IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Agent Based Intrusion Detection System

Prof. Nisha Chaube[1], Onkar Kodape[2], Prajwal Kulkarni[3], Sahil Patil[4], Shrishail Dhole[5]
Guide, Computer Science and Engineering[1]
Students, Computer Science and Engineering[2,3,4,5]
MIT Art Design and Technology University, Pune, India
nisha.chaube@mituniversity.edu.in

Abstract: *With the growing complexity and sophistication of cyber threats, network security has become a vital aspect of any organization's cyber security efforts. Among the critical solutions, effective monitoring and analysis tools(So-In, 2009) play an invaluable role. ABIDS provides a versatile platform for real-time monitoring, alerting, and visualization of the network infrastructure. This paper attempts to demonstrate how ABIDS can serve as a basis for improved network security. Furthermore, I elaborate on ABIDS' features and abilities that make it a good choice for this purpose, such as the ability to collect the data in various ways, its compatibility with multiple protocols and devices, and its flexible alerting system. We also outline practical use-cases for ABIDS in cybersecurity operations(Ou et al., 2011), including practice recommendations on proactive threat hunting, the identification of anomalies, and timely incident responses. By incorporating ABIDS with traditional security infrastructures and solutions, organizations will be able to set up smoother and more insightful security monitoring habitats. Case studies and focused examples explain how ABIDS can help organizations enhance defence, manage risk and protect core assets against persistent cyber adversaries with adaptive capabilities(Tahri et al., 2022). We also discuss some of the deployment techniques and practices to deploy ABIDS in security-intensive environments, including the ability to scale, performance, and resource requirements. In conclusion, this paper is of the opinion that ABIDS should be strategically adopted and integrated into modern cybersecurity methods and approaches as a foundational resultant. Using ABIDS as a tool for security monitoring and analysis would strengthen the organization's defences agains6t potential cyber-attacks while ensuring the availability and integrity of their network infrastructure.*

Keywords: ABIDS

I. INTRODUCTION

ABIDS is a sophisticated monitoring solution developed to equip organizations with extensive visibility of their IT infrastructure, including health, performance, and availability, among other critical metrics. Relying on its rich functionality, ABIDS serves as a hub for device monitoring, service monitoring, application monitoring, and network component monitoring, allowing administrators to detect and resolve emerging issues before they become critical. Primarily, ABIDS is designed for real-time monitoring(Parihar et al., 2014)providing unprecedented visibility of critical performance indicators such as CPU utilization, memory allocation, network throughput, disk space capacity, and other crucial metrics. Another critical ABIDS feature is its flexibility and scalability. No matter whether you are administering a small business network or a large enterprise's infrastructure, ABIDS fits your requirements, enabling you to supervise multiple thousands of devices and services through a single central interface. Its distributed monitoring features facilitate beyond competition scalability around multiple geographical areas. Therefore, if your organization has many branches, using ABIDS would be the most appropriate solution as its capabilities fit perfectly for companies having nearly hundreds of different location deployments. Then, the ABIDS' monitoring sends alerts. It means that the given monitoring solution is set to alarm the administrator according to preset conditions. This means that an administrator can set up a relevant threshold, and the ABIDS sends an error if a particular value is reached or exceeded(Ou, 2012). These alerts allowABIDS organizations to configure various alerts to monitor performance data and generate notifications when pre-set thresholds are exceeded. Alerts can be sent using email, SMS, IM, or custom scripts to make sure IT teams are immediately alerted to any potential problems that require immediate attention. By

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

dealing with alerts proactively, organizations can minimize downtime and reduce exposure to risk. In addition to that, ABIDS also has comprehensive visualization and reporting capabilities to help analyze the data and decide. Its intuitive dashboards and flexible reports enable stakeholders to get the actionable insights into the performance trends, the historical data, and the compliance metrics. Be it performance graphing, trend analysis, SLA compliance report generation; ABIDS provides all the necessary tools to monitor, analyze, and optimize the IT environment (Vij & Saini, 2021).

II. LITERATURE SURVEY

Literature	Summarize abstract	Method used	Limitations	Conclusions
(Mirlekar & Kanojia, 2022)	*Discusses network security, cyber attacks, and Intrusion Detection System importance. Highlights the need for understanding various attack types for mitigation.*	*Reviewing NIDS insights, techniques, and strategies to mitigate cyber attacks. Developing IDS using algorithms after studying cyber attack characteristics.*	*False alarm is a major concern for IDS. IDS can only raise alerts but cannot resolve issues. IDS needs to be trained with new algorithms for analysis.*	*IDS reduces network intrusions by providing alerts on cyber threats. Understanding cyber attacks is crucial to develop effective security systems. NIDS monitors traffic, generates alarms for intrusions, and enhances network security*
(Bhati et al., 2020)	*IDS detects, identifies, and tracks intruders in a network.*	*Discusses various intrusion detection systems and techniques*	*Limited discussion on machine learning algorithms for intrusion detection.*	*Summarizes intrusion detection systems and techniques for network security.*
(Bertin, 1975)	*Intrusion detection monitors network traffic for suspicious activity, issuing alerts.*	*Monitoring network traffic and host processes for suspicious activity.*	*Limited discussion on specific intrusion detection techniques.*	*Emphasizes the importance of intrusion detection for network security.*
(Mescheryakov &Shchemelinin, 2013)	*ZABBIX-based network monitoring system with simple deployment and distributed monitoring.*	*ZABBIX-based network monitoring system with server, switch, router, and terminal. Simple deployment, OS and network monitoring, distributed monitoring, and email alerts.*	*The paper does not mention any limitations.*	*ZABBIX system enables simple deployment, monitoring hosts, and network equipment.*
(Mohd Fuzi et al., 2022)	*Network monitoring detects attacks to maintain network health and performance.*	*Zabbix for network monitoring, Tcpdump for logging, and Telegram for alerts. Detection of ping and*	*SYN flooding detection needs improvement, missed one out of three attacks. Zabbix accurately*	*Zabbix accurately detected ping flooding but needs improvement in SYN attacks. Future work includes*

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

	Zabbix tool used to monitor servers for ping and SYN attacks. Alerts sent via Telegram for ping and SYN flooding attempts.	*SYN flooding attacks on the server. Monitoring server for ping floods and SYN flood attacks.*	*detected ping flooding but not all SYN flooding*	*adding countermeasures for attacks and enhancing SYN detection.*
(Rehak et al., 2008)	*IPrototype of agent-based intrusion detection system for high-speed networks. Integrates anomaly detection techniques using collective trust modeling in agents. Real-time surveillance of gigabit networks based on traffic statistics..*	*Integration of anomaly detection techniques with collective trust modeling. Utilization of traffic statistics in NetFlow format for real-time surveillance.*	*No specific limitations were mentioned in the provided contexts.*	*Prototype integrates anomaly detection techniques using collective trust modeling. Real-time surveillance of gigabit networks based on traffic statistics*
(Krmicek et al., 2007)	*Agent-based system uses software agents to protect networks from attacks..*	*Utilizes a plurality of cooperating software agents for network protection.*	*No specific limitations mentioned in the provided contexts..*	*Utilizes software agents to protect networks against attacks.*
(Application & Data, 2008)	*Security platform with agent-based intrusion detection for high-speed networks. Detection algorithm extends trust modeling techniques for anomaly detection. Heterogeneous methods used by cooperating agents with a reputation mechanism. Hardware-accelerated NetFlow probes for wire-speed data acquisition.*	*Trust modeling techniques extension with uncertain identities and context representation. Heterogeneous anomaly detection methods by cooperating agents with reputation mechanism.*	*The paper does not explicitly mention limitations.*	*Proposed ant algorithm for MKPs outperforms Ant System and Ant-knapsack. Future work includes studying ACOMPD algorithm effectiveness and parameter influence analysis.*

DOI: 10.48175/IJARSCT-18286

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

This table's primary aim is to highlight the need to understand different types of attacks to mitigate them, focusing on reviewing NIDS extraction of insights, techniques and strategies required to mitigate cyber-attacks. In addition to awareness of the attacks, IDS is employed in the detection as well, and later, the section concludes about the generation of false alarms being a significant concern for IDS(Saxena et al., 2017). Despite the limitation, Reduction in network intrusions by providing 'alert' cyber threats, and knowing about cyber-attacks is an essential need to develop proper systems of securities. IDS is mainly used for detecting the intruders and has nothing to do with encryption. detection of the intrusion is the technique used in IDS. IDS possess an 100% threat of detection capabilities in network security. Employing an IDS is the best way of securing the network on the first hand, and also, it would support the virtual private networks but will not support the supported key networks. The section of the detection of this Generic intrusion detection technique is necessary in a network security. This table contains More detailed information about this generic intrusion-based techniques and the different 'intrusion-based techniques'. It contains only the limited exploration of machine three techniques for the intrusion detection methods, This table consists of a summary of the IDS and the types of learning algorithms of this model. zabbix-based This table also introduced a network monitoring system is flawless deployment and highly distributed monitoring system used across different servers, switches, routers and even at different terminals.

In conclusion, This table gives bits of knowledge into the vital part of Interruption Location Frameworks in improving arrange security by recognizing and relieving cyber assaults. It underscores the significance of understanding different assault sorts and creating successful security frameworks. Furthermore, it emphasizes the importance of interruption discovery for arrange security and presents This table's primary aim is to highlight the need to understand different types of attacks to mitigate them, focusing on reviewing NIDS extraction of insights, techniques and strategies required to mitigate cyber-attacks. In addition to awareness of the attacks, IDS is employed in the detection as well, and later, the section concludes about the generation of false alarms being a significant concern for IDS(Saxena et al., 2017). Despite the limitation, Reduction in network intrusions by providing 'alert' cyber threats, and knowing about cyber-attacks is an essential need to develop proper systems of securities. IDS is mainly usedfor detecting the intruders and has nothing to do with encryption. detection of the intrusion is the technique used in IDS. IDS possess an 100% threat of detection capabilities in network security. Employing an IDS is the best way of securing the network on the first hand, and also, it would support the virtual private networks but will not support the supported key networks. The section of the detection of this Generic intrusion detection technique is necessary in a network security. This table contains More detailed information about this generic intrusion-based techniques and the different 'intrusion-based techniques'. It contains only the limited exploration of machine three techniques for the intrusion detection methods, This table consists of a summary of the IDS and the types of learning algorithms of this model. zabbix-based This table also introduced a network monitoring system is flawless deployment and highly distributed monitoring system used across different servers, switches, routers and even at different terminals.A ZABBIX-based arrange checking framework with progressed checking capabilities.

The main function is composed of three systems. The first system is Integrated Network Monitoring using Zabbix with Push Notification via Telegram. in this, Zabbix is directly monitoring the network, and tcp dump is used for logging and alerting using Telegram. UDM feature of Zabbix has detected the ping flood successfully, but it failed in the case of detecting SYN attack. In this, Zabbix has missed one out of three attacks. There are few tactics mentioned in this article regarding detecting and countering the simple network attacks. The future work could be done by incorporating the countermeasures for the attacks and also by improving the detection of the SYN. The second system is CAMNEP: agent-based network intrusion detection system. The third system, Agent-Based Network Intrusion Detection System, containing the plurality of cooperating software agents, focuses on trust modelling techniques extension with uncertain identities and context representation.

In conclusion , This table gives experiences into three distinctive arrange observing and interruption discovery frameworks. The to begin with framework utilizes Zabbix for checking servers for ping and SYN assaults, with the restriction of requiring enhancement in identifying SYN assaults. The moment framework, CAMNEP, presents a model of an agent-based interruption discovery framework that coordinating peculiarity discovery procedures utilizing collective believe modeling and real-time observation based on activity measurements. The third framework emphasizes the utilize of collaborating computer program specialists for arrange security and believe modeling methods

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

expansion, with a center on future work including calculation viability and parameter impact examination. This table by and large highlights the significance of viable arrange checking and interruption discovery for keeping up organize wellbeing and execution.

III. METHODOLOGY

Identification of Monitoring Requirements:

- **Define the scope of monitoring:** Define the scope of observing: Decide what viewpoints of the IT framework require to be checked, such as servers, network devices, applications, etc.
- **Identify key performance indicators (KPIs):**Decide the measurements that are basic for evaluating the wellbeing and execution of the foundation, such as CPU utilization, memory utilization, organize activity, etc.(Teshome et al., 2018)

Installation and Configuration of ABIDS:

- **Install ABIDS server:**Set up the central observing server where all observing information will be collected and stored.
- **Configure ABIDS agents:**Introduce ABIDS agents on the devices to be checked. Agents collect information locally and send it to the ABIDS server.(et al., 2018)
- **Set up monitoring items:**Characterize monitoring things in ABIDS for each metric to be checked, indicating how information ought to be collected (e.g., through SNMP, ICMP, or custom scripts).
- **Create triggers and thresholds:**Characterize triggers in ABIDS to indicate conditions that demonstrate a issue, such as high CPU utilization or low disk space.
- **Configure notifications:** Set up notices to alarm administrator when triggers are activated, utilizing strategies such as mail, SMS, or custom scripts.

Deployment of Monitoring Infrastructure:

- **Deploy ABIDS proxies (optional):**If monitoring a large-scale or distributed infrastructure, we deploy ABIDS proxies to collect data from remote locations and reduce the load on the central server.
- **Organize hosts and groups:** Organize monitored device into logical groups based on things such as area, work, or significance.(Ciuffoletti, 2015)

Data Collection and Visualization:

- **Monitor data collection**: Permit ABIDS to collect monitoring data from agents and proxies concurring to the configured schedule.
- **Visualize monitoring data:** Utilize the ABIDS web interface to make dashboards and reports that visualize the collected information, permitting administrator to effortlessly translate execution patterns and identify issues.

Analysis and Troubleshooting:

- **Analyze monitoring data:** Frequently review monitoring data to recognize patterns, anomalies, and potential issues.
- **Troubleshoot problems:** Utilize ABIDS monitoring information and previous records to analyze and troubleshoot execution issues or blackouts.(Jain & Anubha, 2021)

Optimization and Scalability:

- **Optimize monitoring configuration**: Fine-tune monitoring settings and thresholds to minimize false alarms and improve the accuracy of monitoring

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Fig.1

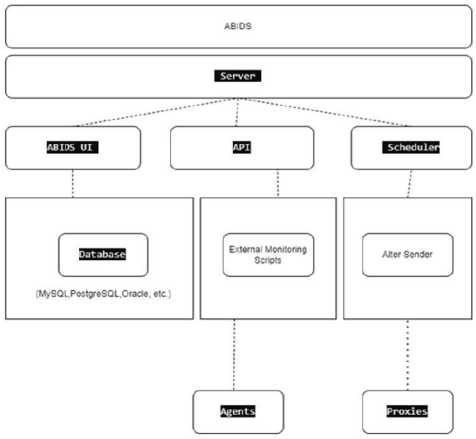
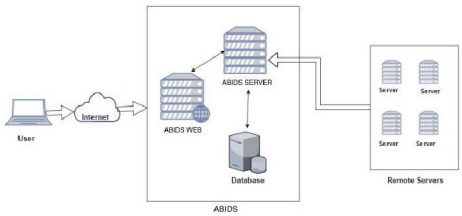


Fig.2



IV. RESULTS

Performance Metrics Comparison:

Present comparative information on execution measurements some time recently and after implementing ABIDS monitoring. Analyze changes or deteriorations in measurements such as uptime, reaction time, and resource utilization.

Incident Response Time:

Evaluate the effectiveness of ABIDS in decreasing incident reaction time by comparing previous data on incident detection and determination times. Provide insights on how rapidly ABIDS alerts were activated and reacted to, driving to issue resolution.

Downtime Reduction:

Quantify the decrease in downtime accomplished through proactive monitoring with ABIDS. Compare downtime insights before and after ABIDS execution to highlight changes in system availability.

Resource Utilization Optimization:

Demonstrate how ABIDS made a difference in optimizing resource utilization by monitoring CPU, memory, disk space, and network bandwidth. Show charts or charts outlining patterns in resource utilization and how adjustmentwas made based on ABIDS monitoring data.

Capacity Planning:

Discuss how ABIDS facilitated capacity arranging by giving insights into resource utilization patterns and estimating future needs. Present scenarios where ABIDS information informed decisions with respect to hardware upgrades or scaling infrastructure.

Security Incident Detection:

Showcase ABIDS capability in identifying security incidents by monitoring for abnormal network activity, unauthorized get to attempts, or abnormal system behavior. Provide cases of security incidents recognized and relieved through ABIDS alerts(Werlinger et al., 2010)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

User Satisfaction and Feedback:

Collect feedback from system administrators or IT staff with respect to their fulfillment with ABIDS as a monitoring solution. Include overview comes about or tributes highlighting the benefits and challenges of utilizing ABIDS in their environment.

Cost Savings:

Estimate cost savings accomplished by utilizing ABIDS compared to commercial monitoring solutions. Consider components such as program licensing expenses, equipment requirements, and labor costs related with checking tasks.

Scalability and Performance of ABIDS:

Evaluate ABIDS scalability by analyzing its performance in monitoring large-scale or dispersed environments. Discuss any limitations experienced and measures taken to optimize ABIDS for high-volume monitoring.

V. DISCUSSION

ABIDS is an open-source network monitoring and administration software, serves as a critical tool for organizations to monitor the wellbeing and execution of their IT foundation. However, with the increasing level of cyber threats, guaranteeing the security of monitoring tools like ABIDS has become vital. Understanding ABIDS security features is essential for organizations to defend sensitive information and maintain the integrity of their monitoring frameworks.

ABIDS offers robust security features and capabilities to help organizations secure their monitoring framework effectively. By implementing solid authentication and authorization mechanisms, encryption protocols, vulnerability administration processes, and logging and auditing capabilities, organizations can improve the security of their ABIDS arrangements and relieve the risk of security breaches. Additionally, by integrating ABIDS with other security tools and technologies, organizations can assist support their security pose and guarantee comprehensive security monitoring and analysis over their IT environments.

VI. CONCLUSION

Our ABIDS project will create a smart system that will watch over computers, keeping them safe from online and offline threats. It will be fast and accurate, striking the right balance. While we'll overcome many challenges, there will be more to be done to stay ahead of new threats. In the end, our ABIDS will make the digital world a safer place

REFERENCES

[1]. Application, F., & Data, P. (2008). (12) United States Patent. 2(12).

[2]. Bertin, E. P. (1975). Detection BT - Principles and Practice of X-Ray Spectrometric Analysis (E. P. Bertin (ed.); pp. 219–284). Springer US. https://doi.org/10.1007/978-1-4613-4416-2_6

[3]. Bhati, N. S., Khari, M., García-Díaz, V., & Verdú, E. (2020). A Review on Intrusion Detection Systems and Techniques. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 28(Supp02), 65–91. https://doi.org/10.1142/S0218488520400140

[4]. Ciuffoletti, A. (2015). Automated Deployment of a Microservice-based Monitoring Infrastructure. Procedia Computer Science, 68, 163–172. https://doi.org/https://doi.org/10.1016/j.procs.2015.09.232

[5]. Jain, G., & Anubha. (2021). Application of SNORT and Wireshark in Network Traffic Analysis. IOP Conference Series: Materials Science and Engineering, 1119(1), 012007. https://doi.org/10.1088/1757-899x/1119/1/012007

[6]. Krmicek, V., Celeda, P., Rehák, M., & Pechoucek, M. (2007). Agent-Based Network Intrusion Detection System. In Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology, IAT 2007. https://doi.org/10.1109/IAT.2007.111

[7]. Kumar Saxena, A., Sinha, S., & Shukla, P. (2018). Performance Analysis of Classification Techniques by using Multi Agent Based Intrusion Detection System. International Journal of Computer Network and Information Security, 10(3), 17–24. https://doi.org/10.5815/ijcnis.2018.03.03

[8]. Mescheryakov, S. V, & Shchemelinin, D. A. (2013). Capacity and Performance Analysis in Cloud Computing. 12, 91–98.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

[9]. Mirlekar, S., & Kanojia, K. P. (2022). Role of Intrusion Detection System in Network Security and Types of Cyber Attacks-A Review. International Journal of Innovations in Engineering and Science, 7(9), 28–32. https://doi.org/10.46335/ijies.2022.7.9.6

[10]. Mohd Fuzi, M. F., Mohammad Ashraf, N. F., & Jamaluddin, M. N. F. (2022). Integrated Network Monitoring using Zabbix with Push Notification via Telegram. Journal of Computing Research and Innovation, 7(1), 147–155. https://doi.org/10.24191/jcrinn.v7i1.282

[11]. Ou, C.-M. (2012). Host-based intrusion detection systems adapted from agent-based artificial immune systems. Neurocomputing, 88, 78–86. https://doi.org/https://doi.org/10.1016/j.neucom.2011.07.031

[12]. Ou, C.-M., Wang, Y.-T., & Ou, C. R. (2011). Intrusion detection systems adapted from agent-based artificial immune systems. 2011 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE 2011), 115–122. https://doi.org/10.1109/FUZZY.2011.6007564

[13]. Parihar, J. S., Rathore, J. S., & Burse, K. (2014). Agent Based Intrusion Detection System to Find Layers Attacks. 2014 Fourth International Conference on Communication Systems and Network Technologies, 685–689. https://doi.org/10.1109/CSNT.2014.144

[14]. Rehak, M., Pechoucek, M., Celeda, P., Novotny, J., & Minarik, P. (2008). CAMNEP: Agent-based network intrusion detection system. Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS, 3, 1813–1816.

[15]. Saxena, A. K., Sinha, S., & Shukla, P. (2017). General study of intrusion detection system and survey of agent based intrusion detection system. 2017 International Conference on Computing, Communication and Automation (ICCCA), 421–471. https://doi.org/10.1109/CCAA.2017.8229866

[16]. So-In, C. (2009). A Survey of Network Traffic Monitoring and Analysis Tools. Cse 576-06 Computer System Analysis Project, June, 1–24. http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3/ind...%5Cnhttp://www1.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3.pdf

[17]. Tahri, R., Balouki, Y., Jarrar, A., & Lasbahani, A. (2022). Intrusion Detection System Using machine learning Algorithms. ITM Web of Conferences, 46, 02003. https://doi.org/10.1051/itmconf/20224602003

[18]. Teshome, A., Rilling, L., & Morin, C. (2018). Verification for security monitoring SLAs in IaaS clouds: The example of a network IDS. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 1–7. https://doi.org/10.1109/NOMS.2018.8406157

[19]. Vij, C., & Saini, H. (2021). Intrusion Detection Systems: Conceptual Study and Review. 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 694–700. https://doi.org/10.1109/ISPCC53510.2021.9609481

[20]. Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. Information Management & Computer Security, 18(1), 26–42. https://doi.org/10.1108/09685221011035241