

No.	No. Trans	Supplier
1.	TRS22051	VIVO CELL
2.	TRS22052	APEL STORE
3.	TRS22053	JUSTOK CELL

Table 4 Hasil Hash & Date Time Enkripsi MD5 Kedalam Bentuk Chipertext

No.	Hasil Hash	Hasil Hash	Time Encrypt
1.	036034881cb0138a7b60ed4410ef25c5	d946d24310c06d3c3e324e7173a7d94d	0.0181 ms
2.	05afacadb02acbf9c4f6572f9f4f8063	929e29d1723f65be32ba936f7ee29470	0.01676 ms
3.	cf52415183496a11ad3a5cd92e65ef18	69905ac90e517e8ffd94c5e837bce60	0.00777 ms

Proses dekripsi MD5 dilakukan menggunakan metode Rainbow Table. Pengujian dengan metode Rainbow Table menunjukkan bahwa MD5 dapat dengan cukup mudah didekripsi menggunakan metode ini. Hal ini menunjukkan hasil yang signifikan dalam proses peningkatan keamanan terhadap serangan cracking teks. Berikut ini adalah hasil pengujian dekripsi menggunakan metode Rainbow Table:

Table 5 Hasil Pengujian Dekripsi Data Menggunakan Rainbow Table

No.	Algoritma	Metode Decrypt	Time Encrypt
1.	MD5	Rainbow Table	0.01386 ms

4. KESIMPULAN

Skripsi ini membahas tentang penggunaan algoritma MD5 dalam sebuah sistem inventory yang dikembangkan dengan menerapkan metode Agile. Algoritma MD5 merupakan salah satu algoritma hash kriptografis yang digunakan untuk mengamankan integritas data. Integritas data berarti bahwa data tidak mengalami perubahan atau manipulasi yang tidak sah, sehingga data tetap akurat dan dapat diandalkan. Dalam konteks sistem inventory, penting untuk memastikan bahwa data inventaris yang disimpan tetap konsisten dan tidak mengalami perubahan yang tidak

diinginkan. Untuk mencapai tujuan ini, penulis skripsi menggunakan algoritma MD5 untuk menghasilkan nilai hash yang unik untuk setiap data yang ada di dalam sistem inventory.

5. SARAN

Berdasarkan dari hasil penelitian yang dilakukan, maka diperoleh kesimpulan:

1. Penerapan Algoritma MD5 dalam aplikasi Inventory System dirancang untuk melindungi data sensitif terkait barang dan juga untuk mengukur waktu yang dibutuhkan untuk melakukan enkripsi data menggunakan metode MD5.
2. Dengan melakukan pengujian dekripsi data menggunakan rainbow table, kita dapat mengukur seberapa cepat waktu yang diperlukan untuk mendekripsi data dalam bentuk ciphertext menjadi plaintext pada antarmuka aplikasi sistem inventaris.

DAFTAR PUSTAKA

- [1] S. Sharofoviya Olimov, "Information Technology in Education," JARSP. [Online]. Available: <http://innosci.org/>
- [2] A. Delgado, "Design of web systems for inventory control in the E-commerce sector under the Agile methodologies approach," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 7, pp. 3129–3133, Jul. 2020, doi: 10.30534/ijeter/2020/41872020.
- [3] T. Ferga and A. Hikmawan, "Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA Dan MD5".
- [4] R. A. Widayat, A. Triayudi, and B. Rahman, "KLIK: Kajian Ilmiah Informatika dan Komputer Algoritma FIFO Untuk Pengendalian Stok Pada Aplikasi Inventory Obat Berbasis Web," *Media Online*, vol. 3, no. 6, pp. 1153–1161, 2023, doi: 10.30865/klik.v3i6.880.
- [5] A. Prasetya, S. Andriana, and R. T. Komalasari, "Rancang Bangun Inventarisasi Barang menggunakan Algoritma Apriori Sebagai Data Mining," *Jurnal Teknologi Informasi dan Komunikasi*, vol. 5, no. 4, p. 2021, 2021, doi: 10.35870/jti.
- [6] L. B. De Guzman, A. M. Sison, and R. P. Medina, "MD5 secured cryptographic hash value," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2018, pp. 54–59. doi: 10.1145/3278312.3278317.
- [7] D. M. Khairina, "ANALISIS KEAMANAN SISTEM LOGIN," 2011.
- [8] N. Hayati, M. A. Budiman, and A. Sharif, "Implementasi Algoritma RC4A dan MD5 untuk Menjamin Confidentiality dan Integrity pada File Teks," 2017.
- [9] E. Setyawati, C. E. Widjayanti, R. R. Siraiz, and H. Wijoyo, "Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5," *Jurnal Manajemen Informatika Jayakarta*, vol. 1, no. 1, p. 56, Feb. 2021, doi: 10.52362/jmijayakarta.v1i1.367.
- [10] H. Mursid, J. Supardi, and M. Q. Rizkie, "Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi Hash MD5, RSA dan Skema Qr-Cod."