Recent Developments in Intelligent Intrusion Detection Systems: A Survey

Usman Adedayo Adeniyi
dept. of cyber security, faculty of computing
Air force institute of technology
Kaduna, Nigeria
adedayousman1@gmail.com

Fatimah Adam-Fika
dept. of cyber security, faculty of computing
Air force institute of technology
Kaduna, Nigeria
faateemahfika@gmail.com

Alimi Maruf Olasunkanmi
dept. of computer science, faculty of computing
Air force institute of technology
Kaduna, Nigeria
alimiom@hotmail.com

Samson Adeyinka
dept. of cyber security, faculty of computing
Air force institute of technology
Kaduna, Nigeria
sadeyinka@actech.education

Abdulraman Alabelewe Tunde
dept. of cyber security, faculty of Air *force institute of technology*
kaduna, Nigeria
alaberahman@hotmail.com

Muhammad Auwal Bello
dept. of cyber security, faculty of
Air force institute of technology
kaduna, Nigeria
nice_aubi@yahoo.com

***Abstract*— This paper offers a concise review of machine learning (ML)-based methods for Intrusion Detection Systems (IDS), highlighting their necessity against evolving cyber threats due to the inadequacy of traditional approaches. It covers conceptual and empirical studies, examining datasets, algorithms, and performance metrics like accuracy, precision, recall, and F1-score. The review's methodology is well-structured, sourcing recent articles (2020–2024) from academic databases such as IEEE Xplore, SpringerLink, and ScienceDirect. Findings reveal that various ML approaches, including supervised, unsupervised, and hybrid techniques, show promising results. Distinct traffic characteristics in datasets are crucial for classifying intrusion patterns. The paper's strengths include comprehensive coverage of ML techniques, relevant and recent citations, and a clear, organized structure. It concludes that deep learning and hybrid models are increasingly dominant, and future work should focus on reducing false positives and improving real-time detection in resource-constrained environments. Overall, it's a well-researched reference for improving IDS efficiency through ML.**

***Keywords*— Intrusion Detection System, Network Security, Machine Learning, Artificial intelligence, Attacks Classification**

I. INTRODUCTION

Intrusion Detection Systems (IDS) are vital tools for identifying and mitigating malicious activities within network environments. Since their formal conceptualisation by Anderson in 1980, IDSs have evolved alongside the rapid growth of computing and networking technologies. Nowadays computers and the Internet are used almost in every part of our lives. Since the personal computer was invented it has been growing faster and faster and it is now impossible to imagine companies or even a little shop that does not keep all the data of their customers in an electronic database or computer. The increasing connectivity of computer systems has heightened the need for robust intrusion detection mechanisms to protect sensitive data and infrastructure from unauthorised access and disruption. To discover unknown hostile threats, the anomaly detection approach employs heuristic methods. As a result, the effectiveness of this anomaly detection approach for detecting anomalies is good despite a high false-positive rate. Various businesses have adopted protocol analysis, which uses a combination of anomaly and signature-based systems, to avoid this problem [15] Modern Industrial Control Systems, vehicular networks, etc. have rapidly evolved in recent years. These systems often work in symbiosis and handle large volumes of information through various communication infrastructures and complex communication networks such as 5G networks. As a result, many hackers and ill-intentioned entities strive to find new ways to break into those computer systems by compromising the communication channels [9]compromised bots can be used to generate malicious network traffic and flood the SDN controller, the controller resources or network resources saturation can lead to the shutdown of the whole network with distributed denial of service attacks [5] Machine Learning (ML) methods are the most frequently preferred methods to perform intrusion detection. ML can empower the experiential learning and decision-making processes of the various systems by improving skills and capacity without any open programming [1] An intrusion detection system is an effective security-enhancing technique for identifying and preventing networks or systems from cyber assaults, IDSs are responsible for the identification of suspicious activities and the overall security of a network infrastructure against cyberattacks and for reducing financial and operational losses [15]. McHugh, Christie & Allen Described intrusion detection system as a system that can provide warnings to an organization that their computer systems are under attack and is typically used in conjunction with other security devices such as firewalls[13]. In terms of network perspectives, network traffic may contain an

imbalanced number of harmful attacks when compared to normal traffic [26] One of the largest keys to any organization's security is maintaining a good security incident response structure [32]. The most critical of tasks during any incident response is the ability to detect that an actual incident has occurred [32]. An intrusion detection system will typically monitor an organizations systems and record events that it deems as potential security incidents. There is network based intrusion detection systems which sit on an organization's network and passively sniff packets. Intrusions are actions that attempt to break one of the following properties of the computer system: confidentiality, integrity, and availability. IDSs are categorized based on the detection technique they employ. This study surveys various machine learning approaches that have been used to build intrusion detection system and provide conceptual and empirical reviewing literature on intrusion detection system as well as the popularity of machine learning approaches for trustful intrusion detection.

II. SURVEY OF WORK ON INTRUSION DETECTION SYSTEM

[26] Developed a transformer-based transfer learning approach to learn detailed feature representation using their semantic anchors, the Synthetic Minority Oversampling Technique (SMOTE) is implemented to balance abnormal traffic, detect minority attack and convolution neural network (CNN) model is designed to extract deep features from the balanced network traffic. Detailed experiments are conducted to test the proposed approach using three standard datasets, i.e., UNSW NB15, CIC-IDS2017, and NSL-KDD. Finally, come up with hybrid approach of the CNN-Long Short-Term Memory (CNN-LSTM) model that can detect different types of attacks from the deep features.

[11] conducted a comprehensive evaluation of machine learning algorithms for intrusion detection, assessing their performance across various datasets and scenarios. The study encompasses a wide range of machine learning techniques, including supervised, unsupervised, and semi-supervised algorithms. The proposed model reveal that while traditional machine learning algorithms, such as Support Vector Machines (SVM) and Decision Trees, offer robust performance in specific contexts, they often struggle with adaptability to evolving threats and scalability issues.

[17]. Employed machine learning techniques, notably the Gaussian Nave Bayes (GNB) and Stochastic Gradient Descent (SGD) algorithms. To lessen the burden on the computer, a principal component analysis and singular value decomposition on the raw traffic data was conducted using WSN-DS dataset, the suggested SG-IDS model achieved a 96% accuracy rate, outperforming state-of-the-art algorithms with higher rates of 98% accuracy, 96% recall, and 97% F1 measurement, in an evaluation of an IoMT dataset, the SG-IDS performed admirably, with an accuracy of 0.87 and a precision of 1.00 in intrusion detection tasks. SG-IDS was used to improve accuracy and memory. Experiments and research on analogous systems show that this scheme has a high detection rate and low false alarms and requires little calculation. It can identify intruders in wireless sensor networks.

[30] Addressed the critical need for robust network intrusion detection systems (NIDS) in today's digital landscape, amidst escalating cyber threats. Leveraging a dataset derived from a simulated military network environment, the proposed study explores various intrusion scenarios encountered in cyber warfare and underscores the critical role of advancement machine learning models in network intrusion detection through comprehensive, evaluation and comparison, then identifies tab transformer as a standout performer, surpassing traditional models like SVM, LR, MLP and a voting model in precision recall and F1 score metrics.

[9] Used different types of Recurrent Neural Networks (RNNs), namely, Long-Short Term Memory (LSTM), Gated Recurrent Unit (GRU) and Simple RNN to assess the performance of the IDS framework, the NSL-KDD and the UNSW-NB15 benchmark datasets are considered. An XGBoost-based feature selection algorithm was implemented to reduce the feature space of each dataset, the results showed that for the binary classification tasks using the NSL-KDD, XGBoost-LSTM achieved the best performance with a test accuracy (TAC) of 88.13%, a validation accuracy (VAC) of 99.49% and a training time of 225.46 sec. For the UNSW-NB15, XGBoost-Simple-RNN was the most efficient model with a TAC of 87.07%. For the multiclass classification scheme, the XGBoost-LSTM achieved a TAC of 86.93% over NSL-KDD and the XGBoost-GRU obtained a TAC of 78.40% over the UNSW-NB15 dataset.

[1] proposed an IDS based on deep learning models to detect intrusion in an IIoT environment. Study was performed using CNN, LSTM and CNN+LSTM methods as intrusion detection systems. Deep learning models were implemented using X-IIoTID and UNSW-NB15 datasets in order to determine the abnormal patterns. The hybrid CNN + LSTM model attained highest accuracy value for intrusion detection in both datasets. The proposed CNN + LSTM architecture attained an accuracy of 93.21% for binary classification and 92.9% for multi-class classification on UNSW-NB15 dataset while the same model attained a detection accuracy of 99.84% for binary classification and 99.80% for multi-class classification in the X-IIoTID dataset. In addition, the accurate detection success of the implemented models regarding the types of attacks within the datasets was evaluated.

[5] Proposed a long short-term memory (LSTM) based approach to detect network attacks using SDN supported intrusion detection system in IoT networks. The study presented an extensive performance evaluation of the machine learning (ML) and deep learning (DL) model in two SDN IoT-focused datasets and LSTM-based architecture for the effective multiclass classification of network attacks in IoT network. Comparative performance analysis showed that the DL model performed better than the ML classifier SVM and more effectively distinguished the network attack types in the dataset compared to the other DL models, DNN and CNN,

evaluation of the proposed model shows that the model effectively identifies and classifies the attack types with an accuracy of 0.971.

[15] Used convolutional recurrent neural network to construct a deep-learning-based hybrid intrusion detection system that can detects attacks over a network. The model was built by combining an RNN with a CNN in which two convolutional layers are followed up by various RNN layers. Experiments are conducted using publicly accessible benchmark CICIDS-2018 data, to determine the effectiveness of the proposed system. The findings of the research demonstrate that the proposed HDLNIDS outperforms current intrusion detection approaches with an average accuracy of 98.90% in detecting malicious attacks.

[16] developed a methodology for the analysis of machine learning (ML) models to detect and understand biased decisions and apply it to two specific scenarios, comparing models trained on different subsets of the original data, and applying model-agnostic post-hoc explanation tools helped to identify bias in a model in general as well as in specific instances. the results show that analysis of models through the lens of statistical analysis and post-hoc explanations helps to detect and understand bias, also observed that post-hoc explanations often fail to detect individual biased instances, and caution against using this category of tools to guarantee model fairness and finally provide insights on how this analysis can help understand the origin and shape of bias.

[21] Used machine learning and deep learning technique to demonstrate intrusion detection approach, experiment was run on renowned NSLKDD dataset in addition to the most recent CICIDS2017 and UNSW-NB15 datasets to create a stable dataset with a proportionate number of regular traffic and malicious samples. The results demonstrated that the proposed hybrid feature dimensionality reduction techniques PCA + FA-RF, PCA + FA-DT, PCA + FANB, and PCA + FA-DBN outperform the individual base models RF, DT, NB, and DBN (without feature dimensionality reduction) in terms of accuracy (ACC), detection rate (DR), and false alarm rate (warning) making the proposed hybrid feature dimensionality reduction a viable option for intrusion detection in WSNs. Additionally, the experimental findings in term of training time show that the proposed model train faster than the single individual models on UNSW-NB15, NSLKDD, and CICIDS2017

[20] Examined the viability of deploying machine-learning-based intrusion detection in resource-constrained IoT environments, and built an intelligent IDS capable of detecting abnormal behaviour on insecure IoT networks by deftly combining feature dimensionality reduction and machine learning methods. The experimental results were evaluated in term of validation dataset, accuracy, the area under the curve, recall, F1, precision, kappa and mattew correlation coefficient (MCC). The findings were also benchmarked with the existing works, and his results were competitive with an accuracy of 99.9% and MCC of 99.97%.

[27] Provided background information on the growing of phishing-based attacks in the internet space and then used selected machine learning algorithms for building URL classification model detection. The study investigates the performance of four supervised machine learning algorithms in the classification of phishing uniform resource locators. Experimental results showed that decision tree classifiers have the best overall performance across accuracy, precision, recall and F1-measure.

[2] Performed and evaluate the efficiency and the performance of the following machine learning classifiers: J48, Random Forest, Random Tree, Decision Table, MLP, Naive Bayes, and Bayes Network. All the tests were based on the KDD intrusion detection dataset. The rate of the different type of attacks in the KDD dataset are approximately 79% of DOS attacks, 19% of normal packets and 2% of other types of attacks (R2l, U2R and PROBE). In the experiments 148753 instances of records have been extracted as training data to build the training models for the selected machine learning classifiers.

[8] Analyzed machine learning techniques in intrusion detection system, it also reviews many related studies in period from 2000 to 2012. And it focuses on machine learning techniques. related studies include single, hybrid, classifier, ensemble, baseline, and datasets used. The instrument was a self-developed survey questionnaire constituting 48 items at a five-point rating scale for data analysis. Correlation analysis was conducted to test relationships among variables. ANOVA and t-test were applied to find out significant differences.

[8] Examined different Machine learning techniques that have been proposed for detecting intrusion such as single classifier and hybrid classifier were used in the domain of intrusion detection and each technique has successfully shown significant improvement over the others.

[25] Focused on developing single, hybrid, and ensemble classifiers. Related studies are compared by their classifier design, datasets used, and other experimental setups. Current achievements and limitations in developing intrusion detection systems by machine learning are present and discussed. A number of future research directions are also provided. The research reviews recent papers which are between 2000 and 2007. The review includes single and ensemble classifiers.

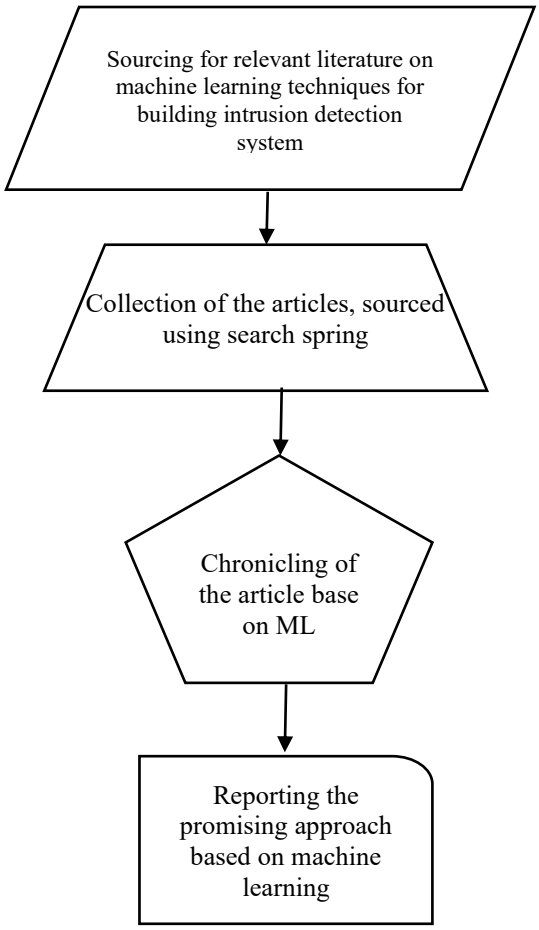
[24] Used ensemble approach to design and maximize the capability to detect intrusion events, independently from the operative scenario, exploiting several evaluation models in order to differentiate the normal events from those related to all classes of attacks. The results show how the proposed ensemble approach outperforms the single classifiers in terms of Specificity, without being significantly penalized in other aspects, because it gets as light deterioration in terms of average F-score but a positive average AUC.

III. METHODOLOGY

This study followed a structured literature review methodology. Research articles were sourced from academic databases including IEEE Xplore, SpringerLink, and ScienceDirect using keywords such as “Intrusion Detection System”, “Machine Learning”, and “Network Security”. Selected papers were screened based on recency (2020–2024), relevance, and use of benchmark datasets. A comparative

analysis was then conducted to examine the methods, datasets, and performance metrics employed in each study.

IV. METHODOLOGICAL OF THE STUDY



Figures 1. FLOW OF THE PROCESSES IN THE STUDY

Figure 1. Illustrates the systematic approach employed in this study to review relevant articles on machine learning based intrusion detection system.

table 1 **TECHNIQUES OF NETWORK INTRUSION DETECTION PUBLISHED BETWEEN 2022/2024**

Name and Year	**TECHNIQUES OF NETWORK INTRUSION DETECTION PUBLISHED BETWEEN 2022/2024**		
	Method	***Dataset***	***Performance Metrics***
Saleh, Marouane, and Fakhfakh (2024)	GNB and SGD	WSN-DS	98% Accuracy
Ullah, Srivastava & Lin (2024)	SMOTE	UNSW NB15, CIC-IDS2017, and NSL-KDD	98.1% Accuracy
Altunaya and Albayrak (2023)	CNN, LSTM and CNN+LSTM	X-IIoTID and UNSW-NB15	93.21% Accuracy
Chaganti, Suliman, Ravi and Dua, (2023)	LSTM	SDN IoT-focused datasets	0.971 Accuracy
Sydney, Mambwe and Kasongo (2023)	LSTM, GRU and Simple RNN	NSL-KDD and UNSW-NB15	99.49% Accuracy
Qazi, Faheem, and Zia (2023)	RNN with a CNN	CICIDS-2018	98.90% Accuracy
Saheed, Baba, Orje-Ishegh, and Longe (2022)	PCA + FA-RF, PCA + FA-DT, PCA + FANB, and PCA + FA-DBN	NSLKDD, CICIDS2017 and UNSW-NB15	99.9% Accuracy

V. FINDINGS AND DISCUSSION

This study reviewed some recent papers that show great promises for developing intrusion detection systems in networks after sourcing pertinent literature from reputable repositories. The study also concentrated on offering an overview of the development of machine learning (ML)-based methods for network intrusion classification. For scholars working in this field, the report offered unambiguous guidance. The reviewed literature identifies multiple categories of network intrusions, each with unique traffic signatures that machine learning models can exploit for accurate classification. It was also noted that ML-based techniques are often used to develop network intrusion

detection. Additionally, it was found that each sample had distinct traffic characteristics that are highly helpful in classifying intrusion and non-intrusion patterns in each of the analyzed areas. Findings also reveal that some of the ML-based studies that were sourced and reviewed used the following as metrics: accuracy, precision, recall, f-measure.

VI. CONCLUSION

This paper presents a structured review of recent advancements in the application of machine learning for network intrusion detection. The findings highlight the growing dominance of deep learning architectures and hybrid models across benchmark datasets. Future work should focus on reducing false positives and improving real-time detection performance in resource-constrained environments.

REFERENCES

[1] H. C. Altunay and Z. Albayrak. A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks. *Engineering Science and Technology, an International Journal*, *38*, 101322. In 2023.

[2] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh. Evaluation of machine learning algorithms for intrusion detection system. *IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)* (pp. 000277-000282), 2017.

[3] G. Anshu and S. Sandeep A survey on anomaly and signature based intrusion detection system (IDS). *Int. Journal of engineering research and applications ISSN*: 2248-9622, 2014

[4] Banu Bijone A Survey on Secure Network: Intrusion Detection & prevention Approaches. *American Journal of Information Systems DOI*:10.12691/ajis-4-3-2, 2016.

[5] R. Chaganti, W. Suliman, V. Ravi, and A. Dua. Deep learning approach for SDN-enabled intrusion detection system in IoT networks. *Information*, *14*(1), 41, 2023.

[6] A. Fatai and I. E. Safiriyu. Application of artificial intelligence in network intrusion detection. World applied programming. 158-166 ISSN: 2222-2510, 2012.

[7] P. R. Ignacio and M.R Maria evaluation of current is intrusion detection system. *International journal LITH-ISY-EX*—08/4160---SE, 2008.

[8] S. Juma, Z. Muda, M. A Mohamed, and W. Yassin.. machine learning techniques for intrusion detection system: A REVIEW. *Journal of Theoretical & Applied Information Technology*, *72*(3), 2015.

[9] S. M. Kasongo. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications* 2023. *199*, 113-125, 2023.

[10] M. M. Lekhraj and B.G Monika. An Effectual and Secure Approach for the Detection and Efficient Searching of Network Intrusion Detection System (NIDS). *International Journal of Computer Applications (0975 – 8887) Volume* 108 – No 15, 2014.

[11] B. R Maddireddy. A Comprehensive Analysis of Machine Learning Algorithms in Intrusion Detection Systems. *Journal Environmental Sciences And Technology*, *3*(1), 877-891, 2024.

[12] A. Monther K. Yaser and A.M Mohammad Application of artificial bee intrusion detection systems published online in wiley online library (wileyonlinelibrary.com). DOL: 10.1002/sec.588 IEEE Transactions and Journals Digital Object Identifier 110.1109/Access, 2017.

[13] J. McHugh, A. Christie and J. Allen . Defending yourself: the role of intrusion detection systems. *IEEE Software* . (2000). *17*(5), 42-51.

[14] I. R. Panagiotis, G. Panagiotis and Sarigianidis. Securing the smart grid A Comprehensive Compilation of Intrusion Detection and Prevention Systems, 2019.

[15] E.U.H TQazi, M.H Faheem and T. Zia. HDLNIDS: hybrid deep-learning-based network intrusion detection system. *Applied Sciences 13*(8), 4921, 2023.

[16] M. Ruggeri, A. Dethise and M. Canini. On Detecting Biased Predictions with Post-hoc Explanation Methods. In *Proceedings of the 2023 on Explainable and Safety Bounded, Fidelitous, Machine Learning for Networking* (pp. 17-23).

[17] H. M. Saleh, H. Marouane and A. Fakhfakh, A. Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning. *IEEE Access*. (2024).

[18] Y. K. Saheed. A Binary Firefly Algorithm Based Feature Selection Method on High Dimensional Intrusion Detection Data. In *Illumination of Artificial Intelligence in Cybersecurity and Forensics* (pp. 273-288). Springer, Cham, 2022.

[19] Y. K. Saheed. Performance Improvement of Intrusion Detection System for Detecting Attacks on Internet of Things and Edge of Things. In *Artificial Intelligence for Cloud and Edge Computing*. (pp. 321-339). Springer, Cham, 2022.

[20] Y. K. Saheed, A.I Abiodun, S. Misra, M.K Holone and R. Colomo-Palacios. A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal* (2022). *61*(12), 9395-9409, 2022.

[21] Y. K. Saheed, U.A Baba, T. Orje-Ishegh and O.B Longe. An Efficient Machine Learning and Deep Belief Network Models for Wireless Intrusion Detection System. 2022.

[22] S. P. Gavhane and V. M Shelake. intrusion detection system using optimal c4.5 algorithim. International journal of computer science engineering and information technology research (ijcseitr). DOI: 10.2151/ijcseitr.3241, 2014.

[23] C. Sampada, S. Khusbu, D.S Neha, A.A Mukherjee and S. Sugata Adaptive Neuro-Fuzzy Intrusion Detection Systems. International Conference on Information Technology: Coding and Computing (ITCC'04). 2004

[24] R. Saia, S. Carta, and D.R Recupero. A Probabilistic-driven Ensemble Approach to Perform Event Classification in Intrusion Detection System. In *KDIR* 2018 (pp. 139-146).

[25] C. F. Tsai, Y.F Hsu, C.Y Lin and W.I Lin. Intrusion detection by machine learning: A review. *expert systems with applications* (2009) *36*(10), 11994-12000.

[26] F. Ullah, S. Ullah, G. Srivastava and J.C.W Lin. IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic. *Digital Communications and Networks* (2024). *10*(1), 190-204.

[27] M. Urvashi and J. Anurag An Improved Method to Detect intrusion using marching learning algorithms. *Informatics Engineering, an International Journal (IEIJ)* 2016. *DOI: 10.5121/ieij.2016.4203.*

[28] Vivian Nalubowa. Smart Home Security Using Intrusion Detection and Prevention Systems. -diva-portal.org. 2019.

[29] K. J. Vahid, R. Mina and K. Armin. Taxonomy of Feature selection in Intrusion Detection ystem. *IJCSNS International Journal of Computer Science and Network Security,* 2017.

[30] X. Wang, Y. Qiao, J. Xiong, Z. Zhao, N. Zhang, M. Feng, and C. Jiang Advanced network intrusion detection with tabtransformer. *Journal of Theory and Practice of Engineering Science*. *4*(03), 191-198. DOI: 10.53469/jtpes.2024.04(03).18, 2024.

[31] S. K. Wagh, V.K Pachghare and S.R Kolhe. Survey on intrusion detection system using machine learning techniques. *International Journal of Computer Applications*. *78*(16) 2013.

[32] R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, and K. Beznosov. The challenges of using an intrusion detection system: is it worth the effort? In *Proceedings of the 4th symposium on Usable privacy and security*, (pp. 107-118). 2008.