DETEKSI SERANGAN SQL *INJECTION* DENGAN METODE *BAYESIAN NETWORK*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :
DENI DANUARTA
09121001045

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2018

HALAMAN PENGESAHAN

DETEKSI SERANGAN SQL *INJECTION* DENGAN METODE *BAYESIAN NETWORK*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

DENI DANUARTA
09121001045

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng
NIP. 197806112010121004

Inderalaya, Mei 2018
Pembimbing

Deris Stiawan, Ph.D
NIP. 197806172006041002

Scanned by TapScanner

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Sabtu
Tanggal : 7 April 2018

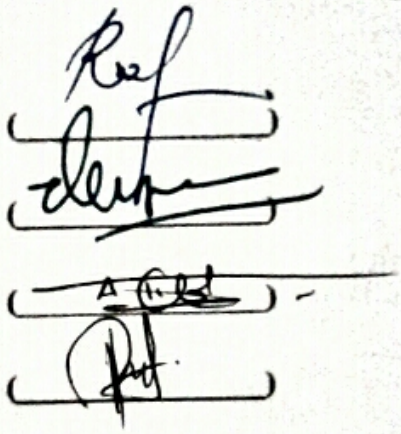
Tim Penguji :

1. Ketua : Dr. Reza Firsandaya Malik, M.T.

2. Pembimbing : Deris Stiawan, Ph.D.

3. Anggota I : Ahmad Heryanto, S.Kom. M.T

3. Anggota II : Rido Zulfahmi, M.T



Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng
NIP. 197806112010121004

Scanned by TapScanner

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Deni Danuarta

NIM : 09121001045

Judul TA : Deteksi Serangan SQL *Injection* Dengan Metode *Bayesian Network*

Hasil Pengecekan *Software iThenticate/Turnitin* : 12%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil plagiat. Apabila ditemukan unsur plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Mei 2018

Deni Danuarta

Scanned by TapScanner

HALAMAN PERSEMBAHAN

MOTO :

SYAIR: ILMU PUNCAK

Usahakan untuk selalu berada dipuncak
meski tidak selamanya berada dipuncak
Pahamilah makna menuju puncak
jangan lupakan tanah dibawah puncak

Motivasi

"Perbedaan antara air dan cermin terlihat pada pantulan sinarnya. Cermin langsung memantulkan sinarnya namun tidak indah dan tidak dapat dinikmati, sedangkan air membutuhkan proses memantulkan cahaya untuk membuatnya menjadi indah dan dapat dinikmati"

Karya Besar ini kupersembahkan kepada :

1. Ayah dan Ibu tercinta.
2. Adik-adik kandungku; Della Mellani, Bella Mellania, Deby Aulia Maharani
3. Bapak Deris Stiawan Ph.D selaku pembimbing Tugas Akhir
4. Keluarga besar Alimudin bin Bona dan Keluarga besar Anwar Hasan bin Hasan
5. Teman-teman seperjuangan Sistem Komputer Angkatan 2012.
6. Teman-teman, Kakak-kakak tingkat, dan Adik-adik tingkat Fakultas Ilmu Komputer dari angkatan 2005-2017 khususnya jurusan Sistem Komputer
7. **Almamaterku.**

KATA PENGANTAR

Alhamdulillah, Puji Syukur kehadirat Allah SWT atas segala rahmat yang telah diberikan, sehingga penulis dapat menyelesaikan laporan Tugas Akhir yang berjudul "Deteksi Serangan SQL *Injection* Dengan Metode *Bayesian Network*". Laporan ini disusun setelah melaksanakan penelitian, yang diajukan untuk memperoleh gelar Sarjana (S1) pada Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.

Sholawat serta salam tidak lupa penulis ucapkan kepada Rasulullah Muhammad SAW yang menjadi panutan dan teladan bagi umat manusia sehingga kehidupan umat manusia lebih baik terutama dalam bidang ilmu pengetahuan. Pelaksanaan dan penyusunan tugas akhir ini tidak mungkin berhasil tanpa adanya bantuan dari berbagai pihak berupa do'a dari Ibu dan Ayah serta dukungan moral seperti bimbingan, nasihat, semangat agar tugas akhir ini dapat terselesaikan. Penulis mengucapkan terima kasih dan penghargaan kepada yang terhormat:

1. Keluarga tercinta Ibu, Bapak, adik-adik yang selalu memberikan dukungan dan do'a sehingga pada akhirnya tugas akhir ini dapat terselesaikan dengan tenang.
2. Bapak Deris Stiawan,. Ph.D selaku pembimbing Tugas Akhir yang telah memberikan dukungan, saran, dan kritik dalam proses pengerjaan tugas akhir sehingga tidak terkendala karena sarana dan prasarana. Terima kasih sebesar-besarnya saya ucapkan kepada beliau.
3. Bapak Firdaus, M.Kom selaku Pembimbing Akademik, terima kasih atas nasihat selama menempuh kuliah di Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.
4. Bapak Dr. Reza Firsandaya Malik, M.T. selaku ketua sidang, Bapak Ahmad Heriyanto, S.Kom. M.T. dan Bapak Rido Zulfahmi, M.T selaku dosen penguji sidang Tugas Akhir yang telah memberi banyak masukan berupa ilmu, kritik, dan saran sehingga konten dari laporan ini menjadi lebih baik.

5. Bapak Rossi Passarella, M.Eng., selaku Ketua Jurusan Sistem Komputer dan Bapak Sutarno M.T. selaku Seketaris Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya. Terima kasih telah membantu kegiatan akademik mahasiswa jurusan Sistem Komputer.
6. Bapak, Ibu dosen Jurusan Sistem Komputer yang selama ini telah memberikan dan menyalurkan ilmu dan pengalamannya.
7. Terkhusus pada beberapa Dosen Bapak Deris Stiawan Ph.D, Ahmad Heriyanto, S.Kom. M.T, dan Bapak Rido Zulfahmi M.T. karena pengaruh dan ilmu dari merekalah, saya memiliki ketertarikan terhadap bidang konsentrasi "Computer Network, Data Communication dan Network Security". Selain itu, pengaruh dari tugas mata kuliah "Basis Data" yang diajarkan oleh Bapak Firdaus M.Kom selaku pembimbing akademik telah membantu memahami pentingnya sebuah *database* pada setiap konsentrasi pada jurusan Sistem Komputer, khususnya pada Keamanan Jaringan.
8. Kak Ahmad Reza Fahlevi selaku staff administrasi Jurusan Sistem Komputer Indralaya saat ini, mbak Oktaria Iis selaku yang pernah menjabar sebagai staff administrasi Jurusan Sistem Komputer Indralaya, mbak Renny Virgansari selaku staff administrasi jurusan Sistem Komputer Bukit dengan kesabaran mereka dapat menyelesaikan proses administrasi baik dalam matakuliah maupun tugas akhir. Untuk mbak Oktaria Iis, terima kasih atas jasa dan kesabaran mbak dalam menangani permasalahan dijurusan semoga diberi kemudahan dalam posisi barunya dibagian akademik.
9. Untuk seluruh teman-teman seperjuangan angkatan 2012, kakak tingkat angkatan 2005 sampai dengan 2011, dan adek tingkat angkatan 2013 sampai 2017, terima kasih atas segala bantuan dan dukungan selama ini semoga jurusan kita dapat terus menjaga solidaritas dan saling menghormati.
10. Khusus kepada Eko Ari Winanto, Kak Ridwan Zalbina, Candra Adi Winanto, Kak Faris Humam, dan Kak Tri Wanda Septian terima kasih telah berperan sangat vital dalam menyelesaikan tugas akhir ini.

11. Tidak lupa juga penulis berterima kasih kepada tempat-tempat yang membantu penulis menyendiri saat "menghilang" dari penulisan Tugas Akhir yang bertujuan untuk memberikan ketenangan, berubah pola pikir,, mencari ilmu dalam menyelesaikan penulisan ini dan yang paling penting mencerahkan suasana hati dalam menyelesaikan tugas akhir ini. Tempat-tempat tersebut adalah *Cyrus Circle,* Komplek Olahraga *Jakabaring Sport City*, Plaza Telkom Cabang Merdeka, Plaza Telkom Cabang Sudirman, Perpustakaan Daerah Sumsel, Taman Purbakala Sriwijaya, Komplek Industri PT. Pusri, Komplek Industri Pertamina Plaju, Air Batu Banyuasin, Tanjung Senai Indralaya dan Mariana Banyuasin.
12. Terima kasih juga kepada laboratorium yang berpengaruh dalam penyelesaian tugas akhir yang berada di lingkungan Universitas Sriwijaya. Tempat tersebut adalah laboratorium Comnets, Eldas Bukit, Bocid, dan Robotik Bukit.
13. Terima kasih kepada para personil Ganteng-Ganteng Skom (GGS) yang sudah membantu banyak hal dalam proses pengerjaan tugas akhir. Personil GGS terdiri dari Abda, Maman, Adhi, Wiyardi, Agung, Rashad, Kak Syarif, Bang Zaki, Ridho Ichwan, Andreas Samosir, Anggoro, Mastoci, Arief, Avid, Bayu, Belly, Benny, Bram, Candra Adi Winanto, Denny, Dwiky, Edi, Eko Saputra, Erick, Ojik, Fahmi, Faiz, Fajik, Faris, Halim, Hanif, Mamat, Kharisma, Sulkhan, Imam, Kak Fadli, Fajar, Maulana, Zikrillah, Orlando, Randra, Fabio, Eko Ari Winanto, Romi, Ojan, Sahat, Syukron, Tahta, Kak Titoyan, Tomok, Visca, Agus, Yogi, dan Yogi TP. Semoga dilancarkan tugas akhirnya dan bagi yang sudah lulus diberi karir yang baik. Aamiin, Gas!
14. Terima kasih kepada penghuni lab Comnets termasuk para pendahulu angkatan 2008, angkatan 2009, angkatan 2010, angkatan 2011, angkatan 2012 maupun penghuni saat ini. Terutama penghuni saat ini Dimas Wahyudi, Fepiliana, Johan Wahyudi, Leny Novitasari, Sri Suryani, Meilinda Eka, Riki Andika, Ratih Gustifa, Fahrul Rozi, dan Rendika Adha semoga diberi kemudahan dan semangat dalam mengerjakan Tugas Akhir.

DETEKSI SERANGAN SQL *INJECTION* DENGAN METODE *BAYESIAN NETWORK*

Deni Danuarta (09121001045)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
email : denidanuarta@students.ilkom.unsri.ac.id

Abstrak

Bayesian Network merupakan salah satu *machine learning* yang memanfaatkan hubungan probabilitas antara suatu variabel dengan variabel lain. Metode *bayesian network* dapat digunakan untuk mendeteksi paket serangan SQL *Injection* melalui URI pada HTTP *Request.* SQL *Injection* merupakan teknik serangan yang memanfaatkan celah keamanan pada sebuah aplikasi web. Target *server* yang digunakan dalam melakukan penelitian adalah DVWA yang memiliki celah keamanan *database.* Pada penerapan metode *Bayesian Network* terhadap pola serangan SQL *Injection* dapat dibagi menjadi dua, yaitu pola serangan *Character Query* dan pola serangan *Percent Encoding.* Hasil deteksi penerapan metode *Bayesian Network* terhadap serangan SQL *Injection* dapat diperoleh TPR mencapai 99% dengan TNR dan *Precision* mencapai 100%. Dengan demikian, hasil deteksi serangan SQL *Injection* memiliki akurasi rata-rata 90%.

Kata kunci: SQL *Injection*, *Bayesian Network,* URI, HTTP *Request*

SQL INJECTION DETECTION USING BAYESIAN NETWORK

Deni Danuarta (09121001045)

Dept. of Computer Engineering, Faculty of Computer Science, Sriwijaya University

email: denidanuarta@students.ilkom.unsri.ac.id

Abstract

Bayesian Network is one of the machine learning that utilizes the probability relationship between a variable with another variable. Bayesian network methods can be used to detect SQL Injection attack packets through URIs on HTTP Request. SQL Injection is an attack technique that exploits vulnerabilities in a web application. The target server used in doing research is the DVWA which has a database security hole. In Bayesian Network method implementation of SQL Injection attack pattern can be divided into two, namely Character Query attack pattern and Percent Encoding attack pattern. The result of Bayesian Network method detection on SQL Injection attack can be obtained by TPR reach 99% with TNR and Precision reach 100%. Finally, SQL Injection attack detection results have an average accuracy of 90%.

Keyword: *SQL Injection, Bayesian Network, URI, HTTP Request*

DAFTAR ISI

Halaman

Halaman Judul.....i
Halaman Pengesahan.....ii
Halaman Persetujuan.....iii
Halaman Pernyataan.....iv
Halaman Persembahan.....v
Kata Pengantar.....vi
Abstrak.....ix
Abstract.....x
Daftar Isi.....xi
Daftar Gambar.....xiv
Daftar Tabel.....xvi

BAB I PENDAHULUAN

1.1. Latar Belakang.....1
1.2. Tujuan.....2
1.3. Manfaat.....3
1.4. Rumusan Masalah.....3
1.5. Batasan Masalah.....3
1.6. Metodelogi Penelitian.....4
1.7. Sistematika Penulisan.....6

BAB II TINJAUAN PUSTAKA

2.1. Diagram Konsep Penelitian.....7
2.2. *Intrusion Detection System*.....8
2.3. Klasifikasi *Intrusion Detection System*.....9
2.3.1. Klasifikasi IDS Berdasarkan Sumber Data.....9
1. *Host-based Intrusion Detection System* (HIDS).....10
2. *Network-based Intrusion Detection System* (NIDS).....10
2.3.2. Klasifikasi IDS Berdasarkan Metode Deteksi.....10
1. *Signature-based* IDS.....10

2. *Anomaly-based* IDS....10
3. *Hybrid-based* IDS....11
2.3.3. Klasifikasi Berdasarkan Waktu Pemeriksaan....11
1. *Off-line Intrusion Detection System*....11
2. *Real-Time Intrusion Detection System*....11
2.3.4. Klasifikasi IDS Berdasarkan Struktur Sistem....12
1. *Centralized Intrusion Detection System*....12
2. *Distributed Intrusion Detection System*....12
2.3.5 Klasifikasi IDS Berdasarkan Perilaku Setelah Deteksi....12
1. *Active Intrusion Detection System*....12
2. *Passive Intrusion Detection System*....12
2.4. Metode Penelitian Umum *Intrusion Detection System*....13
2.5. *Bayesian Methods*....14
2.5.1. *Bayesian Network*....14
2.5.2. *Causal Chain*....16
2.5.3. *Common Cause*....16
2.5.4. *Common Effect*....17
2.6. SQL *Injection*....18
2.6.1 Jenis Serangan SQL *Injection*....18
1. *First Order Attack*....19
2. *Second Order Attack*....19
3. *Lateral Injection*....19
2.6.2. Bentuk *Query* Tipe Serangan SQL *Injection*....19
1. *Tautology*....20
2. *Ilegal / Logically Incorrectly Queries*....21
3. *Piggy-backed Query*....21
4. *Union Query*....21
5. *Stored Procedure*....21
6. *Inference*....22
7. *Alternate Encoding*....22
2.7. *Damn Vulnerability Web Application*....23
2.8. *Percent Encoding*....23
2.9. Arsitektur TCP/IP....25
2.10. *Hypertext Transfer Protocol*....25
2.10.1. Format Pesan HTTP....26
1. *Client Request*....26
2. *Server Response*....27
2.10.2. HTTP *Request Method*....28
1. GET....29
2. POST....29
3. HEAD....29
4. PUT....29
5. DELETE....29
6. TRACE....29
7. OPTIONS....29
8. CONNECT....30
9. PATCH....30

2.11. *Feature Extraction*.....30
2.12. Evaluasi Performa *Intrusion Detection System*.....30

BAB III METODOLOGI PENELITIAN

3.1. Pendahuluan.....32
3.2. Kerangka Kerja Penelitian.....32
3.3. Perancangan Sistem.....34
3.3.1. Kebutuhan Perangkat Keras (*Hardware*).....35
3.3.2. Kebutuhan Perangkat Lunak (*Software*).....36
3.3.3. Bentuk Serangan SQL *Injection* Berdasarkan *Query*.....36
3.4. *Feature Extraction*.....39
3.5. *Skenario Pengujian SQL Injection*.....42
3.6. Penerapan Metode *Bayesian Network* pada Deteksi Serangan *SQL Injection*.....47

BAB IV HASIL DAN ANALISA

4.1. Pendahuluan.....51
4.2. Analisis Dataset.....51
4.3. Pengenalan Pola Serangan SQL *Injection*.....53
4.4. Hasil *Feature Extraction*.....56
4.4.1. Hasil *Feature Extraction* HTTP *Request*.....56
4.4.2. Hasil *Feature Extraction* HTTP *Response*.....59
4.5. Pola Serangan SQL *Injection*.....62
4.6. Implementasi Metode *Bayesian Network*.....69
4.7. Hasil Penerapan *Bayesian Network* Terhadap Serangan *SQL Injection*.....73

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan.....79
5.2. Saran.....79

DAFTAR PUSTAKA.....81
LAMPIRAN

DAFTAR GAMBAR

Gambar 1.1 Diagram Alir Metodologi Penelitian.....5
Gambar 2.1 Diagram Konsep Penelitian.....7
Gambar 2.2 Komponen Arsitektur IDS.....8
Gambar 2.3 Klasifikasi IDS.....9
Gambar 2.4 Metode Umum *Intrusion Detection System*.....13
Gambar 2.5 Contoh DAG dan CPT pada *Bayesian Network*.....15
Gambar 2.6 *Conditional Independence* pada *Causal Chain*.....16
Gambar 2.7 *Conditional Independence* pada *Common Cause*.....17
Gambar 2.8 *Conditional Independence* pada *Common Effect*.....17
Gambar 2.9 Skema Serangan SQL *Injection*.....18
Gambar 2.10 Contoh Serangan SQL *Injection* pada DVWA.....23
Gambar 2.11 Format *HTTP Request*.....26
Gambar 2.12 Format *HTTP Response*.....28
Gambar 3.1 Kerangka Kerja Penelitian.....33
Gambar 3.2 *Topology Dataset* Serangan *SQL Injection*.....34
Gambar 3.3 *Flowchart Feature Extraction*.....39
Gambar 3.4 *Topology* Terjadinya Serangan *SQL Injection*.....42
Gambar 3.5 Contoh Jenis Serangan *SQL Injection Tautology*.....45
Gambar 3.6 Contoh Serangan *SQL Injection* dengan *Union Query*.....45
Gambar 3.7 Contoh Serangan *Inference Blind SQL Injection*.....46
Gambar 3.8 Contoh Serangan *Inference Timing SQL Injection*.....46
Gambar 3.7 *Flowchart* Penerapan *Bayesian Network* Sebagai Deteksi.....48
Gambar 4.1 Statistik Paket Data.....52
Gambar 4.2 Paket HTTP Normal.....53
Gambar 4.3 HTTP *Request* dan HTTP *Response* pada Trafik Normal.....54
Gambar 4.4 DVWA ketika Trafik Normal.....54
Gambar 4.5 Paket HTTP Serangan *SQL Injection*.....55
Gambar 4.6 HTTP *Request* dan HTTP *Response Trafik SQL Injection*.....55
Gambar 4.7 Contoh Tampilan Serangan *SQL Injection*.....56

Gambar 4.8 Pencocokan PCAP *HTTP Request* dengan *Feature Extraction*…57
Gambar 4.9 Pencocokan PCAP HTTP *Response* dengan *Feature Extraction*.60
Gambar 4.10 Penerapan *Bayesian Network* pada Pola Serangan URI.....67
Gambar 4.11 Model Penerapan *Bayesian Network* Terhadap Pola Serangan SQL *Injection*.....70
Gambar 4.12 Hasil Penerapan *Bayesian Network* pada SQL *Injection*.....73
Gambar 4.13 Pembuktian Hasil Penerapan *Bayesian Network* Terhadap Paket yang Terekam pada *Wireshark*.....74
Gambar 4.14 Grafik *Binary Classification* pada Penerapan *Bayesian Network*.....76

DAFTAR TABEL

Tabel 1 Jenis Serangan *SQL Injection* Menurut Bentuk *Query*.....20
Tabel 2 ASCII-Hexadecimal beserta *Character* pada *Persent Encoding*.....24
Tabel 3 Layer TCP/IP.....25
Tabel 4 Struktur *HTTP Request*.....27
Tabel 5 Struktur *HTTP Response*.....28
Tabel 6 *Confusion Matrix* pada *Alarm*.....31
Tabel 7 Spesifikasi Kebutuhan Perangkat Keras.....35
Tabel 8 Spesifikasi Perangkat Lunak.....36
Tabel 9 *Query* Serangan SQL *Injection* Penelitian.....37
Tabel 10 Atribut *Feature Extraction* HTTP.....40
Tabel 11 *Pseudocode Feature Extraction*.....41
Tabel 12 Skenario Pengujian Serangan.....43
Tabel 13 Daftar *Query String* yang Dipisahkan dari URI.....47
Tabel 14 Atribut yang Digunakan pada Penerapan *Bayesian Network*.....49
Tabel 15 *Pseudocode Bayesian Network*.....50
Tabel 16 Jumlah Paket HTTP beserta Paket Serangan.....52
Tabel 17 Jumlah Paket Serangan Berdasarkan *Query* Jenis Serangan SQL *Injection*.....53
Tabel 18 *Query* dan URI Penelitian.....62
Tabel 19 Pola Serangan SQL *Injection* pada URI.....65
Tabel 20 *Percent Encoding* Penelitian.....66
Tabel 21 *Character Query* Penelitian.....66
Tabel 22 Pola Serangan *SQL Injection* Berbasis *Character Query*.....67
Tabel 23 Pola Serangan SQL *Injection* Berbasis *Percent Encoding*.....68
Tabel 24 Peluang Kemunculan dari Karakter URI pada Paket Serangan dan Normal.....71
Tabel 25 *Confusion Matrix* pada Hasil Penerapan *Bayesian Network*.....75
Tabel 26 *Detection Rate* Pada Penerapan *Bayesian Network*.....77

BAB I. PENDAHULUAN

1.1 Latar Belakang

Intrusion Detection System (IDS) adalah perangkat-perangkat yang melakukan monitoring suatu lalu lintas jaringan atau sistem terhadap aktifitas yang mencurigakan yang biasanya terjadi serangan pada komputer [1]. Serangan pada komputer sering terjadi pada *layer Network* sampai pada *layer Application*. Pada penelitian [2], serangan pada komputer dapat dibedakan menjadi beberapa jenis serangan, yaitu *Virus, Worm, Trojan, Network Attack, Denial of Service (DoS), Physical Attack, Password Attack, Information Gathering Attack, User to Root Attack (U2R), Remote to Local Attack (R2L),* dan *Probe.* Pada saat melakukan deteksi serangan, IDS dapat menerapkan tiga metodelogi yaitu *Rule Based*, *Artificial Intelligence* dan *Computational Methods* [3].

Dalam melakukan deteksi serangan, terdapat dua teknik deteksi yang digunakan yaitu *misuse detection* dan *anomaly detection. Misuse detection* merupakan suatu teknik deteksi serangan yang telah diketahui oleh sistem dengan melakukan pencocokan data yang diamati, tetapi saat terjadi serangan tipe baru teknik ini tidak dapat mendeteksinya. Sedangkan *anomaly detection* merupakan sistem deteksi serangan yang menggunakan profil tingkah laku normal sebagai acuan dalam melakukan deteksi serangan yang terjadi pada *host* atau *network* [4]. *Anomaly detection* sangat tepat digunakan untuk mendeteksi serangan-serangan baru yang belum diketahui pada suatu sistem keamanan.

SQL Injection merupakan sebuah teknik serangan yang memanfaatkan celah keamanan pada sebuah web application [5]. Serangan ini termasuk ke dalam jenis serangan *Password Attack* [2]. Akibat dari serangan SQL Injection adalah dapat memanipulasi database melalui aktifitas yang tidak sah. Dengan menggunakan media berupa *Uniform Resource Location* (URL) dan *Uniform Resource Identifier* (URI), serangan SQL Injection ini dapat melakukan proses retrieving data. Menurut penelitian yang dilakukan oleh [6], pada survey yang

dilakukan OWASP (*Open Web Application Security Project*) serangan yang tertinggi pada tahun 2013 adalah serangan SQL Injection.

Pada penelitian [7] mengatakan bahwa pada saat melakukan pendeteksian menggunakan *misuse detection,* serangan *SQL Injecton* dapat terbaca dengan melakukan pencocokan tipe pola serangan yang terdaftar dengan sistem. Namun *string* yang ada pada *SQL Injection* tersebut bisa diubah dengan berbagai macam teknik, contoh seperti teknik *alternative encoding* yang mengubah *string* yang telah ada di sistem tersebut menjadi biner sehingga serangan *SQL Injection* tidak bisa dibaca oleh *misuse detection.* Serangan tersebut merupakan serangan tipe baru yang mengakibatkan serangan tersebut dapat memasuki database yang ditargetkan.

Solusi dari permasalahan tersebut adalah *anomaly detection,* yang dapat mendeteksi serangan-serangan tipe baru [7]. Pada saat melakukan *anomaly detection*, IDS memberikan peringatan dari aplikasi menuju back-end database server. Diperkuat dengan penelitian yang dilakukan oleh [8] yang menerangkan bahwa *anomaly detection* pada IDS sebaiknya dilakukan dengan menggunakan *machine learning.* Metode *machine learning* yang digunakan adalah *Bayesian Network* karena hasil penelitian [9] dinyatakan tingkat deteksi anomaly menggunakan *bayesian network* tersebut rata-rata lebih dari 90%.

Dalam penelitian ini berdasarkan ulasan diatas, serangan *SQL Injection* dapat dideteksi dengan cara pengenalan *payload* HTTP berupa HTTP *Request* pada bagian URI. Dengan penerapan *Bayesian Network*, *SQL Injection* dapat dideteksi dan dikelompokan berdasarkan *query* yang digunakan.

1.2 Tujuan

Tujuan dari penelitian ini dapat dijelaskan sebagai berikut:

1. Mengenali paket serangan *SQL Injection* dalam *raw packet data*
2. Menerapkan metode *Bayesian Network* untuk mendeteksi serangan *SQL Injection*
3. Mengukur akurasi deteksi serangan *SQL Injection*

1.3 Manfaat

Manfaat yang didapatkan dari penelitian tugas akhir ini sebagai berikut:

1. Dapat mempelajari serangan *SQL Injection* pada *raw packet data*
2. Dapat mencegah terjadinya serangan *SQL Injection* lebih dini
3. Dapat menerapkan penggunaan *machine learning* berupa *Bayesian Network* pada *Intrusion Detection System*

1.4 Rumusan Masalah

Pada latar belakang dari penelitian yang telah dikemukakan sebelumnya, inti dari permasalahan utama tersebut adalah

1. Bagaimana membedakan paket data normal dengan paket data serangan *SQL Injection.*
2. Bagaimana merancang *Intrusion Detection System* berbasis *machine learning* berupa metode *Bayesian Network* pada serangan *SQL Injection*.

1.5 Batasan Masalah

Dalam perancangan tugas akhir ini dilakukan dengan batasan-batasan masalah sebagai berikut:

1. Pengujian serangan ini tertuju pada serangan *SQL Injection*
2. Metode yang digunakan pada penelitian ini menggunakan metode *Bayesian Network*
3. *Web framework* yang digunakan untuk pengujian menggunakan *web application* DVWA (*Damn Vulnerable Web Application*) dan *database MySQL*
4. Pengujian dilakukan secara *offline*.
5. Menggunakan *dataset* yang ter*capture* pada trafik normal dan trafik serangan *SQL Injection.*
6. Jenis serangan *SQL Injection* yang digunakan berdasarkan bentuk *query* yaitu *Tautology, Union Query, Inference Timing SQL Injection* dan *Inference Blind SQL Injection.*

7. Tidak melakukan pendeteksian dengan pengenalan pola berdasarkan *regular expression* (*regex*).
8. Tidak membahas cara pencegahan serangan *SQL Injection.*
9. Tidak membahas pengujian dengan menggunakan *tools* antarmuka grafis seperti *SQLMap* dan sebagainya.
10. Tidak melakukan pengujian berdasarkan *https*.
11. Tidak melakukan enkripsi data pada serangan *SQL Injection*

1.6 Metodelogi Penelitian

Pada metodelogi penelitian ini membagi menjadi beberapa tahap sebagai berikut:

1. Tahap Pertama (Studi Pustaka / Literatur)

   Tahapan ini dilakukan setelah masalah yang telah di bahas sesuai dengan kerelevan penelitian sebelumnya yang mengacu banyaknya artikel, paper, jurnal dan buku yang berhubungan dengan penelitian ini yang berjudul "Deteksi Serangan *SQL Injection* Dengan Metode *Bayesian Network*".

2. Tahap Kedua (Perancangan Sistem)

   Tahapan ini merupakan tahapan dimana menentukan perangkat-perangkat yang dibutuhkan pada penelitian ini, baik berupa perangkat keras maupun lunak.

3. Tahap Ketiga (Pengujian)

   Tahapan ini berupa pengujian yang sesuai dengan parameter-parameter serangan yang ditentukan oleh batasan masalah.

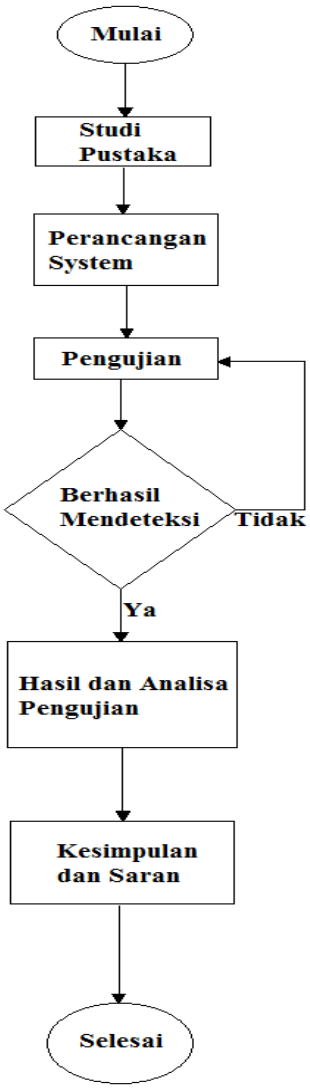
4. Tahap Keempat (Hasil dan Analisa)

   Tahapan ini berisi hasil pengujian pada penelitian tersebut kemudian dianalisa hasil tersebut guna mengetahui apa kelebihan dan kekurangan rancangan penelitian beserta faktor yang mempengaruhi.

5. Tahap Kelima (Kesimpulan dan Saran)

Tahapan terakhir berisi tentang kesimpulan dan saran dari hasil studi pustaka, perancangan sistem dan analisa pada penelitian tersebut. Pada saran berisi poin-poin dari penulis untuk penelitian selanjutnya.

Pada gambar 1.1, dijelaskan tampilan metodologi penelitian dalam bentuk diagram alir yang menggambarkan proses pelaksanaan penelitian:



Gambar 1.1. Diagram Alir Metodologi Penelitian

1.7 Sistematika Penelitian

Dalam penyusunan tugas akhir ini, dibuat sistematika penulisan untuk memudahkan dan menjelaskan inti dari tiap bab yang dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Bab ini terdiri dari Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penelitian yang mengacu pada landasan topik penelitian

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang dasar teori yaitu Intrusion Detection System, *Bayesian Network*, *SQL Injection* yang berhubungan dengan penelitian tugas akhir.

BAB III METODOLOGI PENELITIAN

Bab ini terdiri dari penjelasan secara sistematis mengenai bagaimana proses penelitian dilakukan, tahapan perancangan sistem, dan penerapan metode penelitian.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini menjelaskan tentang hasil pengujian yang dilakukan lalu menganalisa dari hasil data yang didapat

BAB V KESIMPULAN

Bab ini berisi kesimpulan dari hasil pengujian yang dilakukan, menjawab tujuan yang dicapai dari BAB I (Pendahuluan), dan saran untuk penelitian selanjutnya

DAFTAR PUSTAKA

[1] J. Peng, K. K. R. Choo, and H. Ashman, "User profiling in intrusion detection: A review," *Journal of Network and Computer Applications*, vol. 72, pp. 14–27, 2016.

[2] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 1, pp. 303–336, 2014.

[3] S. Akbar, "Intrusion Detection System Methodologies Based on Data Analysis," vol. 5, no. 2, pp. 10–20, 2010.

[4] J. Koziol, *Intrusion Detection Systems with Snort*, vol. 3, no. 1. 2003.

[5] J. Clarke, "SQL Injection Attacks and Defense," *Syngress*, 2012.

[6] J. Abirami, R. Devakunchari, and C. Valliyammai, "A top web security vulnerability SQL injection attack - Survey," *ICoAC 2015 - 7th International Conference on Advanced Computing*, 2016.

[7] R. . Mahapatra and S. Khan, "A Survey of SQL Injection Attacks Countermeasures," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 3, no. 3, pp. 55–74, 2012.

[8] F. Valeur, D. Mutz, and G. Vigna, "A learning-based approach to the detection of sql attacks," *Intrusion and Malware Detection and Vulnerability Assessment*, pp. 123–140, 2005.

[9] M. M. Drugan, "A Bayesian model for anomaly detection in SQL databases for security systems," *Computational Intelligence (SSCI), IEEE Symposium Series on*, 2016.

[10] A. Jamdagni, "Payload-based Anomaly Detection in HTTP Traffic," no. November, p. 190, 2012.

[11] F. Humam, "Perancangan Intrusion Detection System Dengan Visualisasi Training Data Menggunakan Metode Bayesian." pp. 10–48, 2014.

[12] K. B. Korb and A. E. Nicholson, *Bayesian Artificial Intelligence*, vol. 47, no. 1. London: Chapman & Hall/CRC Press LLC, 2004.

[13] D. Bhattacharyya and J. Kalita, *Network anomaly detection: A machine learning perspective*. 2013.

[14] O. A. Marlita, A. P. Kurniati, F. Informatika, and I. T. Telkom, "Anomaly Detection Pada Intrusion Detection System (Ids) Menggunakan Metode Bayesian Network," pp. 53–61, 2015.

[15] M. R. Zalbina, "Sistem Deteksi HTTP menggunakan HTTP Inspect Preprocessor dan Rule Options," Universitas Sriwijaya, 2016.

[16] A. Tajpour, S. Ibrahim, and M. Masrom, "SQL Injection Detection and Prevention Techniques," *International Journal of Advancements in Computing Technology*, vol. 3, no. 7, pp. 82–91, 2011.

[17] N. Khochare, S. Chalurkar, S. Kakade, and B. B. Meshramm, "Survey on SQL Injection attacks and their Countermeasures," *IJCEM International Journal of Computational Engineering & Management*, vol. 14, no. October, pp. 111–114, 2011.

[18] N. M. Sheykhkanloo, "SQL-IDS: Evaluation of SQLi Attack Detection and Classification Based on Machine Learning Techniques," *Proceedings of the 8th International Conference on Security of Information and Networks*, pp. 258–266, 2015.

[19] W. G. J. Halfond, J. Viegas, and A. Orso, "A Classification of SQL Injection Attacks and Countermeasures," *Preventing Sql Code Injection By Combining Static and Runtime Analysis*, p. 53, 2008.

[20] A. Headquarters, "ASCII Character Set and Hexadecimal Values," *Cisco IOS Configuration Fundamentals Command Reference*, no. 6387, p. 1549, Apr-2010.

[21] C. A. Winanto, "DETEKSI SERANGAN DENIAL OF SERVICE MENGGUNAKAN ARTIFICIAL IMMUNE SYSTEM," Universitas Sriwijaya, 2017.

[22] E. A. Winanto, "VISUALISASI SERANGAN REMOTE TO LOCAL (R2L) DENGAN CLUSTERING K-MEANS," Universitas Sriwijaya, 2017.

[23] S. Y. Wu and E. Yen, "Data mining-based intrusion detectors," *Expert Systems with Applications*, vol. 36, pp. 5605–5612, 2009.

[24] Z. Liu, H. Liu, J. Hardy, and L. Liu, "Uniform resource identifier encoded by Base62x," *Proceedings - 2015 IEEE 12th International Conference on*

Ubiquitous Intelligence and Computing, 2015 IEEE 12th International Conference on Advanced and Trusted Computing, 2015 IEEE 15th International Conference on Scalable Computing and Communications, 20, pp. 1087–1093, 2016.

[25] D. Kar, S. Panigrahi, and S. Sundararajan, "SQLiGoT : Detecting SQL Injection Attacks using Graph of Tokens and SVM," *Computers & Security*, 2016.

[26] C. Basta and S. Darwish, "Detection of SQL Injection Using a Genetic Fuzzy Classifier System," vol. 7, no. 6, pp. 129–137, 2016.