Universitas Kristen Wira Wacana Sumba
Fakultas Sains dan Teknologi
SATI: Sustainable Agricultural Technology Innovation
Homepage: https://ojs.unkriswina.ac.id/index.php/semnas-FST
1st Nasional Seminar on Sustainable Agricultural Technology Innovation
27-28 Januari 2023/ Pages: 1-9

PERANCANGAN SISTEM PENGAMANAN DATA PASIEN MENGGUNAKAN METODE KRIPTOGRAFI *VIGENÈRE CIPHER*

Lindra Rambu Kandokang[1], Arini Aha Pekuwali [2], Pingky Alfa Ray Leo Lede [3]

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Kristen Wira Wacana Sumba, Indonesia
Corresponding author: lindrakandokang@gmail.com[1], arini.pekuwali@unkriswina.ac.id[2], pingky.leo.lede@unkriswina.ac.id[3]

ABSTRACT

The use of information technology is widely used from various circles. With technology, you can makes it easy to obtain and provide information, but there is information that is confidential may only be known by certain parties, one of which is the patient's medical record data. Medical record data Patient information is confidential, therefore security is needed for recorded data medical. By using the vigenère cipher method which aims to prevent people who don't interested in knowing this data. Vigenère cipher is a cryptographic algorithm the encryption and decryption process requires the same key length as the plaintext length ciphertext. The medical record data that is secured or encrypted is the patient's name, anamnesis and. Examination is a communication between the doctor and the patient. This way is done with the aim of. Obtain information about the patient's medical history. Diagnostics to report procedures end of medical diagnosis. Therapy is the result of treatment given to patients. To do encryption and decryption process using ASCII code.

Keywords: Cryptography, Vigenère cipher, Medical records, ASCII code.

ABSTRAK

Penggunaan teknologi informasi banyak digunakan dari berbagai kalangan. Dengan adanya teknologi dapat memudahkan untuk mendapat dan memberikan informasi, namun ada informasi yang bersifat rahasia yang hanya boleh diketahui oleh pihak tertentu, salah satunya adalah data rekam medis pasien. Data rekam medis pasien merupakan informasi yang bersifat rahasia oleh karena itu dibutuhkan keamanan terhadap data rekam medis. Dengan menggunakan metode vigenère cipher yang bertujuan untuk mencegah orang yang tidak berkepentingan untuk mengetahui data tersebut. Vigenère cipher merupakan salah satu algoritma kriptografi yang proses enkripsi dan deskripsi membutuhkan panjang kunci yang sama dengan panjang plainteks dan cipherteks. Adapun data rekam medis yang diamankan atau dienkripsikan adalah nama pasien, anamnesis dan pemeriksaan merupakan komunikasi antara dokter dengan pasien cara ini dilakukan dengan tujuan untuk memperoleh informasi tentang riwayat sakit yang dialami oleh pasien. Diagnosa untuk melaporkan prosedur akhir dari diagnosa medis. Terapi merupakan hasil pengobatan yang diberikan kepada pasien. Untuk melakukan proses enkripsi dan deskripsi menggunakan kode ASCII.

Kata kunci: Kriptografi, Vigenère cipher, Rekam medis, kode ASCII.

Universitas Kristen Wira Wacana Sumba
Fakultas Sains dan Teknologi
SATI: Sustainable Agricultural Technology Innovation
Homepage: https://ojs.unkriswina.ac.id/index.php/semnas-FST
1st Nasional Seminar on Sustainable Agricultural Technology Innovation
27-28 Januari 2023/ Pages: 1-9

PENDAHULUAN

Teknologi berkembang begitu cepat sehingga memungkinkan manusia untuk berkomunikasi atau saling bertukar informasi atau data secara jarak jauh. Baik antar wilayah maupun antar negara bahkan antar benua sekalipun bukan merupakan satu halangan dalam melakukan komunikasi dan pertukaran informasi, sehingga ketentuan mengenai keamanan tentang kerahasiaan informasi yang akan dipertukarkan semakin bertambah. Keamanan serta kerahasiaan ketika melangsukan peralihan data dan informasi menjadi perkara yang benar-benar penting pada saat ini, salah satu yang perlu dijaga adalah informasi atau data yang bersifat rahasia yang tidak ingin diketahui oleh orang lain. Keamanan data terus dikembangkan untuk meminimalkan pencurian data. Pengembangan keamanan data selalu dikembangkan supaya data tidak dapat dicuri. sandi atau enkripsi data merupakan adalah dengan mengganti informasi data sehingga data tidak dapat dibaca bagi pihak yang tidak berwewenang. Hasil dari enkripsi adalah informasi yang disandikan atau cipher text. Sedangkan proses pengambilan informasi dari sandi disebut dekripsi.

Kriptografi merupakan bidang yang mengamati cara-cara matematika yang berkaitan dengan keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kriptografi sudah dikenal sejak lama. Kriptografi juga adalah ilmu sekalian seni dalam mengawasi keamanan informasi atau pesan. Kriptografi klasik digunakan sebelum adanya komputer, kriptografi ini berbasis pada karakter yang dimana enkripsi dan deskripsinya dilakukan pada setiap karakter (Munir, 2006).

Keamanan data adalah suatu bagian yang sangat penting dalam sistem informasi untuk itu keamanan data perlu perhatian. Salah satu keamanan data pada rekam medis pasien. Data yang ada pada rekam medis ini bersifat rahasia sehingga diperlukan pengamanan terhadap data-data penting seperti identitas, hasil pemeriksaan, pengobatan dan catatan kesehatan pasien.

MATERI DAN METODE

Kriptografi

Kriptografi berasal dari bahasa yunani, yang dibagi menjadi dua, yaitu kripto dan *graphia*. Kripto yang berarti secret (rahasia) dan *graphia* yang berarti writing (tulisan). Kriptografi adalah suatu bidang yang mengamati bagaimana upaya melindungi agar data atau pesan selalu terlindungi ketika dikirimkan, dari pengirim ke penerima tidak menghadapi hambatan yang disebabkan oleh pihak ketiga (Munir, 2006).

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Proses enkripsi mengganti plainteks menjadi cipherteks (menggunakan kunci tertentu) sehingga isi informasi dari pesan yang tercantum rumit dimengerti. tujuan kriptografi untuk memberikan layanan keamanan sebagai berikut:

1. Confidelity (kerahasiaan) adalah isi pesan yang akan dikirimkan tetap terjaga kerahasianya sehingga tidak diketahui oleh orang yang tidak berkepentingan (selain pengirim dan penerima dan pihak yang sudah diberi ijin). Proses ini dibuat menggunakan satu algoritma matematis yang dapat mengubah data asli menjadi rumit dalam membaca dan memahami.
2. *Data integrity* (keutuhan data) merupakan fasilitas yang dapat menandai atau menemukan jika terjadi pemalsuan (penghilangan, pengbaruan atau penyisipan) data yang tidak resmi bagi pihak yang lainnya.

3. Authentication (autentikasi) merupakan fasiltas yang berkaitan dengan pengenalan, dan autentik yang dilakukan kelompok yang berpartisipasi saat berkirim data atau otentikasi kebenaran data atau berita.
4. Availability (Ketersediaan), yakni pengguna yang memiliki kewenangan dalam mengakses dan diberikan kewenangan untuk mengakses berkas serta tidak mengalami hambat apapun.
5. Non-repudiation (anti-penyangkalan) adalah fasilitas digunakan untuk mengatasi orang dalam aksi peyangkal yang dilaksanakan lebih dulu (membantah apabila pesan bersumber darinya).

Vigenère Cipher

Vigenère Cipher merupakan contoh terbaik dari *cipher* alfabet-majemuk (manual). *Vigènere Cipher* ini dipublikasikan pada tahun 1586 oleh seorang diplomat sekaligus seorang kriptologis dari Prancis, yaitu Blaise de Vigènere pada abad 16.*Vigenère cipher* adalah pengembangan dari ceasar cipher, kelebihan *vigenère cipher* nilai kunci digeser dengan nilai kunci yang berbeda sesuai panjang kata plainteks, sehingga tidak mudah untuk dipecahkan.

Vigenère cipher menggunakan tabel bujursangkar untuk proses enkripsi. Tiap deret tabel dibujursangkar menjabarkan kumpulan abjad dalam bentuk tabel 26x26 yang menggambarkan huruf dan kunci. Pada jurnal ini penulis menggunakan tabel ACII, sebanyak 32 sampai 126 karakter tetapi untuk indeks ASCII karakter dari plainteks, kunci dan cipherteks perlu dikurangi 32. Sehingga indeks 32 dimulai dari 0.. Untuk ASCII 32-126 dapat dilihat pada Tabel 1.

Tabel. 1 ASCII Yang Digunakan

ASCII	Char	ASCII	Char	ASCII	Char	ASCII	Char	ASCII	Char
32	(spasi)	51	3	70	F	89	Y	108	l
33	!	52	4	71	G	90	Z	109	m
34	“	53	5	72	H	91	[	110	n
35	#	54	6	73	I	92	\	111	o
36	$	55	7	74	J	93	]	112	p
37	%	56	8	75	K	94	^	113	q
38	&	57	9	76	L	95	_	114	r
39	‘	58	:	77	M	96	`	115	s
40	(	59	;	78	N	97	a	116	t
41	)	60	<	79	O	98	b	117	u
42	*	61	=	80	P	99	c	118	v
43	+	62	>	81	Q	100	d	119	w
44	,	63	?	82	R	101	e	120	x
45	-	64	@	83	S	102	f	121	y
46	.	65	A	84	T	103	g	122	z
47	/	66	B	85	U	104	h	123	{
48	0	67	C	86	V	105	i	124	|
49	1	68	D	87	W	106	j	125	}
50	2	69	E	88	X	107	k	126	~

Setelah dilakukan pengurangan maka indeks ASCII di mulai dari 0 tujuan dilakukan pengurangan untuk meyesuaikan jumlah karakter dalam tabel ASII sehingga rumus yang digunakan mengalami perubahan yaitu mod 95. dapat dilihat pada Tabel 2.

Tabel 2 Substitusi *Vigenère Cipher* yang diusulkan

Indeks	Char	indeks	Char	Indeks	Char	indeks	Char	indeks	Char
0	(spasi)	19	3	38	F	57	Y	76	l
1	!	20	4	39	G	58	Z	77	m
2	“	21	5	40	H	59	[	78	n
3	#	22	6	41	I	60	\	79	o
4	$	23	7	42	J	61	]	80	p
5	%	24	8	43	K	62	^	81	q
6	&	25	9	44	L	63	_	82	r
7	‘	26	:	45	M	64	`	83	s
8	(	27	;	46	N	65	a	84	t
9	)	28	<	47	O	66	b	85	u
10	*	29	=	48	P	67	c	86	v
11	+	30	>	49	Q	68	d	87	w
12	,	31	?	50	R	69	e	88	x
13	-	32	@	51	S	70	f	89	y
14	.	33	A	52	T	71	g	90	z
15	/	34	B	53	U	72	h	91	{
16	0	35	C	54	V	73	i	92	|
17	1	36	D	55	W	74	j	93	}
18	2	37	E	56	X	75	k	94	~

Rumus enkripsi dan deksripsi *vigenère cipher*:

Enkripsi

$C_i = (P_i + K_i) \bmod 95$

Deskripsi

$P_i = (C_i - K_i) \bmod 95$

Jika plainteks “Lindra” kata kunci “saya” proses perhitungan enkripsi sebagai berikut:
Rumus enkripsi: $C_i = (P_i + K_i) \bmod 95$
Terlebih dulu konversikan plainteks kedalam angka.
L = 44
Nilai kunci s = 83
= 44 + 83 mod 95
= 127 mod 95
= 32
Nilai desimal 32 ASCII mempunya karakter “@”
i = 73
nilai kunci a = 65
= 73 + 65 mod 95
= 138 mod 95 = 43
Nilai desimal 43 ditabel ASCII mempunya karakter “K”
n = 78
nilai kunci y = 89
= 78 + 89 mod 95
= 167 mod 95 = 72
Nilai desimal 72 ditabel ASCII mempunyai karakter “h”
d = 68
nilai kunci a = 65
= 68 + 65 mod 95

= 133 mod 95 = 38
Nilai desimal 38 ditabel ASCII mempunyai karakter “F”
r = 82
nilai kunci s = 83
= 82 + 83 mod 95
= 165 mod 95 = 70
Nilai desimal 70 ditabel ASCII mempunyai karakter “f”
a = 65
nilai kunci a = 65
= 65 + 65 mod 95
= 130 mod 95 = 35
Nilai desimal 35 ditabel ASCII mempunyai karakter “C”
Jadi hasil enkripsi “@KhFfC”

Proses deskripsi sama dengan enkripsi konversikan cipherteks kedalam angka.
Rumus deskripsi: $P_i = (C_i - K_i) \bmod 95$
Atau
$Pi = (((ci – ki) + 95) \bmod 95) C_i \leq K_i$
@ =32
Nilai kunci s = 83
= 32 – 83 mod 95
= -51 + 95 mod 95 = 44
Nilai desimal 44 ditabel ASCII mempunyai karakter “L”
K = 43
Nilai kunci a = 65
= 43-65 mod 95
= - 22 + 95 mod 95 = 73
Nilai desimal 73 ditabel ASCII mempunyai karakter “i”
h = 72
nilai kunci y = 89
= 72 – 89 mod 95
= - 17 + 95 mod 95 = 78
= niali desimal 78 ditabel ASCII mempunyai karakter “n”
F = 38
Nilai kunci a = 65
= 38 – 65 mod 95
= -27 + 95 mod 95 = 68
Nilai desima 68 ditabel ASCII mempunyai karakter “d”
f = 70
nilai kunci s = 83
= 70 – 83 mod 95
= - 13 + 95 mod 95 = 82
Nilai 82 ditabel ASCII mempunyai karakter “r”
C = 35
Nilai kunci a = 65
= 35 – 65 mod 95
= -30 + 95 mod 95 = 65
Nilai desimal 65 ditabel ASCII mempunyai karakter “a”
Jika cipherteks “@KhFfC” kata kuncinya “saya” mempunyai plainteks “Lindra” maka proses deskripsinya berhasil.

Metode Pengumpulan Data

1. **Observasi**

   Pada tahap ini observasi dilakukan yaitu pengumpulan data berupa data pasien, Tahap ini dilakukan dengan cara meninjau dan pengamatan secara langsung terhadap sistem yang sedang berjalan pada Puskesmas Nggoa untuk memperoleh informasi yang dibutuhkan.

2. **Wawancara**

   Wawancara dilakukan secara langsung pada admin dan petugas rekam medis dengan mengajukan beberapa pertanyaan mengenai bentuk rekam medis pasien di Puskesmas Nggoa dan upaya dalam menjaga kerahasian data pasien.

Metode Pengembangan Sistem

Metode yang gunakan dalam melakukan perancangan sistem pengamanan data pasien di Puskesmas Nggoa yaitu menggunakan metode waterfall. Ada beberapa tahap yang dilakukan dalam proses perancangan sistem pengamanan data pesien dimulai dari tahap analisis, tahap desain, dan tahap implementasi.

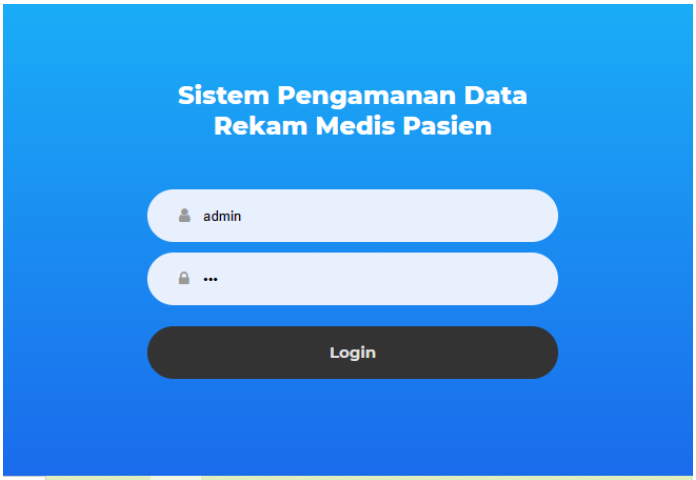
Perancangan Sistem

Perancangan sistem gambaran dari keseluruhan bagaimana sistem akan berjalan. Tujuannya adalah untuk menghasilkan sebuah sistem yang sesuai dengan kebutuhan. Perancangan sistem dengan UML ini terdiri dari perancangan *use case* diagram(*use case diagram* petugas rekam medis), perancangan *activity diagram*(*activity diagram Login, activity diagram* Enkripsi dan Deskripsi), *Sequencediagram*(*Sequence diagram Login, Sequence diagram* rekam medik terenkripsi).

HASIL DAN PEMBAHASAN

Halaman *Login*

Berikut merupakan tampilan halam *login* yang akan dilakukan oleh petugas rekam medis.



Gambar 1 halaman *Login*

Gambar 1 yaitu halaman untuk masuk(*login)*. Jika petugas telah mengunjungi situs pengamanan data pasien maka sistem akan menampilkan halaman *login* pada pengamanan data pasien, selanjutnya petugas menginput *username* dan *password* sistem akan memvalidasi datajika data telah terdaftar sistem akan menampilkan halaman utama pada sistem dan jika data tidak terdaftar maka akan mendapatkan konfirmasi pesan *username* dan *password* yang dimasukkan salah.

Halaman *Dashboard*

Halaman *Dashboard* yang muncul pertama kali setelah berhasil *login* pada sistem pengamanan data pasien.

Gambar 2 Tampilan Halaman *Dashboard*

Gambar 2 merupakan tampilan halaman *dashboard*setelah petugas *login* pada sistem pengamanan data pasien maka sistem menampilkan halaman *dashboard.* Dalam halaman *dashboard*terdapat ucapan selamat datang dan menu rekam medis.

Halaman Rekam Medik

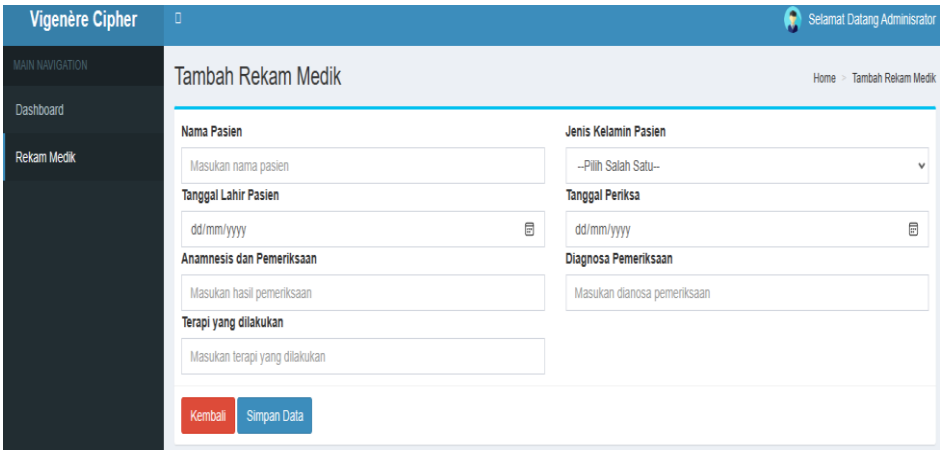
Halaman data rekam medik yang muncul saat petugas memilih menu rekam medik pada sistem pengamanan data pasien.

Gambar 3 Tampilan Rekam Medik Terenkripsi

Pada halaman rekam medik merupakan tabel data pasien yang sudah terenkripsi yang terdiri dari nama pasien, hasil pemeriksaan, diagnosa dan terapi. Pemberian kata kunci dilakukan secara otomatis oleh sistem kata kunci untuk enkrispi dilakukan secara dimanis sesuai panjang kata plainteks yang dimasukkan, sistem akan generate kata kunci secara acak. Proses enkripsi dilakukan secara otomatis oleh sistem, serta petugas juga dapat menghapus data rekam medik pasien.

Tambah Data

Menu tambah data merupakan menu ketika petugas ingin tambah data pasien pada data rekam medik.



Gambar 4 Tampilan Tambah Rekam Medik

Tambah rekam medik terdiri dari nama pasien, jenis kelamin, tanggal lahir pasien, anamnesis dan pemeriksaan, diagnosa, dan terapi. Selanjutnya petugasnya menyimpan dalam *database* sehingga dapat di tambahkan kedalam data pasien tetapi sebelum dilakukan proses enkripsi oleh sistem, yang akan dienkripsikan hanya nama pasien, hasil pemeriksaan, diagnosa dan terapi.

Perancangan sistem informasi yang dibuat diimplementasikan kedalam bentuk perangkat lunak sistem pengamanan data pasien menggunakan metode *kriptografi vigenère cipher* di Puskesmas Nggoa Pengembangan sistem ini dibuat menggunakan bahasa pemrograman *php*, basis data *mysql*, *framework codeIgniter*.Berikut ini merupakan tampilan sistem dari hasil implementasi sistem pada pengamanan data pasien.

Pengujian Sistem

Pengujian sistem ini menggunakan *black box* dilakukan untuk menguji spesifikasi fungsi dari sistem pengamanan data pasien di puskesmas Nggoa. Pada tabel pengujian *black box* merupakan pengujian dari sistem pengamanan data pasien menggunakan metode *kriptografi vigenère cipher*.

Tabel. 1 Pengujian *Black Box*

No.	Pengujian	*Test Case*	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1.	Login ke sistem pengamanan data pasien	Mengisi *username* dan *password*	*Login* sistem	Berhasil	[x] Diterima [ ] Ditolak
2.	Petugas rekam medik mengakses data rekam medik	Menekan rekam medik	Membaca dan melihat data dan menghapus rekam medik pasien	Berhasil	[x] Diterima [ ] Ditolak
3.	Petugas dapat menginput data pasien pada tambah rekam medis	Menambah data pasien,simpan	Sistem dapat mengenkripsikan tambah rekam medis	Berhasil	[x] Diterima [ ] Ditolak

KESIMPULAN

Salah satu cara untuk menjaga kerahasian data pasein yaitu dengan cara menggunakan algoritma *kriptogari vigenère cipher*. Sistem pengamanan data pasien didapat membantu dalam meningkatkan keamanan data pasien. Dalam melakukan perancangan menggunakan UML, implemtasi sistem menggunakan *framework Codeigniter* dengan bahasa pemograman PHP. Sistem akan melakukan proses enkripsi setelah petugas mengisi data pasien pada from tambah data rekam medik selanjutnya petugas menyimpan data pasien, data pasien akan tersimpan dalam *database*. Sistem akan melakukan proses enkripsi, hasil enkripsi akan ditampilkan dalam from rekam medik. Pemberian kata kunci dilakukan secara otomatis oleh sistem.

Dalam proses enkripsi menggunakan kode ASCII*printable characters* tetapi dilakukan pengurangan 32 untuk menyesuaikan jumlah karakter dalam tabel ASCII.

DAFTAR PUSTAKA

Abdullah, D., & Surniyati. (2017). Pengamanan Email Menggunakan Metode Vigenere Cipher. *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research*, 1(1), 2598-8700.

Gunadhi, Erwin., & Sudrajat, A. (2016). Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigènere Cipher. *Jurnal Algoritma Sekolah Tinggi Teknologi Garut*, 13 (2), 2302-7339.

Irawan, M.D. (2017). Implementasi Kriptografi Vigenere Cipher Dengan PHP. JURNAL TEKNOLOGI INFORMASI (JurTI) 1(1), 2580-7927.

Irawan, Sulistyowati. (2017). Implementasi framework codeignter untuk pengembangan website pada dinas perkebunan provinsi kalimatan tengah. *Jurnal saintekom*, volume 7. No.1

Munir. (2006). *kriptografi*, informatika, bandung.

Priyono. (2016) Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks. *Jurnal Riset Komputer (JURIKOM)*, 3(5), 2407-389X.

Sihombing, B., Patresia D., Manrung, S., Ahadi, E., & Gunawan, I. (2020). Pengamanan Pesan Teks Menggunakan Kriptografi Algoritma Vigenere Cipher Dari Serangan Eavesdropping. *Jurnal Teknik Informatika Kaputama(JTIK)*, 4(1), 2686-0880.

Sukmawati, R., & Priyadi, Y. (2019). Perancangan Proses Bisnis Menggunakan UML Berdasarkan Fit/Gap Analysis Pada Modul Inventory Odoo. INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi, 3(2), 104-115.