Intrusion Detection System in IoT to prevent cyber-attacks in organizations

Susmita Paul

Symbiosis Centre for Information Technology, India

Abstract:

Internet of things (IoT) devices are connected objects which are able to collect and exchange data. IoT offers many opportunities to make day-to-day life more fulfilling but is impacted by many security challenges. IoT is fast gaining traction in a wide range of industries, including health care, automotive and logistics. The Internet of Things (IoT) ecosystem has grown in importance as a method of ensuring the security and stability of both information and connection. This paper is based on the analysis of intrusion Detection Systems that is used in organizations and how they can be improved. An IDS is used to detect and remove malicious packets before it enters the network. It is a technique to detect the attack source when cryptography is broken and it also monitors the system activities or network traffic to detect policy violations.

The objective of this research paper is to do a bibliometric analysis and improve the efficiency and security of organizations and human life. An IoT-based environment is used to enable the integration and realization of smart objects in smart industry, Smart health, smart homes and smart buildings. An Intrusion Detection System (IDS) is a technique to detect malicious activities in an IoT network.

Introduction: Smart environments help to improve the efficiency of an organisation and quality of human life. Over the past few decades, technology has become an integral aspect of the workplace and businesses started relying on technology to conduct work effectively and efficiently. Due to the rapid development, the internet is going to connect the world from anywhere and everywhere and thus a new concept arrives i.e., IOT (Internet of Things) but with this technology also comes the protection of IOT otherwise it can have adverse effects. [1]

With advanced technology in businesses, comes the responsibility to take IoT security more seriously. When an organisation is connected via Internet or Intranet, the most crucial aspect for the organisation to make success is to maintain a stable and secure network security system and hence protection of IoT is important and necessary. So, to detect and monitor any malicious packets or malpractices that are happening in and outside the network, IDS is employed.[2]

An Intrusion Detection System monitors the network traffic and warns the user if any malicious activity is going on the network by giving alerts. An IDS will detect the malicious activity in IoT ensuring the organizations that their IoT devices stay connected without any interruption or cyber threats making it protected from the DOS attacks and the network spoofing that is done by the hackers.

Intrusion Detection in IoT:

Classification of intrusion detection system is explained based on the existing research. Figure 1 shows how IDS systems can be classified based on various classifications that is a) type of intruders b) Type of intrusions c) Detection techniques and d) Type of IDS. Intruders are referred to the one who try to gain unauthorised access to exploit a computer system. The difference between the external and internal intruders is that external intruders are the one who doesn't have access in any form and are completely unauthorized users but internal users are the one who have access only to a few sections but not all of them for example employees of an organisation can be an internal intruder.

Intrusion refers to the act of intruding and it affects the CIA (Confidentiality, Integrity and availability) of the information and the resource. There can be many types of intrusions including active attacks, passive attacks, fraud, DOS/DDOS, malicious attacks and others [3,4,5]. If the information is only eavesdropped but is not modified then that type of attack is known as passive attacks and if the information has gained unauthorised access as well as the information has been destroyed or changed then it is known as active attack. There are various types of passive attack like eavesdropping, location disclosure, traffic analysis and the various types of active attacks are malicious packet dropping, and routing attacks like men-in-the-middle attack, sleep deprivation, spoofing. The various types of frauds can be a situation where an account is compromised, phishing, unauthorised transaction, sniffer attack. If a website or resource is made unavailable by flooding a server with traffic then it is known as DOS attack. If a DOS attack is made using multiple computers and machines then it is known as DDOS attack. If an employer's system executes abnormal or unauthorized actions by a Malicious software then it is known as Malicious attacks or Malware/Botnet attacks. [7]

Matching algorithms are used in signature-based intrusion detection systems (SIDS) to locate a previous incursion. An alarm signal is triggered when an intrusion signature is matched against the signature of a previous intrusion that

exists in the signature database. Though SIDS is the effective approach to detect known attacks [6]. For known attacks, it has a high detection accuracy and a low computing cost, with a very low false alarm rate. However, it is unable to identify unknown attacks, evasive attacks and variants of existing attacks. Only the attacks for which they have been trained can be detected. Anomaly-based intrusion detection system (AIDS) methods might be a viable answer to this problem. A normal model of a computer system's behaviour is produced in AIDS utilising machine learning, statistical based, or knowledge based approaches [8,9,10,11,12]. An anomaly is defined as a significant difference between observed behaviour and the model, which might be regarded as an intrusion. AIDS technique is all about how a malicious behaviour differs from normal user behaviour. It can detect unforeseen and new vulnerabilities and also novel attacks or unknown attacks.

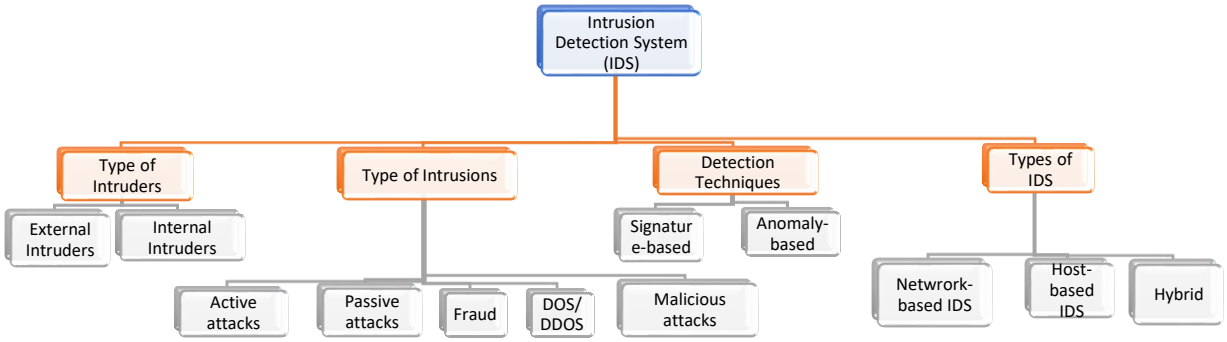

Figure 1: Classification of IDS for IoT

Different types of IDS systems are Host-based, Network based and Hybrid. Host-based IDS (HIDS) monitors the network traffic at the transport layer. It monitors the operating system's audit information for any signs of intrusion on a specific machine, such as mobile devices or servers. The attacks that are skipped by HIDS, can be detected by NIDS i.e., Network based IDS [11,12,13,14,15]. It monitors any form of intrusion in network traffic and application protocol activity between any two machines. The combination of Host-based IDS and Network based IDS is known as Hybrid and it provides in-depth defence.

Literature review:

There are a lot of stakes for organizations of all sizes including big, medium and small for all the data and information it has. Even a small gap in the layered security approach can keep the system vulnerable to malicious attacks. With a mounting number of enterprises that are becoming reliant on Internet of Things, the need for ample security measures is becoming more and more significant. As discussed earlier, there are mainly two types of Intrusion detection system like the anomaly based or the signature based and or as proposed “AS-IDS” model which combines both the approach which is Anomaly-Signature Intrusion Detection System to detect the attacks that takes place in IoT networks.

A review of Intrusion detection systems for IoT based smart environment has been done for improving the efficiency of work. The latest designs of the IoT model’s Intrusion detection systems [2] has been discussed which also gives a brief overview of the IoT architecture, its vulnerabilities and threats and the respective layers of the IoT.

Literature review for this particular topic of IDS on IOT is given to put emphasis on the challenges and up-to-date information. And an analysis has been made to determine the gaps or flaws we found for this particular topic. So, now improvement needs to be done based on the analysis which will also give a future perspective of the topic on how to accept and take the challenging tasks and securities that is based on IOT. After completing full security assessment, organization will be more effective and informed when it comes to vulnerabilities of the IOT systems, including how to mitigate them using IDSs.

Given the rise in cyber-attacks against organizations, we expect cybersecurity to continue to play a key role in the sector. Despite the increased study and attention paid to cybersecurity, there are still gaps in the analysis.

Methodology:

Bibliometric as the name itself talks about statistical analysis of articles, books or/and other publications. Bibliometric analysis is a common research technique for determining the state of the art in a specific subject [13,14]. The approach may be used to describe trends of publishing within a specific time or particular country or specific language or body of literature using statistics and quantitative analysis.

While there are a good number of databases like Scopus, Google Scholar, Web of Science and others to index articles, Scopus was chosen over others since it is said to have the largest citation database which is 'Elsevier's abstract and citation database' and was launched in 2004. First of all, an extensive search was made by including few keywords using Scopus. Then it was excluded using other parameters like years, languages, etc., The keyword list: Scopus (Journals, articles, books, all years, all languages):

Criteria	Explanation
Within 5 Years (YR)	Limited to papers which are within 5 years
English (E)	Language papers which are English language were included.
Open Access (OA)	Open Access Papers only are included
Non-related Subject Area (NSR)	Keywords related to only related Subject Areas

Table 1: Naming Convention of exclusion and inclusion criteria

Articles which were published prior to 5 years were excluded, articles ranging from the year 2016 to 2020 were included which offered only 'Open Access'. Articles that don't follow English language were excluded and only related Subject areas were included. The final keyword list: Scopus (Journals, articles, books, 2016-2021, Open Access, English language, Subject Area -Computer Science, Engineering, etc)

(TITLE-ABS-KEY (intrusion AND detection AND system) AND TITLE-ABS-KEY (IOT) OR TITLE-ABS-KEY (cyber AND attack) OR TITLE-ABS-KEY (cyber-attack) OR TITLE-ABS-KEY (organization) OR TITLE-ABS-KEY (organizations)) AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016)) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (SUBJAREA , "MATH") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "SOCI") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "CENG") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "PSYC") OR EXCLUDE (SUBJAREA , "ARTS"))

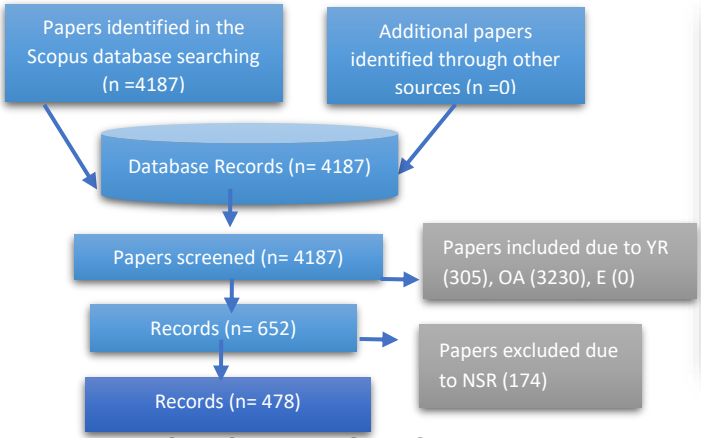

Figure 2: Search Techniques and Results

Search Results: The preliminary search on Scopus having the basic keywords yielded 4,187 document results. Then after making it open access and limiting to only five years publications it gave 652 results. Finally, limiting to English Language and excluding irrelevant subject areas, it yielded 478 results. Figure 2 explains how the search was executed.

Findings:

This section outlines the finding of detection systems upon

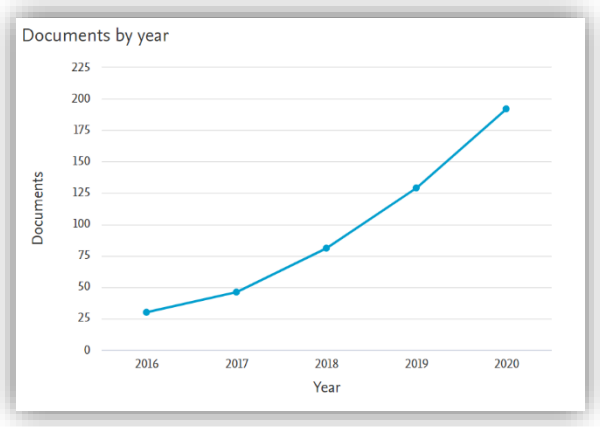

Figure 3: Number of publications year wise

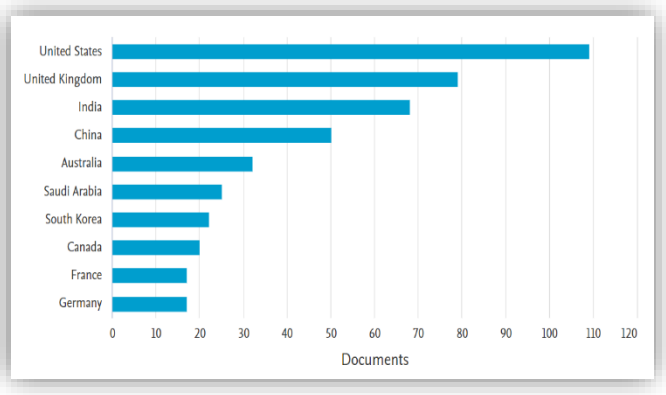

Figure 4: Number of publications Country wise

This section outlines the finding of detection systems upon which the research is done. This section is broken down into many sections which includes number of publications per year, number of publications per country, comparison of document type and productivity of different sources. These results are significant because they combine bibliometric data with publishing rates. Here, the results are discussed and the findings are analysed that was received from the search result section. This finding is important as it helps us to analyse the publishing rates in terms of years, countries and other parameters in an in-depth manner.

Figure 3 shows the number of publications year wise from 2016 to 2020. In 2016, there were only 30 articles and it increased to 192 in the year 2020. The curve rise is increasing almost linear which indicates the publications are increasing except the fact that the increased percentage from 2019 to 2020 is 48.83 percent while previous years have more than 50 percent. The reason may be the affect in publications due to Covid cases.

Figure 4 is comparing the document counts per country or territory and the top ten countries in terms of publications has been shown in the graph. The United States tops the chart having 109 publications followed by the United Kingdom with 79 publications which implies that the United States does most of the research in the Intrusion Detection System of IoT. India is ranked third having 68 active publications in this field. Germany has the least publications in the top ten countries but still has a good number i.e., 17.

This section talks about the categorization of the publications. Table 2 illustrates that major portions that got published are in the form of articles acquiring 61.3 percent of all and followed by Conference Papers which is 33.7% and Review Materials which is 3.8%. Articles which are published in the form of Data Paper, Erratum and Short Survey has only 0.2% which shows research papers were published in the least manner for these three types.

Document Type	No. of Document	No. of Document (%)
Article	293	61.3
Book Chapter	3	0.6
Conference Paper	161	33.7
Data Paper	1	0.2
Erratum	1	0.2
Review	18	3.8
Short Survey	1	0.2

Table 2: Document Type research comparison

Source	Year					
	2016	2017	2018	2019	2020	Total
IEEE Access	1	6	7	20	47	81
Electronics Switzerland	0	1	0	1	18	20
Procedia Computer Science	0	1	4	2	9	16
ACM International Conference Proceeding Series	2	2	5	2	4	15
International Journal Of Innovative Technology And Exploring Engineering	0	0	0	10	0	10
International Journal Of Advanced Computer Science And Applications	0	0	1	3	5	9
Security And Communication Networks	0	1	3	2	3	9
International Journal Of Advanced Trends In Computer Science And Engineering	0	0	0	0	8	8
IEEE Communications Surveys And Tutorials	0	0	2	3	2	7
Future Generation Computer Systems	0	0	1	2	3	6
Future Internet	1	0	1	0	4	6
IEEE Transactions On Smart Grid	0	1	2	3		6
International Journal Of Electrical And Computer Engineering	0	0	1	0	4	5
Proceedings Of The ACM Conference On Computer And Communications Security	1	0	2	2	0	5
Advances In Intelligent Systems And Computing	3	0	0	0	1	4

Table 3: Comparison of sources per year

Table 3 gives a comparative view about productivity among various sources. Productivity refers to the number of publications it had every year or the frequency at which it publishes. It compares the publications of various sources in a year wise manner. This comparison is important as it not only helps the researchers from each source to compare and compete but it also helps them to stay focussed and diligent while doing the research of the detection and prevention systems of the cyber world. Table 3 shows IEEE source gave the major contribution in the number of publications with 81 number of published articles from 2016 to 2020 and is followed by the source, Electronics Switzerland. Top 15 sources in terms of publications have been selected against five consecutive years i.e., 2016 to 2020 and it has been noticed that maximum publications are from IEEE Access having 81 publications followed by Electronics Switzerland (20 publications) and Procedia Computer Science (16 publications).

Analysis:

Analysis technique has been discussed here, where we used VOSviewer tool to analyse the different relationships between the demo graphs, authors, citations and others. Though there are other tools for the network, VOSviewer has been preferred since it gives a standard visualisation for the bibliometric network. The types of visualisation analysis done are as follows:

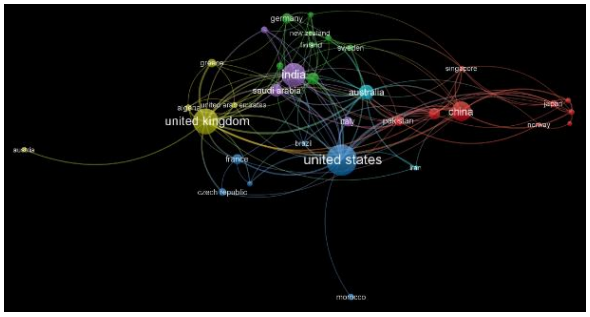

Figure 5: Country – co-authorship clusters

- Types of analysis: Co-authorship
- Unit of analysis: Countries
- Visualisation: Overlay Visualisation

Description: A co-author is any person who has made a significant contribution to a journal article. Here, different colours are used to depict co-authorship that the top countries (in terms of publications) share with other neighbours. Six clusters have been shown where blue colour is the cluster for US with others, Yellow for UK, Purple for India, Red for China, light blue for Australia. In the visualisation it is showing Co-authorship demographic wise and United States holds maximum of it. In the figure 5, the size of the clusters is varied according to the number of publications that a co-author has with respect to other countries, so, we can say for e.g., United States has maximum of co-authors that shares with its neighbouring countries like Australia, Morocco, Czech Republic, Brazil, France and Iran. Similarly, the next largest size is United Kingdom and shares its co-authors with neighbours like Greece, Arab, Austria and others.

- Types of analysis: Bibliographic-coupling
- Unit of analysis: Sources
- Visualisation: Density visualisation

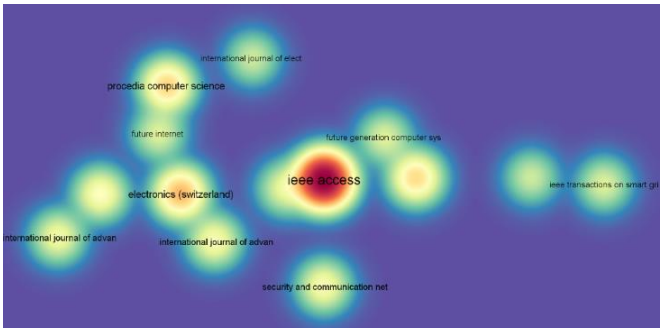

Figure 6: Source clusters

Description: In Bibliographic-coupling, two documents are bibliographically coupled if they both cite one or more documents in common. Heat map has been used here to explain the coupling bond, a heatmap is a diagrammatic representation of data that uses color-coding strategy to represent various values. Here, in the heat map, the deepest and largest maroon colour circle is for the IEEE access. So, it means maximum is from the Source, IEEE Access followed by Electronics Switzerland which means the articles in IEEE Access has more common sources with others.

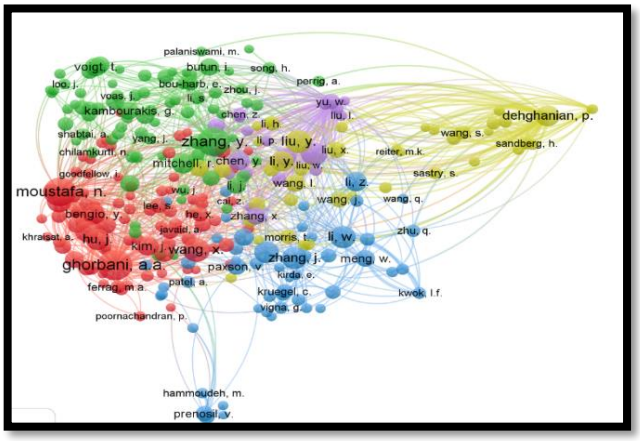

Figure 7: Co-cited author clusters

- Types of analysis: Co-citation
- Unit of analysis: Cited authors
- Visualisation: Network Visualisation

Description: Co-citation is defined as the frequency with which two documents are cited together by other documents. Here, it is inferred that each cited-author cites two or many documents in common. The initial and main source was from dehghanian, p. and is followed by other authors where any two documents are cited by other documents.

Limitations and suggestions:

This paper was limited to the publications based on Scopus database and for a stipulated period of 5 years i.e., 2016 to 2020. We have also limited to English language only with selected Keywords and didn't prefer other languages.

Future Analysis can be made on a more in-depth basis, probably the review can be made particularly on the latest Intrusion detection systems that is used in the industry and the gaps it is overcoming till date. Future reviews can have more analysis on the clusters of sources and suggest on the recovery plans like business continuity and disaster recovery planning, as well as for the prevention of Industry cyber-attacks. Such a narrow emphasis can aid in the synthesis of research findings and the dissemination of quality standards.

Reference:

[1] Otoum, Y. and Nayak, A., 2021. AS-IDS: Anomaly and Signature Based IDS for the Internet of Things. Journal of Network and Systems Management, 29(3).

[2] Elrawy, M., Awad, A. and Hamed, H., 2018. Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1).

[3] Khraisat, A. and Alazab, A., 2021. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1).

[4] A. Abbasi, J. Wetzels, W. Bokslag, E. Zambon, S. Etalle, 2021. "On emulation-based network intrusion detection systems," in Research in attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17–19, 2014. Proceedings, A. Stavrou, H. Bos, G. Portokalidis, Cham: Springer International Publishing, 2014, pp. 384–404 lenges.

[5] Okan CAN, Ozgur Koray SAHINGOZ, 2015. A Survey of Intrusion Detection Systems in Wireless Sensor Network, 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO).

[6] Zhang, Y., Li, P. and Wang, X., 2019. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access, 7, pp.31711-31722.

[7] Aafer, Y., Du, W. and Yin, H., 2021. DroidAPIMiner: Mining API-Level Features for Robust Malware Detection in Android. [online] Eudl.eu. Available at: <https://eudl.eu/doi/10.1007/978-3-319-04283-1_6> [Accessed 30 December 2021].

[8] Lv, L., Wang, W., Zhang, Z. and Liu, X., 2020. A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. Knowledge-Based Systems, 195, p.105648.

[9] M. Bhargavi1, M.Nandha Kumar2, N. Venkata Meenakshi3, and N.Lasya, 2019. Intrusion Detection Techniques Used For Internet of Things, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 24.

[10] Docplayer.net. 2021. Development of Industrial Intrusion Detection and Monitoring Using Internet of Things P. Gokul Sai Sreeram 1, Chandra Mohan Reddy Sivappagari 2 - PDF Free Download. [online] Available at: <https://docplayer.net/3665575-Development-of-industrial-intrusion-detection-and-monitoring-using-internet-of-things-p-gokul-sai-sreeram-1-chandra-mohan-reddy-sivappagari-2.html> [Accessed 30 December 2021].

[11] Aburomman, A. and Reaz, M., 2017. A survey of intrusion detection systems based on ensemble and hybrid classifiers. Computers & Security, 65, pp.135-152.

[12] Zhang, Y., Li, P. and Wang, X., 2019. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access, 7, pp.31711-31722.

[13] Benkhelifa, E., Welsh, T. and Hamouda, W., 2018. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Communications Surveys & Tutorials, 20(4), pp.3496-3509.

[14] Iman, A. and Ahmad, T., 2020. Data Reduction for Optimizing Feature Selection in Modeling Intrusion Detection System. International Journal of Intelligent Engineering and Systems, 13(6), pp.199-207.

[15] Mazini, M., Shirazi, B. and Mahdavi, I., 2019. Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University - Computer and Information Sciences, 31(4), pp.541-5