Jurnal Pendidikan dan Konseling
Volume 4 Nomor 5 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Application Of Machine Learning Directed To Detect And Prevent Network Intrusion In Xyz Switching Company (Financial Switching Company)

Alvin Christian[1], Riyanto Jayadi[2]
[1,2] BINUS Graduate Program, Master of Information Systems Management,
Bina Nusantara University, Jakarta, Indonesia
Email : alvin.christian001@binus.ac.id[1], riyanto.jayadi@binus.edu[2]

Abstrak

Makalah ini menjelaskan perbandingan beberapa model pembelajaran mesin yang akan digunakan untuk mendeteksi dan mencegah intrusi jaringan, berdasarkan data yang dikumpulkan dari PT. Perangkat Firewall Generasi Berikutnya dari XYZ. Lalu lintas yang diterima ke lingkungan perusahaan dibagi menjadi tiga jenis yang berbeda yaitu diterima, dicegah dan ditolak. Algoritma yang dibandingkan adalah Decision Trees, Random Forest, Gradient Boosted Trees dan Naïve Bayes.
Kata Kunci: *Pembelajaran Mesin, Deteksi Intrusi Jaringan, Pencegahan Intrusi Jaringan*

Abstract

This paper explains the comparison of several machine learning models to be used for detecting and preventing network intrusion, based on the data collected from PT. XYZ's Next Generation Firewall Appliance. The traffic received to the company's environment divided to three different kinds which are accepted, prevented and rejected. The algorithms compared are Decision Trees, Random Forest, Gradient Boosted Trees and Naïve Bayes.
Keywords: *Machine Learning, Network Intrusion Detection, Network Intrusion Prevention*

INTRODUCTION

Spiking of numbers in cyberattacks in only 3 months apart in 2020 in Indonesia [1] could only means the evolution of IT world is not only giving positive effects but also negative effects respectively to the Indonesian cyber people. PT. XYZ as a private-owned business also experience this relatively bad trend of cyberattacks spiking. Engaging in financial sector majoring in switching area to facilitate banks as their partners to provide the fund transfer options, they have already implemented Checkpoint Next Generation Firewall as their IPS (Intrusion Prevention System).

For the first semester of 2021, it is reported by Trendmicro [2] that Indonesia has entered CRI zone of elevated risk, and this made Indonesia to the highest risk level of cyber threat that Indonesia has ever been in.

Another case that is currently faced by Indonesia is there is a data breach of the electronic Health Alert Card (eHAC) system, which raised serious concerns about information security of an application named PeduliLindungi, which is a key part of government's tracking tool. [3]

There are also claims that emerges involving Chinese hackers breaching ministries and agencies internal network in Indonesia. The report itself came from a private cybersecurity firm stating that the hack initially discovered by the research division of the firm.

The threat is linked to Mustang-Panda, a well-known threat actor from China. It is known for its espionage campaign targeting SEA region. The first discovery is in April 2021 when a "PlugX malware" command and control (C&C) servers detected to be operated by Mustang Panda group, leveraging their communication with hosts inside the network of the government of Indonesia. [4]

The numbers of cases of cyberattack collected from the IPS in the company ranging around 8.000 to 15.000 cases per month.

Figure 1. Network Attacks to the Company

Checkpoint's Next Generation Firewall knowledge base is routinely renewed and updated from Checkpoint's principal, adding newest Common Vulnerabilities and Exposures (CVE) so that Checkpoint's sensors could detect newest CVEs and prevent cyberattacks. One of the main reasons of the company to purchase this appliance is the increasing trend of cyberattack to the company's premises which could cause financial loss, and if it's left like that, could jeopardize the company's performance and business.

The objectives of this paper are to give recommendations to the company to build a system based on Machine Learning if the results achieved has enough accuracy, also to find an alternative solution from the Checkpoint Next Generation Firewall to cut operational cost and get functional benefit, ultimately if it can be deployed to the system which are not crucial, can be secondary network or non-production environment. With the big number of attacks incoming to the company, this could be a risk for the company's asset inside the network, not only tangible, also intangible if any cybersecurity incident happens. Working in flow using CRISP-DM process as standard methodology, researcher hopes to find and close any gap left by the existing IPS system, this research is conducted by using Machine Learning and fortify the company's Information Security.

Literature Review

EFT Switching

Electronic Fund Transfer or EFT Switching is an integrated system which allows to accept, authorize, and safely direct fund transfer according to the applied regulations. EFT Switching provides the relationship of customers with banks, financial constitutions or regulators so that fund transfer could be done. [5]. PT XYZ is an Interbank Network Company or usually called switching company is a company which core business is to provide mainly fund transfer, cash withdrawal and balance check in ATM which bank is registered to the switching company.

Information Systems Security

Also commonly known as InfoSec, is a process which designed to protect important information and secrets of a business to be modified and tampered. Another meaning of Information Security is a defense to information or information system from an access, usage, trouble, and breaking which are not authorized.

Here are some examples of Information Security:

1. Application Security

   Application security covers software vulnerabilities in web or mobile, and in API (programming interfaces), etc.

2. Cloud Security

   Cloud security focused on a safe hosting of an application. Cloud security covers the networking, and application which connected to the cloud of the third-party provider.

3. Cryptography

   Data encryption if utilized correctly could help to make sure the secrecy and integrity of information. Digital signatures are usually used in the case of cryptography to validate the authenticity of data.

4. Infrastructure Security

   Infrastructure security commonly linked with protecting internal and extranet networks such as laboratories, data centers, servers, desktops, and mobile devices.

Firewall

Firewall is a tool in network security system works as monitoring and controlling incoming and outgoing network traffic based on security rule sets. Firewall establishes a barrier between an untrusted network and a trusted network, for example the Internet. A next-generation firewall is a part of the firewall generation, combining a traditional firewall with network device filtering functions, such as an application firewall using deep packet inspection, an IPS or Intrusion Prevention System. [6].

Next Generation Firewall

In a survey conducted by Neupane, [7] Next Generation Firewall is described as a firewall that is highly capable when compared to traditional static firewalls. Traditional firewalls only work to inspect data based on predetermined policies, unlike the Next Generation Firewall which works with additional features such as application awareness and control, integrated intrusion prevention, as well as threat intelligence sources.

The features that must exist in a firewall so that it can be classified as a next-generation firewall are as follows:

1. Encrypted traffic control: traffic passing through NGFW must be properly encrypted and only NGFW can decrypt it so that the path used cannot be sniffed in the middle.
2. Port hopping: Attackers often choose random ports to attack. NGFW must be able to detect when these random ports are in use
3. Application control: NGFW must be able to distinguish traffic from which application is passing so that if the application is not authorized, the packet can be dropped.
4. Identity based control: NGFW must be able to distinguish the traffic that passes is traffic that is owned by an authorized user.
5. URL filtering: NGFW can filter URLs accessed are safe URLs
6. Data leakage protection: NGFW must have data filtering feature in order to avoid leakage
7. WiFi network control: NGFW must be able to ensure the security level of the wifi in its network.
8. Network access control
9. WAN Routing & Optimization

Intrusion Detection System

IDS (Intrusion Detection System) on the other hand, is a software application or device that works by monitors a network or other system, looking for malicious activity or policy violations. If there is intrusion activity or violation it is typically reported to an administrator or centrally collected by sending the report to a security information and event management (SIEM) system. [8].

Artificial Intelligence Analysis

Artificial intelligence (AI) is intelligence that is created and added to a machine or system that can be managed. AI is created and inserted into machines so that machines can do work like humans,

especially in analysis and decision making. Examples of the application of AI are digital game systems (games) and robotics.

In its current application of AI, AI has different challenges from human intelligence. Things that are considered easy by humans, such as facial recognition and text understanding, are considered difficult by AI. On the other hand, things that are considered difficult for humans such as mathematical calculations, game logic and the ability to remember are done well by AI.

Currently AI has become part of the branch of computer science that studies the application of behavior and adaptation in a machine. AI research focuses on increasing intelligence in machines to automate human tasks that require intelligence such as scheduling, object recognition, control and communication. Today's AI systems have been applied in various everyday fields such as chatbots to answer customers, facial recognition for CCTV, identification of disease symptoms and the movement of robots and household appliances.

AI is developed by imitating and transforming the characteristics of human intelligence into algorithms that are understood by computers and machines. Similar to human intelligence, different approaches can produce 15 different intelligences. Therefore, AI is not only linked to computer science but also other sciences such as Mathematics, Biology, Psychology and others depending on the approach and purpose of the AI being made. For AI to be as smart as human intelligence and utilized by computers and machines, AI needs to be developed and trained by methods and algorithms.

CRISP-DM

CRISP-DM (Cross Industry Standard Process for Data mining) explains a process model that provides a framework for carrying out data mining (DM) projects regardless of the technology used or industrial sector. CRISP-DM goal is to develop data mining projects that are cheaper, repeatable, manageable, and faster. [9].

Machine Learning

Machine learning (ML) is a branch of AI on algorithmic and statistical models used by computer to perform certain activities based on patterns or conclusions. [10] Goal of ML is to recognize patterns in data, informing how problems are treated. In its learning method machine learning is divided into 3 namely: Supervised Learning: ML learns the mapping of input and output data with the correct value given by the supervisor to be applied to the new data. Unsupervised Learning: ML learns input without data from supervisors by looking for patterns and regularity of existing inputs. Reinforcement Learning: ML evaluates the output in the form of provisions or sets of actions that the system has done before so that ML can create a more effective provision or set of actions in achieving the goal. [11]

Decision Trees

The Decision Tree technique classifies the sample through a sequence of decisions, where the current decision will help to make the next decision. The sample classification continues from the root node to the corresponding end leaf node, where each end leaf node represents a classification category. The sample attribute is assigned to each node, and the value of each branch corresponds to the attribute. [12]

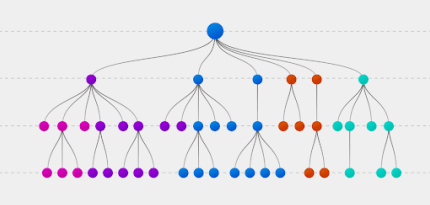

Figure 2. Decision Trees

Random Forest

The Random forest model is a composite of several Decision trees, which can be used for classification or regression functions. The prediction in the case of classification is based on the majority of the predicted values using Decision trees, then in the case of regression, the result is the result of the Random forest itself. The use of more trees will affect the accuracy that will be obtained. Determination of the classification by random forest is taken based on the voting results of the formed tree. [13]

Gradient Boosted Trees

Gradient Boosted Trees is one of the most used algorithms in machine learning these days. [14] Gradient Boosted Trees are easy to adapt, easy to interpret and produce models with high accuracy.

Gradient Boosted Trees have advantages in natural handling based on mixed types (heterogeneous features), predictive power, but Gradient Boosted Trees have weaknesses in terms of scalability due to their sequential nature making them almost non-parallel. [14]

Naïve Bayes

Naïve Bayes is one of the most famous data mining algorithms for classification functions. Naïve Bayes deduces the possibility that a new instance of a class is based on the assumption that all attributes are independent of the class itself. This assumption is supported by the need to predict multivariate probabilities from the training data. In practice, most of the attribute combinations do not exist in the training data or are insufficient. As a result, direct prediction of any relevant multivariate probabilities will not be reliable. Naïve Bayes is a classification model that is very competent in real-world applications. [15]

Related Work

Many related works in the existing literature on intrusion detection are exists. The first one is a paper titled Research on Intelligent Detection of Intrusion Data in Network by author Zhu and Yao [16] which they reviewed the machine learning and data mining methods used in NIDS and introduces articles of network misuse detection and anomaly detection using ML. Chandre et al. [17] proposes a system in order to avoid intrusion, using ML for wireless network utilizing sensor. The proposed system will be used for IPS in the wireless network. Their research verifies and models some protocol for intrusion detection using AVISPA tool and HLPSL language.

Sawant [18] did a research to compare different intrusion prevention system. In their research, it is stated they confronts the challenge in network security and compares IPS systems based on the features and mechanisms. The results are that IPS/IDS could be implemented in the system depends on the architecture of the system itself, which can be configured accordingly. HIPS are suitable to be deployed at the endpoint security, while NIPS could be deployed at network level.

IoT also been utilized and researched more lately, proven by Abdulaziz who did research in 2019 [19] about enhancing cybersecurity in modern IoT using Intrusion Prevention Algorithm for IoT, and the more recent are Sharma and Pippal [20] which research is about analytics of malicious attack and intrusion prevention in IoT network, utilizing Blockchain based security analysis. Both researches focusing on improving the security level for IoT which is getting more popular by the time.

METHOD

The research method used in this study is to use the Cross Industry Standard Process for Data Mining method, commonly abbreviated as CRISP-DM.nCRISP-DM modeling can provide a framework in an independent data mining project regardless of the technology sector or industry (Wirth, 2000)

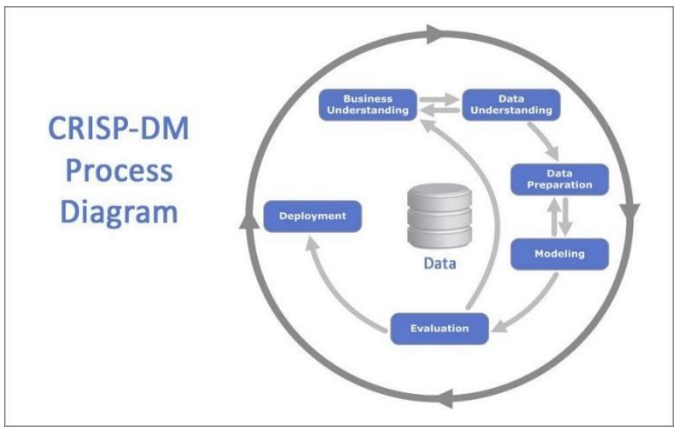

Figure 3. Six Steps of CRISP-DM

Business Understanding

PT. XYZ is one of the 4 switching companies in Indonesia that are regulated by Bank Indonesia directly which main business is handling EFT (Electronic Fund Transfer) or interbank wire transfer as a medium for banks, so they don't have to make separated line to every each of bank. PT. XYZ handles traffic data from banks and billers that it must secure every line that are used to handle those traffics so it could be cleanse and to make sure it's not anomalous traffic and cyberattack.

Data Understanding

In the data understanding phase, it is explained what data is being processed and trained. One sample of attack that could be prevented by Existing IPS System consisting of 25 Fields.

Table.2. Attributes.

No	Attribute	Value
1	*Time*	2020-06-20T08:38:23Z
2	*Id*	0a7e3c73-0100-00c0-5eed-caff00010003
3	*Source*	194.180.224.3
4	*Attack Name*	NTP Enforcement Violation
5	*Attack Information*	NTP Servers Monlist Command Denial of Service
6	*Severity*	High
7	*Industry Reference*	CVE-2013-5211
8	*Performance Impact*	Medium
9	*Protection Type*	IPS
10	*Blade*	IPS
11	*Product Family*	*Threat*
12	*Orig Log Server Ip*	10.26.160.214
13	*Interface Direction*	outbound
14	*Interface Name*	eth1
15	*Threat Prevention Policy*	*Standard*
16	*Threat Prevention Policy Date*	2020-06-20T08:38:23Z
17	*Source Port*	54361
18	*Destination*	10.26.167.203
19	*Destination Port*	123
20	*Action*	*Prevent*
21	*Policy Name*	*Standard*

No	Attribute	Value
22	*Policy Management*	CPMGMTGPS
23	*Policy Date*	2020-06-20T08:38:23Z
24	*Service*	UDP/123
25	*Description*	*Prevented* ntp servers monlist command denial of service originating from 194.180.224.3 against 10.126.67.193

Data Preparation

In the data preparation phase, several preparations are being done to the data collected such as data cleanse or to remove the unused fields, manually using excel then using missing value node in KNime, used for filling any empty fields. After that, attribute split must be done and lastly is to perform formatting the output of the data to be uniform.

Modelling

Modelling phase is the phase where exercising 4 statistical models which are Decision Tree, Naïve Bayes, Random Forest, and Gradient Boosted Trees is done.

Evaluation

Moving on to the evaluation phase, this phase is done by summarizing the results to the business success criteria that is set in the business-understanding phase.

Deployment

The deployment phase consists of 3 actions done which are the first is planning the deployment itself. In this part, author choose the methods to integrate data-mining discoveries into use. The second part is to plan monitoring and maintenance. Monitoring and maintenance will give benefit to the research as it will be done repeatedly. And the last part is to report final results.

RESEARCH AND METHODOLOGY

Using Intrusion Detection System (IDS) data to be learned by machine learning is a common research being conducted by cyber security researchers[21].

1. Business Understanding.

   PT XYZ is a financial services company that is engaged in switching or transfers between domestic and foreign banks, also has a business as a payment gateway.

   PT XYZ was founded in 1991 as a company engaged in the operation of the VSAT satellite communication system or Very Small Aperture Terminal. It was only in 2000, armed with the support of the leading VSAT technology, PT. XYZ is trusted by Bank Indonesia as the regulator to be a switching and communication service provider for one of the largest private bank networks in Indonesia.

   Starting in 2010, PT. XYZ has succeeded in developing other businesses, namely as a Payment Gateway and Aggregator service which is now a Payment Solution for payments from billers or merchants registered throughout Indonesia. In 2015 PT. XYZ developed a business for Top-Up services or electronic money top-ups and until 2017, PT. XYZ is trusted again by Bank Indonesia to be one of the executors and developers and implementers of the GPN or what is commonly known as the National Payment Gateway.

2. Data Understanding.

Table.3. Data Used After Cleansed.

No	Attribute	Value
1	Time	6/22/2020 10:55 AM
2	Source Country	Netherlands
3	Destination	10.126.61.130
4	Source	103.194.171.18
5	Service	TCP
6	Destination Port	57020
7	Action	Accept

From 25 fields from the log data generated, author cleansed the data necessary and relevant to being only 7 fields left.

3. Data Preparation
   a. Data Cleansing done manually using excel. Removed 14 fields leaving out 11 fields relevant.
   b. Using Missing Value Node in KNime to solve a problem which there is some missing value in the Destination field.
   c. Attribute Split, to split the time attribute, originally filled with date and time, split to be time in one field and date in one field.

Table 4. Attributes After Split.

No	Attribute	Value
1	Date	6/22/2020
2	Time	10:55:00
3	Source Country	Netherlands
4	Destination	10.126.61.130
5	Source	103.194.171.18
6	Service	TCP
7	Destination Port	57020
8	Action	Accept

4. Modelling

Table.5. Accuracy of statistics on Dataset is partitioned to 80% training set and 20% testing set.

	Accuracy	ROC Prevent	ROC Detect	ROC Accept	Cohen's Kappa
Decision tree	94.746%	97.25%	99.82%,	99.76%	0.922
Random forest	94.746%	92.17%	99.49%,	95.94%	0.922
Gradient Boosted Trees	94.746%	97.53%	99.86%	99.76%	0.922
Naïve bayes	94.746%	83.6%	94.91%.	96.94%.	0.922

The following figures shows the way that the tool KNIME workflow is used to build and run machine learning Algorithms.

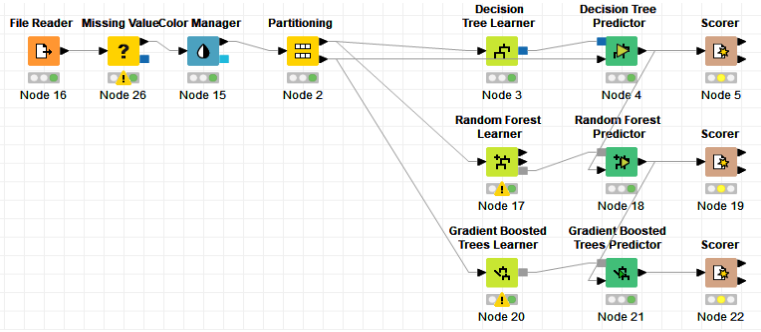

Figure 2. Knime Workflow

The whole Knime workflow can described as:

a. File Reader: using the csv file to input the data to be learned.
b. Missing Value: to solve the missing value problem in the Destination field.
c. Color Manager: to give color code to the 3 actions that being predicted, which are Accept, Detect, or Prevent.
a. Partitioning: set the partitioning to 80% training set and 20% testing set.
b. Learner: to set the boundaries and configuration on how the learner will learn the data.
c. Predictor: node used to predict the data after it has learned.
d. Scorer: the node used to score and display the results.

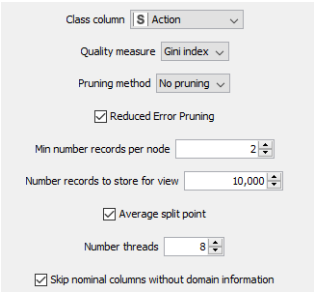

Figure 3. Decision Tree Learner Configuration

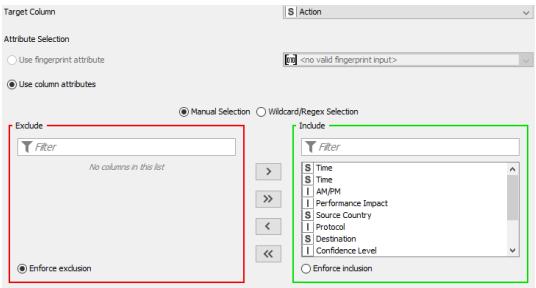

Figure 4. Random Forest Learner Configuration

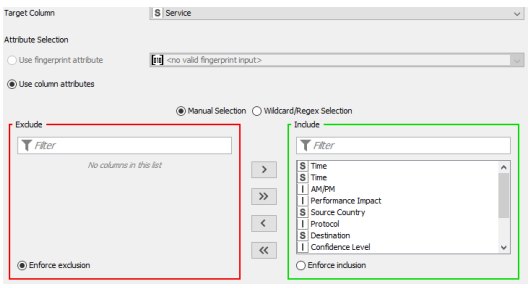

Figure 5. Gradient Boosted Tree Configuration

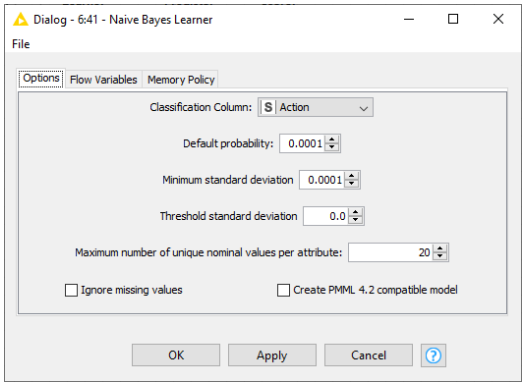

Figure 6. Naïve Bayes Configuration

5. Evaluation

The performance evaluation of algorithms in this research is done by two evaluation metrics, which are ROC curve and Confusion matrix.

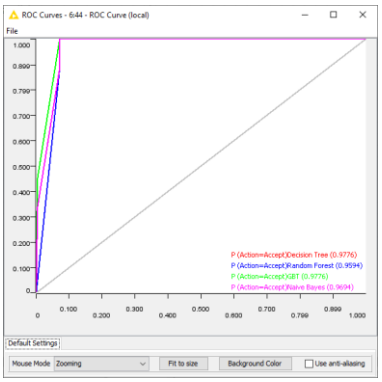

Figure 7. ROC Curve by all algorithms for Accept

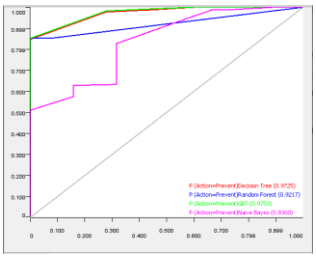

Figure 8. ROC Curve by all algorithms for Prevent

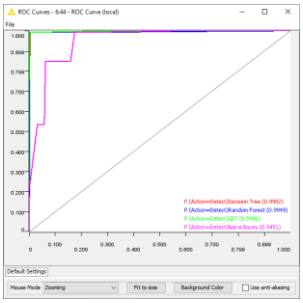

Figure 9. ROC Curve by all algorithms for Detect

Table 6. Model Results

	Accuracy	ROC Prevent	ROC Detect	ROC Accept	Cohen's Kappa
Decision tree	94.746%	97.25%	99.82%,	99.76%	0.922
Random forest	94.746%	92.17%	99.49%,	95.94%	0.922
Gradient Boosted Trees	94.746%	97.53%	99.86%	99.76%	0.922
Naïve bayes	94.746%	83.6%	94.91%.	96.94%.	0.922

6. Deployment

Referring to the comparison of the four algorithms, could be concluded that all the algorithms have the same level of accuracy, but the difference is in the ROC curve from Gradient Boosted Trees algorithm, with 97.53% score, marking the highest from all four.

With that result, the algorithm could be applied to a system for the company to be deployed on site.

For technical recommendation, a system could be deployed to the company could be seen as example below:

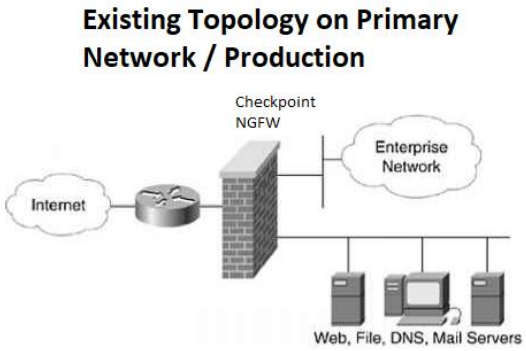

Figure 10. Existing topology of the company

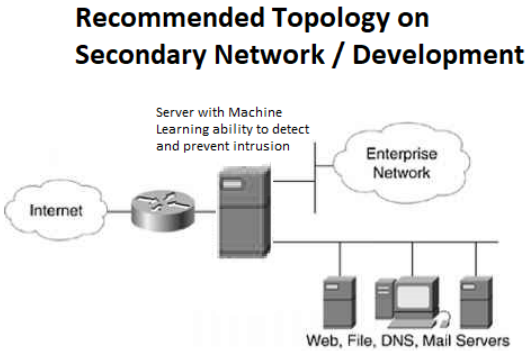

Figure 11. Recommended topology to be deployed to the company

CONCLUSION

The conclusion taken after this research in this paper used in intrusion detection systems data log, it has been conducted that the data is accurate enough, shown by the score given by the workflow, as the 4 algorithm shows that the accuracy has reached 94.746% for every algorithm. This shows that almost every of the tested algorithms of machine learning are excellent.

To answer the objective of this research, the company is recommended to build a new system based on machine learning to act as a filtering system for traffic inbound to the company environment, but since it doesn't have perfect accuracy, the system could be deployed to any secondary environment such as development environment or testing environment.

As for incoming research in the same topic, any researcher could use more algorithm beyond all four that has been used in this research, to find out which algorithm is the best in terms of accuracy and performance. This research is only done in the company's scope so it would be an advantage for future research to do consimilar research for bigger scope and wider target.

REFRENCES

BSSN, "Rekap Serangan Siber (Januari – April 2020)," 2020. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/ (accessed Apr. 07, 2021).

JakartaGlobe, "Indonesia at Highest Risk Level of Cyber Threat: TrendMicro," 2021. https://jakartaglobe.id/tech/indonesia-at-highest-risk-level-of-cyber-threat-trendmicro.

TheJakartaPost, "Cyber-attack haunts Indonesia's COVID-19 strategy," 2021. https://www.thejakartapost.com/news/2021/109/02/cyber-attack-haunts-ris-covid-19-strategy-.html.

Tempo, "Cybersecurity Group Suspects Chinese Hackers Compromised Indonesian Govt," 2021. https://en.tempo.co/read/1505534/cybersecurity-group-suspects-chinese-hackers-compromised-indonesian-govt.

F. Calisir and C. A. Gumussoy, "Internet banking versus other banking channels: Young consumers' view," Int. J. Inf. Manage., vol. 28, no. 3, pp. 215–221, 2008, doi: 10.1016/j.ijinfomgt.2008.02.009.

B. Soewito and C. E. Andhika, "Next Generation Firewall for Improving Security in Company and IoT Network," Proc. - 2019 Int. Semin. Intell. Technol. Its Appl. ISITIA 2019, pp. 205–209, 2019, doi: 10.1109/ISITIA.2019.8937145.

K. Neupane, R. Haddad, and L. Chen, "Next Generation Firewall for Network Security: A Survey," Conf. Proc. - IEEE SOUTHEASTCON, vol. 2018-April, pp. 1–6, 2018, doi: 10.1109/SECON.2018.8478973.

H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[S. Huber, H. Wiemer, D. Schneider, and S. Ihlenfeldt, "DMME: Data mining methodology for engineering applications - A holistic extension to the CRISP-DM model," Procedia CIRP, vol. 79, pp. 403–408, 2019, doi: 10.1016/j.procir.2019.02.106.

M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," vol. 349, no. 6245, 2015.

G. Carleo et al., "Machine learning and the physical sciences," Rev. Mod. Phys., vol. 91, no. 4, p. 45002, 2019, doi: 10.1103/RevModPhys.91.045002.

T. Mitchell, "Machine learning," 1997.

P. A. A. Resende and A. C. Drummond, "A survey of random forest based methods for intrusion detection systems," ACM Comput. Surv., vol. 51, no. 3, 2018, doi: 10.1145/3178582.

J. Ye, J. H. Chow, J. Chen, and Z. Zheng, "Stochastic gradient boosted distributed decision trees," Int. Conf. Inf. Knowl. Manag. Proc., pp. 2061–2064, 2009, doi: 10.1145/1645953.1646301.

S. Chen, G. I. Webb, L. Liu, and X. Ma, "A novel selective naïve Bayes algorithm," Knowledge-Based Syst., vol. 192, no. xxxx, p. 105361, 2020, doi: 10.1016/j.knosys.2019.105361.

G. Zhu and H. Yao, "Research on Intelligent Detection of Intrusion Data in Network," Proc. - 2020 Chinese Autom. Congr. CAC 2020, pp. 5–10, 2020, doi: 10.1109/CAC51589.2020.9326803.

P. R. Chandre, P. N. Mahalle, and G. R. Shinde, "Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification," Proc. - 2018 IEEE Glob. Conf. Wirel. Comput. Networking, GCWCN 2018, pp. 135–140, 2019, doi: 10.1109/GCWCN.2018.8668618.

[18] A. Sawant, "A Comparative Study of Different Intrusion Prevention Systems," Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018, pp. 1–5, 2018, doi: 10.1109/ICCUBEA.2018.8697500.

[19] A. Aldaej, "Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)," IEEE Access, vol. PP, no. c, pp. 1–1, 2019, doi: 10.1109/access.2019.2893445.

[20] R. K. Sharma and R. S. Pippal, "Malicious Attack and Intrusion Prevention in IoT Network using Blockchain based Security Analysis," Proc. - 2020 12th Int. Conf. Comput. Intell. Commun.

Networks, CICN 2020, pp. 380–385, 2020, doi: 10.1109/CICN49253.2020.9242610.
[21] D. H. Deshmukh, T. Ghorpade, and P. Padiya, “Intrusion detection system by improved preprocessing methods and Naïve Bayes classifier using NSL-KDD 99 Dataset,” 2014 Int. Conf. Electron. Commun. Syst. ICECS 2014, 2014, doi: 10.1109/ECS.2014.6892542.