KAEDAH PEMILIHAN CIRI UNTUK PENGESANAN PENCEROBOHAN IOT

NUR NAJWA DAYANA BINTI MURTADZA
TS. DR. HASIMI BIN SALLEHUDIN

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Evolusi besar dalam perhubungan antara alat di mana pelbagai peranti telah disambungkan ke Internet, seperti sensor, kamera, telefon pintar, dan lain-lain, telah menyebabkan munculnya Internet Pelbagai Benda (IoT). Seperti mana-mana rangkaian, IoT menghadapi masalah mencabar keselamatan. Dengan peningkatan trafik rangkaian yang tinggi, penggodam dan pengguna yang berniat jahat ingin merancang cara baru untuk melakukan pencerobohan rangkaian. Banyak teknik telah dikembangkan untuk mengesan gangguan ini berdasarkan kaedah perlombongan data dan pembelajaran mesin. Algoritma pembelajaran mesin bermaksud untuk mengesan anomali menggunakan pendekatan yang diawasi dan tidak diawasi. Kedua-dua teknik pengesanan telah dilaksanakan menggunakan set data IDS seperti DARPA98, KDDCUP99, NSL-KDD, ISCX, ISOT. UNSW-NB15 adalah set data terkini. Set data ini mengandungi sembilan jenis serangan moden yang berbeza dan pelbagai aktiviti normal yang sebenar. Dalam projek ini, tinjauan terperinci mengenai pelbagai teknik berasaskan pembelajaran mesin yang diterapkan pada set data UNSW-NB15 telah dilakukan dan menunjukkan bahawa UNSW-NB15 lebih kompleks daripada set data lain dan dianggap sebagai set data penanda aras baru untuk menilai NIDS. Beberapa kajian penyelidikan telah menangani tugas pengesanan pencerobohan dalam IoT.

Sebilangan besar daripada mereka telah berkonsentrasi untuk menentukan sekumpulan ciri yang dapat meningkatkan ketepatan klasifikasi pencerobohan berdasarkan teknik pemilihan ciri yang diilhamkan oleh statistik dan bio. Pembelajaran mendalam adalah sekumpulan teknik yang menunjukkan prestasi dalam bidang klasifikasi. Kemunculan teknik pembelajaran mendalam telah menyebabkan konfigurasi seni bina baru bagi Neural Network yang dirancang untuk tugas pemilihan ciri. Kajian ini mencadangkan seni bina pembelajaran mendalam yang dikenali sebagai Auto-Encoder (AE) untuk tugas pemilihan ciri dalam pengesanan pencerobohan IoT. Pertama, set data penanda aras untuk pencerobohan IoT telah dipertimbangkan dalam eksperimen. Sebagai tambahan, beberapa tugas normalisasi telah diterapkan untuk mengubah data menjadi format yang sesuai untuk diproses. Setelah itu, AE yang dicadangkan telah dilaksanakan untuk tugas pemilihan ciri dan seni bina mudah bagi Neural Network (NN) untuk tugas klasifikasi. Hasil eksperimen menunjukkan bahawa AE yang dicadangkan menunjukkan ketepatan 99.99% dengan Kadar Penggera Palsu (FAR) 0.0. Membandingkan hasil ini dengan hasil yang diperoleh dari kajian yang berkaitan membuktikan bahawa AE mempunyai prestasi yang lebih tinggi daripada teknik pemilihan ciri statistik dan bio-inspirasi.

1 PENGENALAN

Sepanjang dekad yang lalu, kita telah menyaksikan evolusi besar dalam perhubungan antara alat di mana pelbagai peranti telah disambungkan ke Internet seperti sensor, kamera, telefon pintar dan lain-lain [1]. Evolusi sedemikian itu telah menyebabkan munculnya Internet Pelbagai Benda (IoT) sebagai bidang penyelidikan baru yang meneroka penggunaan sejumlah besar peranti yang disambungkan untuk melakukan tugas-tugas tertentu [2]. Ini telah mengusulkan rumah pintar yang dapat memanfaatkan kamera, sensor dan telefon pintar dalam membangun sistem pintar untuk memberi amaran kepada pemiliknya mengenai kejadian mencurigakan dan kemunculan yang mungkin berlaku semasa ketiadaannya. Di samping itu, kerangka untuk hospital pintar juga dicadang menggunakan alat perubatan untuk menentukan keutamaan dan senarai kecemasan pesakit [3].

Evolusi teknologi besar ini telah membawa banyak cabaran, salah satu cabaran yang membimbangkan adalah keselamatan [4]. Cara melindungi rangkaian IoT dari ancaman atau pencerobohan tradisional seperti virus, cacing, kuda trojan dan lain-lain adalah cabaran utama. Keselamatan itu merupakan permintaan penting terutama jika rangkaian IoT berkaitan dengan agensi perubatan atau swasta yang menjadikan pencerobohan maklumat peribadi tidak dapat ditoleransi [5].

Intrusion Detection (ID) adalah bidang penyelidikan yang meneliti dalam pengenalpastian aktiviti tidak normal yang dilakukan di rangkaian tertentu [6]. ID telah diselidiki secara meluas dalam dua dekad yang lalu di mana sebilangan besar penyelidikan dengan pelbagai teknik telah diusulkan untuk tugas pengesanan. Khususnya, teknik pembelajaran mesin telah ditangani, seperti klasifikasi, ramalan, atau pengelompokan [7]. Walau bagaimanapun, gangguan pada rangkaian tertentu seperti IoT akan mempunyai ciri yang berbeza, yang memerlukan teknik baru yang dapat mengatasi perbezaan ini.

Salah satu teknik berkesan yang dapat menangani ciri pengesanan pencerobohan IoT adalah pemilihan ciri, di mana tujuannya adalah untuk menganalisis ciri pencerobohan IoT dalam mengenal pasti subset ciri yang paling penting. Beberapa penyelidik telah mencadangkan teknik pemilihan ciri untuk tujuan ini. Sebilangan kajian ini telah menggunakan kaedah tradisional seperti Apriori dan Association Rules [8, 9]. Penyelidik lain telah menggunakan kaedah meta-heuristik seperti Algoritma Genetik dan teknik berasaskan Swarm [10-12].

Seperti yang diperhatikan dari kecanggihan dalam pemilihan ciri untuk pengesanan pencerobohan IoT, kebanyakan kajian harus bergantung pada kaedah tradisional seperti berasaskan peraturan dan meta-heuristik. Kekurangan di sebalik kaedah ini terletak pada ketidakmampuan mereka untuk mencari penyelesaian yang optimum di mana sekumpulan ciri terbaik dapat dikenal pasti. Selain dari teknik pemilihan ciri, kaedah klasifikasi yang digunakan dalam literatur untuk mengesan gangguan masih menghadapi beberapa batasan mengenai prestasi pengesanan. Ini kerana kebanyakan pengklasifikasi yang digunakan dalam literatur adalah standard seperti Support Vector Machine (SVM), Naïve Bayes (NB), atau Decision Tree (DT). Pengelasan ini tidak mempunyai paradigma latihan yang luas seperti Neural Network (NN), di

mana prosedur penalaan ralat dipertimbangkan. Ini telah menyebabkan keterbatasan dalam mencapai ketepatan pengesanan yang tinggi dengan Kadar Penggera Palsu (FAR) yang rendah.

Oleh itu, kajian ini mencadangkan Auto-Encoder sebagai pemilihan ciri untuk pengesanan pencerobohan IoT dalam meningkatkan pembelajaran ciri. Di samping itu, kajian ini bertujuan untuk memanfaatkan ciri-ciri dipelajari yang dihasilkan oleh Auto-Encoder dalam mengakomodasi klasifikasi menggunakan Neural Network.

2 PENYATAAN MASALAH

Keselamatan memainkan peranan penting dalam mana-mana rangkaian IoT terutamanya jika rangkaian tersebut mempunyai akses ke data peribadi yang tidak boleh diceroboh. Dalam konteks ini, tugas pengesanan pencerobohan dapat dilakukan untuk memeriksa keselamatan dalam rangkaian IoT. Namun, kerana perbezaan rangkaian IoT dibandingkan dengan rangkaian tradisional, ancaman mungkin masih sama tetapi mekanisme/tingkah laku mungkin berbeza. Oleh itu, penyelidik telah menambahbaik teknik agar sesuai dengan rangkaian IoT.

Pengekstrakan dan pemilihan ciri telah diperhatikan untuk pengesanan pencerobohan IoT. Kemunculan Pembelajaran Dalam telah membawa sekumpulan teknik yang menawarkan pendekatan yang tepat dan cekap untuk beberapa aplikasi seperti klasifikasi, ramalan, pengelompokan, dan pemilihan ciri. Auto-Encoder adalah salah satu teknik pembelajaran mendalam yang telah dicadangkan untuk tugas pemilihan ciri (Mighan & Kahani 2018). Teknik ini menawarkan mekanisme pembelajaran ciri yang menjanjikan di mana ruang ciri akan dibina semula di mana ciri-ciri dapat dipelajari dengan berkesan.

Kajian ini bertujuan untuk mengkaji prestasi Auto-Encoder sebagai pendekatan pemilihan ciri dalam pengesanan pencerobohan IoT untuk meningkatkan ketepatan klasifikasi dengan meningkatkan pembelajaran ciri.

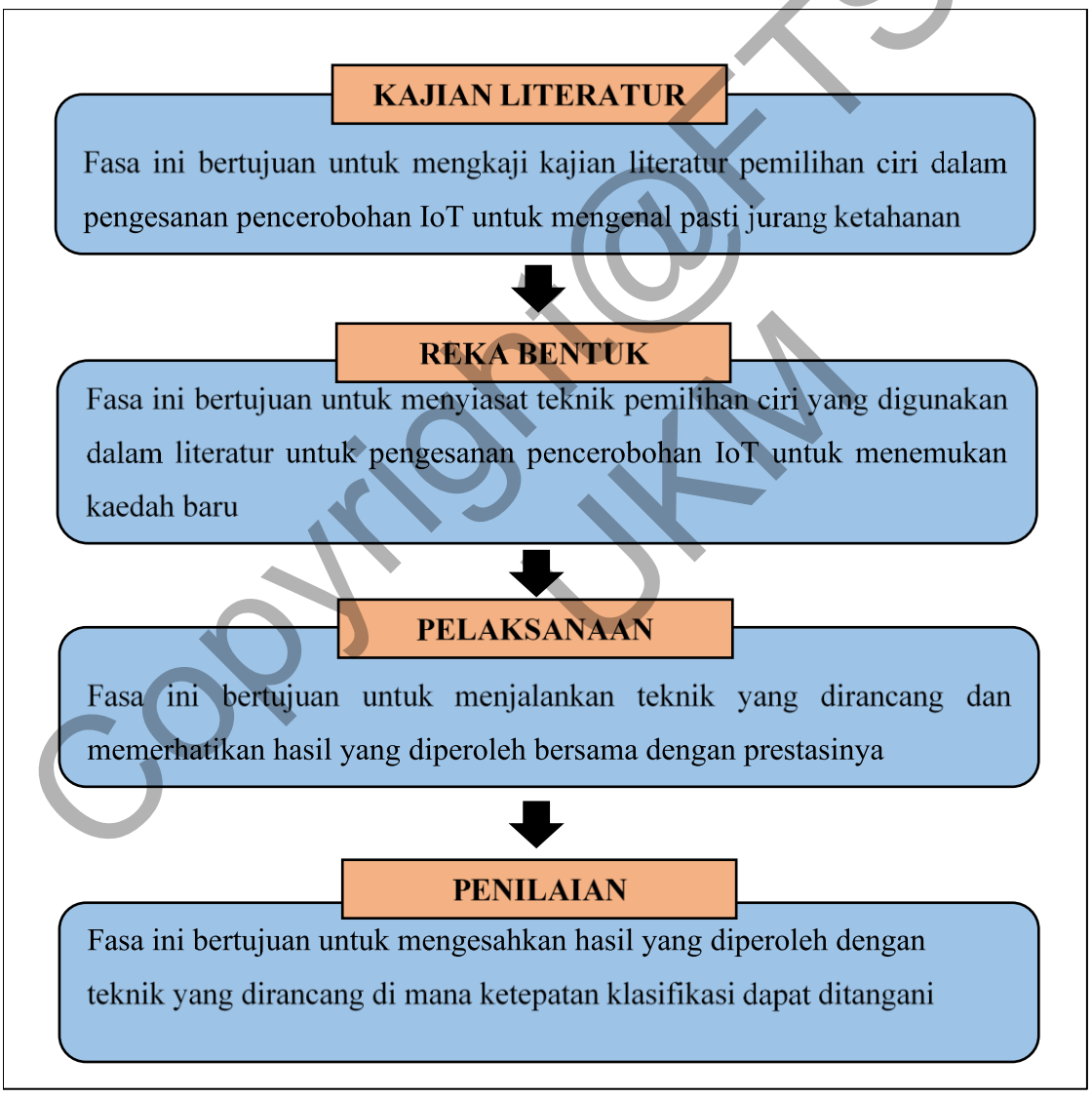
3 OBJEKTIF KAJIAN

Objektif penyelidikan ini dapat dinyatakan seperti berikut:

i. Untuk mencadangkan Auto-Encoder sebagai pemilihan ciri untuk pengesanan pencerobohan IoT dalam meningkatkan pembelajaran ciri.
ii. Untuk memanfaatkan ciri-ciri dipelajari yang dihasilkan oleh Auto-Encoder dalam mengakomodasi klasifikasi menggunakan Neural Network.

4 METOD KAJIAN

Kajian ini telah dijalankan melalui empat fasa. Fasa pertama bertujuan untuk mengkaji kajian literatur pemilihan ciri dalam pengesanan pencerobohan IoT. Pemeriksaan ini bertujuan untuk mencari batasan dan jurang. Fasa kedua bertujuan untuk mengkaji teknik pemilihan ciri yang digunakan dalam literatur untuk melakukan pengesanan pencerobohan IoT. Ulasan ini bertujuan untuk mengenal pasti kaedah baru yang dapat mengatasi jurang. Fasa ketiga dimaksudkan untuk menerapkan teknik yang dirancang yang telah diusulkan pada fasa sebelumnya. Ini memerlukan mencapai set data dan merumuskan eksperimen. Akhir sekali, fasa keempat bertujuan untuk mengesahkan hasil yang diperoleh dengan kaedah yang dicadangkan. Rajah 1 meringkaskan fasa-fasa ini.



Rajah 1 Model Metodologi Kajian

4.1 Kajian Yang Berkaitan

Banyak penyelidik telah mengkaji pemilihan ciri dalam pengesanan IoT. Sebagai contoh, [13] telah memeriksa dimensi ruang ciri dalam pengesanan pencerobohan di IoT. Penulis telah memberi fokus pada tugas yang mencabar untuk mengurangkan kadar positif palsu dalam pengesanan pencerobohan. Untuk tujuan ini, penulis telah mencadangkan gabungan Algoritma Genetik (GA) sebagai teknik pemilihan/pengurangan ciri bersama dengan pengelasan Support Vector Machine (SVM). Set data yang digunakan dalam eksperimen adalah UNSW-NB15, di mana ketepatan purata pengesanan adalah 93.25%, dengan FAR 8.6.

Begitu juga, [14] telah mengusulkan pendekatan pemilihan ciri berdasarkan teknik wrapping. Penulis telah berusaha untuk mengenal pasti ciri-ciri yang paling penting yang bermungkinan mempengaruhi ketepatan pengesanan pencerobohan. Oleh itu, teknik wrapping telah digunakan di mana Algoritma Genetik digunakan sebagai pendekatan pemilihan ciri dengan Decision Tree (DT) sebagai kaedah klasifikasi. Set data yang digunakan dalam eksperimen adalah UNSW-NB15, di mana subset ciri terbaik telah memperoleh ketepatan 81.42% dengan FAR 6.39.

Terlepas dari pendekatan pemilihan ciri meta-heuristik tradisional, [9] telah mengusulkan teknik Association Rule Mining untuk pemilihan/pengurangan ciri dalam pengesanan pencerobohan IoT. Kaedah yang dicadangkan telah tertumpu pada titik pusat atribut penting yang mempengaruhi pengesanan pencerobohan. Set data yang digunakan dalam eksperimen adalah UNSW-NB15, di mana ketepatan purata yang diperoleh dengan kaedah yang dicadangkan adalah 83%, dengan FAR 14.2. Begitu juga, [8] telah menggunakan algoritma Apriori untuk menentukan ciri yang paling ketara dalam pengesanan pencerobohan IoT. Kemudian, algoritma yang dicadangkan telah dijalankan untuk menentukan ciri berdasarkan kepentingannya, di mana yang tidak berkaitan akan ditolak. Selepas itu, dua pengklasifikasi Naïve Bayes dan Logistic Regression telah digunakan untuk mengklasifikasikan contoh data berdasarkan ciri yang dipilih. Set data UNSW-NB15 telah digunakan di mana purata ketepatan yang diperoleh dengan kaedah yang dicadangkan adalah 90% dengan FAR 10.5.

Kajian lain yang menangani pemilihan ciri dalam pengesanan pencerobohan IoT dilakukan oleh [10], di mana gabungan Algoritma Genetik dan Decision Tree telah diusulkan untuk tujuan ini. Sebagai tambahan, GA telah diterapkan untuk membuat aturan induksi untuk aturan yang dihasilkan oleh DT. Seperti semua kajian mengenai pengesanan pencerobohan IoT, set data UNSW-NB15 telah digunakan dalam eksperimen. Hasil ketepatan untuk subset ciri terbaik menunjukkan 84.33%, dengan FAR 8.9.

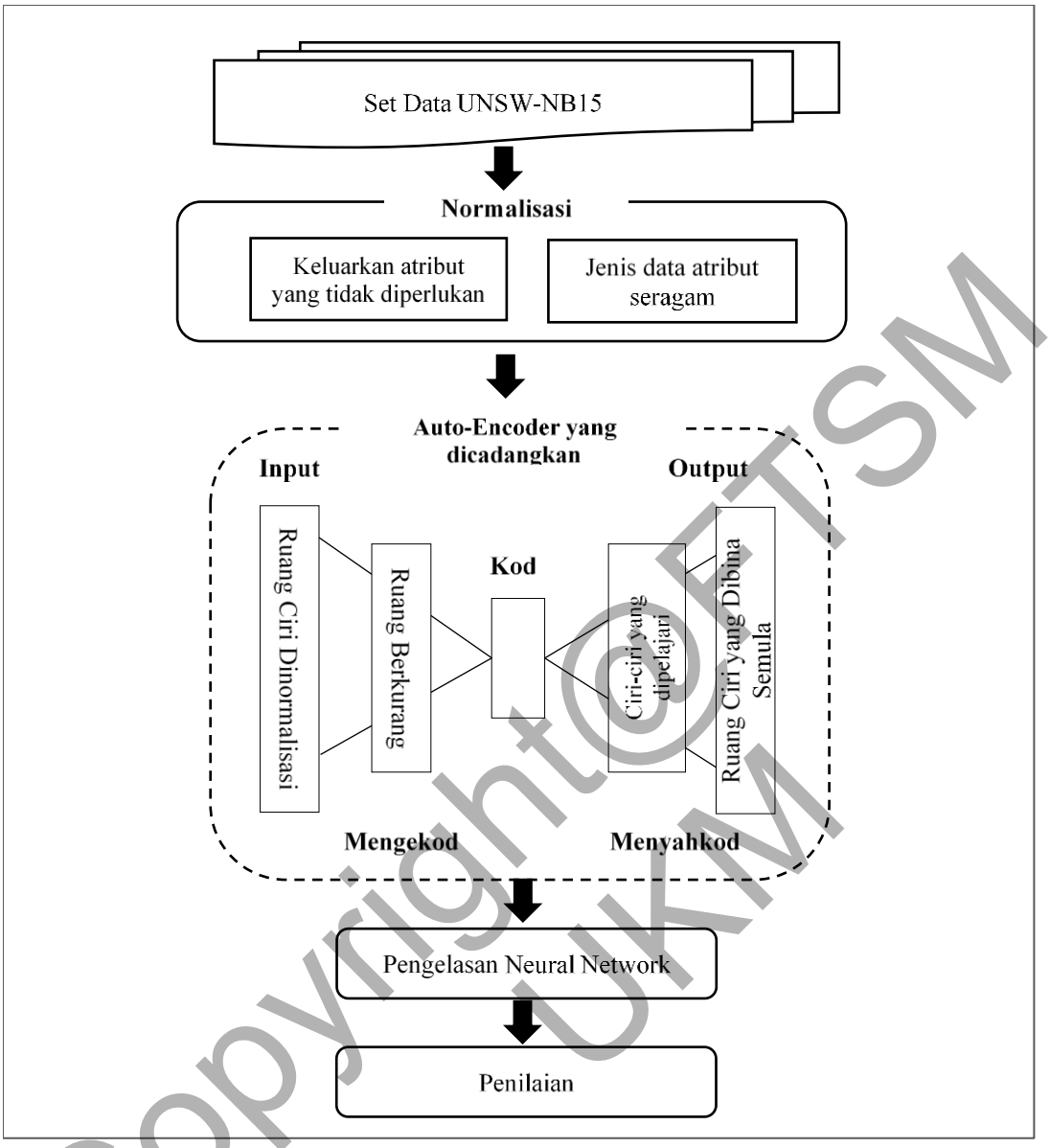
Dalam hal yang sama, [11] telah mengusulkan kombinasi algoritma Artificial Bee Colony (ABC) dan Artificial Fish Swarm (AFS) untuk menampung tugas pemilihan ciri holistik pada pengesanan pencerobohan IoT. Penulis telah memanfaatkan dua algoritma tersebut untuk mencari penyelesaian terbaik untuk ciri. Akhirnya, pengkelasan CART Association Rule telah digunakan untuk mengklasifikasikan pencerobohan berdasarkan ciri yang dipilih. Set data UNSW-NB15 telah digunakan dalam eksperimen dengan ketepatan purata 85% dengan FAR 14.9.

Sebaliknya, sebilangan pengarang telah menggunakan pendekatan pemilihan ciri untuk meningkatkan pengkelasan mereka sendiri dalam pengesanan pencerobohan IoT. Sebagai contoh, Tama & Rhee [12] telah mencadangkan algoritma carian grid untuk mencari parameter pengkelasan terbaik. Setiap pengkelasan mempunyai parameternya, dan kadang-kala, tidak mudah untuk memeriksa setiap parameter secara individu. Oleh itu, carian grid yang dicadangkan telah digunakan untuk mengenal pasti parameter terbaik untuk tiga pengklasifikasi, termasuk Neural Network, Support Vector Machine, dan pengelasan Fuzzy. Hasil kajian menunjukkan bahawa carian grid yang dicadangkan telah meningkatkan semua pengklasifikasi di mana gabungan pencarian grid dan Neural Network mendapat ketepatan tertinggi pada set data UNSW-NB15, di mana purata ketepatan adalah 82.6% dengan FAR 16.2.

Selanjutnya, [5] telah mengusulkan kaedah linear untuk pemilihan ciri, yang disebut Recursive Feature Elimination (RFE), untuk pengesanan pencerobohan IoT. Kaedah yang dicadangkan akan secara automatik membahagikan ruang ciri menjadi subset yang jauh lebih kecil dan menilai setiap ciri secara berulang. Set data UNSW-NB15 telah digunakan dalam eksperimen, dan purata ketepatan yang diperoleh adalah 97%, dengan FAR 7.8.

4.2 Kaedah Penyelidikan

Reka bentuk kajian ini terdiri daripada empat peringkat. Tahap pertama menangani perincian kumpulan data di mana penerangan lengkap diberikan untuk set data tersebut. Tahap kedua bertujuan untuk menampung tugas pra-pemprosesan yang bertujuan untuk membuang data yang tidak perlu dan mengubah data menjadi format yang sesuai. Tahap ketiga bertujuan untuk menerapkan Algoritma Genetik yang asli dan Algoritma Genetik dipertingkatkan yang dicadangkan untuk membuat pemilihan ciri. Peringkat akhir bertujuan untuk menerapkan pengelasan Decision Tree berdasarkan subset terbaik yang dihasilkan oleh GA. Setiap tahap reka bentuk kajian digambarkan dalam Rajah 2.



Rajah 2 Kerangka kaedah yang dicadangkan

4.3 Set Data UNSW-NB15

Cabaran utama dalam sistem pengesanan pencerobohan terletak pada ketersediaan sejarah data yang menerangkan ciri-ciri pencerobohan. Beberapa set data telah dicadangkan untuk tujuan ini, termasuk KDD-CUP99 [15] dan NSL-KDD [16]. Walaupun demikian, evolusi besar teknologi rangkaian telah memudahkan munculnya serangan dan ancaman baru. Oleh itu, kedua-dua KDD-CUP99 dan NSL-KDD nampaknya sudah usang. Oleh itu, kajian ini akan mengkaji set data terbaru yang dikenali sebagai UNSW-NB15 [17]. Apa yang dapat membezakan kumpulan data ini dari yang sebelumnya ialah UNSW-NB15 mengandungi ancaman dan serangan baru seperti Shellcode

yang bertujuan untuk mengeksploitasi perisian tertentu dalam rangkaian tertentu. Jadual 1 menerangkan kelas connection di UNSW-NB15.

Tahap ini bertujuan untuk menggunakan set data penanda aras UNSW-NB15. Tidak seperti set data sebelumnya pengesanan pencerobohan seperti KDD-CUP99 dan NSL-KDD, di mana simulasi dijalankan menggunakan rangkaian tradisional, set data UNSW-NB15 adalah simulasi untuk kedua-dua connection normal dan pencerobohan yang mungkin menyasarkan rangkaian moden seperti Rangkaian Sensor Tanpa Wayar (WSN) dan Internet Pelbagai Benda (IoT) [18]. Perbezaan utama antara set data ini dari yang sebelumnya terletak pada ancaman dan serangan baru yang telah diperkenalkan, seperti Shellcode yang bertujuan untuk mengeksploitasi perisian tertentu dalam rangkaian tertentu. Jadual 1 dan Jadual 2 menunjukkan kelas (contoh, serangan) dan jenis ciri yang telah digambarkan dalam set data.

Jadual 1. Kelas dan serangan set data UNSW-NB15

No.	Serangan/Kelas	Penerangan
1.	Fuzzers	Menyasarkan rangkaian dengan data yang dihasilkan secara rawak
2.	Analysis	Dikaitkan dengan pengimbasan dan penyiasatan serangan
3.	Backdoors	Mencari kelemahan dalam rangkaian
4.	DoS	Eksploitasi sumber rangkaian
5.	Exploits	Mencari kelemahan dalam sistem operasi
6.	Generic	Serangan yang berkaitan dengan cipher blok dan kuncinya
7.	Reconnaissance	Serangan yang bertujuan untuk mengumpulkan maklumat
8.	Shellcode	Memanfaatkan spesifik perisian dalam rangkaian
9.	Worms	Meniru dirinya untuk menyebarkan di dalam komputer rangkaian
10.	Normal	Legitimate connections

Jadual 2. Penerangan ciri UNSW-NB15

Jenis Ciri	Kuantiti	Penerangan
Ciri Aliran	5	Ciri-ciri yang berkaitan dengan perincian IP dan Port
Ciri-ciri Asas	13	Ciri-ciri yang berkaitan dengan protokol dan perkhidmatan yang digunakan oleh connection
Ciri Kandungan	8	Ciri-ciri yang berkaitan dengan ukuran paket yang dihantar dan diterima
Ciri Masa	9	Ciri-ciri yang berkaitan dengan selang masa connection
Ciri-ciri Connection	8	Ciri-ciri yang berkaitan dengan sesi connection
Jumlah	43	

Seperti yang ditunjukkan dalam Jadual 2, UNSW-NB15 mengandungi lima jenis ciri. Jenis pertama adalah ciri aliran, di mana ciri-ciri IP dan port sedang diperiksa. Sebagai tambahan, jenis

kedua adalah ciri asas yang berkaitan dengan protokol dan perkhidmatan yang digunakan oleh connection. Jenis ketiga adalah ciri kandungan yang berkaitan dengan saiz paket yang dihantar dan diterima. Jenis keempat adalah ciri masa yang berkaitan dengan selang waktu connection. Akhirnya, jenis kelima adalah ciri connection yang berkaitan dengan perincian sesi connection. Jadual 3 menunjukkan statistik umum kumpulan data UNSW-NB15.

Jadual 3. Statistik UNSW-NB15

Atribut	Perincian
Jumlah Connections	257,673
Nombor connection latihan	175,341
Nombor connection ujian	82,332
Bilangan ciri	43
Bilangan serangan	9
Bilangan kelas	10 (9 serangan dengan 1 kelas Normal)

4.4 Pra-pemprosesan

Tidak seperti set data lama seperti KDD-CUP99 atau NSL-KDD, di mana banyak data noisy terletak bersama dengan rekod berlebihan, set data UNSW-NB15 telah dirancang dengan teliti. Namun, masih terdapat beberapa masalah yang perlu ditangani dalam set data tersebut. Oleh itu, bahagian ini bertujuan untuk mengkaji isu-isu ini. Jadual 4 menunjukkan contoh connection dari set data.

Jadual 4 Contoh connection dari set data UNSW-NB15

ID Connection	Protokol	Perkhidmatan	Tempoh	….	Kelas	Kelas (Binari)
1	TCP	FTP	0.121478		Normal	0
2	TCP	HTTP	0.649902		Normal	0
3	UDP	HTTP	1.623129		Exploits	1
4	TCP	HTTP	1.681642		Normal	0
5	UDP	FTP	0.449454		DoS	1

Seperti yang ditunjukkan dalam Jadual 4, beberapa connection dibawa dari set data. Pemerhatian pertama akan mendedahkan pelbagai ciri untuk setiap connection, misalnya, ID connection tersebut, protokolnya, perkhidmatannya, dan jangka masa connection. Terakhir, terdapat lajur untuk label kelas di mana connection dikategorikan menjadi 'normal' atau kelas pencerobohan seperti 'eksploitasi' atau 'DoS.' Atribut lain yang berkaitan dengan kelas juga terdapat, iaitu 'Kelas Binari'. Atribut tersebut hanya mengandungi dua nilai, sama ada' 0 'untuk connection biasa atau' 1 'untuk kelas pencerobohan. Sekarang, beberapa atribut tidak diperlukan dalam proses pembelajaran mesin, seperti ID di mana ID tidak dapat menunjukkan status connection apa pun. Di samping itu, jenis data dalam ciri berbeza. Ini dapat menghalang

pembelajaran mesin daripada memperoleh latihan yang baik mengenai ciri-ciri tersebut. Oleh itu, beberapa tugas normalisasi diperlukan.

Tugas pertama bertujuan untuk menyaring atribut. Beberapa atribut tidak mempunyai kepentingan dalam mengenal pasti status connection. Sebagai contoh, atribut pertama adalah ID, di mana nombor pengenalan connection tidak akan mempunyai kepentingan dalam menentukan status connection. Selain itu, atribut 'Binary class' juga tidak perlu kerana hanya mempunyai nilai binari (0 untuk connection biasa dan 1 untuk pencerobohan). Untuk melatih pembelajaran mesin dengan secukupnya, semua kelas harus digunakan. Oleh itu, sifat-sifat yang disebutkan di atas mesti dikeluarkan. Jadual 5 menggambarkan membuang atribut yang tidak diperlukan.

Jadual 5 Mengeluarkan atribut yang tidak perlu

ID Connection	**Protokol**	**Perkhidmatan**	**Tempoh**	**….**	**Kelas**	**Kelas (Binari)**
1	TCP	FTP	0.121478		Normal	0
2	TCP	HTTP	0.649902		Normal	0
3	UDP	HTTP	1.623129		Exploits	1
4	TCP	HTTP	1.681642		Normal	0
5	UDP	FTP	0.449454		DoS	1

Perhatikan bahawa jumlah ciri setelah membuang atribut yang tidak diperlukan adalah 43, bersama dengan satu atribut untuk label kelas. Tugas kedua adalah transformasi atribut. Ciri-ciri tersebut mengandungi jenis data di mana beberapa atribut terdiri dari nilai angka (mis., 0.12), sementara atribut lain terdiri dari nilai nominal (mis. 'FTP' dan 'TCP'). Untuk pembelajaran ciri yang mencukupi dalam MLT, penting untuk mengubah atribut. Dalam hal ini, pendekatan one-hot encoding digunakan untuk mengubah nilai nominal menjadi angka [19]. Jadual 6 menunjukkan contoh penggunaan one-hot encoding pada data dalam Jadual 5.

Jadual 6. Contoh penggunaan one-hot encoding

Protokol_TCP	Protokol_UDP	Perkhidmatan_FTP	Perkhidmatan_HTTP	Tempoh	….	Kelas
1	0	1	0	0.121478		Normal
1	0	0	1	0.649902		Normal
0	1	0	1	1.623129		Exploits
1	0	0	1	1.681642		Normal
0	1	1	0	0.449454		DoS

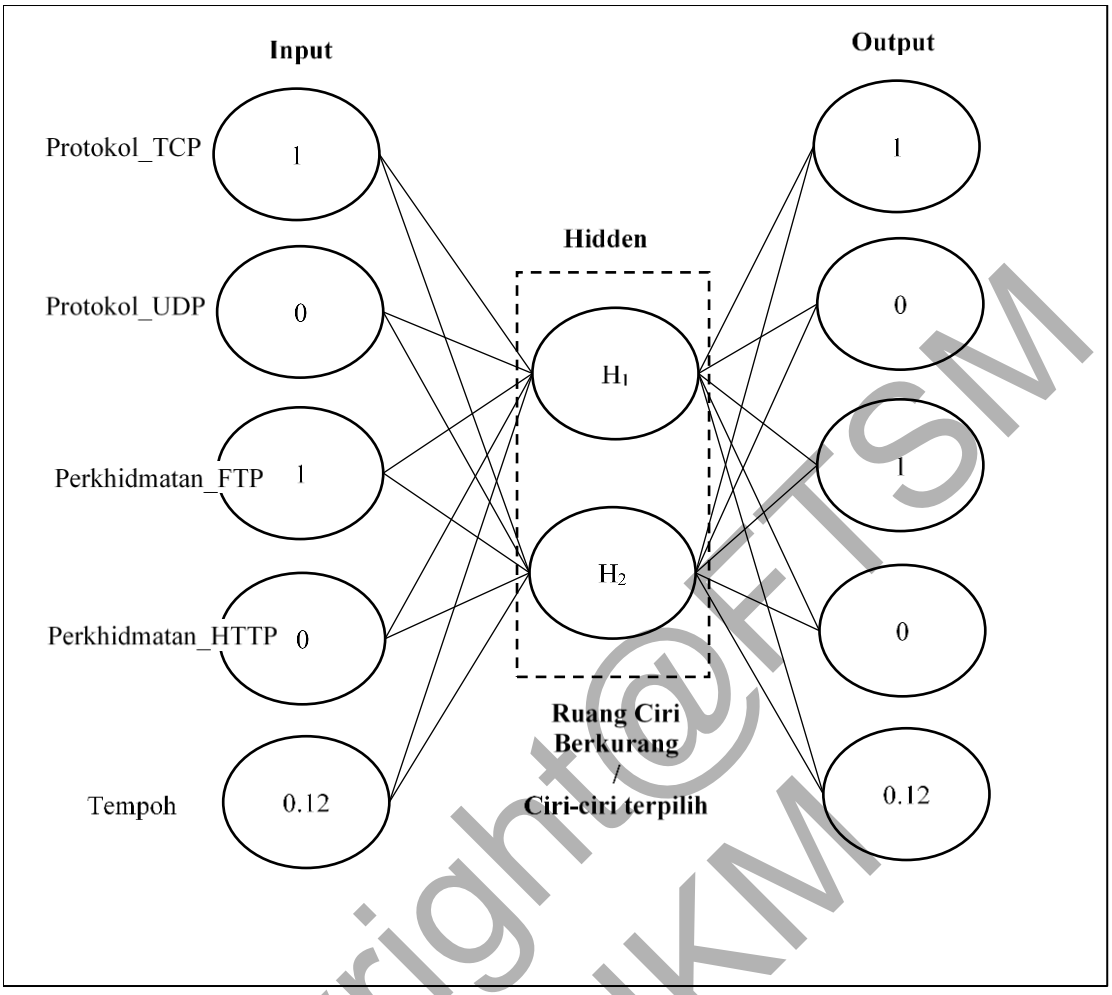
Seperti yang ditunjukkan dalam Jadual 6, one-hot encoding dimaksudkan untuk memeriksa semua kemungkinan nilai dalam atribut nominal dan kemudian mengubah nilai ini menjadi atribut bebas/tambahan. Contohnya, atribut ‘Protocol’ mengandungi dua nilai, termasuk ‘TCP’ dan ‘UDP’; oleh itu, atribut telah dibahagikan kepada dua atribut, termasuk 'Protocol_TCP' dan 'Protocol_UDP.' Setelah atribut nominal dibahagi berdasarkan nilainya, nilai pemadanan akan diisi dengan '1' sementara tiada pemadanan akan ditunjukkan sebagai ' 0 '. Dengan cara ini, jenis data semua atribut akan disatukan menjadi nilai angka. Perhatikan bahawa, setelah membahagikan atribut nominal, jumlah ciri meningkat menjadi 196 atribut.

4.5 Auto-Encoder (AE)

Auto-Encoder adalah salah satu seni bina Neural Network yang diperiksa dari segi pemilihan ciri. Sebarang NN akan mempunyai tiga lapisan utama, termasuk input, hidden, dan output. Input adalah lapisan yang mengambil ciri connection, sedangkan lapisan output akan mewakili label kelas connection. Walau bagaimanapun, lapisan hidden adalah bahagian dari NN di mana ciri-ciri tersebut dianalisis untuk mencari hubungan yang mendalam di antara mereka. Sebaliknya, tujuan utama di sebalik AE adalah mempelajari representasi yang dikompres dan diedarkan dari data yang diberikan [20]. Dengan kata lain, AE bertujuan untuk memproses data sebagai input dan output data yang sama itu sendiri. Sebagai contoh, anggap baris ciri dari sampel dalam Jadual 6 seperti berikut:

Protokol_TCP	Protokol_UDP	Perkhidmatan_FTP	Perkhidmatan_HTTP	Tempoh
1	0	1	0	0.121478

Seterusnya, AE akan memproses baris ciri tersebut di mana inputnya akan menjadi ciri dan outputnya adalah ciri yang sama seperti yang ditunjukkan pada Rajah 3.



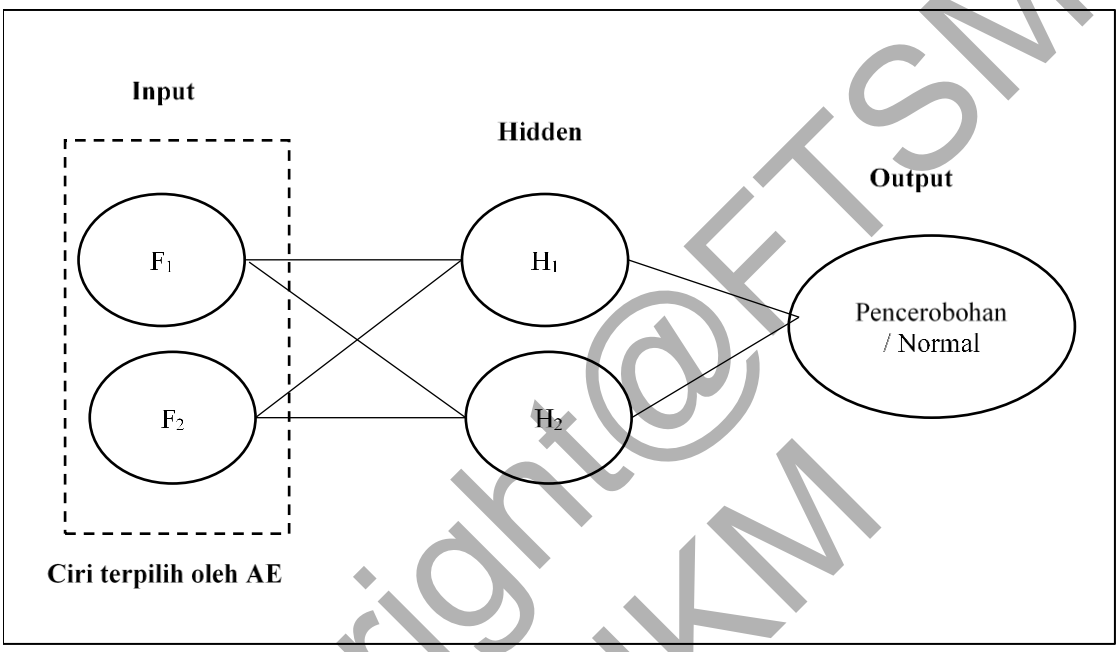
Rajah 3 Pemilihan ciri melalui seni bina AE

Seperti yang ditunjukkan pada Rajah 3, input AE adalah ciri-ciri connection, sedangkan outputnya adalah nilai-nilai yang sama dengan ciri tersebut. Lapisan pertama juga dikenali sebagai pengekodan dalam AE, di mana data sedang dikodkan hingga mendapatkan pengekodan dan kemudian menyahkod data.

Untuk memahami mekanisme seperti itu, pemberat input akan dimulai dengan nilai rawak, dan kemudian yang hidden akan dihitung. Selepas itu, pemberat hidden akan dimulakan dengan nilai rawak untuk mengira output. Kemudian, setelah mempertimbangkan fungsi pengaktifan, output yang diramalkan akan dibandingkan dengan output sebenar untuk mengira ralat. Sekiranya terdapat ralat, Backpropagation akan mengurangkan kadar ralat sehingga output yang diramalkan sesuai dengan output yang sebenarnya. Setelah ralat dikurangkan menjadi sifar di mana output terdahulu sama dengan output sebenar, nilai neuron hidden akan dianggap sebagai ruang ciri yang dipilih dan dikurangkan, seperti yang ditunjukkan pada Rajah 3.

4.6 Pengelasan Neural Network (NN)

Setelah memperoleh ciri-ciri yang dipilih oleh AE yang dicadangkan, simple NN akan digunakan untuk mengklasifikasikan hubungan menjadi pencerobohan dan normal. Seperti yang ditunjukkan dalam Rajah 4, input dari NN ini adalah sekumpulan ciri terpilih dihasilkan oleh AE yang dicadangkan. Dalam Rajah 4, F1 dan F2 merujuk kepada ciri-ciri terpilih yang dihasilkan oleh seni bina AE. Dengan kata lain, ciri-ciri ini adalah nilai nod hidden di AE setelah melatihnya secara meluas.



Rajah 4 Pengelasan menggunakan NN

5 HASIL KAJIAN

Oleh kerana kajian ini menggunakan Neural Network sebagai klasifikasi dan Auto-Encoder sebagai pemilihan ciri, yang juga merupakan Neural Network, ada banyak parameter yang harus ditentukan. Berikut subseksyen akan menunjukkan tetapan percubaan bersama hasilnya.

5.1 Tetapan Eksperimen

Oleh kerana kedua-dua input dan output AE mengartikulasikan ciri-ciri connection dengan demikian, panjangnya sama dengan jumlah ciri. Seperti yang telah disebutkan sebelumnya, jumlah ciri dalam set data UNSW-NB15 adalah 43. Walau bagaimanapun, kajian ini telah menggunakan one-hot encoding untuk mengubah atribut. Oleh itu, bilangan atribut telah meningkat menjadi 196. Oleh itu, kedua-dua lapisan input dan output mempunyai 196 neuron.

Sebaliknya, lapisan hidden yang digunakan dalam kajian ini adalah lapisan tunggal dengan saiz neuron yang berbeza. Lapisan hidden AE dianggap sebagai dimensi ciri yang dikurangkan. Oleh itu, adalah perlu untuk memeriksa bilangan neuron hidden yang berbeza. Jadual 7 menggambarkan perincian tiga lapisan.

Jadual 7 Perincian seni bina AE

Lapisan AE	**Saiz**	**Perincian**
Lapisan Input	196	Panjang ciri connection dalam set data UNSW-NB15
Lapisan Hidden	4, 5, 10, 20, dan 30	Mengeksperimen
Lapisan Output	196	Panjang ciri connection dalam set data UNSW-NB15

Seperti yang ditunjukkan dalam Jadual 7, ukuran lapisan hidden telah ditetapkan ke nilai yang berbeza untuk mengeksperimen hasil yang paling tepat. Cara memilih nilai ini terletak pada pemilihan dimensi yang lebih rendah. Disarankan untuk setiap tugas pemilihan ciri untuk memeriksa jumlah ciri yang turun keempat atau kelima kali keseluruhan ruang ciri. Oleh kerana ruang ciri dalam kajian adalah 196, eksperimen telah dimulakan dengan 30 bilangan ciri. Ini diikuti oleh tugas menurun untuk memeriksa dimensi ciri yang lebih rendah termasuk 20 dan 10. Akhirnya, untuk kedua-dua 4 dan 5 bilangan ciri, disarankan oleh kajian bahawa AE bekerja dengan lebih baik bersama bilangan kecil untuk ukuran lapisan hidden.

Tidak seperti teknik pemilihan ciri tradisional di mana outputnya adalah sekumpulan ciri, ciri-ciri yang dipilih dalam AE mempunyai bentuk yang berbeza. Sama dengan Analisis Komponen Prinsip (PCA), AE akan meringkaskan ciri dengan dimensi yang lebih rendah menggunakan nilai matematik. Nilai-nilai ini digambarkan dalam nod hidden AE dan dapat merangkum atau menggeneralisasi ruang ciri.

Setelah AE yang dicadangkan menghasilkan ciri terbaik, simple NN yang lain akan digunakan untuk mengklasifikasikan hubungan menjadi pencerobohan dan bukan pencerobohan. NN seperti itu akan mempunyai tiga lapisan termasuk input, hidden dan output. Input dipertimbangkan untuk ciri-ciri terpilih yang dihasilkan oleh AE, sedangkan outputnya adalah label kelas sama ada connectionnya adalah pencerobohan atau bukan pencerobohan. Lapisan hidden di sini akan mewakili langkah pembelajaran ciri di mana ciri dari lapisan input sedang dipelajari. Ukuran lapisan input hanya setara dengan ukuran lapisan hidden di AE, sementara ukuran lapisan output hanyalah jumlah label kelas yang 10. Namun, untuk ukuran lapisan hidden, ada pendekatan yang berbeza untuk mendapatkan saiz. Kajian ini telah menggunakan pendekatan purata input dan output yang dapat dihitung sebagai berikut (Liu & Xu 2018):

$$saiz\ hidden = \frac{saiz\ input\ + saiz\ output}{2} \quad (1)$$

Jadual 8 mewakili ukuran tiga lapisan yang digunakan oleh NN.

Jadual 8 Perincian seni bina klasifikasi NN

Lapisan NN	Saiz	Perincian
Lapisan Input	4, 5, 10, 20, dan 30	Saiz lapisan hidden AE
Lapisan Hidden	Input + output / 2	Purata min antara saiz input dan saiz output
Lapisan Output	10	Bilangan label kelas

Setelah menentukan panjang setiap lapisan dalam AE dan NN, penting untuk menyebut fungsi pengaktifan yang digunakan oleh kedua-dua seni bina. Fungsi pengaktifan yang digunakan oleh AE adalah Rectified Linear Units (Relu) yang dapat dikira sebagai berikut:

$$Relu(x) = \max(0, x) \begin{cases} if\ x < 0 & 0 \\ if\ x \geq 0 & x, \end{cases} \quad (2)$$

Menurut Krizhevsky et al. (2012), Relu mempunyai prestasi luar biasa dengan seni bina pembelajaran mendalam. Oleh itu, ia telah digunakan dengan AE yang dicadangkan. Sebaliknya, klasifikasi NN telah menggunakan Logistic Sigmoid yang dapat dikira sebagai berikut:

$$Sigmoid(x) = \frac{1}{1+e^{-x}}, \quad (3)$$

Parameter terakhir yang berkaitan dengan seni bina Neural Network adalah bilangan epoch. Sebenarnya, epoch adalah iterasi yang diperlukan untuk menampung penyelewengan ralat dengan mengubah nilai pemberat untuk mengurangkan kadar ralat. Jadual 9 menunjukkan bilangan epochs.

Jadual 9 Bilangan epoch untuk setiap seni bina Neural Network

Seni Bina	Jumlah Epochs
AE	Mengeksperimen (100 – 1000)
NN	1

Sebenarnya, menentukan jumlah epoch adalah masalah yang mencabar. Ini adalah kesepakatan umum bahawa memilih sebilangan besar epoch akan menghasilkan hasil ketepatan

yang lebih baik. Ini kerana semakin banyak masa akan menyumbang untuk meminimumkan kadar ralat yang secara langsung meningkatkan ketepatan. Walau bagaimanapun, untuk mendapatkan prestasi yang cekap, lebih baik mendapatkan ketepatan tinggi sebanyak mungkin dengan menggunakan bilangan epoch minimum.

Sehubungan dengan itu, kajian ini telah menggunakan nilai yang berbeza untuk bilangan epoch untuk AE yang dicadangkan (iaitu dari 100 iterations hingga 1000). Namun, untuk klasifikasi NN, hanya satu epoch yang dipilih. Sebab di sebalik itu adalah bahawa AE akan melatih data secara meluas untuk menghasilkan sub-set ciri yang paling tepat. Oleh itu, tidak perlu latihan yang exhausted dilakukan pada klasifikasi NN.

Sebaliknya, penilaian akan dibuat berdasarkan Ketepatan dan Kadar Penggera Palsu (FAR). Ketepatan merujuk kepada connection yang dikelaskan dengan betul sehubungan dengan semua connection dan dikira seperti berikut:

$$Ketepatan = \frac{TP + TN}{Jumlah\ connections} \tag{4}$$

di mana TP dan TN adalah contoh gangguan dan hubungan normal yang dikelaskan dengan betul. Sementara, FAR merujuk kepada nisbah connection yang tidak diklasifikasikan dengan betul untuk semua connection yang dapat dikira sebagai berikut:

$$Kadar\ Penggera\ Palsu\ (FAR) = \frac{FP}{Jumlah\ connections} \tag{5}$$

di mana FP adalah bilangan connection yang dikelaskan secara tidak betul.

5.2 Penyiasatan Umum untuk Nombor Ciri

Sebelum menerapkan AE yang dicadangkan, perlu memulai strategi untuk memilih jumlah ciri yang diperlukan (iaitu ukuran hidden AE). Oleh kerana panjang lapisan input dan output adalah 196, maka saiz hidden, atau ruang ciri yang dikurangkan, mestilah kurang dari 196. Oleh itu, terdapat banyak kebarangkalian untuk dipilih (iaitu dari 1 hingga 196). Dalam hal ini, bahagian ini akan menampung penyelidikan umum di mana tiga bilangan ciri digunakan untuk menyoroti persembahan. Setelah mengkaji nombor ciri ini, hasil ketepatan dan FAR akan menyumbang sama ada untuk menambah atau mengurangkan bilangan ciri. Untuk tujuan ini, bilangan ciri telah ditetapkan kepada 10, 20 dan 30.

Jadual 10. Hasil sebilangan besar ciri

No. Epoch	Ciri = 30		Ciri = 20		Ciri = 10	
	Ketepatan	**FAR**	**Ketepatan**	**FAR**	**Ketepatan**	**FAR**
100	0.9994	0.06	0.9999	0.0	0.8251	17.49
200	0.9999	0.0	0.9298	7.01	0.9987	0.12
400	**0.9999**	0.0	0.9999	0.0	0.7258	27.41
600	0.9478	5.22	0.9985	0.14	**0.9992**	0.08
800	0.9944	0.55	**0.9999**	0.0	0.9930	0.69
1000	0.9998	0.01	0.9998	0.02	0.8283	17.17

Seperti yang ditunjukkan dalam Jadual 10, ketepatan untuk tiga nombor ciri telah meningkat seiring bertambahnya jumlah epochs. Walau bagaimanapun, ketepatan tertinggi digambarkan oleh 20 bilangan ciri di mana ketepatannya adalah 99.99%. Seperti yang ditunjukkan dalam Jadual 10, semua ciri angka menunjukkan kadar FAR yang serupa di mana nilainya telah menurun ketika jumlah epochs meningkat di mana nilai minimum FAR adalah 0.0. Ini dapat menunjukkan bahawa bilangan ciri terbaik yang dipilih adalah 20, di mana ia mempunyai ketepatan tertinggi. Oleh itu, pilihan terbaik adalah mengkaji dimensi ciri yang lebih rendah. Oleh itu, bahagian seterusnya akan menggambarkan pemeriksaan tersebut.

5.3 Menspesifikasikan Nombor Ciri

Seperti yang ditunjukkan pada bahagian sebelumnya, jumlah ciri terendah menunjukkan ketepatan terbaik. Oleh itu, bahagian ini akan mengkaji beberapa ciri yang kurang daripada 10. Jadual 11 menunjukkan hasilnya.

Jadual 11 Hasil bilangan ciri yang lebih rendah

No. Epoch	Ciri = 5		Ciri = 4	
	Ketepatan	**FAR**	**Ketepatan**	**FAR**

100	0.8898	11.02	0.9999	0.0
200	**0.9999**	0.0	0.3173	68.26
400	0.9935	0.64	0.5800	41.91
600	0.9086	9.13	0.3671	63.29
800	0.7303	26.96	**0.9999**	0.0
1000	0.8716	12.83	0.6096	39.04

Seperti yang ditunjukkan pada Jadual 11, ketika jumlah ciri adalah 4, ketepatan telah mencapai 99.99% bagi epoch 800 manakala dibandingkan dengan ketepatan maksimum yang diperoleh ketika jumlah ciri adalah 5 iaitu 99.99% bagi epoch 200. Ini dapat membuktikan bahawa 4 bilangan ciri adalah pengurangan paling tepat dari ciri yang dihasilkan oleh AE. Maka, data yang dominan bagi bilangan ciri 4 adalah ‘attack_cat’, ‘dur’, ‘proto’ dan ‘service’. Akhirnya, untuk FAR, kedua-dua bilangan ciri menunjukkan prestasi yang serupa di mana nilai minimum FAR adalah 0.0.

Membandingkan hasil terbaik dicapai oleh AE yang dicadangkan, mempunyai 4 ciri dengan kajian yang berkaitan adalah diperlukan. Sebagai contoh, [13] telah memperoleh ketepatan 93.25% dengan FAR 8.6 menggunakan GA asal dengan pengkelasan DT. Serta, [10] memperoleh ketepatan 84.33% dengan FAR 8.9 menggunakan GA dengan DT. Akhirnya, [5] telah memperoleh ketepatan 97% dengan FAR 7.8. Kaedah yang dicadangkan telah mengungguli semua kerja yang berkaitan dari segi ketepatan dan FAR. Perlu disebutkan bahawa sebahagian besar kajian yang berkaitan berdasarkan teknik pemilihan ciri atau statistik yang diilhamkan oleh bio. Oleh kerana kaedah yang dicadangkan adalah pemilihan ciri berdasarkan Neural Network, dapat diperhatikan bahawa seni bina pembelajaran mendalam mengungguli teknik pemilihan ciri tradisional.

6 KESIMPULAN

Kajian ini telah berjaya mencadangkan dan melaksanakan AE untuk tugas pemilihan ciri dalam pengesanan pencerobohan IoT. Kebaharuan kajian ini ditunjukkan dalam memeriksa pemilihan ciri berasaskan NN daripada teknik pemilihan ciri tradisional yang diilhamkan oleh bio. Hasil penerapan AE menunjukkan peningkatan dalam ketepatan dan FAR di mana ketepatan telah meningkat dibandingkan dengan keadaan canggih, sementara FAR telah dikurangkan. Mengeksperimen dengan tetapan parameter yang berbeza untuk AE, seperti lapisan hidden, neuron hidden, dan fungsi pengaktifan akan menunjukkan peningkatan dalam penyelidikan masa depan.

7 RUJUKAN

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics,* vol. 10, no. 4, pp. 2233-2243, 2014.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials,* vol. 17, no. 4, pp. 2347-2376, 2015.

[3] B. M. Eskofier, S. I. Lee, M. Baron, A. Simon, C. F. Martindale, H. Gaßner, and J. Klucken, "An Overview of Smart Shoes in the Internet of Health Things: Gait and Mobility Assessment in Health Promotion and Disease Monitoring," *Applied Sciences,* vol. 7, no. 10, pp. 986, 2017.

[4] M. N. Magableh, and B. Alshaikhdeeb, "A Comparative Study of Encryption Methods for Cloud Query Processing," *Journal of Computer Science,* vol. 15, no. 11, pp. 1585-1594, 2019.

[5] I. Ullah, and Q. H. Mahmoud, "A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks." pp. 1-6.

[6] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 686-728, 2019.

[7] B. Alshaikhdeeb, and K. Ahmad, "Integrating correlation clustering and agglomerative hierarchical clustering for holistic schema matching," *Journal of Computer Science,* vol. 11, no. 3, pp. 484-489, 2015.

[8] D. G. Mogal, S. R. Ghungrad, and B. B. Bhusare, "NIDS using machine learning classifiers on UNSW-NB15 and KDDCUP99 datasets," *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE),* vol. 6, no. 4, pp. 533-537, 2017.

[9] N. Moustafa, and J. Slay, "A hybrid feature selection for network intrusion detection systems: Central points," *arXiv preprint arXiv:1707.05505,* 2017.

[10] D. Papamartzivanos, F. Gómez Mármol, and G. Kambourakis, "Dendron : Genetic trees driven rule induction for network intrusion detection systems," *Future Generation Computer Systems,* vol. 79, pp. 558-574, 2018/02/01/, 2018.

[11] V. Hajisalem, and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," *Computer Networks,* vol. 136, pp. 37-50, 2018/05/08/, 2018.

[12] B. A. Tama, and K.-H. Rhee, "An in-depth experimental study of anomaly detection using gradient boosted machine," *Neural Computing and Applications,* vol. 31, no. 4, pp. 955-965, 2019/04/01, 2019.

[13] H. Gharaee, and H. Hosseinvand, "A new feature selection IDS based on genetic algorithm and SVM." pp. 139-144.

[14] C. Khammassi, and S. Krichen, "A GA-LR wrapper approach for feature selection in network intrusion detection," *Computers & Security,* vol. 70, pp. 255-277, 2017/09/01/, 2017.

[15] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set." pp. 1-6.

[16] S. Revathi, and A. Malathi, "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection," *International Journal of Engineering Research and Technology. ESRSA Publications*, 2013.

[17] N. Moustafa, and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." pp. 1-6.

[18] S. Hanif, T. Ilyas, and M. Zeeshan, "Intrusion Detection In IoT Using Artificial Neural Networks On UNSW-15 Dataset." pp. 152-156.

[19] C. Seger, "An investigation of categorical variable encoding techniques in machine learning: binary versus one-hot and feature hashing," 2018.

[20] S. N. Mighan, and M. Kahani, "Deep Learning Based Latent Feature Extraction for Intrusion Detection." pp. 1511-1516.

[21] M. Luo, F. Nie, X. Chang, Y. Yang, A. G. Hauptmann, and Q. Zheng, "Adaptive unsupervised feature selection with structure regularization," *IEEE transactions on neural networks and learning systems,* vol. 29, no. 4, pp. 944-956, 2017.

[22] C. Zhang, Y. Liu, and H. Fu, "AE2-Nets: Autoencoder in Autoencoder Networks." pp. 2577-2585.

[23] X. Liu, and L. Xu, "The universal consistency of extreme learning machine," *Neurocomputing,* vol. 311, pp. 176-182, 2018/10/15/, 2018.

[24] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks." pp. 1097-1105.

[25] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 1, pp. 184-208, 2016.