Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 2, Nomor : 1, Januari 2023 : 98-107 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan

Implementation Of RSA Cryptographic Algorithms in Library Information System Applications

Maria SD. Dairi*[1], Munjiat Setiani Asih [2], Khairunnisa[3] (* corespondent author)
[1,2,3]Program Studi Teknik Informatika, Universitas Harapan Medan
E-mail: [*1] mariadairi12@gmail.com, [2] Munjiat.stth@gmail.com,
[3]khairunnisajv2@gmail.com

Abstrak

Perpustakaan merupakan suatu lembaga atau instansi yang mengumpulkan pengetahuan tercetak dan terekam, mengelolanya dengan cara khusus guna memenuhi kebutuhan intelektual penggunanya. Sebuah perpustakaan memiliki data-data yang hanya boleh diketahui oleh pihak tertentu, oleh karena itu perpustakaan harus menjaga kerahasian data dengan cara menggunakan teknik pengamanan data pada sistem Informasi nya. Teknik pengamanan data yang digunakan adalah algoritma kriptografi, yaitu teknik untuk mengubah data kedalam bentuk kode-kode tertentu agar informasi yang tersimpan tidak dapat terbaca oleh siapapun kecuali orang-orang yang berhak. Untuk algoritma kriptografi yang digunakan adalah algoritma kriptografi RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, Yaitu: Ron (R)ivest, Adi (S)hamir dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Dalam kriptografi algoritma RSA terdapat tiga proses yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi, dan proses dekripsi.

***Kata kunci**: Perpustakaan, Kriptografi Algoritma RSA, Enkripsi, Dekrpsi, Pembentukan Kunci*

Abstract

The library is an institution or agency that collects printed and recorded knowledge, manages it in a special way to meet the intellectual needs of its users. a library has data that may be known by certain parties, therefore the library must maintain data confidentiality by using security techniques only on its information system. The data security technique used is a cryptographic algorithm, which is a technique for converting data into certain codes so that the stored information cannot be read by anyone except the authorized person. The RSA cryptographic algorithm used is the RSA cryptographic algorithm. The RSA algorithm was created by 3 researchers from MIT (Massachussets Institute of Technology) in 1976, namely: Ron (R)ivest, Adi (S)hamir and Leonard (A)dleman. The security of the RSA algorithm lies in the difficulty of factoring large numbers into prime factors. In the RSA cryptographic algorithm, there are three processes, namely the process of generating public and private keys, the encryption process, and the decryption process.

***Keywords**: Library, RSA Algorithm Cryptography, Encryption, Decryption, Key Generation*

1. PENDAHULUAN

Ilmu pengetahuan dan teknologi berkembang dengan sangat pesat sekarang ini, salah satunya yaitu bidang komputerisasi. Teknologi komputerisasi sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi/instansi). Kelompok (organisasi/instansi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap aktivitasnya. Berbagai aplikasi dirancang dengan fungsi yang berbeda-beda sesuai dengan kebutuhan yang ada. Aplikasi untuk mengelolah informasi -informasi dan data-data penting suatu instansi dapat memberikan pengaruh positif bagi perkembangan, efisiensi waktu kerja serta data yang didapat lebih terperinci dan akurat. Tetapi yang harus diperhatikan adalah ada sebagian dari informasi maupun data tersebut bersifat rahasia dan keamanannya harus dijaga, permasalahan yang timbul adalah bagaimana suatu instansi dapat menjaga keamanan data tersebut dari kemungkinan pencurian data oleh oknum-oknum yang tidak bertanggung jawab. Oleh karena itu untuk menghindari permasalahan tersebut dibutuhkan suatu sistem yang dapat melindungi keamanan data pada aplikasi tersebut.

Suatu instansi seperti pertpustakaan memiliki informasi atau data–data tentang buku yang dimiliki yang harus dijaga dan disimpan . Namun proses pelayanan yang dilakukan perpustakaan saat ini masih banyak dilakukan secara konvensional yaitu semua pendataannya masih ditulis didalam buku dan saat mencari data yang dibutuhkan harus membuka perhalaman buku, hal tersebut menyebabkan lambatnya dalam pencarian data, layanan sirkulasi ataupun pembuatan laporan. Selain itu, keamanan data-data tersebut juga tidak dapat dijaga dengan baik dikarenakan siapapapun dapat melihat buku data dan membacanya. Untuk memenuhi keamanan data-data tersebut, perpustakaan memerlukan suatu sistem informasi yang dapat membantu para tenaga pengelolah dalam mencari informasi atau referensi tentang data-data buku yang diperlukan serta menjaga kerahasiaan data-data perpustakaan tersebut. Dimana setiap data tersebut diharapkan memiliki keamanan agar data tersebut tetap terjaga kerahasiannya dan tidak gampang untuk diketahui oleh pihak lain yang tidak berhak untuk mengetahui apa isi dari suatu informasi atau data tersebut.

Untuk memenuhi kebutuhan tersebut, usaha yang harus dilakukan perpustakaan adalah pemanfaatan teknologi informasi seperti membangun aplikas sistem keamanan informasi perpustakaan. Dimana aplikasi tersebut tidak hanya untuk mengolah data-data perpustakaan tetapi juga dapat menjaga kerahasiaan data-data dengan adanya proses pengenkripsian dalam sistem informasi yang akan dibangun nantinya. Setiap data diharapkan memiliki keamanan agar data tersebut tetap terjaga kerahasiannya dan tidak gampang untuk diketahui oleh pihak lain yang tidak berhak untuk mengetahui apa isi dari suatu informasi atau data tersebut. Sehingga data-data dalam sistem akan tersimpan dalam *database* dan berbentuk *ciphertext*. Dari penelitian-penelitian yang telah dilakukan para peneliti sebelumnya dijelaskan bahwa ada salah satu teknik yang dapat digunakan dalam pengamanan data yaitu teknik kriptografi. Kriptografi bertujuan agar informasi yang bersifat

rahasia, integrasi data, dan ontentika yang dikirim melalui suatu jaringan internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan. Pada penelitian ini algoritma kriptografi yang dibahas adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, Yaitu: Ron (R)ivest, Adi (S)hamir dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bialngan besar menjadi faktor-faktor prima belum ditemukana Algoritma yang tanggu atau handal, maja selama itu pula kemanan algoritma RSA tetap terjamin.

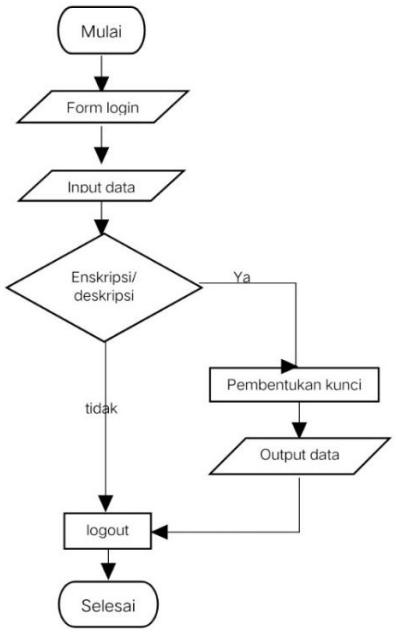
2. METODOLOGI PENELITIAN

Metode penelitian adalah langkah-langkah yang akan dilakukan oleh peneliti dalam rangka untuk mengumpulkan informasi serta melakukan investigasi pada data yang telah didapatkan. Metode penelitian memberikan gambaran rancangan penelitian dalam penelitian ini yaitu menggunakan algoritma kriptografi RSA dalam sistem informasi perpustakaan.

2.1 Analisa Algoritma RSA

Algoritma RSA sendiri terbagi dari tiga tahapan atau proses yaitu:
1. pembangkitan kunci
2. tahap enkripsi dan
3. Tahap dekripsi.

2.2. Flowchart Sistem



Gambar 1. Flowchart Sistem

3. HASIL DAN PEMBAHASAN

3.1. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi , seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Definisi lain menurut kriptografi yaitu seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain [3].

3.1.1. Kriptografi RSA

Algoritma kriptografi RSA merupakan algoritma yang melakukan pemfaktoran bilangan yang sangat besar, oleh karena alasan tersebut RSA dianggap aman. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya, sehingga semakin besar bilangan prima yang digunakan semakin baik atau aman. Dalam kriptografi menggunakan algoritma RSA terdapat tiga proses yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi, dan proses dekripsi. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar [1].

Algoritma RSA merupakan blok *cipher* dimana semua informasi dipetakan ke sebuah *integer*. Algoritma RSA terdiri dari kunci publik dan kunci privat dimana kunci publik dapat diketahui oleh semua orang sedangkan kunci privat hanya diketahui oleh pemilik data. Proses enkripsi menggunakan kunci publik dan proses dekripsi menggunakan kunci privat pemilik data [2].

Berikut adalah tahapan dalam algoritma kriptografi RSA

1. Pembangkitan Kunci Pada RSA

Pengkodean RSA membutuhkan dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Bilangan yang dipilih sebagai kunci adalah bilangan prima yang besar dengan pemfaktoran sebuah bilangan hasil dari perkalian dari dua bilangan prima yang besar menjadi dua bilangan prima yang sesuai akan sangat sulit [4].

Untuk membangkitkan kunci (*generating key*) digunakan algoritma sebagai berikut

1. Dipilih dua buah bilangan prima sembarang yang besar, p dan q. Nilai p dan q harus dirahasiakan.
2. Dihitung n = p x q Besaran n tidak perlu dirahasiakan sebaiknya p ≠ q, sebab jika p = q maka n = p2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n.
3. Dihitung m = (p – 1)(q – 1)

4. Pilih sebuah bilangan bulat untuk kunci publik yang disebut e, yang relatif prima terhadap m. Relatif prima terhadap m artinya faktor pembagi keduanya adalah 1, secara matematis disebut gcd (e,m) = 1.
5. Hitung kunci untuk dekripsi (d) dengan rumus e.d mod m = 1.

Maka hasil dari algoritma diatas yaitu :

1. Kunci publik adalah pasangan (e, n)
2. Kunci privat adalah pasangan (d, n)

Catatan: n tidak bersifat rahasia, namun ia diperlukan pada perhitungan enkripsi/dekripsi.

Berikut contoh proses pembangkit kunci, yaitu :

1. Pilih bilangan prima, misalnya p = 3 dan q = 641
2. Hitung n = p x q = 3 x 641 = 1923
3. Hitung n = (p - 1) (q – 1) = 2 x 640 = 1280
4. Pilih e yang relatif prima terhadap m, ged (e,n) = 1 e = 427 => gcd (427,1280) = 1 nilai e yang diambil adalah 427.

Bukti : (427,1280)
1280 mod 427 = 426
426 mod 427 = 1
1 mod 1 = 0

5. Sehingga cari nilai de = 1 (mod 1280) dan d < 1280

Mencari nilai = d x 427 = 1 mod 1280
d x 427 mod 1280 = 1
d = 427
Bukti : 427 x 3 mod 1280 = 1
Sehingga di dapatkan :
Public key : e(427), n(1923) dan *Private key* : d(3), n(1923)

2. Proses Enkripsi pada Algoritma RSA

Proses selanjutnya setelah pembangkitan kunci pada RSA adalah proses Enkripsi. Enkripsi adalah proses mengubah pesan asli (*plaintext*) menjadi pesan rahasia (*ciphertext*). Pada proses ini pesan asli terlebih dahulu diubah kedalam bentuk desimal, kemudian pesan yang sudah berbentuk desimal kemuadian di bagi-bagi menjadi beberapa blok desimal secara teratur. Setiap blok desimal akan memiliki nilai yang harus lebih kecil dari nilai n yang disebut P. Adapun langkah-langkah yang digunakan untuk melakukan proses enkripsi pada algorimta RSA adalah sebagai berikut (Anwar.dkk, 2019) :

1. Menggunakan *public key* (e,n).
2. *Plaintext* M dinyatakan menjadi blok-blok P1, P2,P3,...
3. Setiap blok M_i di enkripsi menjadi C_i, dengan rumus $\mathbf{C_i = P_i^e \bmod n}$

Contoh proses enkripsi
Publik Key dan *Private Key* sudah diketahui, maka selanjutnya dilakukan enkripsi pada *plaintext* (P) = 10000000 = ASCII : 49 48 48 48 48 48 48 48
Kemudian pecah menjadi sebuah blok yang berukuran 3 digit yaitu :
X1 = 494
X2 = 848
X3 = 484
X4 = 848
X5 = 484
X6 = 800 (diberi penambahan 00)
Maka akan dilakukan perhitungan dengan rumus $C_i = P_i^e \bmod n$ untuk proses enkripsi yaitu :
C1 = 494427 mod 1923 = 533
C2 = 848427 mod 1923 = 209
C3 = 484427 mod 1923 = 874
C4 = 848427 mod 1923 = 209
C5 = 484427 mod 1923 = 874
C6 = 800427 mod 1923 = 1202
Hingga hasil yang didapatkan *ciphertext* (c) = 533.209.874.209.874.1202 dalam karakter ASCII.

3. Proses Dekripsi pada Algoritma RSA

Proses dekripsi pada algoritma RSA mirip dengan proses enkripsinya, hanya saja kunci yang digunakan dalam proses dekripsi adalah kunci privat d. Adapun langkah-langkah yang digunakan untuk melakukan proses dekripsi pada algorimta RSA adalah sebagai berikut (Anwar.dkk, 2019):

1. Menggunakan *private key* (d,n)
2. Pilih *ciphertext* C
3. Setiap blok C_i di dekripsi menjadi blok P_i, dengan rumus $\mathbf{P_i = C_i^d \bmod n}$

Contoh proses dekripsi
Ciphertext (c) = 533.209.874.209.874.1202 dalam karakter ASCII.
Kemudian, dekripsikan kembali dengan menggunakan rumus $P_i = C_i^d \bmod n$:
P1 = 5333 mod 1923 = 494
P2 = 2093 mod 1923 = 848
P3 = 8743 mod 1923 = 484
P4 = 2093 mod1923 = 848
P5 = 8743 mod 1923 = 484
P6 = 12023 mod 1923 = 800
Maka, hasil gabungan P1 sampai P6 = 533.209.874.209.874.1202, adalah 10000000

3.2. Implementasi Program

Berikut adalah hasil implementasi dari program algoritma kriptografi RSA dalam sistem informasi perpustakaan yang dirancang.

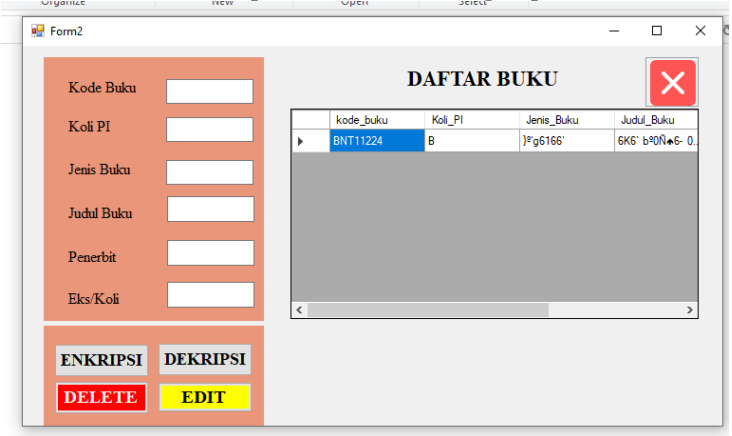
3.2.1. Tampilan Menu Login

Tampilan *form login* merupakan gerbang utama untuk dapat masuk ke dalam program algoritma kriptografi RSA dalam sistem informasi perpustakaan yang dirancang. Pengguna memasukkan *username* dan *password*. *Username* dan *password* tersebut telah tersimpan dalam *database*. *Form login* digunakan untuk membatasi hak akses bagi pengguna untuk melihat dan berinteraksi dengan data. Hanya *user* yang sudah terdaftar yang bisa mengakses data-data dalam sistem. Seperti pada Gambar berikut ini:

Gambar 2. Tampilan *form login*

3.2.2. Tampilan Menu Utama

Tampilan *form* menu utama dapat dilihat pada Gambar 4.2. *Form* menu utama ini digunakan untuk menentukan *user* memilih proses yang ingin dilakukan, seperti mengenkripsikan data, mendekripsikan data, menghapus data serta mengedit data.



Gambar 3. Tampilan Menu Utama

3.3. Pengujian

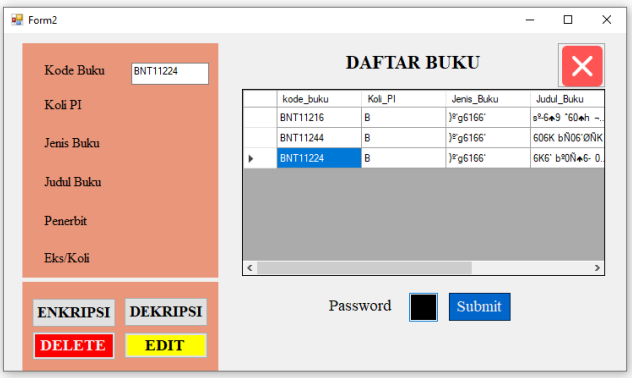
Pengujian merupakan bagian yang tidak dapat dilewatkan dalam pembangunan suatu sistem. Karena pada saat melakukan pengujian pada sistem dapat diketahui apakah sistem yang dibangun berjalan dengan baik sesuai dengan keinginan. Selain itu, dengan adanya pengujian sistem perancang dapat mengetahui kesalahan-kesalahan pada sistem dan memperbaikinya Kembali. Berikut pengujian yang dilakukan pada sistem.

3.3.1. Pengujian Proses Enkripsi

Pada proses ini hal pertama yang dilakukan yaitu memasukan data yang akan di enkripsi pada setiap *form* yang disediakan. Kemudian pengguna mengklik menu enkripsi, jika data yang di *input* sudah benar dan sesuai dengan ketentuan sistem maka secara otomatis data yang di *input* berubah menjadi *ciphertext* dan ditampilkan dalam tabel sebelah kanan tampilan. Tetapi jika data yang di *input* kurang maka akan muncul pesan pemberitahuan bahwa data yang dimasuukan belum lengkap. Perlu dikataui bahwa data pada kode buku yang di*input* tidak berubah menjadi *ciphertext*, hal itu dikarenakan data kode buku merupakan atribut kunci pada *database* dan digunakan juga nantinya pada saat proses dekripsi. Adapun tampilan prosesnya dapat dilihat pada gambar dibawah ini.

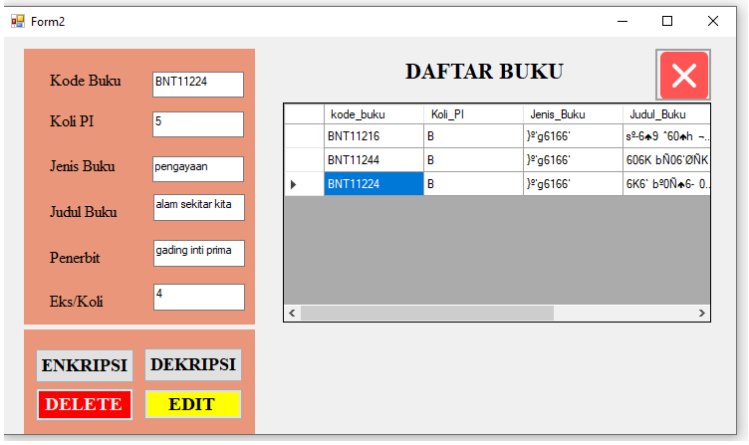
Gambar 4. Pengujian Proses Enkripsi

4.3.1 Pengujian Proses Dekripsi



Gambar 5. Pengujian Proses Dekripsi

Gambar diatas adalah contoh pengujian proses dekripsi. Pada saat proses dekripsi dilakukan ada *password* yang dibutuhkan pengguna saat hendak melakukan dekripsi pada data. Hal tersebut dilakukan untuk menjaga keamanan data asli yang akan ditampilkan oleh sistem. Setelah *password* telah dimasukan maka proses dekripsi akan berjalan dan data *ciphertext* akan berubah menjadi *plaintext* dan tampilannya kemudian berubah seperti tampilan menu utama dengan data asli ditampilkan di *form input* data. Tetapi perlu diketahui bahwa sebelum memulai dekripsi data pengguna harus memasukan kode buku yang ingin dilihat data aslinya. Pada saat inilah kode buku yang tidak berubah jadi *ciphertext* tersebut dibutuhkan.



Gambar 6. Hasil Proses Dekripsi

4. KESIMPULAN

Penerapan algoritma kriptografi RSA dalam proses enkripsi dan dekripsi data itu menggunakan kunci publik dan kunci privat yang dimana pembentukan kunci-kunci tersebut didapatkan dari proses memfaktorkan bilanga-bilangan prima yang sudah ditentukan sebelumnya. Implementasi algoritma kriptografi RSA dalam program yang dirancang penulis yaitu program algoritma kriptografi RSA sistem informasi perpustakaan yang dibuat menggunakan Bahasa pemograman VB.NET menggunakan IDE *Microsoft Visual Studio* 2015.

DAFTAR PUSTAKA

[1]. A. Ulva, "Implementasi Algoritma Kargers Min Cut Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video," Pelita Inform. Inf. dan Inform., vol. 10, no. 2, pp. 58–64, 2021.

[2]. S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," JURTEKSI (Jurnal Teknol. dan Sist. Informasi), vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteksi.v6i1.395.

[3]. M. A. Jihad Plaza R and R. Hartono, "Penerapan Kriptografi Caesar Chiper Pada Aplikasi Chatting Berbasis Local Area Network," J. SIMADA (Sistem Inf. dan

Manaj. Basis Data), vol. 4, no. 1, pp. 1–10, 2021, [Online]. Available: https://jurnal.darmajaya.ac.id/index.php/SIMADA/article/view/2630/pdf.

[4]. B. Anwar, N. B. Nugroho, J. Prayudha, and A. Azanuddin, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer), vol. 18, no. 1, p. 30, 2019, doi: 10.53513/jis.v18i1.100.