Cloud Intrusion Detection System Based on SVM

https://doi.org/10.3991/ijim.v17i11.39063

Khattab M. Ali Alheeti[1(✉)], Ali Azawii Abdu Lateef[2], Abdulkareem Alzahrani[3], Azhar Imran[4], Duaa Al_Dosary[1]
[1] Computer Networking Systems Department, University of Anbar, Anbar, Iraq
[2] Human Resources Department, University of Anbar, Anbar, Iraq
[3] Computer Engineering and Science Department, Al Baha University, Al Baha, Saudi Arabia
[4] Department of Creative Technologies, Air University, Islamabad, Pakistan
co.khattab.alheeti@uoanbar.edu.iq

Abstract—The demand for better intrusion detection and prevention solutions has elevated due to the current global uptick in hacking and computer network attacks. The Intrusion Detection System (IDS) is essential for spotting network attacks and anomalies, which have increased in size and scope. A detection system has become an effective security method that monitors and investigates security in cloud computing. However, several existing methods have faced issues such as low classification accuracy, high false positive rates, and low true positive rates. To solve these problems, a detection system based on Support Vector Machine (SVM) is proposed in this paper. In this method, the SVM classifier is utilized for network data classification into normal and abnormal behaviors. The Cloud Intrusion Detection Dataset is used to test the effectiveness of the suggested system. The experimental results show which the suggested system can detect abnormal behaviors with high accuracy.

Keywords—detection system, Machine Learning, network intrusion detection, Cloud computing, SVM, normal and abnormal behaviors

1 Introduction

In recent decades, cloud computing has become one of the most significant and famous technologies because of the important services it provides to companies and organizations, which have become completely dependent on cloud computing systems. The spread of this concept began when Google, the pioneering company in this field, introduced this concept, which revolutionized the world of information and communication technology. Subsequently, this technology quickly became the best choice for all companies and individuals whose work is based on information technology. With the increasing spread of the concept of cloud computing, it is vital to detect and prevent any potential attack on cloud computing systems.

Universal, on-demand, easy access to a wide range of configurable computing resources (e.g., storage, network, servers, and other services) is provided by this technology with minimal technical effort [1]. For example, it provides virtual, scalable, variable resources quickly and easily and gives users a high sense of security. In addition,

users of this technology only pay for services that are requested, such as systems, applications, servers and storage resources that are provided by cloud computing. Accordingly, excessive spending is avoided for companies, organizations and individuals, which can increase their economic success [2].

Despite the success and spread of cloud computing, it suffers from several issues, the most important of which is data security. This raises concerns among people, organizations and companies that utilize cloud computing due to the cloud work environment, which is open and fully distributed, making it more vulnerable to intrusion. Therefore, it may be possible to penetrate it, or the devices associated with it [3]. Previous surveys related to cloud computing, such as IDG 2013 survey [4], have found that the second major problem is the lack of control.

In the past decade, the emergence and complexity of attacks have increased significantly. There are different sources of hosts and different networks, and it is difficult to detect attacks due to the spread of evidence across many different distributed cloud computing sites. Because of the very powerful capabilities of the resources provided by cloud computing, they can become highly desirable targets and tempt hackers. Therefore, these potential attacks should be prevented by a Collaborative Intrusion Detection System (CIDS), which is an applicable and effective method [5] [6] [7]. The cloud architecture is divided into three layers, namely the system layer, the basic system layer, and the application layer, as shown in Figure 1. The implicit hardware is not considered a part of the cloud but as a fundamental basis. Amazon EC is an example of these layers [8].

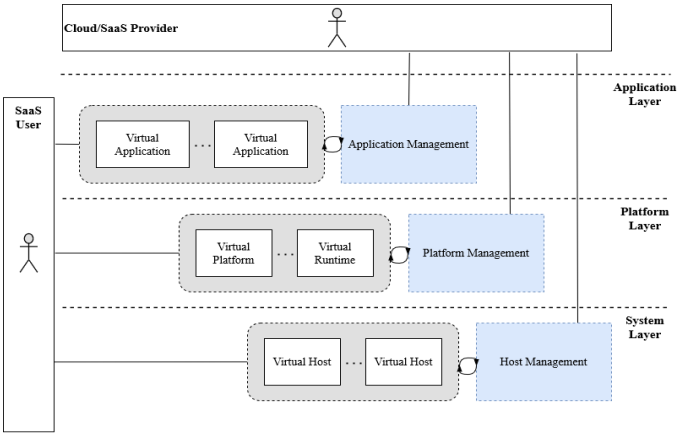

Fig. 1. Architecture of cloud computing [8]

In this paper, a detection system based on SVM is proposed. SVM is chosen as a classifier since it provides an effective rate of accuracy in detection. The remainder of this paper is organized as follows. Section 2 presents the literature review, and section 3 provides an overview of cloud computing. In section 4, the proposed detection system is presented. Sections 5 and 6 present the results and conclusion, respectively.

2 Literature review

In the past few years, many research studies have been conducted to address numerous security problems, including those related to cloud computing. It has become essential to have an organized security architecture, especially with the increasing spread of cloud computing.

The best security training methods in cloud computing, such as a security as a service model for the cloud computing environment, are available from the Cloud Security Alliance (CSA). Therefore, many research studies have been conducted in the field of cloud security, and they have presented intrusion detection systems as a defense approach to alert the system or cloud administrator about any suspicious activity [9] [10].

Mobile devices, tablets and other devices connected to the cloud are registered with the intrusion detection system. Other cloud-related services are proposed by Houmansadr et al. [11] via copying these devices to the Virtual Machines (VMs) in the cloud, thus monitoring the data traffic of these devices and determining whether these devices are intrusive or not and sending an alert to the system administrator through the known mechanisms of intrusion systems.

Other studies such as [12] [13] [14] [15] have presented a set of techniques for detecting intrusion and anomalies in different layers in the cloud. This is due to the use of anomaly detection techniques and unknown attacks at different levels in the cloud, such as network level and system level, to monitor and control suspicious processes. To solve the problem in this work [16] for multi-instance distribution and identification of intrusion coming from the external network, Mazzariello et al. [17] introduced a cloud-based intrusion detection system that relies on deploying Snort on physical devices, which is a fast system and a low-cost solution.

Garfinkel y Rosenblum [12] introduced a hypervisor-based intrusion detection system to allow users to analyze and monitor communications with the virtual interface, which is one of the most important techniques used to detect intrusion in virtual environments, especially the cloud.

To protect VMs outside the organization, Dastjerdi et al. [14] proposed an effective method for detecting intrusion regardless of the place using a mobile phone in the cloud environment. This model allows intrusion detection for VMs that are outside the organization.

The problem of trust in transmitting the alert message was solved by Ahmed et al. [18] by introducing a network-based intrusion detection system, which does not require the distribution of this system to all devices that are connected to the network, with the lowest cost and no false alarm rate.

The process of distributing the Network-based Intrusion Detection Systems (NIDSs) module to all sides of the cloud was introduced by Lo et al. [19]. This helps in the detection and prevention of attacks on the cloud. This process involves notifying all parties if an attack occurs on other parties. This helps add new species to the blocking list. Figure 2 illustrates this process.

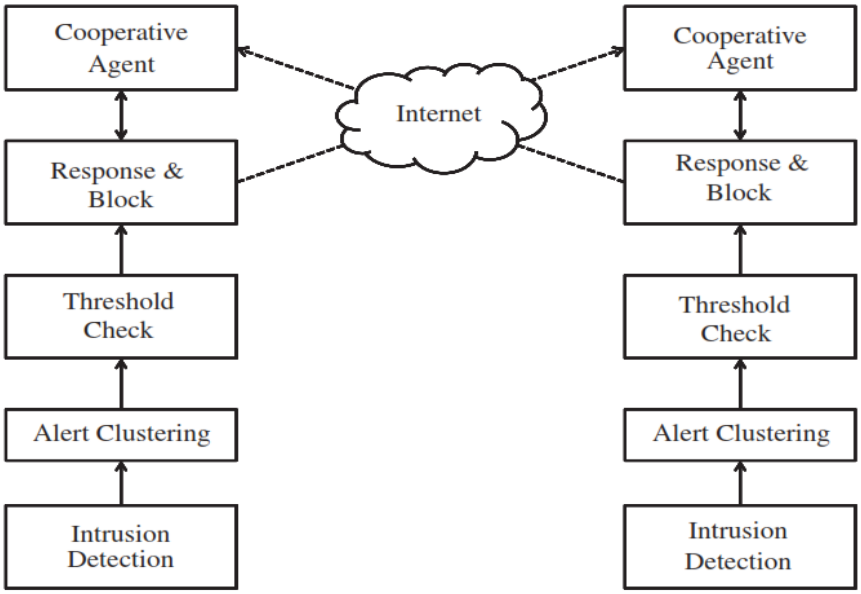

Fig. 2. Block diagram of cooperative agent-based approach [19]

To detect attacks at the hypervisor level, Zhang et al. [20] introduced a virtualization-based security system called Cloud Visor by adding a security layer to the Virtual Machine Monitor (VMM) without the need for Cloud Visor to modify the hypervisor program and add additional protection to VMs.

Our proposed detection system is different to previous works by utilizing SVM to enhance detection system accuracy in the environment of cloud computing. SVM is robust, accurate, and effective for detection.

3 Cloud computing overview

Cloud computing is defined as a computing paradigm to connect a large pool of systems in private/public networks to provide a dynamically adaptable framework for application, file and information storage. With the advent of cloud computing, application hosting, computation cost, delivery and content storage have been reduced efficiently. There are many benefits of cloud computing, such as those presented in Figure 3.

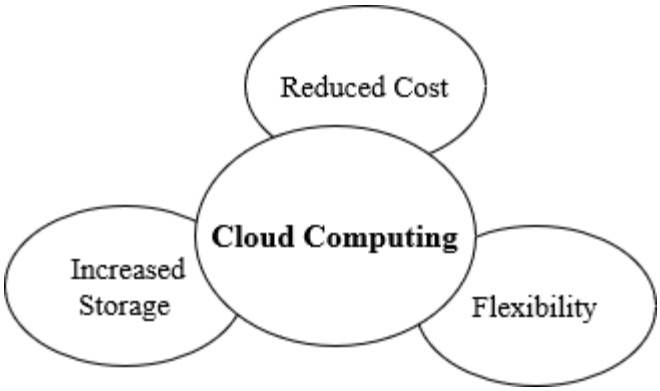

Fig. 3. Cloud computing benefits

Cloud computing is based on the concept of "reusability of IT capabilities". The difference that cloud computing brings compared to traditional concepts of "grid computing," "distributed computing," "utility computing," or "autonomic computing" is that is expands horizons over organizational limits. The cloud services can be categorized into three groups [21], as shown in Table 1.

Table 1. Cloud Services Categories

Cloud Services Category	Description
Software as a Service (SaaS)	A full application is presented to the customer by this category as a service on demand. Today, SaaS is provided by companies such as Google, Microsoft, Salesforce, and Zoho.
Platform as a Service (PaaS)	A layer of the development environment or software is encapsulated and presented as a service. The customer has the option to build their own applications. To meet scalability and manageability requirements.
Infrastructure as a Service (IaaS)	IaaS offers computing capabilities as standardized services over the network. Servers, networking data center space and equipment are gathered and made available to solve workloads.

Mainly, there are four types of cloud [22]:

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud.

4 Proposed detection model

In this paper, a detection model based on an SVM classifier is proposed to provide security for the cloud computing environment. The proposed model is discussed in the following sections.

4.1 Overview

The detection model is proposed to address the challenges in providing security for the cloud. SVM techniques are utilized within a cloud to present a secure system. SVM can improve the security of cloud systems. The basic architecture of the proposed model is presented in Figure 4.

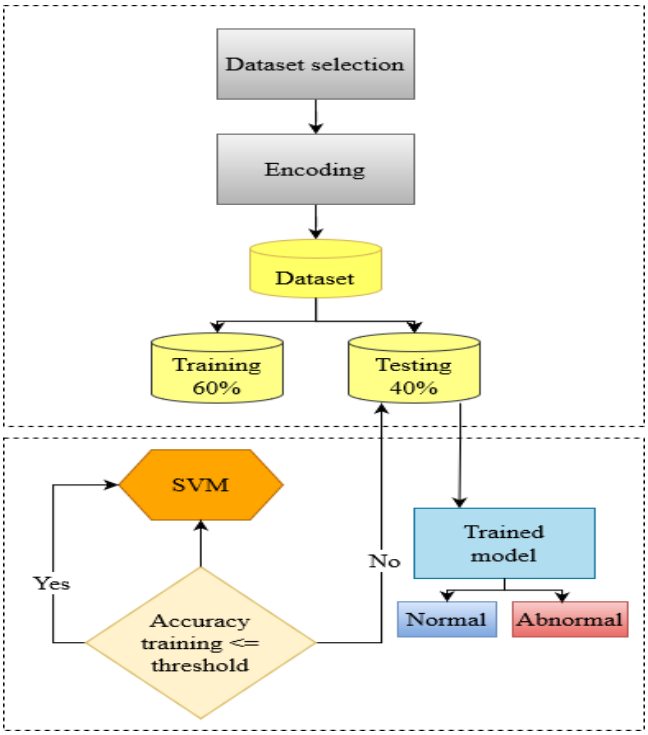

Fig. 4. Block diagram of the proposed system

The security system is considered very important issue for any model [23]. The proposed security model consists of several steps. In the first step, the dataset is collected from the source. In the second step, the encoding phase, all the letters and symbols in the dataset are converted into numbers, as SVM only works with numeric values. In the third step, the dataset is trained by using SVM as the classifier in the detection model. To determine the accuracy rate of detection, the testing phase is exploited for evaluation of the proposed approach.

Dataset description. The Cloud Intrusion Detection Dataset (CIDD) includes the audit parameters for detection of more than 100 instances of attacks in different classes [24]. The CIDD includes both knowledge and behavior based on two sets of audit data:

1. Unix Solaris audits and their identical tcpdump data.
2. Windows NT audits and their identical tcpdump data.

The CIDD contains training and testing data. The CIDD audit training data include tcpdump data and Unix Solaris audits with labeled attacks that can be utilized for training any detection system with attack signatures set, as shown in Figure 5. The CIDD audit testing data are shown in Figure 5.

Fig. 5. CIDD audit training data [25]

The CIDD audit testing data are shown in Figure 6.

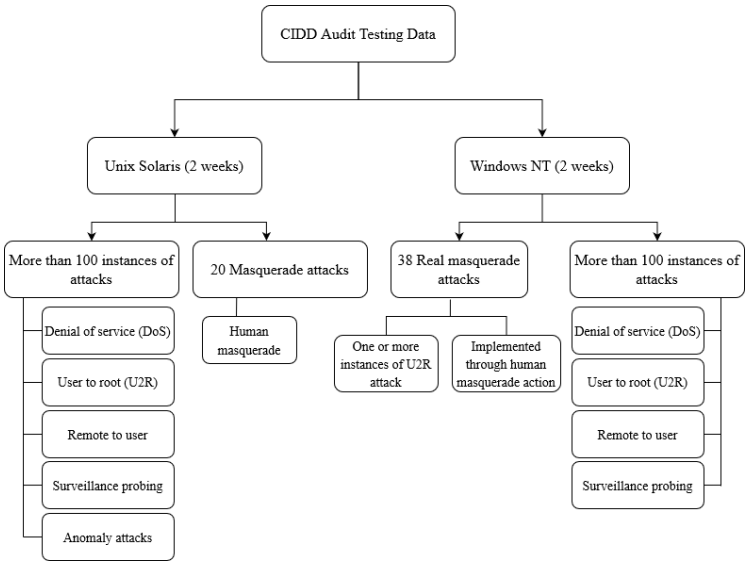

Fig. 6. CIDD audit testing data [24]

5 Results

In this research, SVM is utilized as an intelligent classifier to obtain more accurate results. The dataset for the training and testing phases was selected to evaluate the performance of the proposed system, and the total accuracy of the training is 99.92 %. The metrics used to calculate the accuracy, precision, recall and F1-score to evaluate the efficiency of the proposed system are presented below [26] [27] [28]:

$$Accuracy = \frac{Number\ of\ correclty\ classified\ patters}{Total\ number\ of\ patterns} = TP+TN/TP+FP+TN+FN \quad (1)$$

Precision was calculated according to Equation 1:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall was calculated as follows:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

F1-score was calculated according to Equation 4 as a metric for further evaluation of the proposed system:

$$F1 - score = 2\ X \frac{recall\ X\ precision}{recall+precision} \quad (4)$$

These metrics define four types of alarm (confused matrix) that are necessary for evaluation of the proposed system's performance.

The performance for precision, recall and F1 score of the proposed system is calculated. In Tables 2, 3, 4, 5, 6, and 7, we show the precision, recall, F1-score, support (features numbers), micro average, macro average, and weighted average of SVM for the test set to show how the classifier performed on our proposed system. Precision means the percentage of the results that are relevant. Recall means the percentage of total pertinent results to classify the selected model precisely. F1-score is the measure of the test accuracy (the harmonic mean of precision and recall).

Table 2. Performance metrics of the first round

Class name	Precision	Recall	F1-score	Support
0	0.96	0.92	0.94	25
1	0.1	0.1	0.1	961
Micro Average	0.1	0.1	0.1	986
Macro Average	0.97	0.96	0.99	986
Weighted Average	0.1	0.1	0.1	986

Table 3. Accuracy rate with number of records for the first round

	Number of records	Accuracy
Normal	961	99.89%
Abnormal	25	92.00%

Table 4. Performance metrics of the second round

Class name	Precision	Recall	F1-score	Support
0	0.1	0.94	0.97	32
1	0.1	0.1	0.1	954
Micro Average	0.1	0.1	0.1	986
Macro Average	0.1	0.97	0.98	986
Weighted Average	0.1	0.1	0.1	986

Table 5. Accuracy rate with number of records for the second round

	Number of records	Accuracy
Normal	954	100.00%
Abnormal	32	93.75%

Table 6. Performance metrics of the third round

Class name	Precision	Recall	F1-score	Support
0	0.96	0.1	0.98	22
1	0.1	0.1	0.1	964
Micro Average	0.1	0.1	0.1	986
Macro Average	0.98	0.1	0.99	986
Weighted Average	0.1	0.1	0.1	986

Table 7. Accuracy rate with number of records for the third round

	Number of records	Accuracy
Normal	964	98.89%
Abnormal	22	100%

Figure 7 shows the accuracy rate for normal/abnormal in three rounds.

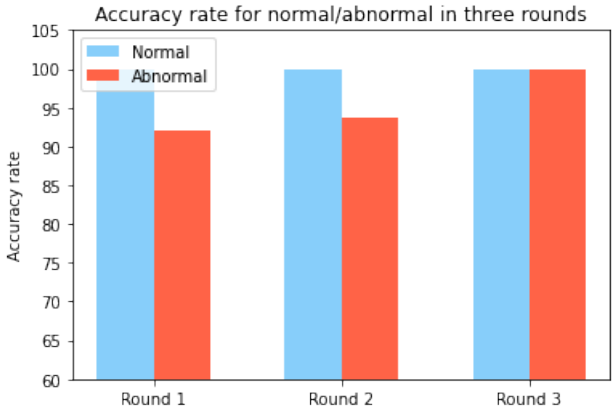

Fig. 7. Accuracy rate for normal/abnormal in three rounds

Figures 8, 9, and 10 show precision, recall, and F1-score rate comparisons in three rounds, respectively

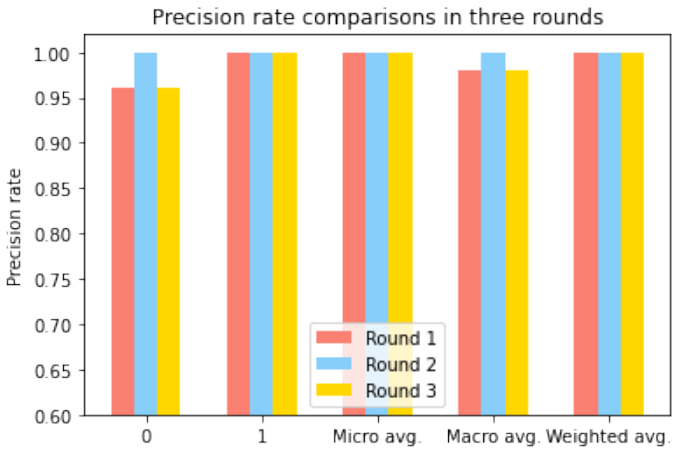

Fig. 8. Precision rate comparisons in three rounds

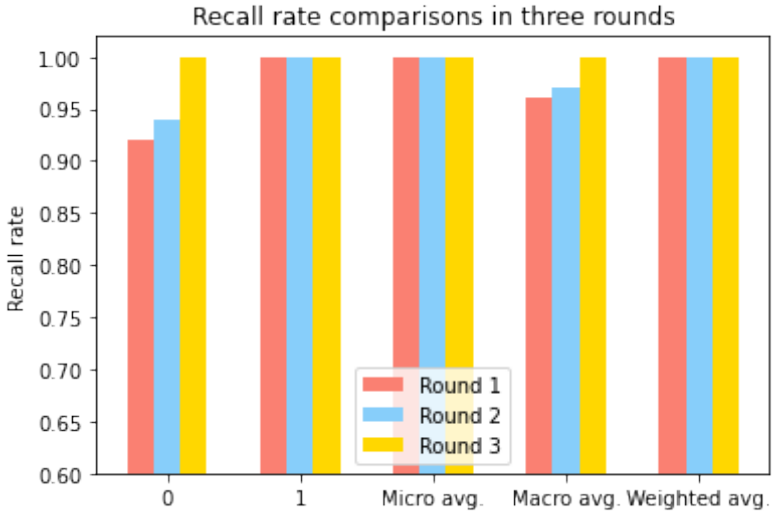

Fig. 9. Recall rate comparisons in three rounds

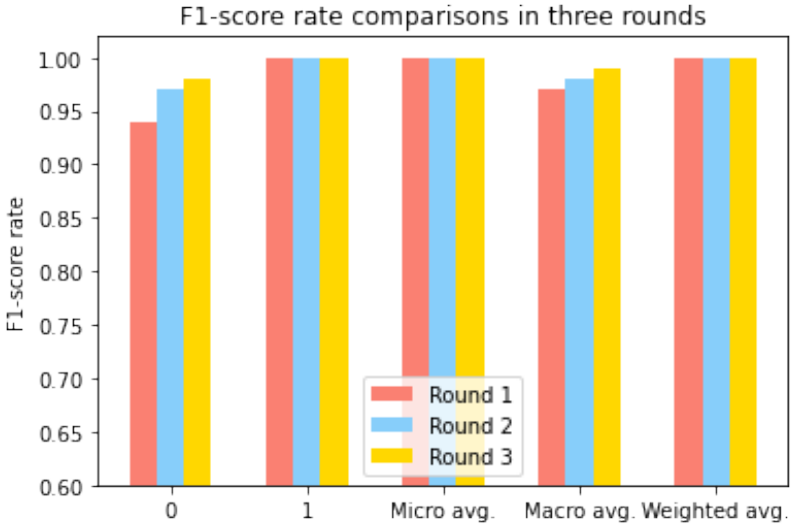

Fig. 10. F1-score rate comparisons in three rounds

6 Conclusions

In this paper, intelligent system is proposed for an improved detection rate at cloud environment. This mechanism provides a detection system by utilizing the SVM classifier. The proposed model comprises three phases. The first phase aims to collect the dataset. The second phase is the encoding phase. It is necessary to convert all the letters

and symbols in the dataset into numbers, as SVM only works with numeric values. The third phase involves training the dataset using SVM as the classifier in the detection model. To determine the accuracy rate of the detection, the testing phase was exploited for evaluation of the proposed approach. Various evaluation metrics, such as accuracy, precision, recall and F1-score, are calculated. The results indicate that the proposed method is suitable for achieving high detection accuracy, and therefore it can be utilized for anomaly detection in the cloud environment.

7 References

[1] Rich Quick. 5 Reasons Enterprises Are Frightened of the Cloud, September 2013. Section: insider.

[2] Yasir Mehmood, Muhammad Awais Shibli, Umme Habiba, and Rahat Masood. Intrusion Detection System in Cloud Computing: Challenges and opportunities. In 2013 2nd National Conference on Information Assurance (NCIA), pages 59–66, December 2013. https://doi.org/10.1109/NCIA.2013.6725325

[3] Sudhir N. Dhage and B.b. Meshram. Intrusion detection system in cloud computing environment. International Journal of Cloud Computing, 1(2-3):261–282, January 2012. Publisher: Inderscience Publishers. https://doi.org/10.1504/IJCC.2012.046711

[4] IDG Enterprise Cloud Research. Cloud Computing Key Trends and Future Effects. Survey Methodology, IDG, 2013.

[5] V. Chatzigiannakis, G. Androulidakis, M. Grammatikou, and B. Maglaris. A Distributed Intrusion Detection Prototype Using Security Agents. In Workshop of the HP OpenView University Association, 2004.

[6] Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera. A survey of coordinated attacks and collaborative intrusion detection. Computers and Security, 29(1):124–140, February 2010. https://doi.org/10.1016/j.cose.2009.06.008

[7] S. H. Teng. A Study on Object-Monitoring-based Distributed and Collaborative Intrusion Detection. The degree of Doctor of Philosophy, Guangdong University of Technology, China, 2008.

[8] Simon Ostermann, Alexandru Iosup, Nezih Yigitbasi, Radu Prodan, Thomas Fahringer, and Dick Epema. An Early Performance Analysis of Cloud Computing Services for Scientific Computing. Technical Report PDS-2008-006, Delft University of Technology,The Netherlands, December 2008.

[9] Clifton L. Smith and David J. Brooks, editors. The Theory and Practice of Security. Butterworth-Heinemann, Boston, January 2013. Version November 6, 2021 submitted to Journal Not Specified 12 of 12

[10] Ellen Messmer. Cloud Security Alliance formed to promote best practices | computerworld. Available online: https://www.computerworld.alliance-formed-to-promote-best-practices.html (accessed on 02/11/2021).

[11] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier. A cloud-based intrusion detection and response system for mobile phones. In 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), pages 31–32, June 2011. ISSN: 2325-6664. https://doi.org/10.1109/DSNW.2011.5958860

[12] Tal Garfinkel and Mendel Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. NDSS, 3, May 2003.

[13] A. Schulter, K. Vieira, C. Westphall, and C. Westphall. Intrusion Detection for Grid and Cloud Computing. IT Professional, 12(04):38–43, July 2010. Place: Los Alamitos, CA, USA Publisher: IEEE Computer Society. https://doi.org/10.1109/MITP.2009.89

[14] Amir Vahid Dastjerdi, Kamalrulnizam Abu Bakar, and Sayed Gholam Hassan Tabatabaei. Distributed Intrusion Detection in Clouds Using Mobile Agents. In 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences, pages 175–180, October 2009. https://doi.org/10.1109/ADVCOMP.2009.34

[15] Yizhang Guan and Jianghong Bao. A CP Intrusion Detection Strategy on Cloud Computing. In Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), pages 84–87, Nanchang, P. R. China, May 2009.

[16] Aman Bakshi and Yogesh B. Dujodwala. Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine. In 2010 Second International Conference on Communication Software and Networks, pages 260–264, February 2010. https://doi.org/10.1109/ICCSN.2010.56

[17] Claudio Mazzariello, Roberto Bifulco, and Roberto Canonico. Integrating a network IDS into an open source Cloud Computing environment. In 2010 Sixth International Conference on Information Assurance and Security, pages 265–270, August 2010. https://doi.org/10.1109/ISIAS.2010.5604069

[18] Martuza Ahmed, Rima Pal, Md. Mojammel Hossain, Md. Abu Naser Bikas, and Md. Khalad Hasan. NIDS: A Network Based Approach to Intrusion Detection and Prevention. In 2009 International Association of Computer Science and Information Technology -Spring Conference, pages 141–144, April 2009. https://doi.org/10.1109/IACSIT-SC.2009.96

[19] Chi-Chun Lo, Chun-Chieh Huang, and Joy Ku. A Cooperative Intrusion Detection System Framework for Cloud Computing Networks. In 2010 39th International Conference on Parallel Processing Workshops, pages 280–284, September 2010. ISSN: 2332-5690.

[20] Fengzhe Zhang, Jin Chen, Haibo Chen, and Binyu Zang. CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, SOSP '11, pages 203–216, New York, NY, USA, October 2011. Association for Computing Machinery. https://doi.org/10.1145/2043556.2043576

[21] D.Wyld. The cloudy future of government IT: cloud computing and the public sector around the world. International Journal of Web & Semantic Technology (IJWesT), 1(1), 2010.

[22] Suyel Namasudra, Pinki Roy, and Balamurugan Balusamy. Cloud Computing: Fundamentals and Research Issues. In 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), pages 7–12, February 2017. https://doi.org/10.1109/ICRTCCM.2017.49

[23] Alheeti, Khattab, Ibrahim Alsukayti, and Mohammed Alreshoodi. "Intelligent Botnet Detection Approach in Modern Applications." Int. J. Interact. Mob. Technol., vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24199

[24] Cloud Intrusion Detection Dataset CIDD. Available online: http://groups.di.unipi.it/hkholidy/projects/cidd/index.html (accessed on 02/11/2021).

[25] CIDD Architecture. Available online: http://groups.di.unipi.it/hkholidy/projects/cidd/blog.html (accessed on 02/11/2021).

[26] Khattab M. Ali, VenusW. Samawi, and Mamoun Suleiman Al Rababaa. The affect of fuzzification on neural networks intrusion detection system. In 2009 4th IEEE Conference on Industrial Electronics and Applications, pages 1236–1241, May 2009. ISSN: 2158-2297.

[27] B. Al-Rami, K. M. A. Alheeti, W. M. Aldosari, S. M. Alshahrani, and S. M. Al-Abrez, "A New Classification Method for Drone-Based Crops in Smart Farming.," Int. J. Interact. Mob. Technol., vol. 66, no. 8, 2022. https://doi.org/10.3991/ijim.v16i09.30037

[28] Alzahrani, Abdulkareem, Khattab Alheeti, and Samer Thabit. "Intelligent Mobile Coronavirus Recognition Centre Based on IEEE 802.15. 4."" Int. J. Interact. Mob. Technol., vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24193

8 Authors

Khattab M. Ali Alheeti is with Computer Networking Systems Department, College of Computer Sciences and Information Technology, University of Anbar, Anbar, Iraq (email: co.khattab.alheeti@uoanbar.edu.iq).

Ali Azawii Abdu Lateef is with Human Resources Department, University of Anbar, Anbar, Iraq.

Abdulkareem Alzahrani is with Computer Engineering and Science Department, Faculty of Computer Science and Information Technology, Al Baha University, Al Baha, Saudi Arabia.

Azhar Imran is with Department of Creative Technologies, PAF Complex, E-9, PAF Complex, E-9, Air University, Islamabad, Pakistan.

Duaa Al_Dosary is with Computer Networking Systems Department, College of Computer Sciences and Information Technology, University of Anbar, Anbar, Iraq.

Article submitted 2023-02-22. Resubmitted 2023-04-27. Final acceptance 2023-05-01. Final version published as submitted by the authors.