Studi Awal Penggunaan Algoritma C4.5 dan Logika Fuzzy pada Klasifikasi Enkripsi Transaksi Keuangan Bebasis XML

Nur Rachmat
STMIK Global Informatika MDP
Magister Teknik Informatika, Universitas Sriwijaya
Jl. Rajawali 14 Palembang, Indonesia
rachmat.nur91@mdp.ac.id

Samsuryadi
Fakultas Ilmu Komputer, Universitas Sriwijaya
Palembang, Indonesia
syamsuryadi@unsri.ac.id

***Abstrak*— XML (*eXtensible Markup Language*) telah digunakan secara luas dalam transportasi data baik dalam transaksi kebutuhan umum hingga transaksi keuangan. Penggunaan XML yang meningkat dalam pesan transaksi keuangan menciptakan ketertarikan yang selaras dengan protokol keamanan yang terintegrasi untuk melindungi pesan XML dalam pertukarannya dengan cara yang efisien namun kuat. Lembaga keuangan melakukan transaksi setiap harinya membutuhkan pengamananan pesan XML dalam skala besar. Mengamankan pesan yang besar akan menimbulkan masalah kinerja dan sumberdaya. Oleh karena itu, sebuah pendekatan dibutuhkan untuk mengamankan dan mengenkripsi bagian tertentu dari dokumen XML, sintaks dan membuat batasan yang merepresentasikan bagian yang harus diamankan.**

Dalam penelitiaan ini penulis mengajukan pendekatan untuk mengamankan transaksi keuangan dengan Logika *Fuzzy* dan algoritma C4.5 untuk optimasi *rule fuzzy*. Pada fase klasifikasi *fuzzy*, sebuah nilai dipasang pada atribut yang dinamakan "*Importance Level*". Nilai yang diberikan pada atribut tersebut mengindikasikan sensitifitas data untuk setiap tag XML. Algoritma C4.5 digunakan untuk mengurangi ketergantungan terhadap *expert* dalam pemilihan *rule* yang bertujuan untuk menyederhanakan *rule* dan meningkatkan performa komputasi

Penelitain ini juga akan menerapkan pengklasifikasian enkripsi isi pesan XML dengan mengenkripsi elemen yang dipilih saja *(element-wise)*, yang telah ditetapkan pada fase klasifikasi. Proses enkripsi menggunakan kunci simestris berupa algoritma AES dengan besaran kunci yang berbeda. Kunci 128-bit digunakan pada *tag* yang diklasifikasikan sebagai elemen yang ditandai sebagai "*Medium*" sedangkan kunci 256-bit pada *tag* "*High*".

Kata Kunci—C4.5; Logika Fuzzy; XML; XML Encryption;

I. PENDAHULUAN

Saat ini eXtensible Markup Language (XML) telah banyak diterapkan di banyak lembaga keuangan dalam transaksi harian mereka. Hal disebabkan oleh sifat fleksibel XML yang menyediakan sintaks umum untuk perpesanan sistem secara umum dan dalam pesan keuangan khususnya[1]. Penggunaan XML yang meningkat dalam transaksi keuangan menarik minat penelitian dalam protokol keamanan yang terintegrasi ke dalam XML untuk melindungi pesan yang dipertukarkan dengan mekanisme yang efisien namun kuat. Ada beberapa pendekatan yang diajukan oleh peneliti untuk mengamankan XML.

W3C memainkan peran utama, menyediakan bentuk standard untuk mengamankan data XML dengan metode yang aman dan terpercaya. W3C mengenalkan XML Encryption[2], XML Signature[3], dan XML Key Management[4]. Standar Enkripsi XML mendefinisikan cara mengenkripsi pesan XML. Model enkripsi yang ditawarkan dapat mengenkripsi keseluruhan pesan, mengenkripsi sebagian pesan dengan memilih bagian dari setiap pesan, atau bahkan mengenkripsi elemen eksternal yang menyertai pesan itu sendiri. Meskipun model ini mampu mengamankan pesan XML, beberapa masalah muncul terkait kinerja dan penggunaan memori yang tidak efisien [5],menyebabkan keterlambatan pengiriman file, sehingga menyisakan ruang untuk perbaikan dan penyempurnaan yang lebih banyak.

Lembaga keuangan melakukan transaksi dalam jumlah besar setiap hari yang memerlukan enkripsi XML dalam skala besar. Mengenkripsi keseluruhan isi pesan dalam sekala besar akan menimbulkan masalah kinerja dan sumber daya. Oleh karena itu, diperlukan pendekatan untuk mengenkripsi bagian tertentu saja dari dokumen XML dan menerapkan aturan untuk mendekripsinya. Enkripsi W3C XML memiliki fitur untuk mengenkripsi bagian dari dokumen XML yang disebut *element-wise encryption*, yaitu proses mengenkripsi bagian dokumen XML. Untuk menghindari masalah kinerja atau sumber daya, perlu dipertimbangkan mekanisme lain untuk memilih bagian dokumen XML mana yang akan dienkripsi dengan cepat dengan memilih bagian tersebut berdasarkan hasil klasifikasi yang mendeteksi informasi sensitif dalam dokumen XML.

Logika *Fuzzy* hadir dengan tujuan mengatasi ketidakmampuan matematika konvensional untuk model sistem nonlinear. Sistem nonlinear merupakan suatu sistem yang sifatnya tidak tetap, mudah berubah, sulit dikontrol, dan sulit diprediksi. Logika *Fuzzy* juga memiliki kemampuan untuk menyimpulkan hasil yang valid (ketepatan dalam pengukuran) dari basis aturan yang berisi pengetahuan yang diekstraksi berdasarkan pengetahuan dan pengalaman pakar. Algoritma C4.5 adalah salah satu algoritma *decision tree* yang

terkenal karena efisiensi dan fitur yang lengkap. Cara kerja algoritma C4.5 yaitu rekursif mengunjungi setiap node (simpul) keputusan, memilih split (pembagian) optimal sampai tidak ada lagi kemungkinan pembagian.

Berdasarkan beberapa penelitian terdahulu, terdapat beberapa kelemahan dalam penggunaan Logika *Fuzzy*. Diantaranya adalah meningkatnya beban komputasi yang bertambah secara eksponensial seiring dengan bertambahnya jumlah variable dan jumlah rule dalam Logika *Fuzzy*. Dalam penelitian sebelumnya para peneliti menyatakan bahwa dengan melakukan pemangkasan jumlah rule, maka beban komputasi menjadi berkurang. Alogoritma klasifikasi C4.5 diharapkan mampu untuk mengatasi masalah tersebut.

II. STUDI LITERATUR

Flexibilitas dan kemudahan pengguanan XML menjadi motif bagi para peneliti dalam menyoroti bagian keamanan XML. Peneliti memfokuskan minat mereka pada cara mengamankan data XML karena meningkatnya kebutuhan akan XML dalam berbagai kasus bisnis dan pendidikan. Model yang efisien telah diajukan untuk menambah lapisan keamanan saat pergantian data XML. Tujuan utama dalah untuk memastikan kerahasiaan dan keaslian data. Banyak ancaman keamanan XML[5] Oversized Payload, Schema Change, XML Routing, dan Recursive Payload. Ancaman semacam itu memaksa peneliti untuk lebih memperhatikan pengiriman dan pertukasan pesan XML.

W3C telah mengembangkan metode untuk mengenkrisi dan mendekripsi XML. Mereka menggunakan sitaks XML untuk mewakili elemen yang diamankan dalam XML. Pendekatan itu mampu menkripsi keseluruhan pesan, simpul penuh, dan sub-pohonnya. Namun, tidak dapat mengenkripsi elemen sekaligus menjaga turunannya dari simpul yang sama, dan juga tidak dapat menangani enkripsi atribut. Oleh karena itu, solusi telah diusukan[6] untuk menangani keterbatasan ini. Ed Simon mengusulkan untuk mengubah atributnya sehingga dienkripsi dengan atribut *EncryptedDataManifest* dan menyertakan detail lainya di dalam elemetn. Solusi lainnya adalah menggunakan XSLT untuk perubahan atribut kedalam elemen untuk proses enkripsi. Sayangnya, solusi ini tidak berhasil karena bagian yang ter deskripsi harus diubah kembali ke atribut aslinya untuk validasi pesan terhadap skelma XML yang sama.

Sebuah sistem telah diusulkan untuk enkripsi, yang memiliki kemampuan menghapus informasi sensitif dari file output. Sistem tesebut mengurai pesan XML yang akan dienkripsi kedalam pohon DOM, dimana setiap simpul diberi label dan semua informasi yang berhubungan posisinya terikat dengan simpul yang sama. lalu setiap simpul terenkripsi secara individual dengan sebuah kunci enkripsi. Meskipun model ini memecahkan masalah menghapus informasi sensitif dari pesan utama dan menyembunyikan ukuran konten yang dienkripsi, namun memiliki kelemahan sebagai berikut: (1) Posisi awal untuk masing-masing simpul perlu dilampirkan, karena penambahan " informasi posisi, "(2) peningkatan ukuran pesan, karena kumpulan kunci simpul, (3) peningkatan ukuran pesan, (4) penggunaan sumber daya dan alokasi bandwidth yang tinggi, (5) membutuhkan penyimpanan lebih besar dan banyak proses, dan (6) kunci simpul unik harus dihasilkan untuk setiap simpul.

Penelitan [7] mengembangkan pengamanan data penting pada dokumen XML berdasarkan level enkripsi. Level enkripsi di atur secara manual pada element yang dianggap penting dengan memberikan nilai 1 untuk level paling rendah hingga 16 untuk level tertinggi. Kunci enkripsi yang diapkai adalah 32-bit hingga 448-bit. Sayangnya, algoritma enkripsi simetris dan kekuatan kunci enkripsi dijalankan sesuai level yang ditentukan secara manual oleh pengguna.

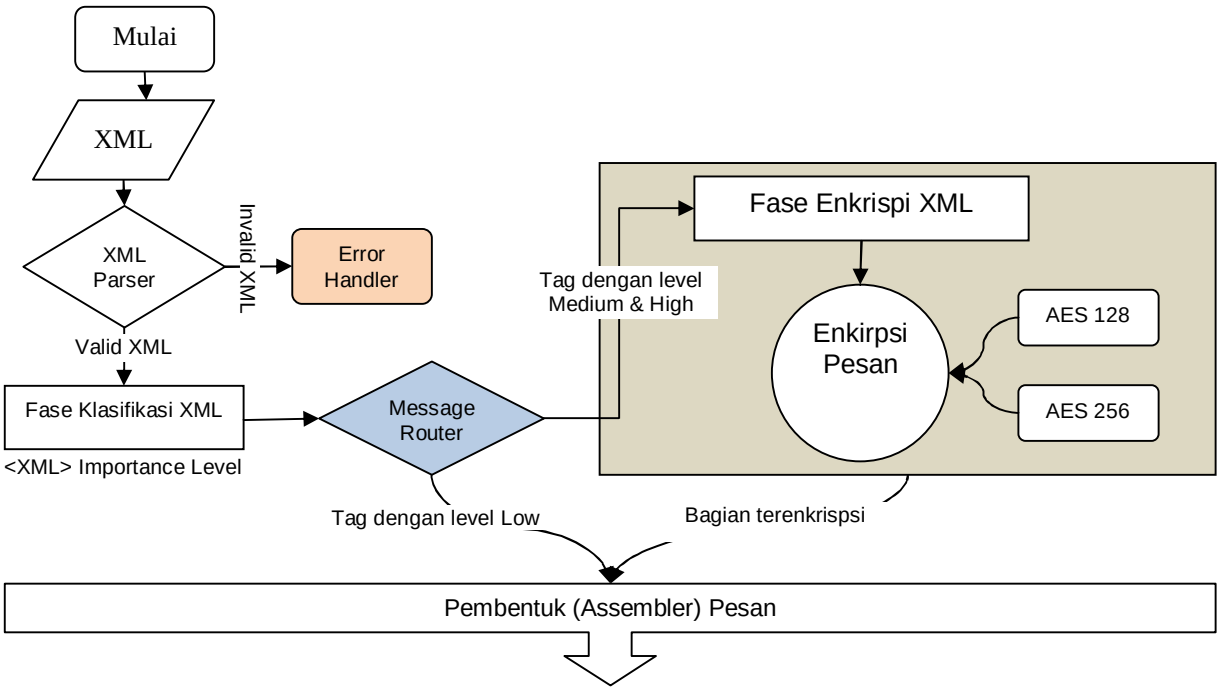
Penelitian sebelumnya telah menggunakan Logika *Fuzzy* untuk membedakan bagian sensitif dalam setiap dokumen XML [1], [8], [9]. FL memberikan cara yang mudah untuk mendapatkan kesimpulan yang pasti berdasarkan informasi masukan sifatnya tidak tetap, mudah berubah, sulit dikontrol, dan sulit diprediksi. Penulis menggunakan kombinasi data historis serta pengetahuan pakar/ahli untuk menilai dan membuat aturan *(fuzzy rule)* yang ditanamkan pada logika *fuzzy*. Namun, perlu pendekatan dalam membuat fuzzy *rule* secara otomatis untuk mengurangi intervensi kepakaran dari manusia, peningkatan kinerja, mengurani beban komputasi dari Logika *Fuzzy*.

Penelitian tersebut juga telah berhasil menggunakan teknik klasifikasi fuzzy untuk mengamankan pesan XML pada transaksi keuangan. Enkripsi menggunakan kunci simestris berupa algoritma AES dengan besaran kunci yang berbeda. Kunci 128-bit digunakan pada *tag* yang diklasifikasikan sebagai elemen yang bertingkat kepentingan "*Medium*" sedangkan kunci 256-bit pada *tag* yang bertingkat "*High*". Penulis menggunakan logika *fuzzy* untuk membedakan bagian sensitif dalam setiap dokumen XML.

Banyak keuntungan yang didapat menggunakan Logika *Fuzzy*, namun kelemahan dari menggunakan Logika *Fuzzy* adalah ukuran *rule-base* (basis aturan) fuzzy yang tumbuh secara eksponensial. Sehingga beberapa cara manual dilakukan untuk memilih dan pemangkasan *rule* yang bertujuan untuk menyederhanakan *rule* (aturan). Beberapa penelitian telah dilakukan untuk pemangkasan jumlah *rule* salah satunya adalah penggunaan algoritma C4.5[10]–[12] Hasil yang didapatkan telah mendekati nilai optimum untuk penentuan jumlah aturan. Pengintegrasian aloritma C4.5 dengan Logika *Fuzzy* telah berhasil memangkas aturan yang awalnya 288 *rule* menjadi hanya 52 *rule*, hal tersebut pastinya menyebabkan beban komputasi berkurang [12].

III. METODOLOGI PENELITIAN

Kerangka kerja yang diusulkan untuk proses penelitian disajikan pada Gambar 1.



Gambar 1. Rancangan Kerangka Kerja

Seperti yang terlihat pada gambar, terdapat dua komponen utama yang ditampilkan sebagai unit yang terpisah. Masing-masing unit melakukan serangkaian operasi sebagai masukan ke fase lainnya. Terdapat dua fase utama dimana, tahap pertama adalah melakukan pengklasifikasian pada pesan XML dengan Logika *Fuzzy*. Proses klasifikasi dirancang untuk mendapatkan ouput berupa nilai kepentingan dari setiap elemen XML. Rule fuzzy yang tebentuk selanjutnya akan diklasifikasi kembali dengan Algoritma C4.5 untuk proses pemangkasan rule. Pada saat proses klasifikasi, sebuah nilai baru akan dibuat pada tag XML yang dinamakan "*Importace Level* ". Elemen XML akan diklasifikasikan menjadi 3 (tiga) tingkat (*level)* antara lain adalah *Low, Medium* dan *High.*

Pada fase kedua, elemen akan dienkripsi menggunakan kunci simestris berupa algoritma AES dengan ukuran kunci yang berbeda. Nilai *Importace Level* yang telah dibuat pada fase pertama akan menentukan ukuran kunci yang akan digunakan pada algorirma enkripsi. Kunci 128-bit digunakan pada *tag* yang diklasifikasikan sebagai elemen yang bertingkat "*Medium*" sedangkan kunci 256-bit pada *tag* yang bertingkat "*High*".

A. Fuzzy Classification

Proses klasifikasi fuzzy akan diterapkan dengan menggunakan metode fuzzy tipe mamdani[13]. Metode inferensi mamdani memiliki empat langkah dasar.

Langkah 1 (Fuzzifikasi) : fuzzifikasi merupakan suatu tahapan untuk mengubah suatu nilai masukan dari bentuk nilai pasti menjadi fuzzy input (variabel linguistik). Bentuk variable linguistik disediakan dalam bentuk himpunan-himpunan fuzzy dengan fungsi keanggotaannya masing-masing.

Langkah 2 (Evaluasi Aturan) : Ambil masukan *fuzzy* dan terapkan pada aturan *fuzzy* yang memenuhi syarat. Operator fuzzy (AND / OR) digunakan jika terjadi ketidakpastian untuk mendapatkan satu nilai. Hasilnya disebut "Nilai Kebenaran", yang akan diterapkan pada fungsi keanggotaan untuk evaluasi aturan.

Langkah 3 (Agregasi dari keluaran aturan) : Proses penyatuan output dari semua peraturan. Menggabungkan aturan skala menjadi himpunan fuzzy tunggal untuk setiap variabel.

Langkah 4 (Mengubah *fuzzy output* menjadi nilai *crisp*) : Contoh nilai *output crisp* yang diharapkan [*Low, Medium,* dan *High*]. Outputnya harus memiliki nilai yang jelas dan *crisp* dimana akan diatur ke setiap *tag* yang diklasifikasikan.

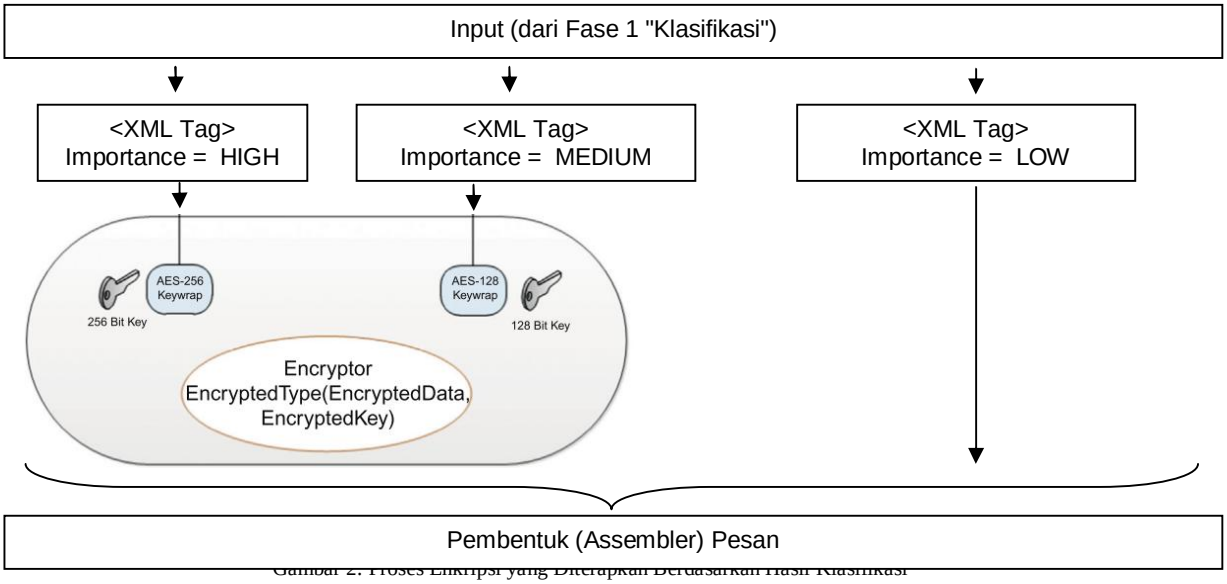
Low : Tag ini berarti tingkat kepentingan rendah. Elemen dan tag akan langsung diteruskan ke pemmentuk pesan, melewatkan fase enkripsi.

Medium: Tag ini penting sampai batas tertentu, dan atribut tag diberi nilai medium, jadi enkripsi akan diterapkan dengan menggunakan algoritma AES dengan kunci 128-bit.

Tinggi: Tag ini harus ditangani dengan sangat penting dan dienkripsi pada fase berikutnya dengan menggunakan algoritma AES dengan kunci 256-bit.

B. Algoritma C4.5

Algoritma C4.5 adalah salah satu algoritma decision tree yang terkenal karena efisiensi dan fitur yang lengkap[11]. Algoritma C4.5 merupakan pengembangan dari algoritma ID3 untuk menghasilkan pohon keputusan. Algoritma C4.5 bekerja secara rekursif mengunjungi setiap node keputusan, memilih



Gambar 2. Proses Enkripsi yang Diterapkan Berdasarkan Hasil Klasifikasi

split (pembagian) optimal, sampai tidak ada perpecahan lebih lanjut yang memungkinkan. Algoritma C4.5 menggunakan konsep information gain atau pengurangan entropi untuk memilih pembagian optimal[12].

Tahapan dalam membuat sebuah pohon keputusan dengan algoritma C4.5 adalah :

1. histori yang pernah terjadi sebelumnya dan sudah dikelompokkan dalam kelas- kelas tertentu.

2. Menentukan akar dari pohon dengan menghitung nilai gain yang tertinggi dari masing-masing atribut atau berdasarkan nilai indeks entropi terendah. Sebelumnya dihitung terlebih dahulu nilai indeks entropi.

Untuk memilih attribut sebagai akar, didasarkan pada nilai gain tertinggi dari atribut-atribut yang ada. Untuk menghitung gain digunakan rumus sebagai berikut :

$$Gain\ S,A = Entropy\ S - \sum_{i=1} |Si|/|S| * Entropy(Si) \quad (1)$$

$$Entropy\ S = \sum_{i=1} - pi * log_2 pi \quad (2)$$

C. Enkripsi

Fase enkripsi memiliki dua kemungkinan, pertama menjalankan enkripsi menggunakan algoritma AES dengan kunci 256-bit, dan yang kedua menjalankan enkripsi menggunakan algoritma AES dengan kunci 128-bit. Ukuran kunci ditentukan berdasarkan nilai "*Importance Level*" yang ditentukan pada fase klasifikasi fuzzy. Ilustrasi proses enkripsi dapat dilihat pada Gambar 2

Tag yang terkait dengan tag induk juga dienkripsi menggunakan tingkat enkripsi yang sama. Perilaku tag anak diambil dari nilai "*Importance Level*" orang tua. Gambar 3 mengilustrasikan pesan XML setelah fase klasifikasi fuzzy, di mana atribut "*Importance Level*" diberi nilai. Gambar 4 menggambarkan pesan XML yang sama setelah enkripsi, tergantung pada hasil klasifikasi yang dilakukan sebelumnya. Tag yang terkait dengan tag induk juga dienkripsi menggunakan tingkat enkripsi yang sama. Perilaku tag anak diambil dari nilai "*Importance Level*" orang tua. Pada Gambar 4, Nama, ID, Kode Produk, dan No Referensi dienkripsi menggunakan enkripsi AES dengan ukuran kunci 256-bit. Pada dasarnya, pewarisan mewarisi perilaku enkripsi dari orang tua kepada anak sesuai dengan proses kategorisasi, dan proses kategorisasi dibangun berdasarkan relevansi dan evaluasi tag induk.

```
<TransactionDetails src='/paymentsystem.xml'>
    <Account ImportanceLevel="High">
        <Nama>Nur Rachmat</Nama>
        <NoID>1620250001</NoID>
        <JumlahTagihan>1250000</JumlahTagihan>
        <NMPOREF>111111111111</NMPOREF>
        <KdProduk>0001</KdProduk>
        <NmProduk>Pembayaran UK 1</NmProduk>
    </Account>
    <Detail ImportanceLevel="Medium">
        <TglTransaksi>2016/01/08</TglTransaksi>
        <WaktuTransaksi>17:08:14</WaktuTransaksi>
        <IPAddress>116.90.208.1</IPAddress>
    </Detail>
</TransactionDetails>
```

Gambar 3. Pesan XML Setelah Fase Klasifikasi

```
<TransactionDetails src='/paymentsystem.xml'>
    <Encrypted_Data src='xmlenc#'>
        <EncryptionMethod Algorythm='xml#AES'/>
        <Key_Info src='XML_Sig'>
            <Key_Name>AMD</Key_Name>
        </Key_Info>
        <Ci_Data>
            <Ci_Value>54544464fsdf?#</Ci_Value>
        </Ci_Data>
    </Encrypted_Data>
    <Detail ImportanceLevel="Low">
        <TglTransaksi>2016/01/08</TglTransaksi>
        <WaktuTransaksi>17:08:14</WaktuTransaksi>
        <IPAddress>116.90.208.1</IPAddress>
    </Detail>
</TransactionDetails>
```

Gambar 4. Pesan XML Setelah Fase Enkripsi

IV. HASIL AWAL

Pengujian dilakukan pada data transaksi keuangan mahasiswa perguruan tinggi dalam format dokumen XML. Transaksi keuangan berupa pembayaran biaya pendidikan pada tahun akademik 2016/2017.

Pada fase klasifikasi, dikategorikan kedalam 6 karakterisitik transaksi dalam 3 lapisan yang berbeda. Layer tersebut adalah *Account Segment* dan *Detail Segment*. Pengelompokan ini untuk mempermudah proses klasifikasi *fuzzy*. Proses klasifikasi *fuzzy* akan diterapkan dengan menggunakan metode *fuzzy* tipe mamdani. Tabel 1 dan 2 menunjukkan variable linguistik untuk proses fuzzifikasi berdasarkan katagori transaksi dan lapisan.

Rule yang dihasilkan dari proses klasifikasi *fuzzy* akan mengalami proses pemangkasan *rule* dengan algoritma C4.5. Algoritma C4.5 diharapkan dapat menghasilkan *rule* yang optimal dan mengurangi beban komputasi dari Logika *Fuzzy*.

TABLE I. FUZZIFIKASI PADA LAPISAN *ACCOUNT SEGMENT*

NoID	**JumlahTagihan**	**MLPOREF**	***Account Segment***
Non-Sensitive	Non-Sensitive	Non-Sensitive	Low
Normal	Normal	Sensitive	Medium
Sensitive	Non-Sensitive	Sensitive	High
Normal	Non-Sensitive	Sensitive	Medium
Sensitive	Non-Sensitive	Non-Sensitive	Low

TABLE II. FUZZIFIKASI PADA LAPISAN *DETAIL SEGMENT*

KdProduk	**KdStatus**	**WaktuTransksi**	***Detail* Segment**
Non-Sensitive	Non-Sensitive	Non-Sensitive	Low
Normal	Normal	Sensitive	Medium
Sensitive	Non-Sensitive	Sensitive	High
Normal	Non-Sensitive	Sensitive	Medium
Sensitive	Non-Sensitive	Non-Sensitive	Low

V. KESIMPULAN

Hasil awal didapatkan usulan kerangka kerja yang akan dilakukan dalam mengamankan data transaksi keuangan pada file XML. Beberapa modul akan dikembangkan antara lain adalah modul klasifikasi *fuzzy* yang membentuk *fuzzy rule* dan pemangkasan *fuzzy rule* menggunakan algoritma C4.5. Modul enkripsi akan memproses elemen XML untuk dienkripsi berdasarkan *"Importance Level"* dari hasil yang didapatkan pada proses klasifikasi. Pengujian dilakukan pada data transaksi keuangan mahasiswa perguruan tinggi. Transaksi keuangan berupa pembayaran biaya pendidikan pada tahun akademik 2016/2017 dalam format dokumen XML.

VI. UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada seluruh dosen dan jurusan Magister Teknik Informatika, Fakultas Ilmu Komputer Universitas Sriwijaya.

Referensi

[1] F. T. Ammari and J. Lu, “Securing Financial XML Transactions Using Intelligent Fuzzy Classification Techniques,” 2014, pp. 214–326.

[2] T. Imamura, B. Dillaway, and E. Simon, “XML encryption syntax and processing,” 2002. [Online]. Available: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

[3] W. W. W. Consortium, “{XML} {S}ignature,” 2006. [Online]. Available: http://www.w3.org/TR/xmldsig-core.

[4] P. M. Hallam-Baker and S. H. Mysore, “XML Key Management Specification (XKMS) Bindings --- Version 2.0,” 2005.

[5] M. B. Juric, R. Loganathan, P. Sarang, and F. Jennings, *SOA Approach to Integration XML, Web services, ESB, and BPEL in real-world SOA projects*. 2007.

[5] V. Witary and N. Rachmat, "Optimasi Penjadwalan Perkuliahan dengan Menggunakan Algoritma Genetika (Studi Kasus : AMIK MDP, STMIK GI MDP dan STIE MDP)", 2013

[6] M. Boston, “XML-Encryption Minutes.” [Online]. Available: https://www.w3.org/Encryption/2001/Minutes/0103-Boston/minutes.html.

[7] V. Sankar and G. Zayaraz, “Securing confidential data in XML using custom level encryption,” in *2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*, 2016, pp. 227–230.

[8] F. T. Ammari, J. Lu, and M. Aburrous, “Intelligent Banking XML Encryption Using Effective Fuzzy Logic,” in *Emerging Trends in ICT Security*, Elsevier, 2014, pp. 591–617.

[9] F. T. Ammari, J. Lu, and M. Abur-rous, “Intelligent XML Tag Classification Techniques for XML Encryption Improvement,” in *2011 IEEE Third Int’l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int’l Conference on Social Computing*, 2011, pp. 1249–1252.

[10] U. Hanik, “Fuzzy Decision Tree dengan Algoritma C4.5 pada Data Diabetes Indian Pima (Januari 2011),” 2011.

[11] N. G. A. P. H. Saptarini, “PENGGUNAAN ALGORITMA C4.5 DAN LOGIKA FUZZY UNTUK KLASIFIKASI TALENTA KARYAWAN (Studi Kasus : Politeknik Negeri Bali),” 2012.

[12] Veri Ilhadi, “Analisis Algoritma C4.5 dan Fuzzy Sugeno untuk Optimasi Rule Base Fuzzy,” 2017.

[13] Min Liu, De-Gang Chen, and Cheng Wu, “The continuity of Mamdani method,” in *Proceedings. International Conference on Machine Learning and Cybernetics*, vol. 3, pp. 1680–1682.

[14] N. Rachmat and O. Octaria, "Sistem Pemanggilan Antrian Menggunakan Websocket", *Annual Research Seminar (ARS)*, Vol. 2, no. 1, pp. 445-448