An Intrusion Detection Framework for Non-expert Users

Bernardo Breve, Stefano Cirillo, Vincenzo Deufemia
Department of Computer Science
University of Salerno
84084 Fisciano (SA), Italy
{bbreve,scirillo,deufemia}@unisa.it

Abstract

The wide spreading of the Internet and its integration in everyday objects lead to the born of a whole interconnected world, based on different devices communicating each other and performing operation remotely activated. Among all these devices, smart voice assistants are gaining particular attention thanks to their ease of use, allowing users to comfortably deploy commands for controlling other devices. The wide diffusion of these devices and their simplicity of use lead to that category of users with little or no knowledge, to interact with complex systems without being perfectly aware of the risks they are exposed to. For this reason, the common network defenses and monitoring systems are too complex to be used by non-expert users. This paper presents a framework for intrusion detection specifically designed to be configurable and usable by every category of users. The system will be based on specific automatic behaviors so as to minimize human intervention. Moreover, it will include several visual interfaces aiming to simplify the user interaction with the framework, allowing him/her to properly configure and run an Intrusion Detection System (IDS). The use of voice assistants as a communication channel between the user and the system will provide an additional contribution in order to improve the overall user experience.

Index terms— Intrusion detection system, Voice assistant, Computer networks, Human-computer interfaces

1   Introduction

The spread of the Internet in all socio-economic sectors has led to the need to educate people on the use of this tool. The main goal is to create a society able to exploit the power of the Internet with the aim of improving daily life. For this reason, the Internet of Things (IoT) has spread in the last few years. The IoT has become one of the most important technologies of this century, allowing us to connect each type of object, e.g. kitchen appliances, cars, thermostats, baby monitors, to the internet in order to establish continuous communication between people, processes, and things.

A large number of organizations benefit from the use of these types of devices in their business processes. In sectors as automotive [6, 22], public sector [33] and healthcare [3, 13], IoT has led to a real revolution. The use of intelligent systems that take advantage of IoT devices has improved safety in cars, has speeded up the time for the rescue of a person, or simply increased the productivity of the public administration. However, this has led to the birth of new security issues, since it is necessary to ensure that no one can interfere with their operations. Thus, the field of information security has become vitally important to the safety and economic well-being. The personal information of each person and what is connected to has enormous value and therefore must be preserved. To this end, new secure and safe information systems have been provided, by using firewalls, intrusion detection and prevention systems, authentication, and other hardware and software solutions.

The reasons that may induce an attack can been grouped into three categories: access information, alter information or render a system unusable [4]. These have led to the birth of intrusion detection systems (IDS), which provide tools for monitoring suspicious activities on the network. IDS can be defined as an alarm that monitors the network and reports intrusion to users. Over the years, a large number of IDSs [8] have been developed, which were later extended through the use of data mining tools [24], data relationships [10, 36], and machine learning approaches [16]. In general, we can consider several desirable characteristics for an IDS. In particular, an IDS should be run continuously without human supervision, and be fault-tolerant and survivable. Moreover, it should impose minimal overhead and be easily adapted to a specific network to observe the anomaly in network traffic.

Although there are a large number of IDSs, one of the main problems is to install and configure these systems to monitor a specific network. In fact, most of the existing

IDSs are used by domain experts who are able to carry out complex configurations and installations. However, most of the people subject to these types of attacks do not have skills for configuring these systems. Furthermore, being the IDSs similar to alarms, it is required to customize the devices and the notification methods of these systems. Although several visual languages and visualization techniques have been proposed to support the management of security issues in the context of Web applications [9, 11], it is necessary to use technologies that are familiar to a large part of users.

Voice assistants are increasingly popular and functional, and they have become a routine part of everyday life for many people. Initially, these assistants did not bring big news. But their developers knew they still had a bright future because, like any other technology, voice recognition needed some more time to evolve. In fact, over time, a large number of features have been developed that take advantage of artificial intelligence (AI) and machine learning for allowing users to use complex tools through their voice.

For these reasons, in this paper, we propose a new framework that allows non-expert users to install and configure an IDS on the network. In particular, we propose a new modular architecture with an easy-to-use user interface to customize an IDS. Moreover, we propose an innovative module for interacting with Alexa for executing and monitoring the status of an IDS via voice commands.

The paper is organised as follows. Section 2 describes recent work concerning IDSs and tools to support non-expert users in the use of systems that require a deep domain knowledge. Section 3 provides an overview of the different types of IDSs. Section 4 presents the architecture of the proposed framework by describing the underlying components. Section 5 briefly discusses the most crucial aspects for non-expert users interacting with an IDS and how we are focusing our efforts to meet their needs. Section 6 concludes the paper by presenting our conclusions and future directions.

2 Related Works

The goal of the proposed solution is to allow a large number of users to use IDS systems despite their inexperience. In fact, the recently proposed IDSs do not consider how they can be used by non-expert users.

In [18] the authors proposed a new IDS that takes advantage of a deep learning approach based on the self-taught learning technique (STL). The authors explicitly declare that this tool is targeted at network administrators, and not at common users.

One of the most relevant work has been presented in [20]. Here the authors proposed an innovative network IDS to combat increasingly sophisticated network attacks. It takes advantage of a Hidden Naïve Bayes multiclass clas-

sifier to create an effective IDS that outperforms one of the most used IDS based on SVM [2]. The goal of both researches were to create efficient tools without considering if non-expert users are capable to use them or not.

In this work we introduce an innovative framework to support non-expert users in the use of different types of IDSs. Through this framework we can increase the user's awareness of what is happening on their network. This topic has been widely discussed by researchers, who have created several tools and user interfaces to increase interaction between users and systems.

Recently, one of the studies that addressed the problem described above is [14]. The authors developed a visual interface for non-expert users, in order to increase awareness of what happens on the network during daily browsing sessions. Indeed, they have shown that most users are unaware of the type of information are exchanged during the browsing sessions and need specific tools to solve this problem. The proposal has been deeply evaluated and analyzed from the point of view of the user experience in [9].

In [7], authors have compared 13 different visualization tools for network analysis aiming to outline their pros and cons. They have used qualitative coding as part of their research design in order to select several metrics to evaluate the advantages and disadvantages of the analyzed tools. Their primary purpose is to increase the security analyst's situational awareness without considering the final users.

In literature, different tools have been proposed to facilitate the use of IDSs by non-expert users. In [28], authors have defined a simplified sound-assistant that mitigates the sound in order to uniquely notify network attacks. In particular, they exploit distinctive sounds for each attack scenario so that the users easily identify the type of attack. The proposed tool could be integrated within network IDSs.

Other research on human-computer interfaces for supporting IDS has focused on bimodal applications, visual and sound, to notify network intrusions. For example, in [25] the authors introduce immersive spatial audio representations of network events that exploit 3D visual representations for interactive auto-stereoscopic.

3 Overview of IDSs

In this section we provide a general overview of Intrusion Detection Systems (IDSs). The latter can be classified as Network-based IDSs (NIDSs) and Host-based IDSs (HIDSs) [35].

A NIDS is designed to observe the passing traffic on the entire subnet, detecting attacks that involve all the devices on the network [32]. A HIDS, instead, runs on an independent device of the network and monitor the incoming and outcoming packets from the device, looking for the presence of any malicious activity occurring to the system

the HIDS is attached to. Alongside these two categories of IDSs, there also exist hybrid solutions, which combine the information provided by both the network and single devices' feedback to develop a complete view over the network system [34].

IDSs can also be classified based on the methodology used for the identification of intrusions. In this case, they can be classified in two main categories: Signature-based detection (SD), Anomaly-based detection (AD) [5, 19].

3.1 Signature-based detection

Signature-based detection systems relies on a set of specific patterns (or strings), called *signatures*, representing the network traffic trend during a certain type of known malicious attack. Following the analysis of the network traffic performed by the system, the extracted data is compared with the stored signatures. When a correspondence is found, this would immediately lead to a report of an attack in progress, and it would provide details about the type of attack and its characteristics. The comparison with the stored signatures can be performed with different techniques such as data mining [30], design patterns [15, 26], or involving both centralised and distributed components [17]. The main advantage of this intrusion detection methodology relies on the simplicity of the identification process, which mainly involves an extrapolation process followed by a comparison [23]. This method is ideal for identifying known attacks and obtaining simultaneously all the details about them. On the contrary, identifying an attack based on a restricted set of patterns limits the number of intrusions that could be recognized. Also, the knowledge base requires to be kept continuously updated, which is often a difficult and time-consuming process [31].

3.2 Anomaly-based detection

The anomaly-based detection methodology relies on the application of machine learning techniques for building a trustful activity model [29]. This methodology looks for any deviation from the known behavior derived from monitoring the system activities over a certain period. Indeed, after the system has been trained long enough to generate a model of what activities, hosts or even users affect the system, any incoming and outcoming anomaly traffic will be compared and declared dangerous if some of its characteristics cannot be found in the model.

The main advantages are the high dynamicity and extensibility of the model, since they capable of identifying new and unforeseen anomalies afflicting the system. On the contrary, its weak point relies on the low accuracy of acquiring attacks' information since the methodology does not use a proper knowledge base, as done by signature-based approaches, since it is strictly connected to the information acquired from the observed events. Moreover, the system cannot be operative straight away after its installation, but requires a certain amount of time for training the model, and adapt its analysis in response to the usual behavior of the network (or host) activities.

4 Framework

The proposed framework has been designed to improve the user' awareness of the network traffic and to simplify the IDS configuration process for receiving alerts when an attack is identified. The main idea is to create a modular framework that adapts to the different types of IDSs. This framework allows the user to manage their network through a visual interface and voice commands. The goal is to facilitate the installation and configuration of an IDS while ensuring the correct operations. The architecture of the proposed framework and its phases are described in the following sections.

4.1 System architecture

Normally, people use different types of devices without knowing what really happens during each usage and what the risks are. Therefore, it is difficult for them to configure network security tools. For these reasons, we have analyzed all the communication phases, starting from the interaction between users and devices, in order to design different components for the architecture of the proposed framework. The architecture involves components designed to ensure high modularity, adaptability, and ease of configuration.

The first challenge was to define an easily configurable and usable module by any type of device (Figure 1(a)). Thus, we have divided the architecture in three different layers that contain all the main components involving during network packets exchange. More specifically, our purpose is to monitor the outgoing and incoming traffic from the network during the connection between the devices and the local network controller. The first layer (Figure 1(b)) is divided into two distinct modules: devices and security configuration modules. The first is connected to Alexa so that it listens to voice messages and extracts the intents of the users. Through this module, the user defines the IDS configuration parameters. The security configuration module communicates with the third layer (Figure 1(c)). Using the parameters defined by the user, it automatically configures and executes the IDS manager on the network, in order to monitor web traffic. *IDS Manager* is a stand-alone component that can be easily replaced or updated as long as the framework configuration phase is repeated. Moreover, one of the main components of IDS is the *Notifier*. It is one of
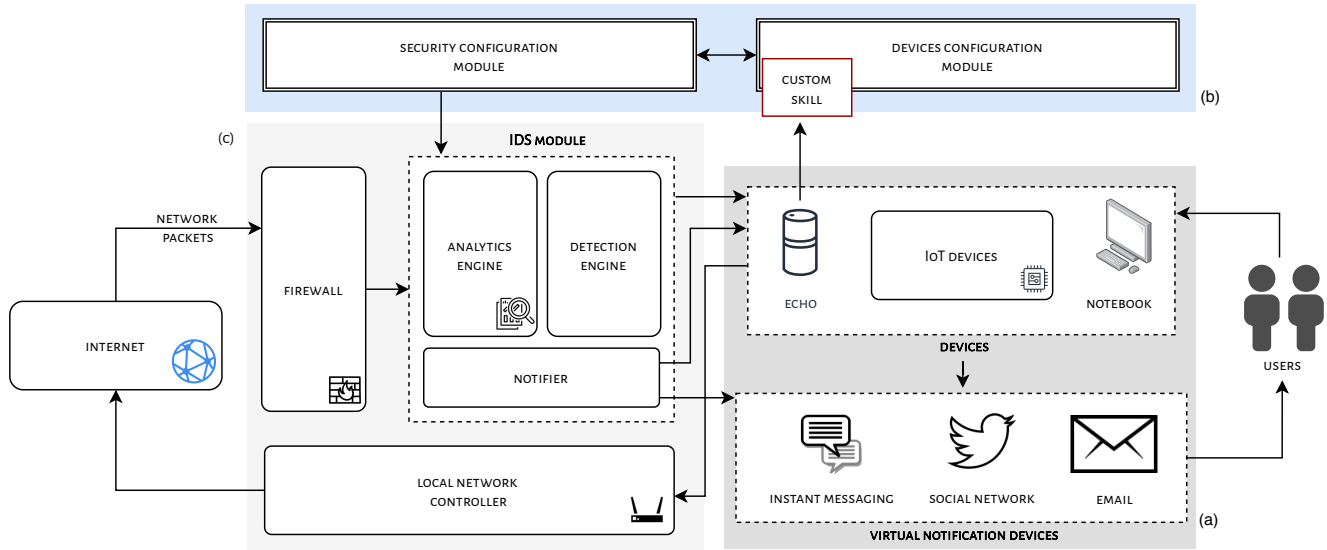
Figure 1: Architecture of the proposed framework.

the main elements of interaction with the user. In fact, the Notifier communicates directly with devices for sending reports of attacks to physical and virtual devices. The interaction modules with instant messaging apps and some of the most well-known social networks will be integrated into the framework. Users will be able to customize the notification devices by using the device configuration module.

The framework allows each user, with experience or not, to configure an IDS for their network and customize any device for receiving any alert.

4.2 Alexa custom skill architecture

One of the main proposals concerning this paper relies on the usage of voice assistant capabilities to ease the overall user experience with the system. Interaction with domestic voice assistants has been gaining prominence in the last period, becoming a very useful and simple communication channel [27]. Voice assistants, such as Google Home or Alexa, provide SDKs for the implementation of customized functionalities allowing for the definition of both the interaction model with the user, and the logic to deploy the commands on other devices. For this reason, we are planning the implementation of a customized functionality for the Amazon Alexa voice assistant, called "skill" [1], through which the user can vocally interact with the IDS modules.

Figure 2 shows in detail how the vocal requests of the users are transformed into the corresponding commands that are deployed to the IDS modules. In particular, the user can launch the skill by pronouncing its name preceded by a keywords like: "Alexa run" or "Alexa start". This starts the skill and enables the process of communication between

the user and the framework through the voice assistant. Any pronounced command deployed by the user to the skill is received and passed through the API at the cloud orchestrator. It has the goal of communicating and synchronizing the actions of all the other modules in the Amazon cloud. The first involved module is the Speech Language Understanding (SLU) whose task is trying to match the specific request with the action. Indeed, all the actions a skill can execute, called *intents*, are associated with several utterances the user can pronounce to trigger that intent. When a match is found, the corresponding intent is passed back to the cloud orchestrator, which asks the Alexa Skill Service to perform that intent. The custom skill we are planning to design will at this point contact the IDS to fulfill the user's request. After that, the system will return back to the skill with responses like the system status and notification about any intrusion occurring. In the last phase, the response received from the system are sent from the cloud orchestrator to the Text to Speech (TTS) module, which is responsible to translate the textual content into the voice that will be played by the Alexa device.

5 Discussion

In this section we will go through some of the most crucial and difficult aspects that a non-expert user needs to tackle down to correctly setup an IDS. We will also provide a general discussion about the solutions we are planning to implement for making all these steps possible.

We identified four main phases required for correctly using an IDS and we will walk through each of them describing our contribution plans.
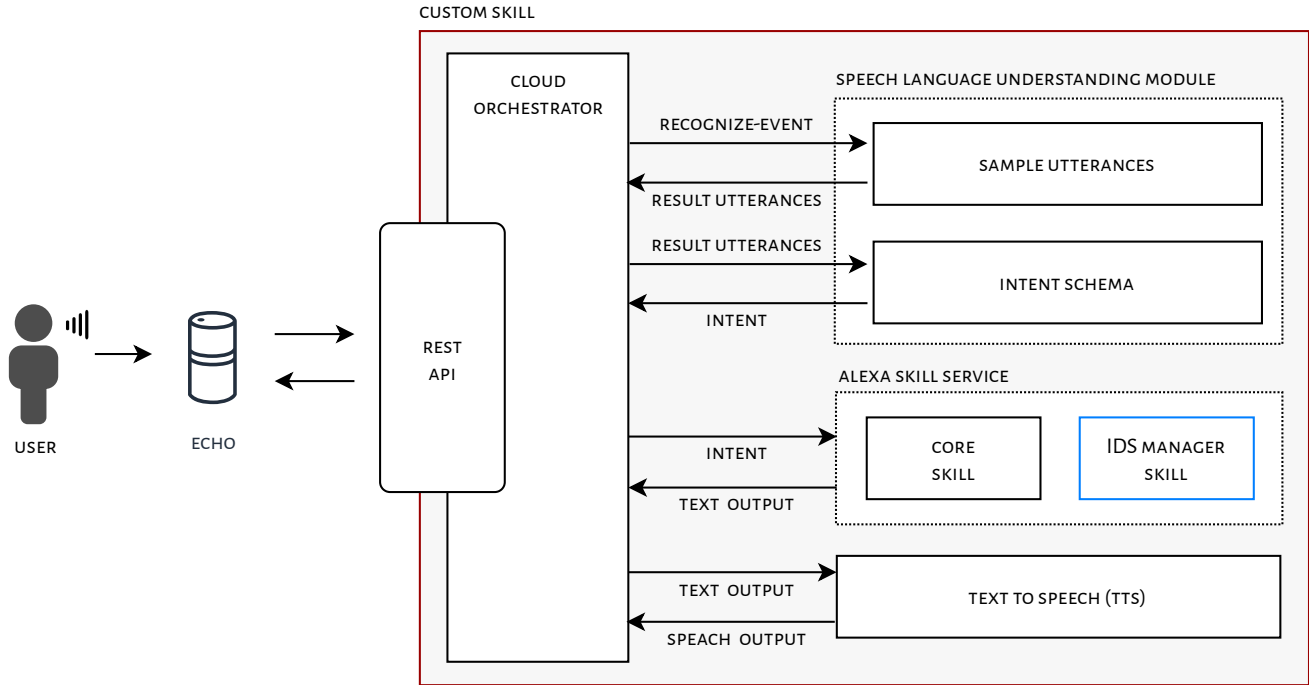
70

Figure 2: Architecture of the proposed skill.

5.1 Installation

The installation process is the first step a non-expert user needs to face when approaching an IDS. The main problem with this phase relies on the conspicuous amount of prerequisites the user have to deal with before actually proceed with the installation. Furthermore, most of the commands need to be deployed through a console command line, which represent a uncomfortable tool to interact with. To ease this issue, we are planning to include all the installation steps in an installer, a GUI-based software commonly found in the Microsoft Windows OS domain. An installer is composed of several windows describing the necessary steps to pursue with the installation of the software.

Hence, through a minimal interface user will have the possibility to specify the paths where all the required file will be saved and granting the mandatory authorizations for a correct execution of the IDS.

5.2 Configuration

After the installation phase, another crucial step is configuring the IDS. Indeed, it is necessary for the user to provide some essential parameters to obtain a correct network traffic monitoring together with the identification of intrusions. For example, it is fundamental for the user to provide the name of his/her network interface, i.e., the physical inbound and outbound connection port connecting the com-

puter on which the IDS has been installed to the router and so the Internet.

To ease this type of process, we have planned to rely on a specifically designed visual interface, which will implement several visual metaphors designed to be suitable for the knowledge level of the non-expert users approaching it. The introduction of this new level of abstraction will help the users to complete a correct system configuration without getting lost into the details of technical terms.

5.3 Usage

Being a monitoring system whose main task is to silently monitor and evaluate in background the quality and type of network packets being exchanged, the active contribution by the non-expert users is reduced to the necessity of starting the IDS. However, this operation needs to be performed through a command launched from bash, which as mentioned above represents a particularly complicated step for inexperienced users. For this reason, we have planned the introduction of a series of automatism allowing the system to start without the user having to forcefully act on the system.

Alongside this choice, a useful alternative in this scenario would have been provided by the interaction capabilities offered by voice assistants. The Alexa custom skill we described earlier would allow the user to easily interact with

71

the whole system, requesting to start the IDS and asking for information regarding its state of running.

5.4 Notification

Finally, the last step is the one that involves how to notify the user of the presence of an intrusion within the system. Even at this juncture, the use of a voice assistant providing immediate notification of the system's security status seems to be a suitable choice with respect to the knowledge level of the non-expert users. For this implementation phase, the challenge will be to program the type of message that the voice assistant will have to pronounce, avoiding phrases that can mislead the user and make the seriousness of the danger unclear. For example, the use of a phrase such as: "The system is under DDoS attack" is totally incomprehensible to a user who is unable to understand the seriousness of the danger of a DDoS attack which, in the IoT context, was the cause of one of the most devastating hacker attacks, the Mirai Botnet [21].

Therefore, it will be essential to find the right formulation to prevent the user from underestimating (or overestimating) the severity of the intrusion

5.5 User involvement

Being a framework specifically designed for end-users, the overall involvement of them in the realization and testing phases, plays a fundamental role in the achievement of a simple, functional, and effective system. For this reason, the development of the user interface will see the collaboration of some users, to whom we will submit some surveys to test their preferences. By doing so it is possible to direct the system towards the development of an interface more akin to user needs.

Another important phase will be the evaluation of the quality of the user experience. Thus, this type of evaluation, will be planned with the involvement of a large group of users, which we'll seek among who has little or none knowledge of computer technologies. Moreover, we will ask them to fill in different surveys in order to evaluate the usability and effectiveness of the framework.

6 Conclusion

Intrusion detection systems (IDS) have been defined as an essential security measure in any type of network. They are an important component that permits to identify network attacks by analyzing network traffic. This paper presents a framework that allows non-expert users to monitor their network and identify any attacks. In particular, we have defined two different modules connected to the main components of an IDS. Through this approach, it is possible to

adapt our framework in different IDS systems. Moreover, an innovative skill for Alexa has been proposed, in order to allow users to run the IDS through voice commands.

In the future, we would plan to implement the framework, integrating it with different IDSs. Moreover, we intend to develop the skill for Alexa to test the framework with non-expert users in order to obtain constructive feedback and highlight their difficulties. Finally, we plan to extend the approaches proposed to capture the user navigation intents [12] for improving the intent understanding task.

References

[1] Amazon. Alexa Skill Kit. `https://developer.amazon.com/it-IT/docs/alexa/sdk/alexa-skills-kit-sdks.html/`, 2020. [Online; accessed 10-April-2020].

[2] T. Ambwani. Multi class support vector machine implementation to intrusion detection. In *Proceedings of the International Joint Conference on Neural Networks, 2003*, volume 3, pages 2300–2305. IEEE, 2003.

[3] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco. RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of things journal*, 1(2):144–152, 2014.

[4] J. P. Anderson. Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Company*, 1980.

[5] F. Anjum, D. Subhadrabandhu, and S. Sarkar. Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols. In *Proceedings of 2003 IEEE 58th Vehicular Technology Conference*, volume 3, pages 2152–2156. IEEE, 2003.

[6] I. B. Aris, R. K. Z. Sahbusdin, and A. F. M. Amin. Impacts of IoT and big data to automotive industry. In *Proceedings of 2015 10th Asian Control Conference (ASCC)*, pages 1–5. IEEE, 2015.

[7] A. E. Attipoe, J. Yan, C. Turner, and D. Richards. Visualization tools for network security. *Electronic Imaging*, 2016(1):1–8, 2016.

[8] S. Axelsson. Intrusion detection systems: A survey and taxonomy. Technical report, Chalmers University of Technology, 2000.

[9] B. Breve, L. Caruccio, S. Cirillo, D. Desiato, V. Deufemia, and G. Polese. Enhancing user awareness during internet browsing. In *Proceedings of the Fourth Italian Conference on Cyber Security*, pages 71–81. CEUR Workshop Proceedings 2597, 2020.

[10] L. Caruccio, S. Cirillo, V. Deufemia, and G. Polese. Incremental discovery of functional dependencies with a bit-vector algorithm. In M. Mecella, G. Amato, and C. Gennaro, editors, *Proceedings of the 27th Italian Symposium on Advanced Database Systems*, volume 2400 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2019.

[11] L. Caruccio, V. Deufemia, C. D'Souza, A. Ginige, and G. Polese. A tool supporting end-user development of access

control in web applications. *International Journal of Software Engineering and Knowledge Engineering*, 25(2):307–331, 2015.

[12] L. Caruccio, V. Deufemia, and G. Polese. Understanding user intent on the web through interaction mining. *J. Vis. Lang. Comput.*, 31:230–236, 2015.

[13] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone. An IoT-aware architecture for smart healthcare systems. *IEEE Internet of Things Journal*, 2(6):515–526, 2015.

[14] S. Cirillo, D. Desiato, and B. Breve. Chravat-chronology awareness visual analytic tool. In *Proceedings of 23rd International Conference Information Visualisation (IV)*, pages 255–260. IEEE, 2019.

[15] A. De Lucia, V. Deufemia, C. Gravino, and M. Risi. Detecting the behavior of design patterns through model checking and dynamic analysis. *ACM Trans. Softw. Eng. Methodol.*, 26(4):13:1–13:41, 2018.

[16] N. F. Haq, A. R. Onik, M. A. K. Hridoy, M. Rafni, F. M. Shah, and D. M. Farid. Application of machine learning approaches in intrusion detection system: a survey. *International Journal of Advanced Research in Artificial Intelligence*, 4(3):9–18, 2015.

[17] P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis. A signature-based intrusion detection system for the internet of things. In *Proceedings of IEICE Information and Communication Technology Form*, 2018.

[18] A. Javaid, Q. Niyaz, W. Sun, and M. Alam. A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, pages 21–26, 2016.

[19] V. Jyothsna, V. R. Prasad, and K. M. Prasad. A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, 28(7):26–35, 2011.

[20] L. Koc, T. A. Mazzuchi, and S. Sarkani. A network intrusion detection system based on a hidden naïve bayes multiclass classifier. *Expert Systems with Applications*, 39(18):13492–13500, 2012.

[21] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[22] X. Krasniqi and E. Hajrizi. Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles. *IFAC-PapersOnLine*, 49(29):269–274, 2016.

[23] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[24] G. Nadiammai and M. Hemalatha. Effective approach toward intrusion detection system using data mining techniques. *Egyptian Informatics Journal*, 15(1):37–50, 2014.

[25] C. Papadopoulos, C. Kyriakakis, A. Sawchuk, and X. He. Cyberseer: 3D audio-visual immersion for network security and management. In *Proceedings of ACM Workshop on Visualization and Data Mining for Computer Security*, pages 90–98, 2004.

[26] R. M. Patil, M. R. Patil, K. V. Ramakrishnan, and T. Manjunath. Iddp: Novel development of an intrusion detection system through design patterns. *International Journal of Computer Applications*, 7(12):22–29, 2010.

[27] E. Polyakov, M. Mazhanov, A. Rolich, L. Voskov, M. Kachalova, and S. Polyakov. Investigation and development of the intelligent voice assistant for the internet of things using machine learning. In *Proceedings of Moscow Workshop on Electronic and Networking Technologies (MWENT)*, pages 1–5. IEEE, 2018.

[28] L. Qi, M. V. Martin, B. Kapralos, M. Green, and M. García-Ruiz. Toward sound-assisted intrusion detection systems. In *Proceedings of OTM Confederated International Conferences On the Move to Meaningful Internet Systems*, pages 1634–1645. Springer, 2007.

[29] P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo. Practical real-time intrusion detection using machine learning approaches. *Computer Communications*, 34(18):2227–2235, 2011.

[30] V. Singh and S. Puthran. Intrusion detection system using data mining a review. In *Proceedings of 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*, pages 587–592, 2016.

[31] M. Uddin and A. A. Rahman. Dynamic multi layer signature based intrusion detection system using mobile agents. *International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4*, 2010.

[32] G. Vigna and R. A. Kemmerer. Netstat: A network-based intrusion detection system. *Journal of Computer Security*, 7(1):37–71, 1999.

[33] B. W. Wirtz, J. C. Weyerer, and F. T. Schichtel. An integrative public IoT framework for smart government. *Government Information Quarterly*, 36(2):333–345, 2019.

[34] K. Zaraska. Prelude IDS: current state and development perspectives. *URL http://www.prelude-ids.org/download/misc/pingwinaria/2003/paper.pdf*, 2003.

[35] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga. A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37, 2017.

[36] Y. Zuo and B. Panda. Fuzzy dependency and its applications in damage assessment and recovery. In *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.*, pages 350–357. IEEE, 2004.