Revista Cubana de Ciencias Informáticas
Vol. 14, No. 1, Enero - Marzo, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 58-78

Tipo de artículo: Artículo de revisión
Temática: Inteligencia Artificial
Recibido: 26/08/19 | Aceptado: 30/10/19

A Systematic Literature Review on Intrusion Detection Approaches

Una revisión sistemática de la literatura sobre los enfoques de detección de intrusiones

Hilma Aludhilu [1] https://orcid.org/0000-0002-2710-4534
Rafael Rodríguez-Puente [1*] https://orcid.org/0000-0003-1556-491X

[1] Computer Science Departament School of Computin University of Namibia

*Autor para la correspondencia: rpuente@unam.na

ABSTRACT

Nowadays, intrusion detection systems play a major role in system security. Ideally, intrusion detection systems are capable of detecting intrusions in real time to prevent intruders from causing any harm to computer systems. Intrusion detection systems can be implemented using different intrusion detection approaches with its strengths and limitations. This paper provides an overview of the strengths and limitations of the different intrusion detection approaches, including Statistical-Based Anomaly, Pattern Matching, Data Mining and Machine Learning approach. The results show that Machine Learning is the most suitable approach for implementing intrusion detection system solutions, because of its ability to work as an automated process, which hardly needs human intervention. Using this partial conclusion, different machine learning techniques are studied and presented, also with their strengths and limitations. After the

study, it can be concluded that the best technique to implement this kind of system is recurrent neural networks. An intrusion detection systems that hardly needs human intervention, can be developed and implemented, using this technique.

Keywords: Intrusion Detection Systems; IDS; Intrusion Detection Approaches; System Security.

RESUMEN

Hoy en día, los sistemas de detección de intrusos juegan un papel importante en la seguridad de los sistemas informáticos. Idealmente, los sistemas de detección de intrusos son capaces de detectar intrusiones en tiempo real para evitar que los intrusos causen daños a los sistemas informáticos. Los sistemas de detección de intrusos se pueden implementar utilizando diferentes enfoques de detección de intrusos con sus puntos fuertes y limitaciones. Este documento proporciona una visión general de las fortalezas y limitaciones de los diferentes enfoques de detección de intrusos, incluido el enfoque de anomalías basadas en estadísticas, coincidencia de patrones, minería de datos y aprendizaje automático. Los resultados muestran que el aprendizaje automático es el enfoque más adecuado para implementar soluciones de sistemas de detección de intrusos, debido a su capacidad para funcionar como un proceso automatizado, que apenas necesita intervención humana. Usando esta conclusión parcial, se estudian y presentan diferentes técnicas de aprendizaje automático, enfatizando en sus fortalezas y limitaciones. Después del estudio realizado, se puede concluir que la mejor técnica para implementar este tipo de sistema son las redes neuronales recurrentes. Mediante esta técnica, se puede desarrollar e implementar un sistema de detección de intrusos que apenas necesita intervención humana.

Palabras clave: sistemas de detección de intrusiones; SDI; enfoques de detección de intrusiones; seguridad de sistemas.

Introduction

Computer systems are vulnerable to intrusions. Intrusion is the act of intruding or gaining unauthorised access to a system, with the aim of compromising it by breaking its security (Schell, Martin 2006). The objective

of the intruder is to gain access to a system and attempt to acquire confidential information. Intruders may also try to steal or modify information found on the system which they got unauthorised access to. Additionally, intruders also aim to compromise the availability, integrity and confidentiality of information on a system.

Behaviours of intruders are believed to be different from those of an authorised user. The difference in the behaviour between an authorised user and an intruder makes it possible to detect intruders through different techniques. According to (Kadam, Deshmukh 2007), intrusion detection is the act of detecting actions and behaviours that attempt to compromise the integrity, confidentiality, or availability of a computer resource. Intrusion detection is carried out by an Intrusion Detection System (IDS), which is the security system or software that detects actions and behaviours that are different from the "normal" behaviour that usually happens on a system.

An IDS is defined as "a security system that monitors computer systems and network traffic and analyses that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization" (Sarmah 2019).

IDSs aims to detect intrusions in real time and respond to the intrusions accordingly before the intruder gets hold of confidential information or causes any harm to the system. Desirable characteristics of an IDS includes: minimum human supervision, ability to update itself by an automated process, high accuracy, where the number of false alarm rate should be low, ability to detect all the attacks and it should be able to give quick response (Choudhary, Swarup 2009; Richariya, Singh, Mishra 2012). An IDS is expected to have most of the desirable characteristics mentioned above.

There are several intrusion detection approaches that can be used to implement an IDS. These approaches include Statistical-Based Anomaly, Pattern Matching, Data Mining and Machine Learning approach. This paper provides an overview of the aforementioned approaches with their strengths and limitations. It will identify the best approach according to the desirable characteristics described above and an overview of the techniques used within the approach will be also presented.

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 1, Enero - Marzo, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 58-78

Methodology

The methodology used in this literature review is based on the Guideline for conducting a Systematic Literature Review of Information Systems Research by (Okoli, Schabram 2012). A review of the existing literature regarding the use of different approaches to develop an IDS was carried out, as well as a review of machine learning techniques used to develop this type of system. The strengths and weaknesses of the different approaches and machine learning techniques used for developing IDSs are outlined as part of this research.

Searching for the literature

To search for the literature to be included in the study, the following electronic database resources were used: Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Research Gate, Springerlink, Sciencedirect, Association for Computing Machinery (ACM) Digital Library and Google Scholar. The search terms used for finding studies regarding the approaches were: "Intrusion Detection Approaches", "Approaches of Intrusion Detection System", "Approaches for Intrusion Detection", "Intrusion Detection Techniques", Techniques of Intrusion Detection", "Intrusion Detection using Statistical-Based Anomaly", "Intrusion Detection using Pattern Matching", "Intrusion Detection using Data Mining", and "Intrusion Detection using Machine Learning". Using the keywords mentioned above, more than 60 papers were retrieved.

For Machine Learning techniques, the search terms used are: "Machine Learning techniques", "Intrusion Detection using Support vector machines", "Intrusion Detection using Fuzzy logic", "Intrusion Detection using Neural Network", "Intrusion Detection using Decision Tree", "Intrusion Detection using Genetic Algorithm", "Intrusion Detection using Machine Learning" and "Review of Intrusion Detection using Machine Learning". Using the keywords mentioned above to search for papers focusing on Machine Learning techniques for developing IDS, more than 50 papers were retrieved.

Practical screen

The studies considered for examination are those published in journals, conference proceedings and published between 2009 and 2018. All the papers selected for review are published in English. On the other hand, studies which are not published between 2009 and 2018 in English and those that do not focus explicitly on the IDS approaches and IDS using Machine Learning techniques were eliminated without further examination.

Quality appraisal

After the practical screen, certain criteria were used to judge articles if they are of quality to be reviewed in this study. The criteria involved if the article provided a performance analysis results or highlighted out certain strengths and limitations of IDS approaches or machine learning technique used for intrusion detection system. A total of 32 papers were considered for review as they met the criteria used to judge the quality of the articles.

Data extraction and synthesis of studies

After identifying the studies considered to be of quality, applicable information regarding IDS approaches or machine learning techniques for IDS was then systematically extracted from each study. The facts extracted from the studies were then combined.

Literature Review

In this section, we first give an overview of the main type of attacks to an IDS. Then we describe the approaches and techniques that are being used to develop this kind of system, as well as metrics to evaluate the performance of the techniques.

An attack is a security threat that involves, but is not limited to, attempting to steal, obtaining and altering information without authorized access or gaining access to a network without permission. An attack can be

anything that has characteristics that can compromise information or a network. The four major categories of attacks that exist are Denial of Service (DoS), User to Root (U2R), Remote to User (R2L) and Probing (Ahmed, Naser Mahmood, Hu 2016; Agrawal, Soni, Agrawal 2017). In the next sessions, these categories of attacks are described.

Denial of Service Attack

Denial of Service is a type of attack whereby the attacker aims to prevent the authorised user from using the computer services. DoS can be done by flooding the network and disrupting a connection or service. Examples of DoS attacks include Smurf, Land and Ping of Death (Pod) (Dias, Cerqueira, Assis, Almeida 2017).

User to Root Attack

The user to root attack is a type of attack whereby the attacker gets access to a normal user account and then exploits system vulnerabilities to gain root privileges. Examples of U2R attacks are Loadmodule, Rootkit and Buffer_overflow (Dias, Cerqueira, Assis, Almeida 2017).

Remote to User Attack

The remote to User attack is a type of attack whereby the attacker aims to get unauthorised access to a local machine to send packets over the network. An R2L attack allows the attacker to have privileges which a local user normally have when using that computer. Examples of U2L attacks are Ftp_write, Warezclient and Imap (Dias, Cerqueira, Assis, Almeida 2017).

Probing

A probe is a program that can be used to automatically scan and monitor the network activities or collect data from the network. The attacker collects information about the network and also finds vulnerabilities which can be used to attack the network. Examples of probing attacks are Ipsweep, Nmap and Portsweep (Dias, Cerqueira, Assis, Almeida 2017).

Performance metrics/variables

Various performance metrics can be used to evaluate and assess the performance of different techniques. Some of the performance metrics that have been used in several studies (Kumar 2014; Agrawal, Soni, Agrawal 2017) are described below.

Accuracy

Accuracy is how the IDS is able to detect intrusions and to give true alarms when an intrusion is truly present and detected. The Accuracy of the IDS is measured by the ratio between the correctly classified instances to the total number of samples present in the dataset (Agrawal, Soni, Agrawal 2017).

Timeliness

It is the average time taken by the IDS to detect or report an intrusion from the time it occurred. The IDS should be able to give a quick response regarding an intrusion (Agrawal, Soni, Agrawal 2017).

Efficiency

The use of resources allocated to the system in carrying out intrusion detections. The system is regarded to be efficient if it uses the resources to detect intrusions in a timely manner (Kumar 2014).

Effectiveness

Effectiveness is the ability of the system to distinguish between intrusion activities and non-intrusion activities (Kumar 2014). An IDS is effective if it has a low number of false alarm rate which is regarded as the ratio between incorrect instances of the total number of normal instances (Agrawal, Soni, Agrawal 2017).

Reliability

It is how well a detection approach performs its required functions in a particular time period under stated conditions or in the case of a failure (Kaur, Kumar, Bhandari 2017).

Implementation cost

Total cost needed for implementing a particular detection technique on the source-end, victim end or core-end network (Kaur, Kumar, Bhandari 2017).

Intrusion detection approaches

An intrusion detection system is a device or software application that monitors the network or system for malicious activities or policy violation (Agrawal, Soni, Agrawal 2017). Several approaches are used for creating intrusion detection systems. These approaches include Statistical-Based Anomaly, Pattern Matching, Data Mining and Machine Learning.

Statistical-Based Anomaly

The Statistical-Based Anomaly detection approach uses statistical analysis to assess the user or system behaviour by checking the values of various variables such as login session variables (Jose, Malathi, Reddy, Jayaseeli 2018). This approach uses statistical properties during anomaly detection to determine if a certain action is an intrusion or normal action to the system.

Pattern Matching

Pattern matching approach detects intrusions based on matching the existing patterns with the incoming traffic patterns (Agrawal, Soni, Agrawal 2017). Intrusions are detected by comparing the current pattern with the known patterns or attack signatures that are already known. This means that the attack signatures are updated frequently and the system will recognise the known attacks from the saved signatures.

Data Mining

The data mining approach is used to extract data from databases. It is also used to detect intrusions where the data set is very large to process (Agrawal, Soni, Agrawal 2017).

Machine Learning

Machine learning is an approach whereby a system learns and keeps improving its learning capabilities. Machine learning is used when new attacks need to be recognised frequently (Agrawal, Soni, Agrawal 2017). Machine Learning techniques include Neural Networks, Fuzzy Logic and Support Vector Machine techniques. Table 1 outlines the aforementioned approaches with their main strengths and limitations.

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 1, Enero - Marzo, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 58-78

Table 1 - Strengths and limitations of the different approaches used to implement IDS.

Detection Approach	**Strengths**	**Limitation**
Statistical-Based Anomaly	- Does not require previous knowledge of security issues (Marcelino, Pessoa, Vieira, Salvador, Mendes 2018) and of the normal activity of the target system (García-Teodoro, Díaz-Verdejo, Maciá-Fernández, Vázquez 2009). - It can detect new attacks (Jose, Malathi, Reddy, Jayaseeli 2018). - Has the ability to learn the expected behaviour of the system from observations (García-Teodoro, Díaz-Verdejo, Maciá-Fernández, Vázquez 2009). - Can provide accurate notification of malicious activities occurring over long periods of time (García-Teodoro, Díaz-Verdejo, Maciá-Fernández, Vázquez 2009).	- Requires assumption based parameters of a process which cannot be suitable for accurate anomaly detection systems. - Highly rely on an assumption that the data is generated from a particular distribution. This assumption is usually incorrect. - Can be trained by an attacker, causing the network traffic generated during the attack to be considered as normal. - Can generate high numbers of false alarms.
Pattern Matching	- Simple to implement and used to detect simple misuse detection (Agrawal, Soni, Agrawal 2017). - Not very complex and not resource consuming (Agrawal et al., 2017).	- It can only recognise the known attacks; cannot find new activities. - Limited to misuse detection. - Anomaly detection is not possible with pattern matching.
Data Mining	- Detects both misuse and anomaly detection (Agrawal, Soni, Agrawal 2017). - Useful for extracting patterns from a large data store (Agrawal, Soni, Agrawal 2017). - Reduces storage of a large amount of data by creating the metadata useful for anomaly detection (Jose, Malathi, Reddy, Jayaseeli 2018).	- Time-consuming on huge databases. - Fail to be applied in real-time detection environment. - Due to unpredictable changes in the behaviour patterns of users, a large number of false alarms are produced.
Machine Learning	- Detects both misuse and anomalous intrusions automatically (Agrawal, Soni, Agrawal 2017). - Hardly needs human intervention (Agrawal, Soni, Agrawal 2017). - Very flexible and adaptable (García-Teodoro, Díaz-Verdejo, Maciá-Fernández, Vázquez 2009). - The testing phase is fast as each test instance is compared against the pre-computed model (Khandagale, Kalshetty 2013).	- Can only label test instances and cannot give meaningful anomaly score.

Partial conclusions

Statistical-Based Anomaly approach and the data mining approach generates high numbers of false alarms. This shows that these approaches can be considered to be less accurate as the number of false alarm rate should be low for the IDS to have high accuracy. With regards to accuracy, the Statistical-Based Anomaly approach is further not recommended for anomaly detection systems that need to be accurate as it does not provide high accuracy.

Data Mining Approach is known to be not suitable to be applied to real-time detection environments. This is a limitation as intrusion detection needs to be detected early, requiring the IDS to perform tasks in real time. Intrusion detection systems are developed using different approaches. Ideally, the IDS should be able to detect intrusions, especially the four major categories of attacks (DoS, U2R, R2L and Probing).

Different intrusion detection approaches have their strengths and limitations. The machine learning approach is an automated process which hardly needs human intervention. The ability of the IDS to run continually with minimal or no human supervision is emphasised to be a desirable characteristic of an IDS. Therefore, the machine learning approach meets the desirable characteristic of IDS of minimal human supervision and automation.

Intrusion detection approaches can be used according to the needs and requirements of the IDS. However, with the strong characteristics of the machine learning approach described, this study recommends the use of the machine learning approach to implement an IDS that needs to be running all the time with no (or very small) human supervision.

Machine learning techniques

Bellow, we examine different machine learning techniques that can be used to develop an IDS.

Support Vector Machine

Support vector machines (SVM) is a type of machine learning technique which performs different classification tasks, analyse data and recognise patterns (Chowdhury, Ferens, Ferens 2016). SVMs are used to implement IDS which are able to provide real-time detection of intrusions (Shah, Hayat, Awan 2015).

Fuzzy Logic

Fuzzy logic can be used in anomaly IDS as it deals with decision making and reasoning (Shah, Hayat, Awan 2015). Additionally, fuzzy logic techniques are used for anomaly detection as they allow an object to belong to different classes at the same time, making it useful for detecting intrusions (Singh, Nene 2013).

Artificial Neural Network

Artificial Neural Network (ANN) is a mathematical model that can be used for classification (Shah, Hayat, Awan 2015). It estimate if the input data matches the characteristics that it has been trained to recognize (Jha, Ragha 2013). (Patel, Jhaveri 2015) points out that the main objective of using neural network approach for intrusion detection is to learn the behaviour of different actors in the system. IDSs can be developed using Deep Learning which is defined by (Chollet 2017) as "a subfield of machine learning: a new take on learning representations from data that puts an emphasis on learning successive layers of increasingly meaningful representations". According to (Ponkarthika, Dr, Saraswathy 2018), Deep Learning achieves a high level abstractions in data by using a complex architecture which causes the IDS to have a high detection rate. Currently, Convolutional Neural Networks (CNN) and the Recurrent Neural Networks (RNN) are the two Deep Learning architectures that can be used to build IDSs.

CNNs are an extension to traditional feed forward networks, which according to, improves the accuracy of intrusion detection for threat classification by using enhanced behaviour features. Several studies (LIU, LIU, ZHAO 2017; Vinayakumar, Soman, Poornachandran 2017; Mohammadpour, Ling, Liew, Chong 2018) have indicated that CNNs for IDSs needs future work such as improving false alarm rate, improving normal data learning quantity to reduce false alarm rate and provide real data for learning and testing.

RNNs can be used for supervised classification learning and has the ability to generalise the knowledge that can be used to identify seen and unseen threats in IDSs (Mohammadpour, Ling, Liew, Chong 2018). Additionally, RNNs also has a strong modelling capabilities for intrusion detection with high accuracy and detection rate and a low false positive rate, especially when it comes to classification of the NSL-KDD dataset (Lin, Lin, Wang, Wu, Tsai 2018). In detecting intrusions, RNNs tend to outperform other models such as CNN with high accuracy percentages since CNNs are designed for image processing applications (Vani 2007).

Decision Trees

Decision Trees constitute a powerful model (Shah, Hayat, Awan 2015) used for classification problems (Singh, Nene 2013). (Rai, Devi, Guleria 2016), describes Decision Trees as a tree-like graph consisting of internal nodes which represent a test on an attribute, branches which are the outcome of the test and leaf nodes which is a class label. Since decision trees are powerful for classification, they used to implement IDSs which are able to classify intrusions and be able to detect them.

Genetic Algorithm

Genetic Algorithms (GA) conform a search method or optimization technique that is based on genetic principle and natural selection (Wang, Yang, Ren 2009). According to (Sharma, Nema 2013), GA has been recently used to support IDSs, by creating new rules from available rules and GAs also allows an IDS solution to be of high quality as the GA uses the principle of selection and evolution.

Naïve Bayesian Networks

Naïve Bayesian networks are one of the most widely used graphical models to represent and handle uncertain information (Amor, Benferhat, Elouedi 2003). A study have shown that Naïve Bayes with it's simple structure and strong assumption is able to provide competitive results when it comes to detecting intrusions. also suport that the Naïve Bayesian Network has certain properties that makes them useful and accurate, which are desired characteristics of an IDS (Amor, Benferhat, Elouedi 2003)

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 1, Enero - Marzo, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 58-78

Table 2 Outlines the aforementioned Machine Learning techniques, together with their strengths and limitations.

Table 2 - Strengths and weaknesses of machine learning techniques used to develop IDS.

Machine Learning Technique	**Strengths**	**Limitations**
Neural Networks	- Does not need expert knowledge and it can find unknown or novel intrusions (Shah, Hayat, Awan 2015). - It is flexible, fast and can analyse the non-linear data set with multi-variable (Shah, Hayat, Awan 2015). - Can make decisions quickly and provides real-time detection.	- Over-fitting may happen during neural network training.
Bayesian Network	- Can incorporate both Prior knowledge and data (Shah, Hayat, Awan 2015).	- May not contain any good classifiers if prior knowledge is wrong.
Support Vector Machine	- Can learn a larger set of patterns and be able to scale better (Singh, Nene 2013). - has the ability to update the training patterns dynamically whenever there is a new pattern during classification (Jha, Ragha 2013).	- Mostly uses binary classifier which cannot give additional information about detected type of attack. - Requires processing of raw features for classification which increases the architecture complexity and decreases the accuracy of detecting intrusion.
Genetic Algorithm	-Can solve many practical classification problems, involving small samples and non-linear problem (Singh, Nene 2013).	- Cannot assure constant optimization response times.
Fuzzy Logic	- Effective against port scans and probes (Shah, Hayat, Awan 2015).	- Involves high resource consumption.
Decision Tree	- Works well with huge datasets (Singh, Nene 2013). - High detection accuracy (Jha, Ragha 2013; Shah, Hayat, Awan 2015). -Fast adaptation (Jha, Ragha 2013) - Works well in real-time Intrusion Detection as it gives the highest detection performance (Singh, Nene 2013).	- Too many categories can significantly reduce the classification accuracy.

Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 58-78

Discussion

Intrusion detection systems are developed using different approaches. Ideally, the IDS should be able to detect intrusions, especially the four major categories of attacks (DoS, U2R, R2L and Probing). Different intrusion detection approaches have their strengths and limitations. The machine learning approach is an automated process which hardly needs human intervention.

Statistical-Based Anomaly approach and the Data Mining approach generates high numbers of false alarms. This shows that these approaches can be considered to be less accurate as the number of false alarm rate should be low for the IDS to have high accuracy. With regards to accuracy, the Statistical-Based Anomaly approach is further not recommended for anomaly detection systems that need to be accurate as it does not provide high accuracy. Data Mining Approach is known to be not suitable to be applied to real-time detection environments. This is a limitation as intrusion detection needs to be detected early, requiring the IDS to perform tasks in real time.

The ability of the IDS to run continually with minimal or no human supervision is emphasised to be a desirable characteristic of an IDS, therefore, the machine learning approach meets the desirable characteristic of IDS of minimal human supervision and automation.

Intrusion detection approaches can be used according to the needs and requirements of the IDS. However, with the strong characteristics of the machine learning approach described, this study recommends the use of the machine learning approach in implementing an IDS that needs to be running all the time with no (or very small) human supervision.

Different Machine Learning techniques used for intrusion detection have their strengths and limitations.

Bayesian Networks technique can incorporate prior knowledge in detecting intrusions. The lack of good classifiers can cause the IDS to not perform with high accuracy as expected.

Fuzzy Logic is known to be effective in detecting probes, unfortunately it involves high resource consumption in detecting the intrusions.
Genetic algorithm cannot assure constant optimization response times which is not suitable for IDS as they require an optimised response time to detect intrusions.

Decision Tree works well when detecting intrusions from huge data sets, providing high detection accuracy. Additionally, Decision Tree also work well in real-time intrusion detection where they give the highest detection performance. However, the classification accuracy of Decision Tree can be significantly reduced due to many categories.

Support Vector Machine technique provides real-time detection capability and, the ability to update the training patterns dynamically whenever there is a new pattern during classification. On the other hand, the raw features required by SVM for classification increases the architecture complexity, decreasing the accuracy of detecting intrusion.

Neural Networks have the ability to make decisions quickly and detect intrusions in real time, providing high accuracy. This is a strong characteristic of Neural Networks in detecting intrusions as intrusions are expected to be detected in real time to prevent attackers from causing harm to the system. Neural network also does not need expert knowledge, meaning it needs minimum human intervention in order to detect intrusions. Recurrent Neural networks specifically offers a higher accuracy and detection rate, together with low false positive rate and therefore can be considered ideal for building.

Conclusions

This study provided an overview of the different intrusion detection approaches used in implementing IDS. The results show that different intrusion detection approaches have their strengths and limitations which could be improved to make the approaches better. It is concluded that the Machine Learning approach is suitable for implementing IDS solutions in real time with no (or little) human supervision because of its ability to work as an automated process which hardly needs human intervention. The study, therefore, recommends the use of Machine Learning approach to implementing an IDS.

This study also provided an overview of the Machine Learning techniques used in implementing IDSs. The results show that the Machine Learning techniques have different strengths and limitations. It is concluded that the Neural Network is suitable for implementing IDS solutions in real time as they have the ability to make decisions quickly. Neural Networks also needs minimum human intervention in order to detect intrusions. The study specifically found the Recurrent Neural Networks to be ideal for building IDS as they provide a high accuracy and detection rate, together with low false positive rate. The study, therefore, recommends the use of Neural Networks to implement effective IDSs that needs minimum human intervention and detect intrusions in real time.

References

1. AGRAWAL, Gaurav, SONI, Shivank Kumar and AGRAWAL, Chetan, 2017. A SURVEY ON ATTACKS AND APPROACHES OF INTRUSION DETECTION SYSTEMS. *International Journal of Advanced Research in Computer Science*. 30 August 2017. Vol. 8, no. 8, p. 499–504. DOI 10.26483/ijarcs.v8i8.4771.

2. AHMED, Mohiuddin, NASER MAHMOOD, Abdun and HU, Jiankun, 2016. *A survey of network anomaly detection techniques*. 1 January 2016. Academic Press.

3. AMOR, Nahla Ben, BENFERHAT, Salem and ELOUEDI, Zied, 2003. Naive Bayesian Networks in Intrusion Detection Systems. In: *The Fourteenth European Conference on Machine Learning*. 2003.

4. CHOLLET, François, 2017. *Deep Learning with Python*. Manning Publications.

5. CHOUDHARY, Amit Kumar and SWARUP, Akhilesh, 2009. Neural network approach for intrusion detection. In: *ACM International Conference Proceeding Series*. 2009. p. 1297–1301. ISBN 9781605587103.

6. CHOWDHURY, Md. Nasimuzzaman, FERENS, Ken and FERENS, Mike, 2016. Network Intrusion Detection Using Machine Learning. In: *International Conference on Security and Management*. 2016.

7. DIAS, L. P., CERQUEIRA, J. J.F., ASSIS, K. D.R. and ALMEIDA, R. C., 2017. Using artificial neural network in intrusion detection systems to computer networks. In: *2017 9th Computer Science and Electronic Engineering Conference, CEEC 2017 - Proceedings*. Institute of Electrical and Electronics Engineers Inc. 8 November 2017. p. 145–150. ISBN 9781538630075.

8. GARCÍA-TEODORO, P., DÍAZ-VERDEJO, J., MACIÁ-FERNÁNDEZ, G. and VÁZQUEZ, E., 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers and Security*. February 2009. Vol. 28, no. 1–2, p. 18–28. DOI 10.1016/j.cose.2008.08.003.

9. JHA, J. and RAGHA, L, 2013. Intrusion detection system using support vector machine. In: *International Conference and workshop on Advanced Computing*. 2013. p. 25–30.

10. JOSE, Shijoe, MALATHI, D., REDDY, Bharath and JAYASEELI, Dorathi, 2018. A Survey on Anomaly Based Host Intrusion Detection System. In: *Journal of Physics: Conference Series*. Institute of Physics Publishing. 26 April 2018.

11. KADAM, Priya U and DESHMUKH, ProfManjusha, 2007. Various Approaches for Intrusion Detection System: An Overview. *International Journal of Innovative Research in Computer and Communication Engineering (An ISO* [online]. 2007. Vol. 3297, no. 11. [Accessed 2 December 2019]. Available from: www.ijircce.com

12. KAUR, Parneet, KUMAR, Manish and BHANDARI, Abhinav, 2017. A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering* [online]. 20 January 2017. Vol. 5, no. 1, p. 301–320. [Accessed 2 December 2019]. DOI 10.1080/21642583.2017.1331768. Available from: https://www.tandfonline.com/doi/full/10.1080/21642583.2017.1331768

13. KHANDAGALE, Vaishali V and KALSHETTY, Yoginath, 2013. Review and Discussion on different techniques of Anomaly Detection Based and Recent Work. *International Journal of Engineering Research & Technology (IJERT)* [online]. 2013. Vol. 2, no. 10, p. 5. [Accessed 2 December 2019]. Available from:

www.ijert.org

14. KUMAR, Gulshan, 2014. *Evaluation Metrics for Intrusion Detection Systems - A Study*. 2014.

15. LIN, Wen Hui, LIN, Hsiao Chung, WANG, Ping, WU, Bao Hua and TSAI, Jeng Ying, 2018. Using convolutional neural networks to network intrusion detection for cyber threats. In: *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*. Institute of Electrical and Electronics Engineers Inc. 22 June 2018. p. 1107–1110. ISBN 9781538643426.

16. LIU, YUCHEN, LIU, SHENGLI and ZHAO, XING, 2017. Intrusion Detection Algorithm Based on Convolutional Neural Network. In: *4th International Conference on Engineering Technology and Application (ICETA 2017)*. DEStech Publications. 23 March 2017.

17. MARCELINO, Maria José, PESSOA, Teresa, VIEIRA, Celeste, SALVADOR, Tatiana and MENDES, António José, 2018. Learning Computational Thinking and scratch at distance. *Computers in Human Behavior*. 2018. Vol. 80, p. 470–477. DOI 10.1016/j.chb.2017.09.025.

18. MOHAMMADPOUR, L, LING, T.C., LIEW, C. S. and CHONG, C. Y., 2018. A Convolutional Neural Network for Network Intrusion Detection System. In: *Proceedings of the Asia-Pacific Advanced Network* [online]. 2018. p. 6. [Accessed 3 December 2019]. Available from: http://journals.sfu.ca/apan/index.php/apan/article/view/239

19. OKOLI, Chitu and SCHABRAM, Kira, 2012. A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electronic Journal*. 5 January 2012. DOI 10.2139/ssrn.1954824.

20. PATEL, Nirav J. and JHAVERI, Rutvij H., 2015. Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey. In: *International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE*. Institute of Electrical and Electronics Engineers Inc. 10 March 2015. p. 468–472. ISBN 9781479961085.

21. PONKARTHIKA, M, DR and SARASWATHY, V R, 2018. Network Intrusion Detection Using Deep Neural Networks. *Asian Journal of Applied Science and Technology (AJAST) (Open Access Quarterly International Journal* [online]. 2018. Vol. 2, no. 2, p. 665–673. [Accessed 2 December 2019]. Available from: www.ajast.net

22. RAI, Kajal, DEVI, S. and GULERIA, Ajay, 2016. Decision Tree Based Algorithm for Intrusion Detection. *International Journal Advanced Network and Applications*. 2016. Vol. 7, no. 4, p. 2828–2834.

23. RICHARIYA, Vineet, SINGH, Uday Pratap and MISHRA, Renu, 2012. *Distributed Approach of Intrusion Detection System: Survey*.

24. SARMAH, Abhijit, 2019. *Intrusion Detection Systems: Definition, Need and Challenges* [online]. [Accessed 2 December 2019]. Available from: https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343

25. SCHELL, Bernadette H. and MARTIN, Clemens., 2006. *Webster's new world hacker dictionary*. Wiley Pub. ISBN 0470047526.

26. SHAH, Asghar Ali, HAYAT, Malik Sikander and AWAN, Muhammad Daud, 2015. Analysis of Machine Learning Techniques for Intrusion Detection System: A Review. *International Journal of Computer Applications*. 2015. Vol. 119, no. 3, p. 19–29.

27. SHARMA, Vikas and NEMA, Aditi, 2013. Innovative genetic approach for intrusion detection by using decision tree. In: *Proceedings - 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013*. 2013. p. 418–422.

28. SINGH, J and NENE, MJ, 2013. A survey on machine learning techniques for intrusion detection systems. *International Journal of Advanced Research in Computer and Communication Engineering* [online]. 2013. Vol. 2, no. 11, p. 4349–55. [Accessed 2 December 2019]. Available from: http://www.sciepub.com/reference/212012

29. VANI, R, 2007. Towards Efficient Intrusion Detection using Deep Learning Techniques: A Review. *International Journal of Advanced Research in Computer and Communication Engineering ISO*. 2007. Vol. 3297. DOI 10.17148/IJARCCE.2017.61066.

30. VINAYAKUMAR, R., SOMAN, K. P. and POORNACHANDRAN, Prabaharan, 2017. Evaluation of recurrent neural network and its variants for intrusion detection system (IDS). *International Journal of Information System Modeling and Design*. 1 July 2017. Vol. 8, no. 3, p. 43–63. DOI 10.4018/IJISMD.2017070103.

31. WANG, Juan, YANG, Qiren and REN, Dasen, 2009. An intrusion detection algorithm based on decision tree technology. In: *Proceedings - 2009 Asia-Pacific Conference on Information Processing, APCIP 2009*. 2009. p. 333–335. ISBN 9780769536996.

Conflicto de interés

No existe conflicto de interés con este trabajo.

Contribuciones de los autores

El primer autor contribuyo el 60% del trabajo y el segundo el 40%.

Financiación

No se obtuvo financiamiento para realizar este trabajo.