PERANCANGAN SISTEM PENUNJANG KEPUTUSAN BIAYA KEBUTUHAN MAHASISWA DENGAN WAKTU TERCEPAT MELALUI METODE BACKWARD CHAIN DAN ALGORITMA RSA

Maulani Dewi Sara Aulia[1)]

1) Teknik Informatika STMIK AMIKOM Yogyakarta
Jl Ringroad Utara, Condongcatur,Depok,Sleman, Yogyakarta Indonesia 55283
email : maulani0035@students.amikom.ac.id[1)]

Abstrak

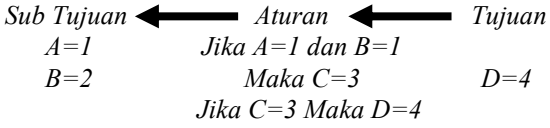
Banyaknya kebutuhan mahasiswa pada saat ini membuat mereka bingung dalam melakukan penentuan estimasi biaya yang harus dikeluarkan .
Untuk menentukan mana kebutuhan yang harus di utamakan terdapat bnayak kriteria yang akan dijadikan pertimbangan.Pengunaaan Sistem metode Pengambilan Keputusan dalam menentukan persoalan yang melibatkan metode Backward Chain akan memudahkan mahasiswa dalam menghitung jumlah biaya yang harus dikeluarkan tiap bulannya.
Penggunaan algoritma yang tepat akan menampilkan secara rinci daftar kebutuhan yang harus dikeluarkan.
Dalam paper ini akan dimuat bagaimana sistem akan berjalan sesuai rule dan akan menentukan apakah tujuan untuk pengeluaran biaya akan tercapai atau tidak. Jika tercapai maka sistem akan mencapai tujuan akhir dari fakta-fakta yang telah ditentukan oleh pengguna.
Untuk keamanan data sistem ini akan menggunakan Algoritma RSA karena dapat dengan aman memudahkan pengguna menggunakan sistem ini. Data dan informasi pribadi user akan terjaga dengan baik.

Kata Kunci : *Sistem penunjang keputusan, Metode Backward Chain, Algoritma RSA*

1. Pendahuluan

Teknologi informasi (TI) telah diadopsi dalam berbagai bidang kehidupan. Hal ini dimungkinkan karena teknologi komputer mampu berkolaborasi dengan banyak bidang ilmu lainnya [1].
TI telah membawa peribahan yang sangat mendasar bagi organisasi baik swasta maupun publik [2]. Sehingga TI sudah mejadi backbone utama bagi banyak aspek di kehidupan kita sekarang [3].
Sistem merupakan kumpulan elemen yang saling berkaitan yang bertanggung jawab memproses masukan *(input)* sehingga menghasilkan keluaran *(output)*. Fungsi sistem yang utama adalah menerima masukan, mengolah masukan, dan menghasilkan masukan. Agar dapat menjalankan fungsinya ini, sistem akan memiliki komponen-komponen *input*, proses, keluaran, dan kontrol untuk menjamin bahwa semua fungsi dapat berjalan dengan baik .

Runut balik (*backward chaining*) merupakan strategi pencarian yang arahnya kebalikan dari runut maju (*forward chiaining*). Proses pencarian dimulai dari tujuan, yaitu kesimpulan yang menjadi solusi permasalahan yang dihadapi. Mesin inferensi mencari kaidah-kaidah dalam basis pengetahuan yang kesimpulannya merupakan solusi yang ingin dicapai, kemudian dari kaidah-kaidah yang diperoleh, masing masing kesimpulan dirunut balik jalur yang mengarah ke kesimpulan tersebut. Jika informasi-informasi atau nilai dari atrubut-atribut yang mengarah ke kesimpulan tersebut sesuai dengan data yang diberikan maka kesimpulan tersebut merupakan solusi yang dicari. Runut balik memulai proses pencarian dengan tujuan sehingga strategi ini disebut juga goal-driven [4].



Sebagai suatu sistem sangat rawan terhadap penyadapan, pencurian, dan pemalsuan informasi. Proses pengiriman data pada suatu jaringan harus menjamin keamanan dan keutuhan, jika tidak, akan terjadi kemungkinan-kemungkinan seperti yang dijelaskan sebelumnya. Untuk itu salah satu cara untuk mengamankan data dari kejadian kejadian tersebut, di perlukan penyandian terhadap data yang akan dikirim.
Algoritma kriptografi RSA didesain sesuai fungsinya sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi. Algoritma RSA disebut kunci publik karena kunci enkripsi dapat dibuat publik yang berarti semua orang boleh mengetahuinya, namun hanya orang tertentu yang dapat melakukan dekripsi terhadap pesan tersebut. Keamanan algoritma RSA didasarkan pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor primanya [5]. Besar-besaran yang digunakan pada algoritma RSA adalah:

1. P dan q merupakan bilangan prima yang di ambil secara acak. Sifat kedua bilangan ini adalah rahasia. Semakin besar p dan q maka semakin aman.

2. n=p.q, sifat dari n tidak rahasia, artinya orang lain dapat mengetahuinya.
3. e(kunci enkripsi), sifatnya tidak rahasia.
4. d(kunci dekripsi), sifatnya rahasia.
5. P(plainteks), merupakan informasi awal yang bersifat rahasia.
6. C(cipherteks), merupakan informasi yang telah dienkripsi dan bersifat tidak rahasia.

Sistem ini dapat mempermudah para mahasiswa untuk mengatur keuangannya sendiri secara mobile membuat keuangan dapat tersalurkan secara efektif dan efisien. Kebutuhan-kebutuhan yang penting akan di utamakan terlebih dahulu oleh sistem. Faktor gaya hidup mahasiswa jaman sekranng menjadi faktor utama kenapa terkadang keuangan mereka tidak teratur. Maka diperlukan sistem ini untuk membantu para mahasiswa untuk mengatur keuangan mereka sendiri layaknya asisten pengatur keuangan dan akan di lengkapi pengamanan data yang optimal menggunakan Algoritma RSA .

2. Pembahasan

Berikut ini pengimplementasian sistem inferensi menggunakan *backward chaining* untuk mendeteksi pengeluaran biaya mahasiswa yang sesuai dengan kebutuhan tercapai atau tidak, langkah-langkah yang harus dilakukan sebagai berikut [6] :

1. Identifikasi konklusi sebagai goal utama.
2. Cari konklusi list untuk pengisian pertama sekali dari nama konklusi. Jika ketemu, tempatkan rule pada *conclusion stack* berdasarkan nomor rule dan satu yang mempresentasikan nomor klausa.
3. Jika tujuan utama tidak ditemukan, maka *inference engine* akan mencari sebuah tujuan baru yang dijadikan sub *goal* untuk menemukan IF_part dari sebuah rule.
4. Kemudian *knowledge base* akan mencocokkan lagi aturan-aturan sehingga menemukan sub goal.
5. Selanjutnya *inference engine* akan mengulang kembali proses pencarian rule hingga tidak menemukan rule di dalam *knowledge base*.

Berikut ini sebagai contoh kasus menggunakan metode inferensi *backward chaining* untuk menelusuri apak pengeluaran biaya pada mahasiswa dapat mencapai target tujuan atau tidak.
Premis yang digunakan ditunjukkan pada **Tabel 1.** *Fakta-fakta* sebagai berikut :

Tabel 1. *Fakta-fakta*

KODE	Premis
A	Jumlah uang
B	Kebutuhan Wajib per bulan
C	Sisa uang yang didapat setelah dikurangi premis (A-B)
D	Tujuan yang akan dicari
E	Premis pilihan untuk menentukan kebutuhan yang di inginkan
F	Premis pilihan setelah memilih premis E
K	Sisa uang setelah dikurangin premis F
L	Hasil dari premis K yang bernilai minus
M	Hasil dari premis K yang bernilai plus
N	Pernyataan tujuan tercapai dilihat dari premis M
O	Pernyataan jika tujuan tercapai dan terdapat uang sisa
P	Sisa paling akhir uang yang dihasilkan dengan tujuan yang telah tercapai

Hipotesis konklusi ditunjukkan pada **Tabel 2.** *Rule* sebagai berikut :

Tabel 2. *Hasil inputan di sistem*

NOMOR	RULE
R1	If O then P
R2	If (M and D) then O
R3	If (M and D) then N
R4	If (K and M) then D
R5	If K then L
R6	If K then M
R7	If (L and E and F) then K
R8	If C then E
R9	If (A and B an E) then C

Ketika mahasiswa akan memproses sistem ini akan ada beberapa input yang harus di isi sesuai dengan kebutuhan mahasiswa inginkan. Ada kasus mahasiswa yang bernama Rian Prabowo mempunyai uang sejumlah Rp.1.500.000 yang diberikan orang tuanya untuk kebutuhan perbulan. Lalu dengan kebutuhan mendesak Rian membutuhkan sebuah keyboard untuk mengganti keyboard lamanya yang sudah rusak, tetapi Rian juga ingin menjadi anak mandiri yang mempunyai uang tabungan nya sendiri agar tidak merepotkan orang tuanya.
Hasil inputan oleh Rian untuk sistem ditunjukan pada **Tabel 3.** *Hasil inputan di sistem* sebagai berikut :

Tabel 3. *Hasil inputan di sistem*

Kode Premis	Keterangan
A	**1.500.000**
B1	**400.000 (uang kos perbulan)**
B2	**20.000 (uang listrik perbulan)**
F1	**Makan 3 kali sehari**
F2	**Makan 2 kali sehari**
E2	**14.000(Makan ayam bakar 10 hari)**
E3	**10.000(Makan di burjo 20 hari)**
D1	**350.000(biaya keyboard)**
D2	**50.000(uang tabungan)**

Iterasi ke-1

Database	Stack
M F E B A	D

Knowledge Base
R4: If (K and M) then D
R5: If K then L
R6: If K then M
R7: If (M and E and F) then K
R8: If C then E
R9: If (A and B an E) then C

Gambar 1. *Iterasi 1*

Pada **Gambar 1**. *Iterasi 1* menunjukan bahwa kotak stack mempunyai goal D dimana telah mengeksekusi R4. Hipotesis dibalik karena menggunakan metode *Backward Chain.*
D ada di database tetapiK tidak ada di database, simpan di stack. R1,R2,R3 tidak dipakai untuk iterasi ini karena jika sudah mencapai goal D sesuai metode makan iterasi sudah selesei. Iterasi tersebut hanya sebagai tambahan unutk bahan pemrograman.

Perhitungan
R4: 1.500.000 – ((350.000)+(50.000))= 1.100.000
Jadi hasil perghitungan di R4 ialah sejumlah Rp 1.100.000.
Premis D1 dan D2 telah tercapai.

Iterasi ke-2

Database	Stack
M F E B A	D K

Knowledge Base
R4: If (K and M) then D
R5: If K then L
R6: If K then M
R7: If (M and E and F) then K
R8: If C then E
R9: If (A and B an E) then C

Gambar 2. *Iterasi 2*

Pada **Gambar 2**. *Iterasi 2* menunjukan bahwa kotak stack mempunyai goal K dimana telah mengeksekusi R6.
Perhitungan
R6: 1.100.000
Jadi hasi perhitungan untuk iterasi ke-2 sejumlah Rp 1.100.000 karena dalam iterasi ini sistem tidak melakukan perhitugan melainkan melakukan analisa apakah jumlah biaya mencapai tujuan premis M atau tidak. Jika memenuhi akan dilanjutkan ke iterasi selanjutnya.
Premis M telah tercapai.

Iterasi ke-3

Database	Stack
M F E B A Fakta Baru K	D M

Knowledge Base
R4: If (K and M) then D
R5: If K then L
R6: If K then M
R7: If (M and E and F) then K
R8: If C then E
R9: If (A and B an E) then C

Gambar 3. *Iterasi 3*

Pada **Gambar 3**. *Iterasi 3* menunjukan bahwa kotak stack mempunyai goal M dimana telah mengeksekusi R7.Telah terjadi perubahan di database karena masuknya premis K ke dalam database sehingga menghasilkan fakta baru.

Perhitungan
R7: 1.100.000 – ((2X10(14.000)+(2X20(10.000))) = 420.000
Jadi hasil perhitungan R7 sejumlah Rp 420.000 dan telah memenuhi premis E dan F serta M , sehingga akan dilanjutkan dengan iterasi selanjutnya.

Iterasi ke-4

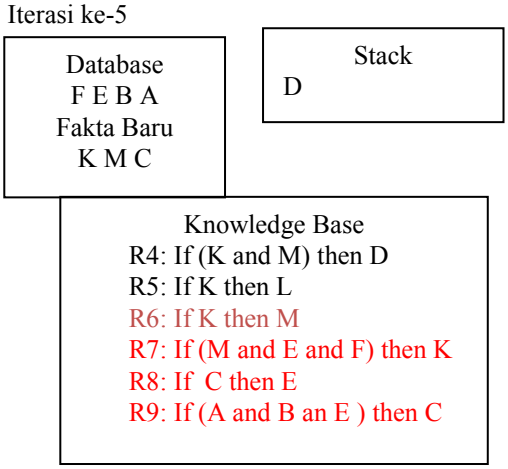
Database	Stack
M F E B A Fakta Baru K L	D C

Knowledge Base
R4: If (K and M) then D
R5: If K then L
R6: If K then M
R7: If (M and E and F) then K
R8: If C then E
R9: If (A and B an E) then C

Gambar 4. *Iterasi 4*

Menurut **Gambar 4.** *Iterasi 4* rule R6,R7 dan R8 telah tercapai, sehingga premis M, E, dan F akan masuk ke database dan dilanjutkan dengan iterasi berikutnya sehingga ditemukan lagi fakta fakta baru.

Iterasi ke-5



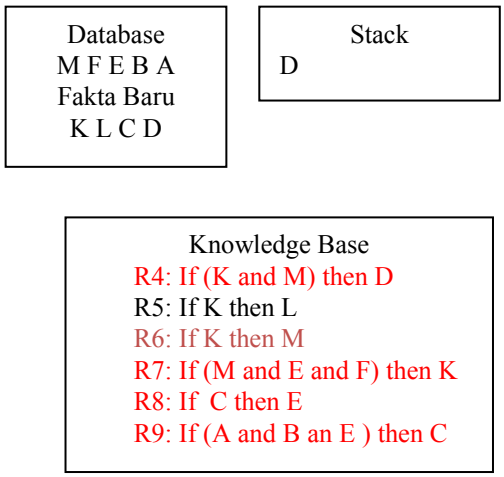
Gambar 5. *Iterasi 5*

Pada **Gambar 5**. *Iterasi 5* menunjukan bahwa kotak stack mempunyai goal D dimana telah mengeksekusi R4. Telah ditemukan fakta-fakta baru A dan B, karena fakta A dan B sudah ada di database maka tidak di identifikasi sebagai faktu baru.

Perhitungan
R9: 420.000((400.000)+(20.000))=0

Jadi pada rule R9 tujuan telah tercapai dan memasuki tahap akhir pada sistem. Jika tujuan telah tercapai maka akan dilakukan iterasi terakhir yaitu pemasukan premis ke dala database.

Iterasi ke-6



Gambar 6. *Iterasi 6*

Pada **Gambar 6**. *Iterasi 6* menunjukan bahwa kotak stack mempunyai goal D dimana telah mengeksekusi semua *knowledge base*.
Karena goal D ditemukan di database, maka proses pencarian dihentikan. Disini terbukti bahwa D bernilai benar. Dengan jumlah uang Rp.1.500.000 dapat memperoleh dua kali makan dalam sehari dimana dapat makan di ayam bakar 10kali dalam sebulan dan 20 kali mkan di burjo dalam sebulan. Dengan hasil dapat membeli keyboard baru dan menabung sejumlah Rp 50.000.

Dalam proses pembangkitan kunci baik itu kunci publik maupun kunci privat pada algoritma RSA, dalapat dilakukan dengan langkah-langkah sebagai berikut :
Misalkan tentukan nila p dan q :
p=3,q=7

Maka akan didapat :
n= p.q=3x7=21, m=(p-1)(q-1), e*d mod 12 = 1
Maka nilai c dan d sebagai berikut:
e=5,d=17

Diketahui:
public key =(e,n)=(5,21)
private key =(d,n)=(17,21)

Contoh data yang ingin di enkripsi:

T	O	M	I
84	79	77	73

T=84

Table 4. *Enkripsi 1*

Enkripsi	Deskripsi
C=M^e mod n	M=C^e mod n
8^5 mod 21 = 8	8^17 mod 21 = 8
4^5 mod 21 = 16	4^17 mod 21 = 4

O=79

Table 5. *Enkripsi 2*

Enkripsi	Deskripsi
C=M^e mod n	M=C^e mod n
7^5 mod 21 = 7	7^17 mod 21 = 7
9^5 mod 21 = 18	18^17 mod 21 = 9

M=77

Table 6. *Enkripsi 3*

Enkripsi	Deskripsi
C=M^e mod n	M=C^e mod n
7^5 mod 21 = 7	7^17 mod 21 = 7
7^5 mod 21 = 7	7^17 mod 21 = 7

I+73

Table 7. *Enkripsi 4*

Enkripsi	Deskripsi
C=M^e mod n	M=C^e mod n
7^5 mod 21 = 7	8^17 mod 21 = 7
3^5 mod 21 = 12	4^17 mod 21 = 3

Dapat diketahui dari hasil proses perhitungan dan engkrisi pada **Table 4.** *Enkripsi 1,* **Table 5.** *Enkripsi 2,* **Table 6.** *Enkripsi 3,* **Table 7.** *Enkripsi 4* adalah hasil dari semua hasil cipherteks yang diperoleh pada proses dekripsi akan diubah kembali menjadi plainteks.

3. Kesimpulan

Berdasarkan analisis,perancangan, dan implementasi sistem yang telah dilakukan, serta berdasarkan rumusan masalah yang ada. Maka dapat disimpulkan yaitu :

1. Sistem ini dijadikan media untuk mendapatkan informasi tentang berapa banyak kebutuhan mahasiswa dalam jangka waktu sebulan. Sehingga menbantu para mahasiswa dalam mengatasi madalah-masalah pengeluaran biaya yang terduga maupun tidak terduga dan sekaligus memberikan pemecahan masalah secara tepat serta tepat.

2. Sistem ini dapat membantu pengguna untuk mengetahui tips mengenai kebutuhan apa saja yang seharusnya didahulukan untuk mendapatkan pengeluaran biaya yang efektif dan efisien. Pengimplementasian menggunakan inferensi *backward chaining* akan memberikan output berupa solusi dari suatu masalah berdasarkan kumpulan pengetahuan yang ada dalam *knowledge base* .

3. Sistem ini dapat mebantu pengguna untuk mengetahui seberapa besar biaya yang ingin dikeluarkan dengan beberapa premis dengan tepat.

4. Validitas pesan yang akan dikirm setelah melakukan proses enkripsi dan dekripsi adalah 100% sehingga untuk keamanan pengiriman data ke database terjamin aman.

5. Informasi data yang diperoleh akan di lindungi dengan algoritma yang sesuai dan ama sehingga pengguna dapat dengan aman untuk menggunakan sistem ini secara privat.

6. Penyamaran data menjadi cipherteks pada saat proses enkripsi dengan Algoritma RSA dapat mencegah orang lain untuk mengetahui pesanasli yangdimaksud.

Daftar Pustaka

[1] L. Abdillah., et al., "Pengaruh kompensasi teknologi informasi terhadap kinerja dosen (KIDO) tetap pada Universitas Bina Darma," *Jurnal Ilmiah MATRIK*, vol 9,pp 1-20, April 2007.

[2] L.A. Abdillah and D.R. Rahardi, "Optimalisasi pemanfaatan teknologi informasi dalam menumbuhkan minat mahasiswa menggunakan sistem informasi," *Jurnal Ilmiah MATRIK*, vol.9,pp 195-204,2007

[3] L. A. Abdillah, "Managing information and knowledge sharing cultures in higher educations institutions," in *The 11th International Research Conference on quality, Innovation, and Knowledge Management (QIK2014)*, The Trans Luxury Hotel, Bandung, Indonesia, 2014.

[4] Bill Brandon , "Konsep Dasar Sistem Pakar", *The Power of Backward Chaining,* 2003.

[5] Sulistyanto, H, "Autentikasi dalam Basis Data Jaringan Menggunakan Kriprosistem Kunci Publik RSA ," *Jurnal Teknik Elektro dan Komputer Emitor*, vol.4,pp 40-41,2004.

[6] Muhammad Dahria, "Implemetasi inferensi backward chaining untuk mengetahui kerusakan monitor kumputer," *Jurnal Ilmiah SAINTIKOM*, vol.11,pp 40-46,Januari 2012.

Biodata Penulis

Maulani Dewi Sara Aulia, saat ini sedang menempuh pendidikan semster lim apada program studi Bachelor of Informatic Technology (BCIT)STMIK AMIKOM Yogyakarta, masuk pada tahun 2014.

ISSN : 2302-3805