Development of Intelligent Network Defense System to enable detection and analysis of cyber-attacks using an intrusion detection and prevention system based on honeypots

Eng. Mouner Alwaza

Dr. Sameer Krman **Dr. Mohamed Nour Shama**

Abstract

The networks of universities and educational institutes are normally exposed to cyber-attacks, either internally or from outside the network. Sharing of knowledge associated with means of protection, which are responsible for defending the network, will effectively contribute to preventing or mitigating these attacks. We have developed a model for search, detection and analysis of network breaches and malwares by using of an intrusion prevention and detection system based on honeypots. Machine learning algorithms are implemented for classifying the attacks and discovering new threat. This system is able to capture and analyze cyber-attacks and malwares, and share the results of the analysis with other networks in real time, taking advantage of virtualization and thus saving in cost and time, since these systems are open source and free.

Keywords: Intrusion Detection system; Intrusion Prevention System; Honeypots; Machine learning algorithms

تطوير نظام دفاع ذكي للشبكات لتمكين اكتشاف وتحليل الهجمات الإلكترونية باستخدام نظام منع وكشف الاختراق المعتمد على مصائد مخترقي الشبكات

م. منير الوزة

د. سمير كرمان د. محمد نور شما

الملخص

تتعرض شبكات الجامعات والمعاهد التعليمية عادة للهجمات الإلكترونية، من داخل أو من خارج الشبكة. يساهم تبادل المعرفة المرتبطة بوسائل الحماية المسؤولة عن الدفاع عن الشبكة، بشكل فعال في منع هذه الهجمات أو التخفيف من حدتها. طورنا نموذجًا للبحث واكتشاف وتحليل خروقات الشبكة والبرامج الخبيثة باستخدام نظام منع وكشف الاختراق المعتمد على مصائد مخترقي الشبكات. طبقنا خوارزميات التعلم الآلي لتصنيف الهجمات واكتشاف التهديد الجديد. هذا النظام قادر على التقاط وتحليل الهجمات الإلكترونية والبرامج الخبيثة، ومشاركة نتائج التحليل مع الشبكات الأخرى في الزمن الحقيقي، مستفيداً من مبدأ الافتراضية وبالتالي توفير التكلفة والوقت، كون هذه الأنظمة مفتوحة المصدر ومجانية.

الكلمات المفتاحية: نظام كشف الاختراق، نظام منع الاختراق، مصائد مخترقي الشبكات، خوارزميات تعلم الآلة

1. Introduction

Computer networks have been developed in parallel with the rapid progress of science and technology that widely used in all areas of life. These networks are more vulnerable to cyber-attacks, data theft, viruses and other attacks, being connected and opened to each other, which threaten information security and confidentiality [1]. The attackers, especially in the field of education and the networks of universities and institutes, seek to obtain personal information about the university, its educational staff, students, and employees, and to steal the intellectual characteristics and research on which it is based, taking advantage of some security flaws in these networks. In most cases, the attackers' attitudes are the same on all university networks; they isolate it first from the rest of other universities, research centers and institutes [2]. Sharing information about any attack that university may be exposed to with the rest of the universities is useful practice to expose the nature of the attack and its causes and take actions that contribute to preventing or mitigating it in other universities if they are subjected to a similar attack in the future. Being an integral part of this educational field, we have developed an intelligent network defense system model that can evolve with time and can detect and analyze cyber-attacks and share them with other universities and thus stop or mitigate attacks on other universities' networks and help them to make appropriate decisions when they are exposed to similar attacks and benefit from the results of analysis. The attacks are assumed at educational level and can be generalized at the country level. The means and techniques applied for network defense and network security have been developed frequently over time.

Firewalls are one of the most important means of ensuring network security by using packet-filtering technology, effectively controlling network access permissions and defining security policies. The firewall monitors incoming and outgoing network traffic where all communications must flow through it [3], establishes a policy for access to hosts and services, and blocks access to users' privacy details. However, the firewall cannot protect the network from attacks that bypass it, especially those coming from the internet, or internal threats such as an employee cooperating with third parties [4]. Additionally, the high cost of installation and maintenance as well as the possibility of being penetrated by malicious programs represent a drawback of firewalls [3].

The Intrusion Detection System is an effective technology designed to maintain network security by discovering vulnerabilities that target any computer, application or system. The Intrusion Detection System is based on monitoring network traffic and captures suspicious activities and network policy violations and finally notifies the system administrator about these violations. The bad packets are often destroyed and stopped by the intrusion detection system and therefore cannot be analyzed, and the intrusion detection system needs to be constantly updated in order to protect it against new vulnerabilities, and it is not often able to process the encrypted packets [3].

The intrusion prevention system is able to provide security for computer systems and effective in facing threats, detecting, preventing and stopping old and new attacks, by actively and in-depth monitoring of network activities and stopping any behavior or strange content, either by, for example, leaving a user account or shutting down the system, stopping the process and disconnecting the connection, and often combines with intrusion detection system [5]. The problem of detecting false positives or false negatives is one of the most common problems faced by the intrusion prevention system, so IPS can identify a normal traffic as a malicious one, causing a false positive, or a malicious traffic as normal, causing a false negative [6], and as it may stop the activity in the network, causing a denial of service in addition to its high price [7].

Honeypots are defined, according to Lance Spitzher, the inventor of the honeypot idea, as "a source of information whose value depends on the unverified or prohibited use of that source" [8]. Thus, it is a source of information used in the field of security whose value has been attacked or controlled. It aims at entrap the attackers from the black hat community into a trap and focus on the silent collection of information about them by interacting with these communities and observing their behavior without knowing that they are being watched. It also helps obtaining information about the attackers, such as their IP address, the country they are from, and what information they want to obtain. It can serve as an early alert and sophisticated security monitoring tool that reduces the risk of attacks to the security system and networks. Honeypots are classified based on several factors:

Relying on interacting with hackers:

- **Low-Interaction Honeypot**: It issued to detect and deceive attackers by simulating Operating System services and gateway services on the Operating System host. The interaction is limited and the honeypot does not have its own operating system, and the primary mission is to slow down the attack.
- **Medium Interaction Honeypot**: It has the same principle as the Low Interaction Honeypot. It provides the attacker with phishing by having an operating system, as the attacker communicates with a large number of simulated services.
- **High Interaction Honeypots**: Includes real operating systems and applications like a real FTP server. It has the greatest threat as it exposes itself to the attacker for an extended period of time. They should be kept under constant surveillance due to their security risks [8].

Depending on the purpose or goal:

- **Productive network honeypots**: are systems that help mitigate the risk to the organization, and are placed close to the servers in the network. They are intended to simulate real production systems so that the attacker will spend time and resources attacking them.
- **Research Honeypots**: mainly used to uncover information about new methods of attacks, viruses, and worms. They are difficult to maintain and complex in structure and provide information on the Black hats and their offensive policies [9].

Honeypots reduce the generation of false negatives and false positives, and they also capture malicious activities within the system only, and thus resources are minimal, sufficient, and characterized by simplicity and flexibility. It does not need any sophisticated algorithm and is able to capture and record every activity and can discover new attack tactics. Conversely, if the honeypots are not precisely configured, the attacker can gain access to the honeypots themselves and recover the information they have gathered on them. Also, there is no automatic initialization process and therefore it requires human interaction [10].

Machine learning belongs to the artificial intelligence area, which avoids conventional programming methodologies by using computer- based systems to understand methods and data structure and to construct them into models that can be utilized to solve complex problems [11]. Machine learning algorithms are implemented in many research areas of network intrusion detection systems. K-means clustering and linear regressing algorithms are preferred due to their efficiency and accuracy. Km clustering provides localized best solutions concerning the cluster error, and it is a fast-iterative algorithm that has been used in many clustering applications [12]. Linear Regression algorithm is utilized to compute a function of linear hypothesis among the input and output variables as a tool of classification and regression [13].

The insufficiency of one single network defense tool, mentioned earlier, in preventing the attacks raised the need of joint efforts, working together and sharing results and analyzes with each other, so that we obtain an adaptive and stable network defense model that is capable of repelling various attacks and discovering, analyzing and stopping new attacks in real time.

2. Related work

Lee et al. Presented an advanced system that deploys an intrusion detection system, which is based on mixed honeypots and is capable of increasing the stability of network security and enhancing the ability of honeypots to predict attacks [14]. Ball and colleagues developed a signature generator-based intrusion detection system using honeypots. This system protects against attacks generated by polymorphic worms, isolates suspicious traffic, gathers information on various attacks, and detects new attacks of unknown worm species [15]. Beham and colleagues combined the idea of honeypots with intrusion detection systems and leveraged virtualization technology to enhance security in virtual cluster environments [16]. Pomasathit introduced an intrusion detection system with honeypots across distributed networks. The study aims to compare the effectiveness of collecting intrusion detection systems with and without the use of honeypots, and the study proved the efficiency of this use [17]. Musca and his colleagues proposed a Snort-based system that would be able to isolate harmful traffic, create automatic signatures for attacks, and gather information about these attacks [18]. Chaitanya and Thyagarajamurthy introduced the integration of honeypots and machine learning technologies in network security and proposed a comprehensive and robust security framework that protects the organization from malicious software [19]. Vinayakumar et al. analyzed Convolutional Neural Network for network intrusion detection by modeling the network traffic events as time series of TCP/IP packet [20].

The previous mentioned models showed the absence of completed security system that contains intrusion prevention and detection systems with the help of honeypots and able to analyze the results of attacks, share knowledge with other security systems, discover new attacks, and contribute to saving cost and time.

3. The proposed model:

Figure 1 is a high-level diagram of the proposed system architecture. Data are obtained with both low and high-interaction honeypots. Where the output is data collected and then directed to a real-time data analyzer that coordinates the data and sorts it according to the port or protocol. Then the analyzed data is sent to a database collector and a policy arbitrator that creates firewall rules from analyzes of data that are done in real time and in comparison with reference databases of a policy-controlled host, where policies are then sent to the firewall that acts on the basis of them either by blocking the attack or the port. Also these data are sent to a database analysis manager (that must have a high capacity for analyzing the data and the resulting policies). On the other hand, the data can also be analyzed by wireshark, and at the end the analyzed data and policies are presented on a display system for the information analysis system manager. Also, we make use of the data collected through the Honeypots and the Intrusion Prevention and Detection System. The data are captured by the honeypots as we mentioned previously, and then collected in the database where these data are analyzed and the signatures are extracted, where they are transferred to the intrusion detection and prevention system. At the same time they are directed to the Suricata intrusion detection system, where they are compared with the Suricata database, which depends on anomaly and misuse detection and sent to the Suricata Intrusion Detection and Prevention System which converts it onto the firewall.

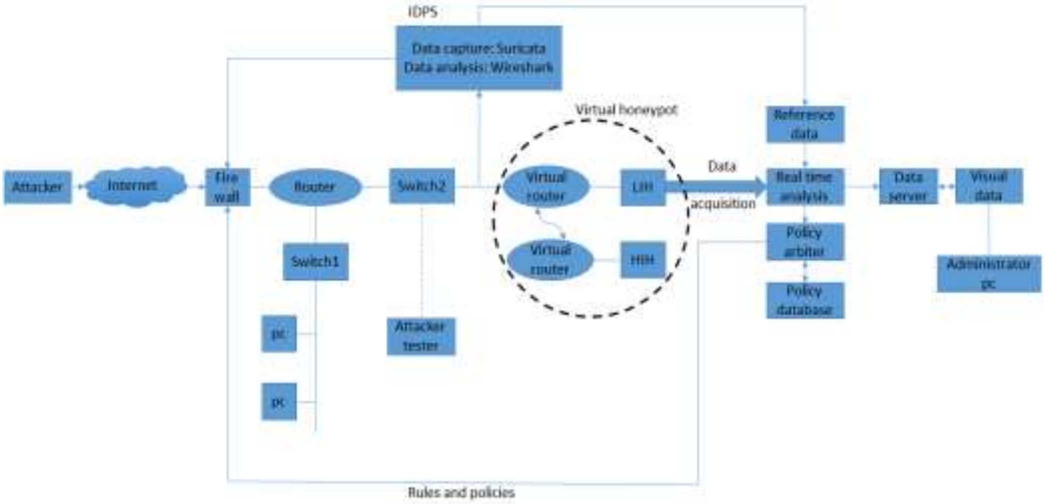

Figure (1) high-level diagram of the proposed system architecture

Figure 2 represents the architecture of a Suricata Intrusion Prevention System that is based on a predefined set of rules whose accuracy determines the error rate. Its architecture is based on the use of a multiple detection approach, which allows for more efficient use of the system and improved performance in the network traffic analysis process. Compared to Snort, Suricata has the advantage of automation and automatic detection of the protocol, thus increasing the opportunity to detect malware and reducing the rate of positive detection. The data, collected from logfiles and their real-time analysis, helps catching new attacks in real time [21].

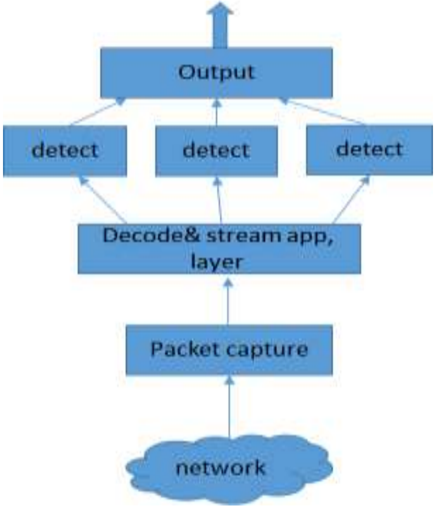

Figure (2) Architecture of a Suricata Intrusion Prevention System

The data collected from both sides is sent to a database collector and then to an analysis system that has various machine learning algorithms and is utilized and compared with previously stored databases in order to extract knowledge and deduce threats to the network. This information will be stored in the analysis publisher's database and then published to a policy database distributed across several systems.

The system will be tested by Hping3 program which simulate attacks on honeypots from a networked computer includes synflog, Dos, smurf and floding by using Ipspoofer.

The aim of this project is to spread the proposed model in more than one of the university's networks, connect these models with each other and create synchronization between them, so that each network can benefit from the results of the rest of the networks and thus prevent or mitigate at least the cyber-attacks that could affect them.

Data sources:

There are several primary sources of data, the most important of them are:

- Data from the attack on honeypots(logfiles)
- System accesses that are issued by the distributed services operating on the system and the network.
- Packet capture files (PCAP) that are generated by the Sniffer
- Protocol Analysis Tools (Wireshark)
- Output of open source intrusion detection systems such as Snort or Suricata
- The output of an application such as Kismet can be utilized if there is a wireless network within the network
- Information from scanning ports and information on previous attacks

We used open source intrusion prevention software, Fail2ban, that takes real-time information from the database server and checks logins to look for outrageous behavior and the IP addresses from which those behaviors emanate. Consequently, updating the firewall rules for blocking IP addresses and generalizing these addresses on the rest of the firewalls in other universities [22].

Knowledge discovery and new threat paradigms inferred:

Our system aims at gaining the highest level to collect and capture data about the attackers in a way that attracts the attackers to precisely prepared traps that are able to attract the attention of the attackers and lure them to interact with them. Then, these data and method of attacks can be analyzed and new types of threats can be discovered. That help the network by using new techniques of data collection and processing and by employing security experts. The process of discovering knowledge from the collected data can be done with the help of Knowledge Discovery in Databases (KDD) and data mining, as it was defined in Paper [23], as it expresses the comprehensive process in which the discovery of useful knowledge is obtained from data using data mining and that applies specific algorithms to extract useful data. . KDD needs to prepare, format, filter and appropriately integrate useful data with previous knowledge and data in order to gain the correct interpretation of this data. KDD leverages research areas such as machine learning, pattern recognition, artificial intelligence, and high-performance computing.

Figure 3 represents the process of knowledge discovery, whereby information is initially collected and analyzed in our system by the data analyzer or by IDPS, and then a preliminary processing is performed on this information (sorted by port or by protocol) by clarifying and merging it and deducing common formulas between the two methods. Then this data is converted into formulas and models that are suitable for machine learning algorithms or models that are processed using high-performance computing [24]. New attack models are subsequently explored by comparing them with previous models, thus creating a clear knowledge of new threats. The process of storing, processing and classifying data will depend on machine learning algorithms such as classifications and clusters to create models and predict new models based on past and current states. The designed honeypots and Intrusion detection system will save the gathered data vector, including the log, internet protocol (IP) and the length of packet in the KDDCup 999 data set to build profile of the user, then KM cluster algorithm clusters the data into analogous categories and LR problem is employed to model every categories and a decision if it threat or not is made. The new information and models are shown visually, as security experts are used to analyze these models and conclude and take appropriate decisions either directly, such as blocking a specific service or addresses, stopping the system, or proposing and modifying the security policies that universities follow in maintaining the security of their information.

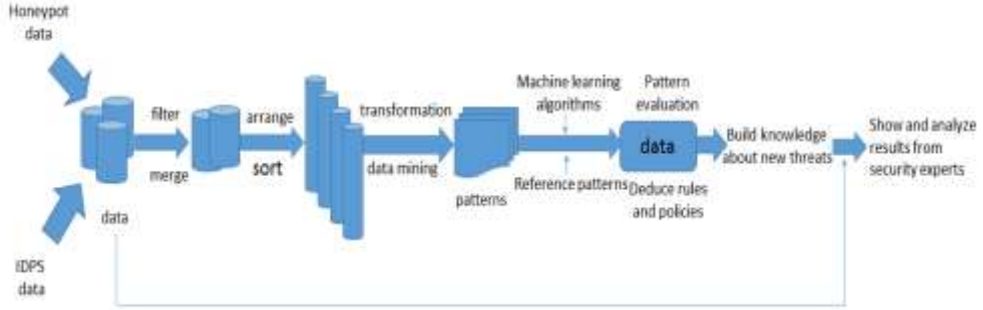
Honeypot data
IDPS data
data
filter
merge
arrange
sort
transformation
data mining
patterns
Machine learning algorithms
Reference patterns
Pattern evaluation
data
Deduce rules and policies
Build knowledge about new threats
Show and analyze results from security experts

Figure (3) The process of knowledge discovery

4. Discussion and results:

We have performed some tests on this model in order to verify its workability by simulating some types of attack on the proposed system from a computer on the network using the hping3 program. The testing and simulation of the attack process does not fully test the proposed model and represent a real attack on it. Rather, it is an effective testing process for the response of honeypots and intrusion detection and prevention system as well as how the data is captured by the network protocol analyzer.

Installing hping3: In the beginning, we installed the program hping3 on a computer connected to the network. And we will edit and simulate attacks scenarios that will be explained later.

Honeypots configuration: We used a virtual host to simulate network delay and packet loss rate. The honeypots simulation network consists of two virtual hosts representing honeypots and the Cisco router number 2. The first router separates the network 192.168.7.0/24 from the network 172.16.0.0/24 while the second router separates the network 172.16.0.0/24 from the network 172.20.0.0/ 24. The first honeypot is labeled 172.16.0.2/24-running Linux, 2.6.20-1, and the second honeypot is titled 172.20.0.2/24 and running winxp professional operating system.

Suricata Configuration: Suricata is an open source with high-performance IPS / IDS network monitoring engine that uses an externally developed set of rules to monitor network traffic and provide alerts to the system administrator when suspicious events occur. It provides great speed and efficiency in traffic analysis and hardware acceleration and is designed with the benefit of the parallel processing power of the latest multi-core CPU chipsets.

```
tar xzvf suricata-6.0.0.tar.gz
cd suricata-6.0.0
./configure
make
make install
```

We will release the flood attack in several possibilities and using several protocols.

First scenario:

A flood attack using the TCP protocol to flood the target machine, which is a honeypot, and the command form used is:

```
# hping3 <Victim’s IP> -V -c 10000 -d 512 -s -w 32 --flood
```

The second scenario:

Use UDP to flood the target machine and the command is:

```
# hping3 <Victim’s IP> -V -c 10000 -d 512 -s -w 32 -2 --flood
```

Third scenario:

Use ICMP to overwhelm the target machine and the command is:

```
# hping3 <Victim’s IP> -V -c 10000 -d 512 -s -w 32 -1 --flood
```

Activities are captured by Suricata Intrusion Detection and Prevention System and Wireshark starts listening on the network interface and showing results.

To evaluate our system and Knowledge discovery approach, we utilized KDDCup99 data set. Simulation result utilized 5000 normal records and 1000 abnormality records. Simulation results evaluated on various classes of attacks like probe attacks and DOS attacks.

The most commonly evaluation metrics were used for measuring the performance of Machine Learning methods for IDS are:

True Positive (TP): The data instances correctly predicted as an Attack by the classifier.

False Negative (FN): The data instances wrongly predicted as Normal instances.

False Positive (FP): The data instances wrongly classified as an Attack.

True Negative (TN): The instances correctly classified as Normal instances.

Precision: It is the ratio of correctly predicted Attacks to all the samples predicted as Attacks.

Precision= TP/(TP+FP)

True Positive Rate or Recall: It is a ratio of all samples correctly classified as Attacks to all the samples that are actually Attacks. It is also called a Detection Rate

Recall = Detection Rate = TP/(TP+FN)

False Positive Rate: is the ratio of wrongly predicted Attack samples to all the samples that are Normal.

False Positive Rate = FP/(FP+TN)

F1-Score: It is defined as the harmonic mean of the Precision and Recall. In other words, it is a statistical technique for examining the accuracy of a system by considering both precision and recall of the system.

F1-Score = 2(Precision*Recall/ Precision+Recall)

The details of metric statistics is reported in Table 1

Table (1): metric statistic

Class of attack	Precision	Rcall	False Positive Rate	F1-score
Probe	0.75	0.72	0.011	0.735
Dos	0.53	0.50	0.009	0.515
U2R	0.44	0.43	0.008	0.435
R2L	0.40	0.38	0.007	0.390

5. Conclusion and future work:

In our paper, we have discussed the use of previous models in protecting the network and applying multiple techniques to get an optimal solution in cost and time to maintain the security of our network. We have developed a new model that searches and contributes to discover and analyze the breaches and threats to university networks using the intrusion prevention and detection system with the help of honeypots. Our solution is considered a new model as it combines multiple security techniques and depends on open source programs, thus reducing costs and can be operated in real time. Additionally, it is possible to develop and generalize this model in other universities, as our new model can contribute to the discovery of new types of real-time attacks and threats. In the next step, we will develop and update the model so that it is able to communicate with networks of other universities and take the advantage of high-performance computing technology of processing data in a very high speed, as well as processing communication and sharing of results and analysis in real time.

Acknowledgements

Prof. Hasan Abou Alnoor has contributed to the work presented here but unfortunately passed away just before submitting it. Authors sincerely dedicate this work to the memory of Prof. Abou Alnoor.

References

[1] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, 80 (2014) 973-993.

[2] T.C. Amick, L.R. Soles, D.H. Snider, Moving towards an adaptive enterprise intrusion detection and prevention system, ICAI 2015: Proceedings of the 2015 International Conference on Artificial Intelligence: WORLDCOMP'15, July 27-30,, Las Vegas, Nevada, USA 2015.

[3] S.S. Vichare, Comparative Study on Firewall and Intrusion Detection System, International Journal of Engineering Science and Computing, 7 (2017) 13716-13718.

[4] G. Singh, B. Singh, Network security technology based on firewall and intrusion detection system, nternational Journal of Computer Science and Mobile Applications, 6 (2018) 43-51.

[5] U.A. Sandhu, S. Haider, S. Naseer, O.U. Ateeb, A Survey of Intrusion Detection & Prevention Techniques, International Conference on Information Communication and Management IPCSIT, IACSIT Press,Singapore, Singapore, 2011, pp. 66-71.

[6] C.-Y. Ho, Y.-D. Lin, Y.-C. Lai, I.-W. Chen, F.-Y. Wang, W.-H. Tai, False Positives and Negatives from Real Traffic with Intrusion Detection/Prevention Systems, International Journal of Future Computer and Communication, 1 (2012) 87-90.

[7] A.A. Abdelkarim, H.H.O. Nasereddin, Intrusion prevention system, International journal of academic research, 3 (2011) 432-434.

[8] L. Spitzner, Honeypots: Tracking Hackers, Addison-Wesley Professional, Boston, MA, 2002.

[9] S.D. Lakshmi, G. Arunkumar, V.M. Viswanatham, Network Security Enhancement through Honeypot based Systems, International Journal of Engineering and Technology, 7 (2015) 290-293.

[10] A. Mairh, D. Barik, K. Verma, D. Jena, Honeypot in network security: a survey, ICCCS '11: Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM Digital Library, Rourkela, Odisha, India, 2011 pp. 600–605.

[11] Z. Ullah, F. Al-Turjman, L. Mostarda, R. Gagliardi, Applications of Artificial Intelligence and Machine learning in smart cities, Computer Communications, 154 (2020) 313-323.

[12] S. Ray, R.H. Turi, Determination of number of clusters in K-means clustering and application in colour segmentation, The 4th International Conference on Advances in Pattern Recognition and Digital Techniques, 1999, pp. 137-143.

[13] M. Schleich, D. Olteanu, R. Ciucanu, Learning Linear Regression Models over Factorized Joins, Proceedings of the 2016 International Conference on Management of DataJune 2016 2016, pp. 3-8.

[14] S. Li, Q. Zou, W. Huang, A new type of intrusion prevention system, 2014 International Conference on Information Science, Electronics and Electrical Engineering, Sapporo City, Hokkaido, Japan, 2014, pp. 361-364.

[15] S. Paul, B.K. Mishra, Honeypot-based Signature Generation for Polymorphic Worms, International Journal of Security and Its Applications, 8 (2014) 101-114.

[16] M. Beham, M. Vlad, H.P. Reiser, Intrusion detection and honeypots in nested virtualization environments, 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Budapest, 2013, pp. 1-6.

[17] A. Pomsathit, Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Honeypot, 2012 Spring Congress on Engineering and Technology, Xi'an, China, 2012, pp. 1-4.

[18] C. Musca, E. Mirica, R. Deaconescu, Detecting and Analyzing Zero-Day Attacks Using Honeypots, 19th International Conference on Control Systems and Computer Science, Bucharest, Romania, 2013, pp. 543-548.

[19] T.A. Chaitanya D Patil, Integration of Honeypots and Machine Learning in Network Security, International Journal of Advanced Science and Technology, 29 (2020) 6512 - 6519.

[20] R. Vinayakumar, K.P. Soman, P. Poornachandran, Applying convolutional neural network for network intrusion detection, 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1222-1228.

[21] S.A.R. Shah, B. Issac, Performance comparison of intrusion detection systems and application of machine learning to Snort system, Future Generation Computer Systems, 80 (2018) 157-170.

[22] Fail2ban, Fail2Ban (https://www.fail2ban.org/wiki/index.php/Main_Page), 2016.

[23] U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, Knowledge discovery and data mining: towards a unifying framework, Proceedings of the Second International Conference on Knowledge Discovery and Data Mining, AAAI Press, Portland, Oregon, 1996, pp. 82–88.

[24] J. Han, M. Kamber, J. Pei, Data Mining: Concepts and Techniques, Third ed., Elsevier Inc., Waltham, MA 02451, USA, 2012.