Intrusion Detection Systems

Subjects: Computer Science, Software Engineering

Contributor: __ Imran

Intrusion detection systems and intrusion prevention systems are to prevent network intruders' attack and malicious compliance. Network communities have produced benchmark datasets available for researchers to improve the accuracy of intrusion detection systems. The scientific community has presented data mining and machine learning-based mechanisms to detect intrusion with high classification accuracy.

Keywords: intrusion detection ; intrusion accuracy ; automated machine learning ; CICIDS2017 ; UNSW-NB15

1. Introduction

An expeditious rise in the development of network and communication technologies leads to an immense amount of network data generated from a wide range of services. For instance, pervasive computing networks such as the Internet of Things (IoT) generate enormous data [1][2][3]. A wide range of network applications is developed in every domain of life, including business, healthcare, smart homes, and smart cities, to name a few [4][5][6][7]. The plethora of high-dimensional data increases the need for analysis tools based on advanced data mining and statistical methods [8][9]. There is a dire need to tune the contemporary data mining and statistical methods to address the challenges of the growing internet applications, such as bandwidth handling, network intrusion detection, and scalability. Network applications and resources' security using intrusion detection systems, intrusion prevention systems, and hybrid systems are becoming more challenging due to the enormous number of diverse networking applications. However, the rule-based approach for the analysis of enormous data has many limitations. The existing state-of-the-art intrusion detection-based systems focus on increasing the reliability aspect of these applications [10]. An efficient intrusion detection system can strengthen the defense system of such applications against anomalies and network intrusion attacks. The intrusion detection system also provides real-time analysis of the collected critical reconnaissance data during defensive attacks. Intrusion detection systems based on artificial intelligence(AI) hold a significant potential to enhance the performance of detection mechanisms by learning from historical data and real-time data patterns.

Scientific community has presented various machine learning-based intrusion detection systems such as support vector machine (SVM) [11], Naive Bayes (NBs) [12], clustering [13], artificial neural network (ANN), and deep learning network (DNN) [14]. Conventional machine learning algorithms can better classify small and low dimension datasets. However, the classification accuracy of these algorithms deteriorates when it comes to addressing problems involving high dimensionality and nonlinearity. Hence, the need for intrusion detection models to address the classification accuracy problem increases as AI advances. For example, a convolutional neural network (CNN) [15] and long short-term memory (LSTM) [16] have been applied in natural language processing (NLP) and computer vision applications. The problem with deep learning techniques such as CNN and LSTM is adaptability to nonlinear and high-dimensional data. The issue of nonlinearity has been addressed in CNN and LSTM for modeling nonlinear systems [17][18][19][20][21][22]. In literature, the issues of high dimensional data are handled in CNN, and LSTM using a deep learning paradigm [23][24][25][26]. Automated machine learning (autoML) is a newly emerged subfield of machine learning and data science. The feasible adaptability of autoML makes it equally useful for trainees of machine learning, data scientists, and machine learning engineers. Research articles demonstrate that autoML can revolutionize constructing machine learning models without machine learning expertise and knowing technical specifications. AutoML architectures produce a code pipeline by suggesting and selecting a model from a list of machine learning model-based input datasets [27]. The selection is performed based on the accuracy of these machine learning models. AutoML results in coding the pipeline of the best performing model, which will be very difficult to find using manual configurations of the models' parameters.

2. Anomaly Detection in Network Intrusion Environments

Artificial intelligence is taking over the current era and is changing the current era into a revolutionary practical world. Data analysis, predictive analytics and optimization models are used for many real-life applications [28][29][30]. Anomaly detection is a type of data analysis used to identify irregular and abnormal data from a given data set. Anomaly detection is the approach used in data mining applications for discovering and finding patterns inside the data [31]. It is also used as a standalone module in many studies related to machine learning and statistics applications. Deviation detection, outlier detection, and exception mining are related terms used for anomaly detection [32]. Narayana et al. defined anomaly as a mechanism generated from the deviation of several observations [33]. Anomaly detection is used in several scientific domains such as healthcare, intrusion detection, sensor network, and fraud detection, to name a few. Detecting irregularities in the network, identifying anomalies in financial transactions, detecting fraudulent activities, and detecting anomalies in medical images are some anomaly detection applications [34]. In networks, anomaly patterns can be identified based on the classification of packet data containing abnormal patterns.

Xie et al. published a survey study related to intrusion detection in wireless sensor networks [35]. According to most of the studies, intrusion detection depends on the communication medium; for example, wired connection-based techniques cannot be applied to the wireless communication medium. The survey emphasizes the need for standard anomaly detection techniques for all types of networks. One challenge for detecting anomalies in the network is the lack of a comprehensive dataset. Most of the current anomaly detection systems are based on supervised approaches that use labeled data knowledge. During the past few years, research has been conducted in network intrusion detection segregated into audit source, network behavior, detection method, location, frequency of usage, and detection method. In [36], Debar et al. presented a standard technique based on the extension of transaction-based detection paradigm. Axelsson et al. [37] proposed a study based on detection principle and focus on operational aspects. Furnell et al. [38] proposed an intrusion matrix based on the data scale and output type. Estevez-Tapiador et al. presented a wired-based network intrusion detection based on anomaly detection [39]. Boukerche et al. presented an outlier-based classified detection approach using the unsupervised and supervised models [40]. Under the supervised category, a proximity-based technique has been used recently [41].

Chandola et al. also presented another detailed survey study on anomaly detection [42]. Their study presents different techniques related to intrusion detections. Some studies proposed several anomaly detection techniques based on supervised, unsupervised, and clustering methods [43][44][45][46][47]. The lack of discussion and research problems in the available datasets are one of the research gaps that need to be addressed. The most used datasets for network anomaly detection are the DARPA/KDD, which developed in 2013. Various variants of datasets are developed based on this dataset to address the causes of data errors and inconsistency. As network anomaly detection based on the aforementioned dataset has no significant performance improvements; therefore, more anomaly detection datasets have been introduced recently to improve intrusion detection system efficiency. Some research surveys focused on these dataset issues and challenges to develop an efficient intrusion detection system [48]. The network attack profile feature relies on classification-based techniques and the size of the data [49]. The intrusion detection system process is based on the signature of the attack and the capability of intrusion detection system to detect the attack from data patterns [50]. The intrusion detection engine can also enhance the defense system using intelligent mechanisms for various attacks' variants. This process is quite expensive for creating a new attack in case of loss or replacement [51]. Furthermore, the regular traffic does not contain the knowledge base attack, and it will be raising the wrong alarms.

In summary, anomaly detection mechanisms are costly in terms of time and are relying on the existing network traffic dataset. Furthermore, keeping the standard profile up-to-date is very difficult in today's network. The network traffic analysis dataset does not have easy access due to privacy limitations. Examples of benchmark datasets for intrusion detection are DARPA/KDD, UNSW-NB15, CICIDS2017, and CSE-CIC-IDS2018 [52]. The main challenge that needs to be addressed is improving intrusion detection systems' accuracy on these benchmarks' datasets. **Table 1** presents a summary of existing intrusion detection and prevention systems organized as applications, datasets, models, and relative demerits.

Table 1. Summary of existing intrusion detection and prevention systems.

Application	Datasets	Model	Relative Demerits
Anomaly Detection [53]	**InSDN**	**TRW-CB algorithm**	**Standardized programmability and can predict anomalies in SOHO Network**
DoS attacks detection [54]	**KDD-99**	**Self-organizing maps, ANN**	**Lightweight DDoS Flooding Attack but do not have any flow rules installed.**
Anomaly Detection [55]	**NSL-KDD**	**DNN approach**	**Does not scale well for commercial product but is a good alternative solution for signature-based intrusion detection system**

Application	Datasets	Model	Relative Demerits
DDoS Detection System [56]	**Simulated data**	**Stack auto-encoder and DNN**	**Detect all DDoS attack, but has a Controller bottleneck in a wide networks.**
Intrusion Detection [57]	**Simulated data**	**Self organizing map and learning vector quantization**	**Detect U2R attacks but limited to deep packet inspection technique.**
Monitor traffic flow [58]	**Simulated data**	**Flow analysis tool**	**Improve computation time of flow but difficult to handle due to batch processing. Flow analysis tools are not compatible with the MapReduce interface.**
P2P botnet detection [59]	**CAIDA, simulated data**	**Random forest**	**Process high bandwidth and efficiently analyze malicious traffic data. However, the high drop rate of packets and delay in detection make it inefficient for new complex threats.**
Intrusion detection [60]	**NSL-KDD 99**	**NB tree, random forest**	**Improved performance accuracy reduces false-positive rate for hybrid approaches, but the false-positive rate is high for non-hybrid approaches.**
Phishing-based attack detection [61]	**Simulated data**	**Collaborative mechanism**	**Practical method for generalization to any attacks but no validation with real datasets.**
Intrusion detection [62]	**KDD 99, CMDC 2012**	**OneR algorithm, KNN, SVM**	**Faster but feature reduction and training mechanism is real overhead.**
Malware detection [63]	**Simulated data**	**Choi–Williams distribution**	**Effective for Kelihos injection but not tested with real datasets.**
Intrusion detection system [64]	**Simulated data**	**RSFSA, fuzzy logic based SVM**	**Faster mechanism for decision attributes and log data reduction though not tested with real datasets.**
Network traffic monitoring [65]	**CAIDA**	**IP Trace Analysis System**	**Useful for passive analysis but does not provide a fine-grained analysis.**

3. Conclusions

An expeditious rise in the development of network applications leads to an immense amount of network data generated from a wide range of services for large user groups. Safeguarding network applications and things connected to the internet has always been a point of interest for researchers. Many studies propose solutions for intrusion detection systems and intrusion prevention systems. Nevertheless, there is a dire need to tune the contemporary data mining and statistical methods to address the challenges of the growing internet applications, such as bandwidth handling, network intrusion detection, and scalability. We present an intrusion detection system based on the ensemble of prediction and learning mechanisms to improve anomaly detection accuracy in a network intrusion environment. Case studies of intrusion detection are implemented using publicly available benchmark intrusion detection datasets UNSW-NB15 and CICIDS2017. The performance of the proposed model is compared with some contemporary models, including DNN, autoML, and other algorithms from the literature on these benchmark datasets. The performance evaluation is compared in terms of accuracy, precision, recall, and F1 score. The proposed model accuracy for the UNSW-NB15 dataset is 98.801 percent, and the CICIDS2017 dataset is 97.02 percent. The performance comparison analysis shows significant improvements in the intrusion accuracy, detection rate, and F1 score. As part of future work, the proposed intrusion detection model will be leveraged for IoT-cloud applications for detecting anomalies in the sensing data.

References

1. Ghaffar, Z.; Alshahrani, A.; Fayaz, M.; Alghamdi, A.M.; Gwak, J. A Topical Review on Machine Learning, Software Defined Networking, Internet of Things Applications: Research Limitations and Challenges. Electronics 2021, 10, 880.
2. Ahmad, S.; Kim, D. Design and Implementation of Thermal Comfort System based on Tasks Allocation Mechanism in Smart Homes. Sustainability 2019, 11, 5849.
3. Ahmad, S.; Kim, D.H. Quantum GIS Based Descriptive and Predictive Data Analysis for Effective Planning of Waste Management. IEEE Access 2020, 8, 46193–46205.

4. Iqbal, N.; Ahmad, S.; Kim, D.H. Health Monitoring System for Elderly Patients Using Intelligent Task Mapping Mechanism in Closed Loop Healthcare Environment. Symmetry 2021, 13, 357.
5. Imran; Ahmad, S.; Kim, D.H. A Task Orchestration Approach for Efficient Mountain Fire Detection Based on Microservice and Predictive Analysis in IoT Environment. J. Intell. Fuzzy Syst. 2021, 40, 5681–5696.
6. Iqbal, N.; Ahmad, S.; Kim, D.H. Towards Mountain Fire Safety Using Fire Spread Predictive Analytics and Mountain Fire Containment in IoT Environment. Sustainability 2021, 13, 2461.
7. Iqba, N.; Ahmad, S.; Ahmad, R.; Kim, D.-H. A Scheduling Mechanism Based on Optimization Using IoT-Tasks Orchestration for Efficient Patient Health Monitoring. Sensors 2021, 21, 5430.
8. Camastra, F. Data dimensionality estimation methods: A survey. Pattern Recognit. 2003, 36, 2945–2954.
9. Di Mauro, M.; Galatro, G.; Fortino, G.; Liotta, A. Supervised feature selection techniques in network intrusion detection: A critical review. Eng. Appl. Artif. Intell. 2021, 101, 104216.
10. Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. 2013, 36, 16–24.
11. Bhati, B.S.; Rai, C. Analysis of Support Vector Machine-based Intrusion Detection Techniques. Arab. J. Sci. Eng. 2020, 45, 2371–2383.
12. Kanth, A.R. Gaussian Naıve Bayes Based Intrusion Detection System. In Proceedings of the 11th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2019), Hyderabad, India, 13–15 December 2020; Springer Nature: Berlin/Heidelberg, Germany, 2020; Volume 1182, p. 150.
13. Markiewicz, R.P.; Sgandurra, D. Clust-IT: Clustering-based intrusion detection in IoT environments. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual, 25–28 August 2020; pp. 1–9.
14. Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; Khan, A.I. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry 2020, 12, 754.
15. Zarándy, Á.; Rekeczky, C.; Szolgay, P.; Chua, L.O. Overview of CNN research: 25 years history and the current trends. In Proceedings of the 2015 IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, Portugal, 24–27 May 2015; pp. 401–404.
16. Irie, K.; Tüske, Z.; Alkhouli, T.; Schlüter, R.; Ney, H. LSTM, GRU, Highway and a Bit of Attention: An Empirical Overview for Language Modeling in Speech Recognition. In Proceedings of the Interspeech 2016, 17th Annual Conference of the International Speech Communication Association, San Francisco, CA, USA, 8–12 September 2016; pp. 3519–3523.
17. Jiang, Y.; Yang, F.; Zhu, H.; Zhou, D.; Zeng, X. Nonlinear CNN: Improving CNNs with quadratic convolutions. Neural Comput. Appl. 2019, 32, 8507–8516.
18. Gonzalez, J.; Yu, W. Nonlinear system modeling using LSTM neural networks. IFAC-PapersOnLine 2018, 51, 485–489.
19. Tan, Y.; Hu, C.; Zhang, K.; Zheng, K.; Davis, E.A.; Park, J.S. LSTM-Based Anomaly Detection for Non-Linear Dynamical System. IEEE Access 2020, 8, 103301–103308.
20. Marchi, E.; Vesperini, F.; Weninger, F.; Eyben, F.; Squartini, S.; Schuller, B. Nonlinear prediction with LSTM recurrent neural networks for acoustic novelty detection. In Proceedings of the 2015 International Joint Conference on Neural Networks (IJCNN), Killarney, Ireland, 12–17 July 2015; pp. 1–7.
21. Zoumpourlis, G.; Doumanoglou, A.; Vretos, N.; Daras, P. Nonlinear convolution filters for CNN-based learning. In Proceedings of the IEEE International Conference on Computer Vision, Venice, Italy, 22–29 October 2017; pp. 4761–4769.
22. Corinto, F.; Biey, M.; Gilli, M. Nonlinear coupled CNN models for multiscale image analysis. Int. J. Circ. Theory Appl. 2006, 34, 77–88.
23. Shamsolmoali, P.; Jain, D.K.; Zareapoor, M.; Yang, J.; Alam, M.A. High-dimensional multimedia classification using deep CNN and extended residual units. Multimed. Tools Appl. 2019, 78, 23867–23882.
24. Cheikhrouhou, O.; Mahmud, R.; Zouari, R.; Ibrahim, M.; Zaguia, A.; Gia, T.N. One-Dimensional CNN Approach for ECG Arrhythmia Analysis in Fog-Cloud Environments. IEEE Access 2021, 9, 103513–103523.
25. Praanna, K.; Sruthi, S.; Kalyani, K.; Tejaswi, A.S. A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data. J. Inf. Comput. Sci. 2020, 10, 1362–1370.
26. Malaiya, R.K.; Kwon, D.; Kim, J.; Suh, S.C.; Kim, H.; Kim, I. An empirical evaluation of deep learning for network anomaly detection. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 893–898.

27. Yao, Q.; Wang, M.; Chen, Y.; Dai, W.; Yi-Qi, H.; Yu-Feng, L.; Wei-Wei, T.; Qiang, Y.; Yang, Y. Taking human out of learning applications: A survey on automated machine learning. arXiv 2018, arXiv:1810.13306.

28. Wahid, F.; Fayaz, M.; Aljarbouh, A.; Mir, M.; Aamir, M.; Imran. Energy Consumption Optimization and User Comfort Maximization in Smart Buildings Using a Hybrid of the Firefly and Genetic Algorithms. Energies 2020, 13, 4363.

29. Rizwan, A.; Iqbal, N.; Ahmad, R.; Kim, D.-H. WR-SVM Model Based on the Margin Radius Approach for Solving the Minimum Enclosing Ball Problem in Support Vector Machine Classification. Appl. Sci. 2021, 11, 4657.

30. Khan, A.-N.; Iqbal, N.; Rizwan, A.; Ahmad, R.; Kim, D.-H. An Ensemble Energy Consumption Forecasting Model Based on Spatial-Temporal Clustering Analysis in Residential Buildings. Energies 2021, 14, 3020.

31. Agrawal, S.; Agrawal, J. Survey on anomaly detection using data mining techniques. Procedia Comput. Sci. 2015, 60, 708–713.

32. Pathan, A.S.K. The State of the Art in Intrusion Prevention and Detection; CRC Press: Boca Raton, FL, USA, 2014.

33. Narayana, V.L.; Gopi, A.P.; Khadherbhi, S.R.; Pavani, V. Accurate identification and detection of outliers in networks using group random forest methodoly. J. Crit. Rev. 2020, 7, 381–384.

34. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. An Advanced Abnormal Behavior Detection Engine Embedding Autoencoders for the Investigation of Financial Transactions. Information 2021, 12, 34.

35. Xie, M.; Han, S.; Tian, B.; Parvin, S. Anomaly detection in wireless sensor networks: A survey. J. Netw. Comput. Appl. 2011, 34, 1302–1325.

36. Debar, H.; Dacier, M.; Wespi, A. A revised taxonomy for intrusion-detection systems. In Annales Des Télécommunications; Springer: Berlin/Heidelberg, Germany, 2000; Volume 55, pp. 361–378.

37. Aldweesh, A.; Derhab, A.; Emam, A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowl. Based Syst. 2020, 189, 105124.

38. Tucker, C.J.; Furnell, S.M.; Ghita, B.V.; Brooke, P.J. A new taxonomy for comparing intrusion detection systems. Internet Res. 2007, 17, 1.

39. Estevez-Tapiador, J.M.; Garcia-Teodoro, P.; Diaz-Verdejo, J.E. Anomaly detection methods in wired networks: A survey and taxonomy. Comput. Commun. 2004, 27, 1569–1584.

40. Boukerche, A.; Zheng, L.; Alfandi, O. Outlier detection: Methods, models, and classification. ACM Comput. Surv. (CSUR) 2020, 53, 1–37.

41. Gogoi, P.; Bhattacharyya, D.; Borah, B.; Kalita, J.K. A survey of outlier detection methods in network anomaly identification. Comput. J. 2011, 54, 570–588.

42. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. ACM Comput. Surv. (CSUR) 2009, 41, 1–58.

43. Patcha, A.; Park, J.M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Comput. Netw. 2007, 51, 3448–3470.

44. Hodge, V.; Austin, J. A survey of outlier detection methodologies. Artif. Intell. Rev. 2004, 22, 85–126.

45. Kiani, R.; Keshavarzi, A.; Bohlouli, M. Detection of thin boundaries between different types of anomalies in outlier detection using enhanced neural networks. Appl. Artif. Intell. 2020, 34, 345–377.

46. Safaei, M.; Asadi, S.; Driss, M.; Boulila, W.; Alsaeedi, A.; Chizari, H.; Abdullah, R.; Safaei, M. A systematic literature review on outlier detection in wireless sensor networks. Symmetry 2020, 12, 328.

47. Markou, M.; Singh, S. Novelty detection: A review—Part 2: Neural network based approaches. Signal Process. 2003, 83, 2499–2521.

48. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. J. Netw. Comput. Appl. 2016, 60, 19–31.

49. Treinen, J.J. System, Method and Program Product for Identifying Network-Attack Profiles and Blocking Network Intrusions. U.S. Patent 8,056,115, 8 November 2011.

50. Mhatre, A.J.; Kiggins, A.J.; Diggins, M.F. Attack Traffic Signature Generation Using Statistical Pattern Recognition. U.S. Patent 8,997,227, 31 March 2015.

51. Peng, Y. Research of network intrusion detection system based on snort and NTOP. In Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 29–31 May 2012; pp. 2764–2768.

52. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada,

8–10 July 2009; pp. 1–6.

53. Mehdi, S.A.; Khalid, J.; Khayam, S.A. Revisiting traffic anomaly detection using software defined networking. In Proceedings of the International Workshop on Recent Advances in Intrusion Detection, Menlo Park, CA, USA, 20–21 September 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 161–180.
54. Braga, R.; Mota, E.; Passito, A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. In Proceedings of the IEEE Local Computer Network Conference, Denver, CO, USA, 10–14 October 2021; pp. 408–415.
55. Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M. Deep learning approach for network intrusion detection in software defined networking. In Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 26–29 October 2016; pp. 258–263.
56. Niyaz, Q.; Sun, W.; Javaid, A.Y. A deep learning based DDoS detection system in software-defined networking (SDN). arXiv 2016, arXiv:1611.07400.
57. Jankowski, D.; Amanowicz, M. On efficiency of selected machine learning algorithms for intrusion detection in software defined networks. Int. J. Electron. Telecommun. 2016, 62, 247–252.
58. Lee, Y.; Kang, W.; Son, H. An internet traffic analysis method with mapreduce. In Proceedings of the 2010 IEEE/IFIP Network Operations and Management Symposium Workshops (NOMS Wksps), Osaka, Japan, 19–23 April 2010; pp. 357–361.
59. Singh, K.; Guntuku, S.C.; Thakur, A.; Hota, C. Big data analytics framework for peer-to-peer botnet detection using random forests. Inform. Sci. 2014, 278, 488–497.
60. Bhat, A.H.; Patra, S.; Jena, D. Machine learning approach for intrusion detection on cloud virtual machines. Int. J. Appl. Innov. Eng. Manag. 2013, 2, 56–66.
61. Chen, Z.; Han, F.; Cao, J.; Jiang, X.; Chen, S. Cloud computing-based forensic analysis for collaborative network security management system. Tsinghua Sci. Technol. 2013, 18, 40–50.
62. Chen, T.; Zhang, X.; Jin, S.; Kim, O. Efficient classification using parallel and scalable compressed model and its application on intrusion detection. Expert Syst. Appl. 2014, 41, 5972–5983.
63. Marnerides, A.; Watson, M.R.; Shirazi, N.; Mauthe, A.; Hutchison, D. Malware analysis in cloud computing: Network and system characteristics. In Proceedings of the 2013 IEEE Globecom Workshops (GC Wkshps), Atlanta, GA, USA, 9–13 December 2013; pp. 482–487.
64. Muthurajkumar, S.; Kulothungan, K.; Vijayalakshmi, M.; Jaisankar, N.; Kannan, A. A rough set based feature selection algorithm for effective intrusion detection in cloud model. In Proceedings of the International Conference on Advances in Communication, Network, and Computing, Beijing, China, 23–24 May 2013; pp. 8–13.
65. Wang, H.; Ding, W.; Xia, Z. A cloud-pattern based network traffic analysis platform for passive measurement. In Proceedings of the 2012 International Conference on, Cloud and Service Computing (CSC), Shanghai, China, 22–24 November 2012; pp. 1–7.

Retrieved from https://encyclopedia.pub/entry/history/show/33031