Teknik Deteksi Spam Efisien untuk Perangkat IoT berbasis Pembelajaran Mesin

Muchammad Daniyal Kautsar
Departemen Teknik Elektro Teknologi Informasi
Fakultas Teknik
Universitas Gadjah Mada
Sleman, Indonesia
muchammad.daniyal.kautsar@mail.ugm.ac.id

***Abstract*—Internet of Things (IoT)* terus berkembang dan semakin dibutuhkan oleh masyarakat luas. Kebutuhan akan *IoT* perlahan mulai memasuki aspek-aspek mendasar di kehidupan manusia. Beragam perangkat berbeda saling terhubung satu dengan lainnya. Beragam manusia dengan kebiasaannya masing-masing mempengaruhi bagaimana perangkat tersebut bekerja. Pengamanan sistem untuk menjaga privasi pengguna bergantung dengan banyak aspek. Beragam ancaman terus bermunculan. Dengan berkembangnya metode-metode pembelajaran mesin, terjadi peningkatan keamanan perangkat *IoT*. Dengan menggunakan lima model pembelajaran mesin untuk melakukan deteksi spam dan membandingkan kelimanya terhadap beberapa perangkat *IoT* melalui skor spam untuk mengetahui model mana yang paling optimal berdasarkan kondisi tertentu.**

Keywords—Internet of Things, keamanan, pembelajaran mesin, deteksi spam

I. PENDAHULUAN

Internet of Things (IoT) memungkinkan terjadinya integrasi antara banyak obyek di dunia nyata tanpa batas ruang dan waktu. Integrasi tersebut terjadi dengan implementasi jaringan yang mana membutuhkan kontrol dan managemen perlindungan keamanan privasi yang baik dalam lingkungan seperti itu. Sistem *IoT* perlu melakukan perlindungan data untuk menjaga keamanan sistem misalnya dari intrusi, serangan sproofing, serangan DDoS, spam, malware, dan serangan cyber lain.

Pengamanan sistem *IoT* bergantung dari ukuran, jenis, lokasi, bentuk penggunaan, kebiasaan pengguna, ataupun kompleksitas sistem itu diaplikasikan. Kebiasaan pengguna juga memberikan pengaruh terhadap bagaimana sistem itu diamankan. Misalnya pada penggunaan *wearable devices* dimana perangkat tersebut akan mengirimkan data kesehatan pengguna ke *smartphone* pengguna dan penyimpaan awan yang mana perlu dipastikan keamanan datanya agar dapat menjaga privasi penggunanya. Selain itu, sekitar 25-30% karyawan yang bekerja menghubungan perangkat *IoT* pribadi mereka dengan jaringan kantor atau organisasi dimana mereka bekerja. Perkembangan dan semakin meluasnya penggunaan *IoT* juga mebuka celah untuk serangan *cyber*.

Dengan semakin berkembangnya Pembelajaran Mesin *(Machine Learning)*, kemampuan perangkat IoT dalam memutuskan strategi keamanan juga semakin berkembang. Meskipun hal ini cukup berat untuk perangkat dengan sumber daya terbatas untuk memperkirakan kondisi dan waktu serangan.

II. HASIL DAN PEMBAHASAN

Sistem *IoT* rentan terhadap serangan jaringan, fisik, dan aplikasi dan juga terhadap kebocoran data privasi, dan sebagainya. Terdapat beberapa skenario penyerangan terhadap sistem *IoT*.

1. Serangan *Denial of service (DDoS)*.

   Serangan ini dilakukan dengan cara membanjiri basis data target dengan permintaan-permintaan untuk memutus perangkat *IoT* ke beberapa layanan. Biasanya permintaan-permintaan ini dilakukan oleh jaringan yang disebut bots. Serangan ini dapat melumpuhkan layanan dan dapat membuat pengguna tidak dapat mengakses layanan.

2. Serangan RFID.

   Serangan ini terjadi pada level fisik dari perangkat *IoT* yang mana membuat perangkat kehilangan sejumlah data dan kemampuan penggunaannya. Penyerang akan mengubah sejumlah data di node penyimpanan atau saat sedang dalam proses transmisi dengan jaringan. Serangan ini dapat diatasi melalui proteksi kata sandi, enkripsi data, dan kontrol akses terbatas.

3. Serangan internet:

   Perangkat IoT bekerja dengan terhubung dengan Internet untuk mengakses berbagai sumber daya. Para spammer yang ingin mencuri informasi sistem lain akan terus menerus menggunakan teknik spamming. Misalnya adalah penipuan iklan *(Ads fraud)* yang menghasilkan klik buatan pada suatu web target untuk menghasilkan keuntungan. Kelompok mereka disebut *cyber criminal*.

4. Serangan NFC (Apabila diaplikasikan).

   Serangan ini biasanya terfokus pada penipuan pembayaran elektronik. Serangan yang dapat terjadi melalui lalu lintas pembayaran yang tidak terenkripsi, modifikasi tag, dan sebagainya. Solusi dari serangan ini adalah menerapkan proteksi privasi kondisional yang mana dapat menggagalkan penyerang untuk membuat profil yang sama dengan pengguna dengan bantuan dari kunci publik pengguna yang mana akan diacak oleh sistem.

Beragam teknik pembelajaran mesin sudah diimplementasikan untuk meningkatkan keamanan. Setiap teknik pembelajaran mesin memiliki fungsi dan tipe yang beragam dalam mendeteksi serangan.

1. Teknik pembelajaran mesin *Supervised.* Teknik ini mencangkup metode *support vector machines (SVMs), random forest, naïve Bayes, K-nearest neighbor (K-NN), dan neural network* yang masing-masing digunakan untuk memberikan label terhadap jaringan untuk mendeteksi serangan. Dalam perangkat *IoT*, model-model tersebut mampu mendeteksi serangan *Dos, DDos*, intrusi dan serangan malware.
2. Teknik pembelajaran mesin *Unsupervised*. Teknik ini memiliki kemampuan diatas teknik lain tanpa adanya

label. Teknik ini bekerja dengan membentuk kluster-kluster. Pada perangkat *IoT*, analisis korelasi multi variasi digunakan untuk mendeteksi serangan *DoS.*

3. Teknik pembelajaran mesin *Reinforcement.* Teknik ini memberikan kemampuan terhadap sistem *IoT* untuk menentukan sendiri sistem keamanan dan parameter yang akan dipakai dengan cara mencoba tiap kemungkinan serangan. Metode *Q-learning* telah digunakan untuk meningkatkan peforma dari autentikasi dan dapat membantu mendeteksi serangan malware.

Untuk melindungi perangkat *IoT* dari informasi berbahaya dan ancaman serangan, dilakukan percobaan untuk mendeteksi spam web dengan beberapa jenis algorithma pembelajaran mesin. Percobaan ini dilakukan untuk mengatasi permasalahan terhadap perangkat *IoT* yang ada. Model pembelajaran mesin yang akan digunakan sebagai berikut.

1. *Bagged Model.*

   Bagging (agregasi bootstrap) yang termasuk dalam keluarga algoritma pembelajaran acak berbasis ensemble, dapat dianggap sebagai perpanjangan bootstrap untuk meningkatkan akurasi dan stabilitas pengklasifikasi dengan mengurangi varians perkiraan melalui pemungutan suara mayoritas atau rata-rata di seluruh kumpulan peserta didik yang lemah. Oleh karena itu, ini menyediakan cara yang efektif untuk membuat keputusan yang kuat dengan menggabungkan model acak dari data pelatihan asli. Ini sangat menarik ketika data sparsity menjadi masalah untuk estimasi model yang andal. [2]

2. *Bayesian Generalized Linear Model (BGLM).*

   Metode ini bekerja dengan alur yang pertama, memasukkan informasi yang telah ada. Umumnya, informasi sebelumnya sudah ditentukan secara kualitatif dalam bentuk distribusi dan representasi distribusi kemungkinan untuk suatu koefisien. Kedua, informasi yang ada dipasangkan dengan kemungkinan yang dihasilkan oleh suatu fungsi yang mana fungsi tersebut memiliki kemungkinan untuk merepresentasikan hasil. Ketiga, kombinasi dari informasi yang ada dan hasil dari Langkah kedua menghasilkan nilai koefisien distribusi. Keempat, dilakukan simulasi dari distribusi posterior untuk membentuk distribusi empiris untuk suatu parameter populasi dari nilai kemungkinan. Kelima, digunakan langkah statistik sederhana untuk meringkas hasil distribusi dari simulasi posterior.

3. *Boosted Linear Model.*

   Pohon keputusan dibuat untuk elemen-element data dengan membagi seri data menjadi sejumlah kelas data. Oleh karena itu, sebagai fungsi linier, masing-masing kelompok data dimodelkan.

4. *eXtreme Gradient Boosting (xgboost).*

   Metode ini adalah metode dengan sistem peningkatan gradien. Paket termasuk penyelesaian model linear yang efektif dan algorithma pembelajaran pohon yang mendukung berbagai fungsi seperti regresi, pengelompokan, dan pemeringkatan. Metode ini bekerja dengan vector numerik yang bekerja dengan kecepatan sepuluh kali lebih cepat dibanding algorithma *gradient boosting.* Metode ini menggunakan pendekatan yang lebih akurat untuk mencari model pohon.

   Setiap putaran pelatihan (iterasi), metode ini akan membentuk hasil pembelajar yang buruk dan prediksinya akan dicocokkan dengan hasil yang seharusnya. Jarak dari prediksi dan hasil yang seharusya adalah nilai error model yang dapat digunakan untuk mengkalkulasikan gradien. Gradien berfungsi untuk mengoptimalisasikan cara untuk menyesuaikan parameter sistem agar kesalahan pada iterasi berikutnya dapat diminimalisir.

5. *Generalized Linear Model (GLM) With Stepwise Feature Selection*.

   GLMs menyediakan rangka kerja *(framework)* dinamis untuk menjelaskan bagaimana sebuah variable dependen dapat diinterpretasikan melalui sejumlah penjelasan variable-variabel prediksi. Parameter dependen dapat berbentuk kontinu ataupun diskrit dan variabel penjelas juga dapat berbentuk empiris ataupun kategorial. Model yang digunakan juga telah disesuaikan dengan *stepwise feature selection*. Metode ini terus diulang hingga terdapat efek yang signifikan pada persamaannya. Persamaan dispesifikasikan dengan bantuan fungsi glmulti di R.

Setelah mengevaluasi model pembelajaran mesin yang akan digunakan, perlu diformulasikan persamaan untuk menghitung skor spamicity, yang didefinisikan dengan:

$$e[i] = \sqrt{\frac{\sum_{i=1}^{n}(p_i - a_i)^2}{n}}$$

$$S \leftarrow RMSE[i] * V_i$$

Pada persamaan diatas, e[i] adalah nilai error antara prediksi dan nilai sebenarnya. *S* adalah skor spamicity, yang semakin besar nilainya juga sebanding dengan kemungkinan terjadinya spam, dimana dihitung dengan algorithma:

1. **procedure** FUNCTION(PageRank)
2. **for** i = 1 to n **do**
3. **for** i = I to 15 **do**
4. Matrix representation z_i // Formulation of matrix n*15
5. Set j ← j + 1
6 Set i ← i + 1
7. **end for**
8. **end for**
9. **for** I = 1 to 15 **do**
10. Set $V_i =\leftarrow x$ // Where x is the feature importance score
11. **end for**
12. $p[i] \leftarrow Y$
13. **for** I = 1 to 15 **do**

14. Compute RSME[i] = $\sqrt{\frac{\sum_{i=1}^{n}(p_i - a_i)^2}{n}}$ // p_i is the predicted array and a_i is the actual array
15. **end for**
16. **for**
17. **end for**
18. **end procedure**

Model	Presisi	Recall	Akurasi
Model 1	0.650	1	79.81
Model 2	0.541	1	83.22
Model 3	0.567	1	84.35
Model 4	0.598	1	88.9
Model 5	0.513	1	91.8

Tabel 2 Peforma Model

Perangkat	Konektivitas Internet	Metode 1	Metode 2	Metode 3	Metode 4	Metode 5
Filter Udara	✓	0.650	0.396	0.399	0.371	0.628
Alarm Jam	×	0.348	0.580	0.947	0.637	0.217
Alarm Radio	×	0.246	0.607	0.686	0.633	0.175
Aquarium	×	0.671	0.709	0.143	0.878	0.489
Scanner	×	0.695	0.230	0.110	0.212	0.228
Pembuat Roti	×	0.820	0.683	0.261	0.789	0.217
Chiller	✓	0.045	0.635	0.466	0.732	0.213
Dekstop PC	✓	0.981	0.615	0.558	0.819	0.274
Games Console	✓	0.453	0.563	0.825	0.962	0.240
Laptop	✓	0.633	0.534	0.925	0.964	0.928

Tabel 1 Skor Spamicity dari beberapa Perangkat

Pada tabel 1, perbandingan tiap-tiap model pembelajaran mesin yang akan digunakan untuk melatih tiap-tiap set data. Sesuai dengan tabel, terlihat apabila model 1 memiliki tingkat presisi tertinggi dan model 5 memiliki akurasi tertinggi.

Pada tabel 2, dipaparkan skor spamicity dari beberapa perangkat yang sebagian diataranya terkoneksi dengan internet dan sebagian lainnya tidak terkoneksi dengan internet. Secara umum, perangkat yang terkoneksi dengan internet memiliki nilai yang lebih tinggi daripada perangkat yang tidak terkoneksi dengan internet. Hal ini sesuai dengan kemungkinan salah satu ancaman yaitu ancaman internet.

Pada model pertama, perangkat desktop pc dan pembuat roti berada pada posisi skor paling tinggi dengan masing-masing dengan dan tanpa koneksi internet. Sedangkan pada posisi terendah atau teraman dari serangan yaitu pada perangkat chiller dan alarm radio. Pada model kedua, posisi paling rentan adalah chiller dan aquarium. Sedangkan pada posisi terendah adalah filter udara dan scanner. Pada model ketiga, posisi paling rentan adalah laptop dan alarm jam. Sedangkan pada posisi terendah adalah filter udara dan scanner. Pada model keempat, posisi paling rentan adalah laptop dan aquarium. Sedangkan pada posisi terendah adalah filter udara

dan scanner. Pada model kelima, posisi paling rentan adalah laptop dan aquarium. Sedangkan pada posisi terendah adalah chiller dan alarm radio. Secara keseluruhan, perangkat dengan konektivitas internet yang paling rentan adalah laptop dan yang paling aman adalah chiller. Sedangkan perangkat tanpa konektivitas internet yang paling rentan adalah alarm jam dan paling aman adalah scanner.

III. KESIMPULAN

Kerangka kerja dapat mendeteksi parameter spam dari perangkat-perangkat *IoT* menggunakan model-model pembelajaran mesin. Data-data yang digunakan dari perangkat *IoT* telah diproses dengan prosedur keteknikan. Dengan menggunakan kerangka kerja dan model-model pembelajaran mesin, tiap-tiap perangkat *IoT* diberikan sejumlah skor spam. Hal ini dapat menyempurnakan kondisi yang harus diambil oleh perangkat *IoT* di sistem rumah pintar.

REFERENCES

[1] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021.

[2] X. Cui et al., "Hidden Markov Acoustic Modeling With Bootstrap and Restructuring for Low-Resourced Languages," in IEEE Transactions on Audio, Speech, and Language Processing, vol. 20, no. 8, pp. 2252-2264, Oct. 2012.