Proceedings of the Second International Conference on Automation, Computing and Renewable Systems (ICACRS-2023)
DVD Part Number: CFP23CB5-DVD; ISBN: 979-8-3503-4022-8

Review of DDoS Attack Detection in Big Data with Cloud using Machine Learning

P. Radhika, Research Scholar,
Department of Computer Science
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies
Pallavaram, Chennai, India
radhika0788@gmail.com

Dr. S. Kamalakkannan, Associate Professor
Department of Information Technology
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies
Pallavaram, Chennai, India
kannan.scs@velsuniv.ac.in

Dr. P. Kavitha, Assistant Professor
Department of Computer Applications
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies
Pallavaram, Chennai, India
pkavikamal@gmail.com

***Abstract*—Cloud Computing (CC) is a massive breakthrough in Information Technology (IT) that provides end users to access flexible and virtualized sources at affordable infrastructure cost and management. One of the most significant technologies in the big-data era is the CC Data Centres (DCs). The Distributed Denial of Service (DDoS) attacks are one of the most serious issues when it comes to the privacy of DC. DDoS attacks using Transmission Control Protocol (TCP) traffic are taken into consideration, which are becoming more prevalent but challenging to identify. The DDoS attack is the focus of this study, along with the technique used to prevent it and lessen the vulnerability of the big data server side. The system entails the delivery of packets in the form of DDoS attacks to cloud-based websites and even addresses the real-time prediction of software layer DDoS attacks using various Machine Learning (ML) and Deep Learning (DL) techniques. As a result, it stands apart among numerous hosts. Additionally, the objective of this paper was to offer a succinct introduction to attack detection approaches for early researchers working on cloud-based big data applications. As a result, these approaches are categorised according to how they function, their strengths and shortcomings are reviewed, and finally, several research papers that used each method are examined.**

Keyword*: *Cloud computing, Distributed Denial of Service attacks, Machine Learning, Deep learning, Big Data

I. INTRODUCTION

The term "cloud computing" is a fantastic way to describe the centralization of several computer services on a single server. Data and programmes are being transferred to the "cloud" from desktop and laptop computers. The "pay as you go" and low-cost services offered by cloud computing make it a fierce rival in the IT industry. Data has been moved into the cloud by all significant businesses and industries. By offering services with the least number of resources, the shortest amount of time, and the least amount of work, the cloud computing industry has reduced several concerns with time, effort, and cost. Although cloud computing offers a variety of services to its consumers, IaaS, PaaS, and SaaS are the three most useful and often used services. Additionally, cloud computing has another feature, which is depicted in Figure 1. Everything that makes life easier for humans inevitably has drawbacks. Due to the enormous volume of data stored on the cloud, security issues are becoming more prevalent. As cloud computing becomes more popular, these challenges will only become worse. There is also the issue of security, which is the biggest concern. During a DDOS attack, millions of packets are thrown at a target to disrupt all of its services, which involves numerous systems attacking one system at once.

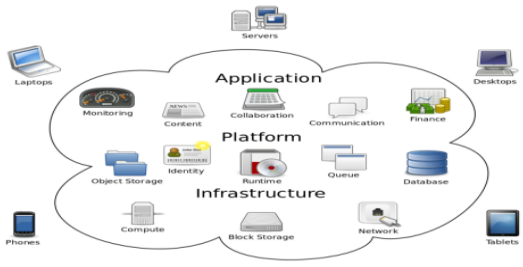

FIGURE 1 FRAMEWORK OF CLOUD COMPUTING

II. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

Broad Network Access

It is referred to as the cloud is connected to a broad network. Many businesses use cloud services to stay in touch with their clients and other businesses in this case because a user can access the services offered by the cloud. In any case, this is dependent on the type of network used by a particular business. When a network is private, the information offered would only be available to its members, however when a cloud is public, anybody should be able to access the information as well as the services it offers. Users most often offer private cloud networks to eliminate security problems when it deal with public clouds, user data can be exposed, thus users would prefer to use private clouds to avoid this issue.

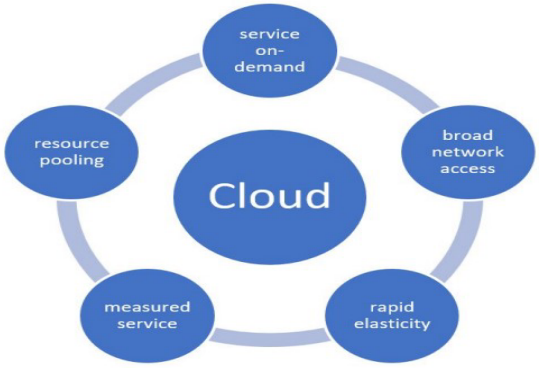

FIGURE 2 CHARACTERISTICS OF CLOUD COMPUTING (CC)

Rapid Elasticity

An important feature of the cloud is that it offers its consumers all the amenities in a very trustworthy manner. Users can access the cloud more conveniently on demand, and it is the sole platform that offers all services readily available. Additionally, the cloud has given its users the significant benefit of storage, allowing them to take advantage of new services based on the free storage [1].

Measured Services

The resources utilised in cloud computing are metered, and each organisation is only charged for what they use. Pay-per-use features can be used in the case of resource utilisation optimisation. The service provider in the cloud is monitoring, measuring, and reporting on the virtual server instances that are kept in the cloud [2].

On Demand Self Service

Customers can use on-demand self-service to obtain various kinds of services from any location and at any time. This option allows users to request services when they need them. As needed automatically without human intervention, such as server time and network storage. The most well-known companies employed as in-demand sellers include a variety of firms like HP, IBM, and Microsoft [3]. These businesses merely need to provide services and resources to their clients in order to facilitate their purchases of goods on demand.

Measured Service

Paid-for cloud services entail paying according to consumption. Metered service is another name for it. All issues and failures are managed and seen in measured services. IT professionals refer to distributed computing as measured service.

Resource Pooling

A cloud method called resource pooling allows users to access resources and release them as needed. The resource pool is usually employed by PaaS users to get the resources when they need and return them to the resource pool when they are no longer required. All the difficulties that arise while employing the resource pool approach in the cloud would be reduced in this way. Resource sharing enables cloud service providers to offer all resources to their clients and users. Every user can obtain resources that are available on demand by means of resource pooling [4].

III. BIG DATA ANALYTICS

A conventional database system cannot handle enormous datasets such as Big data, possibly exceeding hundreds of terabytes and petabytes, which is the type of data that is being stored in the cloud. Data is stored in the cloud by several of the largest companies in the world. Through the utilisation of their customised features implemented on the cloud or with the use of integrated cloud capabilities, these businesses are capable of study an extremely detailed data in order to learn truths they weren't aware of. Big data sets with near real-time capabilities are undoubtedly advantageous to enterprises, thus the cloud must have unique data architecture, tools and analytical techniques.

Characteristics of Big Data

Volume, Velocity, Variety, Veracity are the 4Vs that make up the big data feature characteristics. Volume, the first V, denotes the size and quantity of the data. This is the primary and most noticeable feature of Big Data. The rate of data collection or change is referred to as velocity. One second intervals are used to monitor and gather some types of big data, such as stock market

prices, which are tracked and gathered at an extremely fast pace. The third aspect, Variety, describes the variety of sources from which the data is derived; these sources can include logs, social media, and even click streams. Veracity's final feature describes the quality of the data. The consistency, absence, incompleteness, approximation, deception, ambiguity, and latent of the data are patterns that can be used to gauge the standard of the data.

Storage Management and Cloud

A variety of software programmes are available on the cloud to support cloud computing. If there are unstructured data sources, such as lengthy texts, NoSQL can be employed instead of enterprise data warehouses. HBase, Hadoop, Map Reduce and Spark are the most commonly used frameworks. The computing solution provided by the framework is adaptable and fault tolerant. Hadoop Distributed File System (HDFS) stores and connects data across both local and cluster nodes in Hadoop cluster using a centralized information storage system. This greatly increases reliability. A NoSQL programme with the HDFS and Hadoop infrastructure is called HBase. When huge data is unstructured and varied, it is more commonly employed for storage. For analysing enormous amounts of data, Spark is another open-source platform with a single analytics engine. A cluster of nodes can be programmed with Spark's implicit parallelism and fault tolerance. Cloud storage enables workloads to be scaled up and down appropriately when data velocity is high. With the help of the services, it is possible to optimise work by building data pipelines. Additionally, costs can be greatly decreased by building clusters as needed and charging for the services that you need. According to the demands of the user, the cloud also offers a variety of additional open-source clusters, such as Apache Interactive Query, Apache Storm and Kafka. Numerous programming languages, including Go, Scala, Java, Python, Clojure and .NET are supported by the cloud for data processing.

Big Data Processing

Processing has four essential criteria.

1. The capacity to load data fast is a prerequisite.
2. Quick query handling.
3. Effective storage space utilisation.
4. High adaptability to a constantly changing workload.

The cloud service companies assist us by offering Map Reduce Software, which is available in both Amazon EWS and Azure HDInsight. This allows us to easily meet all four needs. The framework's parallel programming model greatly facilitates processing. Instead of boosting a server's or computer's storage capacity or processing power, the Map Reduce architecture merely adds further computers and servers. As a result, the core idea is that we scale out rather than up. The efficiency of a work is increased in Map Reduce by segmenting it into phases that are carried out concurrently. As the name implies, the working is relatively straightforward; the smaller jobs are "mapped" and given the proper key value pair using the first term, "Map." This is very beneficial because cloud architecture is extremely quick, and when combined with the use of parallel processing, productivity is superior to that of a standard local computer. When such a system is deployed on the cloud, it is very useful, and Big Data with high volume and velocity can help firms and exchanges like NSE, BSE, and NASDAQ. When compared to conventional computers, the storage, analytics, and processing are all carried out more effectively and at a cheaper cost.

IV. DDOS ATTACKS: CONCEPTS AND CATEGORIES

Attackers have used a variety of strategies and tactics to carry out DDoS attacks. New attack types have developed along with advancements in detection and mitigation techniques. There are two types of attacks that can be taken into consideration when talking about attack rate: attacks that occur at low and high rates, as indicated below

Low-rate attacks

This type of DDoS attack providing the target a sluggish stream of harmful traffic. The congestion management system of TCP is vulnerable, and this attack takes advantage of it. A "constant attack" is when harmful traffic is supplied continuously at a low pace rather than intermittently, as in a "pulsing attack" [5]. If a DDoS attack's rate is less than 1000 bps or it accounts for 10 to 20% of the background network traffic on the target, it is referred to as a low-rate attack [6]. A novel low-rate DDoS attack called the slow Ternary Content-Addressable Memory (slow-TCAM) attack was proposed by Pascoal et al. in 2020 as an example of a low-rate attack. Compared to existing similar attacks, which operate at a rate of 1000 packets per second, they showed that there is obstructive at four packets per second [7]. This form of attack delivers distinct packets to Software Defined Network (SDN) switches in an effort to deplete their memory and add new fictitious entries to their flow table [8]. Attacks with low rates consume less bandwidth than volumetric attacks, resulting in fewer packets per attack. Due to the difficulty in separating their generated traffic from legal traffic, this makes them difficult to identify.

High-rate attacks

On the other hand, high-rate attacks include the attacker delivering a lot of packets to the target to make its services less

available. Due to the massive amount of malicious traffic, they produce. Including HTTP flood, ICMP flood, UDP flood, and SYN flood these types of attacks are usually called flooding or volumetric attacks [9] [10]. In general, two alternative techniques such as directly or through reflectors, these can be used to carry out high-rate DDoS attacks [11]. A botnet is frequently used by attackers to launch direct attacks. In contrast, reflection attacks target victims by utilising reflectors combined with other devices (such as botnets). The discussion of these attacks will come later in this section.

Challenges of security in cloud computing

Network level, data level, general issues and user authentication level are the four categories that best describe the difficulties with safety in cloud computing systems.

1. User authentication level: Issues with dispersed data, inter-node communication, and distributed nodes are examples of challenges that might be categorised as network level issues.
2. Network level: The issues that fall under the user authentication level category relate to different encryption/decryption methods, authentication approaches including identification of nodes and applications, logging, and administration privileges for nodes.
3. Data level: The issues that fall under the category of data level pertain to availability and include dispersed data and data protection.
4. General types: Traditional security tools and the utilisation of diverse technologies are examples of difficulties that fall into this category.

V. ML-BASED DDOS DETECTION METHODS

ML is a branch of study that is continually being developed through training and data mining. It is recognised as a component of artificial intelligence. Many research that sought to recognise and stop the DDoS onslaught employed classification algorithms. DDoS attacks can be swiftly and readily executed by taking advantage of network weaknesses and making service requirements for software [12, 13]. The passage of time during any type of actual monitoring of DDoS attacks creates a difficulty as DDoS attacks are challenging to identify and avoid and can have substantial consequences [14]. Many research has used Spark ML, a big data framework, in recent years to get improved outcomes, however, they did not perform the same evaluation of the running time as we do [15–17] after utilising Spark. Additionally, ML algorithms and the big data strategy can identify a variety of concealed trends in the context and resolve many complex issues. Big data applications like fake profile identification or the management of supply chains with blockchain technology help to tackle very complicated issues that arise in social media [18, 19].

Al-Qatf et al. [20] developed a network intrusion detection method based on anomalies. The suggested model can handle enormous of data and produces results quickly. The proposed strategy made use of Apache Spark and Hadoop, two big data tools. The methodologies using ML and data mining techniques used in cyber analytics for IDS were summarised by the authors. The outcomes demonstrated that the systemused Apache Hadoop and Spark to quickly manage the massive network packet analysis. Jha et al. [21] obtained valuable information using the method of data analysis. To further big data research, numerous clustering method architecture structures have been developed. In this work, they demonstrated a sustainable cluster with gradual improvement. Scalable Random Sampling with Iterative Optimisation Fuzzy c-Means algorithm (SRSIO-FCM) was used to address the significant data collecting challenges in an Apache Spark cluster. SRSIO-performance FCMs were evaluated for the Apache Spark cluster using a proposed extended execution of the Literal Fuzzy c-Means (LFCM) and Random Sampling with Extension Fuzzy c-Means. Based on the length and storage issues, the time of operation and clustering calculations indicate that SRSIO-FCM can be done in a minimum time period without affecting cluster productivity. Table 1 has illustrated the methodology with outcome and its challenges of ML in big data.

Table 1 Outcome and challenges of various research studies

Author	Methodology	Outcome	Challenge
S.Khan and S.Parkinson, 2018 [22]	Model to analyse security event records of a system is examined and configured using a security expert, extracts critical field expertise indicating their expert decision making, as well as automatically incorporates learned information to formerly undiscovered systems by non-experts	Recovery, data backup and maintaining the foster of the system during an event like a disaster also have minimized the cost saving in the data storage system.	Due to bad internet, an inadequate supply of electricity, and a shortage of DCs, Cloud Service Providers (CSPs) must contend with a number of challenges that make the Data Management System (DMS) challenging.
M.Hina et al., 2021 [23]	SeFACED is a brand-new, effective method for multiclass email classification which relies on LSTM-based Gated Recurrent Neural Networks (GRNN).	Data can be gathered using this technique at different scales as well as resolutions. In this section, it can observe the speed at which data gets examined and processed. With the aid of such technology, food in a zone may be tracked and forest fries more easily detected, which makes them simpler to control.	This technology may produce data that is temporary and not constantly complete. Remote sensing is an expensive technology used to study small areas. Another serious flaw in this method is its classification accuracy.
M.K. Hasan et al., 2023 [24]	The important developments in wireless technology, such as ZigBee, wireless mesh networks and WiMax, as well as the benefits and limitations they bring to intelligent networks.	The ML is used to propose an anomaly detection model in accordance with the Hadoop distributed processing technique like CC and the framework of MapReduce monitoring.	Meeting the real-time as well as large-scale challenges
A. Narayan et al., 2019 [25]	A hypothetical architecture of the SCADA system is put in place with an emphasis on combining ICT data into decision-making of smart grid.	Describe the benefits of the most significant strategies and provide a full analysis of the Big Data clustering problems.	The data used are enormous, complex and dynamic in nature. Collecting, storing, and analysing data is difficult with traditional data handling.
X. Sui et al., 2019 [26]	The load forecasting technique using the	This article analyses current issues, prospects,	Real-time processing is extremely challenging to

	Genetic Algorithm (SVR_GA), the k-means clustering strategy using optimised min-max, and even an adaptive Differential Evolution algorithm (ESA_DE) are some of the suggested fixes for the load imbalance problem in cloud DC.	trends, and challenges related to big data for considering the variety in further detail. This even discusses a workable solution to the massive data variety problem.	accomplish.

VI. RESEARCH GAP

Table 1 illustrates the research gap generated in lacking or not explored by earlier researchers. Typically, the researchers might either strive to create a new framework or approach or improve on current ways by recommending new techniques. The idea for new research and the driving force for existing research are typically gaps. It discussed DDoS attacks in the prior parts and how they are classified as infrastructure-level attacks. Multiple optimizations with a hybrid deep model for identifying DDoS attacks are needed to resolve this issue. Traditional solutions frequently enter the local optimum as the problem becomes more complex and are unable to discover the ideal global solution. The Metaheuristic Intelligent Optimization (MIO) algorithm has gained favor among academics in recent years because, in contrast to the conventional solution which may successfully jump out of the best local option to locate the global optimal solution.

Solution as discussion

The MIO algorithms can be completely split into four groups based on the different idea sources used.

1. Metaheuristic algorithms based on evolution
2. Swarm intelligence-based metaheuristic algorithms
3. Physics-based Metaheuristic Algorithms
4. Human-social-behaviour-based metaheuristic algorithms

This study focuses on swarm intelligence-based metaheuristic algorithms that help to prioritize choosing of dataset characteristics and optimize the features extracted in providing the best fit of the model for decision-making. The subsequent classification in metaheuristic algorithms based on swarm intelligence such as Swarm Optimization (PSO), Crow Search Algorithm (CSA), Earthworm Optimization Algorithm (EWA), Colony Predation Algorithm (CPA), Hunger Games Search (HGS), Particle Dingo Optimization Algorithm (DOA), Whale Optimization Algorithm (WOA), Monarch Butterfly Optimization (MBO), Slime Mould Algorithm (SMA), Virus Colony Search (VCS), Grey Wolf Optimization, Remora Optimization Algorithm (ROA), Harris Hawks Optimization Algorithm (HHOA), Artificial Bee Colony, Moth-Flame Optimization (MFO), Sailed Fish Optimizer (SFO) and White Shark Optimizer Algorithm (WSOA) [27, 28]. Despite having varied origins, these algorithms may be loosely divided into five parts. Creating a solution of random candidate set within the viable region.

1. Determine the candidate solution's fitness value.
2. Update the candidate solutions location.
3. Determine to update the candidate solution location.
4. Determine the number of iterations have exceeded.

The ROA is a contemporary metaheuristic population-based algorithm, was inspired by the foraging parasite action of Remora in the waters. In accordance with a variety of hosts, ROA controls a number of position update rules. Zheng et al. [29] have utilized an Autonomous Foraging Mechanism (AFM), creating IROA, an upgraded variant of ROA. The Brownian motion-based ROA version was modified by Liu et al. [30], and lens opposition-based ROA was also developed.

VII. CONCLUSION

In the modern digital age, big data and cloud computing are extremely important. Big Data's use in cloud computing

appears to have enormous potential in the years to come. Big data often plays a significant role in providing insight in cloud computing applications that use software as a service. Big Data offers a wide range of applications in various industries when used with cloud computing. increased analysis due to enormous data sizes, the development of an effective infrastructure while lowering long-term costs, and increased integrity, availability, and security of the cloud platform are a few of these applications. The novel hybrid meta-heuristic approach comprising several optimization method for solving the problem of business data transmission by avoiding DDoS attack. This review have determined that metaheuristic intelligent optimization algorithms assist in detecting the DDoS attack accurately while compared to existing ML methods.

REFERENCES

[1] Tabassum, Nadia & Khan, Muhammad & Abbas, Sagheer & Alyas, Tahir & Athar, Atifa. (2018). Intelligent reliability management in hyper-convergence cloud infrastructure using fuzzy inference system. ICST Transactions on Scalable Information Systems. 6. 159408. 10.4108/eai.13-7-2018.159408.

[2] S. Boroujerdi and S. Ayat, "A robust ensemble of neuro-fuzzy classifiers for DDoS attack detection," Proc. 2013 3rd Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2013, pp. 484–487, 2014.

[3] L. Kwiat, C. A. Kamhoua, K. A. Kwiat, and J. Tang, "Risks and Benefits: Game-Theoretical Analysis and Algorithm for Virtual Machine Security Management in the Cloud," Assur. Cloud Comput., pp. 49–80, 2018.

[4] X. Jing, Z. Yan, and W. Pedrycz, "Security data collection and data analytics in the internet: A survey," IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 586–618, 2019.

[5] Zhou L, Liao M, Yuan C, Zhang H. Low-rate DDoS attack detection using expectation of packet size. Secur Commun Netw. 2017;2017. doi:10.1155/2017/3691629

[6] Zhijun W, Wenjing L, Liang L, Meng Y. Low-rate DoS attacks, detection, defense, and challenges: a survey. IEEE Access. 2020;8:43920-43943.

[7] Pascoal TA, Fonseca IE, Nigam V. Slow denial-of-service attacks on software defined networks. Comput Netw. 2020;173:107223. doi:10.1016/j.comnet.2020.107223

[8] Isyaku B, Mohd Zahid MS, Bte Kamat M, Abu Bakar K, Ghaleb FA. Software defined networking flow table management of OpenFlow switches performance and security challenges: a survey. Future Internet. 2020;12(9). doi:10.3390/fi12090147

[9] Ranjana P, Kalai Vani YS. Anomaly detection of DDOS attacks using Hadoop. Emerging Research in Computing, Information, Communication and Applications. Springer; 2019:543-552.

[10] Kolahi SS, Treseangrat K, Sarrafpour B. Analysis of UDP DDoS flood cyber attack and defense mechanisms on web server with Linux Ubuntu 13. Paper presented at: 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15). 2015:1-5.

[11] Bhuyan MH, Bhattacharyya D, Kalita JK. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognit Lett. 2015;51:1-7.

[12] Polat, H.; Polat, O.; Cetin, A. Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. Sustainability 2020, 12, 1035.

[13] Ochôa, I.S.; Leithardt, V.R.Q.; Calbusch, L.; Santana, J.F.D.P.; Parreira, W.D.; Seman, L.O.; Zeferino, C.A. Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems. Appl. Sci. 2021, 11, 1255.

[14] Dos Anjos, J.C.S.; Gross, J.L.G.; Matteussi, K.J.; González, G.V.; Leithardt, V.R.Q.; Geyer, C.F.R. An Algorithm to Minimize Energy Consumption and Elapsed Time for IoT Workloads in a Hybrid Architecture. Sensors 2021, 21, 2914.

[15] Awan, M.J.; Rahim, M.S.M.; Nobanee, H.; Yasin, A.; Khalaf, O.I.; Ishfaq, U. A Big Data Approach to Black Friday Sales. Intell. Autom. Soft Comput. 2021, 27, 785–797.

[16] Awan, M.J.; Rahim, M.S.M.; Nobanee, H.; Munawar, A.; Yasin, A.; Azlanmz, A.M.Z. Social Media and Stock Market Prediction: A Big Data Approach. Comput. Mater. Contin. 2021, 67, 2569–2583.

[17] Ahmed, H.M.; Javed Awan, M.; Khan, N.S.; Yasin, A.; Shehzad, H.M.F. Sentiment Analysis of Online Food Reviews using Big Data Analytics. Elem. Educ. Online 2021, 20, 827–836.

[18] Park, K.O. A study on sustainable usage intention of blockchain in the big data era: Logistics and supply chain management companies. Sustainability 2020, 12, 10670.

[19] Awan, M.J.; Khan, M.A.; Ansari, Z.K.; Yasin, A.; Shehzad, H.M.F. Fake Profile Recognition using Big Data Analytics in Social Media Platforms. Int. J. Comput. Appl. Technol. 2021, in press.

[20] Al-Qatf, M.; Lasheng, Y.; Al-Habib, M.; Al-Sabahi, K. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. IEEE Access 2018, 6, 52843–52856.

[21] Jha, P.; Tiwari, A.; Bharill, N.; Ratnaparkhe, M.; Nagendra, N.; Mounika, M. Fuzzy-Based Kernelized Clustering Algorithms for Handling Big Data Using Apache Spark. In Proceedings of 6th International Conference on Harmony Search, Soft Computing and Applications, ICHSA 2020, Advances in Intelligent Systems and Computing; Nigdeli, S.M., Kim, J.H., Bekda,s, G., Yadav, A., Eds.; Springer: Singapore, 2021; Volume 1275.

[22] Khan, S., & Parkinson, S. (2018). Eliciting and utilising knowledge for security event log analysis: An association rule mining and automated planning approach. Expert Systems with Applications, 113, 116–127.

[23] Hina, M., et al. (2021). SeFACED: Semantic-based forensic analysis and classifcation of E-Mail data using deep learning. IEEE Access, 9, 98398–98411.

[24] Hasan, M.K.; Habib, A.K.M.A.; Islam, S.; Balfaqih, M.; Alfawaz, K.M.; Singh, D. Smart Grid Communication Networks for Electric Vehicles Empowering Distributed Energy Generation: Constraints, Challenges, and Recommendations. Energies 2023, 16, 1140.

[25] Narayan, A.; Krüger, C.; Göring, A.; Babazadeh, D.; Harre, M.C.; Wortelen, B.; Luedtke, A.; Lehnhoff, S. Towards future SCADA systems for ICT-reliant energy systems. In ETG-Kongress 2019-Das Gesamtsystem im Fokusder Energiewende; VDE: Esslingen am Neckar, Germany, 2019; pp. 364–370.

[26] Sui, X.; Liu, D.; Li, L.; Wang, H.; Yang, H. Virtual machine scheduling strategy based on machine learning algorithms for load balancing. Eurasip J. Wirel. Commun. Netw. 2019, 2019, 160.

[27] Tu J., Chen H.,Wang M., & Gandomi A. H. (2021). The colony predation algorithm. Journal of Bionic Engineering, 18, 674–710. https://doi.or g/10.1007/s42235-021-0050-y.

[28] Rajamoorthy R., Arunachalam G., Kasinathan P., Devendiran R., Ahmadi P., Pandiyan S., & Sharma P. (2022). A novel intelligent transport system charging scheduling for electric vehicles using Grey

Wolf Optimizer and Sail Fish Optimization algorithms. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, 44, 3555–3575 . https://doi.org/10.1080/15567036.2022.206 7268.

[29] Zheng, R.; Jia, H.; Abualigah, L.; Wang, S.; Wu, D. An improved remora optimization algorithm with autonomous foraging mechanism for global optimization problems. Math. Biosci. Eng. 2022, 19, 3994–4037. [CrossRef]

[30] Liu, Q.; Li, N.; Jia, H.; Qi, Q.; Abualigah, L. Modified remora optimization algorithm for global optimization and multilevel thresholding image segmentation. Mathematics 2022, 10, 1014. [CrossRef]