e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:07/July-2022 Impact Factor- 6.752 www.irjmets.com

ARTIFICIAL INTELLIGENCE TRENDS IN IOT INTRUSION DETECTION SYSTEM: A SYSTEMATIC MAPPING REVIEW

Bharatwaja Namatherdhala[*1], Noman Mazher[*2], Gopal Krishna Sriram[*3]

[*1]Adobe Inc, USA.

[*2]University Of Gujarat, India.

[*3]EdgeSoft Crop, USA.

ABSTRACT

The Internet of Things (IoT) is a prodigious technology of the current century that invades the technological advancement of the modern era. IoT aims to connect all physical devices of the world and establish an internet of all physical devices connected and communicating. The considerable popularity of IoT attracts cyber attackers' attention to this physical device's network. Enormous research efforts are on the way to overcoming IoT's security challenges. Intrusion Detection Systems (IDS) is one of the leading contributions to the IoT security paradigm. This research will attempt to bring all of the existing research into one canvas to relinquish all the contributions and find out research gaps for new researchers.

Keywords: Internet Of Things, Intrusion Detection System, Systematic Mapping Study.

I. INTRODUCTION

Information Communication Technology (ICT) is reshaping in the current century by introducing gigantic new technologies. Cloud computing, wireless sensor networks, and broadband internet access increase the potential of smart embedded devices in human life. Smart devices with internet connections and computing capabilities bring the concept of IoT [1]. According to Cisco, the IoT industry's revenue will reach $ 14.4 Trillion by 2022[2]. Comprehensive spreading implementation of IoT technology also suffers from potential issues. Security and privacy are the primary concern of all[1, 3, 4]. The increased popularity of IoT aroused the interest of cyber attackers in the IoT globe. Although immense research has been done in IoT security, there is a need to care about the security standard of IoT. IoT security researchers are putting their effort in different directions, such as securing data confidentiality by authentication methods, trust between the user and things, and enhancing security policies. Still, another line of defense must stop coming into the IoT network[3]. This line of defense can be possible by employing an Intrusion Detection System (IDS). Since IoT technology has different communication standards and technologies, the classical IDS does not fulfill the need to secure an IoT system. Immense. IDS was designed for securing IoT by researchers in recent years. With new communication standards and technologies like 5G communication standards, new attacks have also come into the ground. Furthermore, each IoT IDS was designed for a specific security issue. There is a need for a comprehensive survey to envisage further vital points such as the strength and weaknesses of available IDS, the contribution of modern IDS tools to tackle enhancing security needs, improving security strategies, and other such contributions. This research aims to conduct a quality survey of IoT IDS to achieve the abovementioned goals. The survey strategy is a Systematic Mapping Study (SMS), one of the most comprehensive survey techniques[1, 5]. No SMS has been conducted related to IoT IDS to our best knowledge. The rest of this research paper is compiled in the following sections. Section II will discuss related work that covers preliminary knowledge. Sections IV will discuss in detail SMS as a research methodology. In section V, experimental results and afterward discussion will be done.

II. RELATED WORK

This section will include preliminary knowledge about IoT, IDS, and other related terminology that readers should know before entering more detailed knowledge. The term Internet of Things (IoT) was coined by Kavin Ashton, a consumer sensor expert and innovator, in 1999, as "the network of connected objects of the physical world"[]. The rudimentary concept of IoT is still evolving with the collaboration of new technologies. With the growth of IoT networks bringing new challenges, security is one of the most panic challenges in the IoT world. The immense research contribution is continuing in the IoT security paradigm. IDS are part and parcel of IoT security global. This research will reveal existing IoT IDS research work and provide a comprehensive

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:07/July-2022 Impact Factor- 6.752 www.irjmets.com

statistical analysis to find answers to the research question. This section will discuss existing literature reviews, particularly survey work of IoT IDS. Security has been the most interesting taking issue in all technology fields.[6-10]. Like other areas, IoT security has been a great deal of interest for researchers[4]. In [11], discuss 18 research papers related to IoT IDS and all of them regarding attack detection strategies. The author of this paper confined only to a particular domain of attack detection strategies and did not explore other aspects of IoT IDS.

Furthermore, this survey only covers the paper between 2009 to 2016, and hence a massive gap between literature reviews of IoT IDS. The further existing literature review will be discussed in detail in this section. After reviewing all approaches to the IoT IDS survey, it can be concluded that the survey approach in this research work is highly novel and can be a precious contribution to knowledge.

III. RESEARCH METHODOLOGY

In this section, the research methodology will be discussed in detail. A systematic mapping study (SMS) will survey IoT IDS in this research.

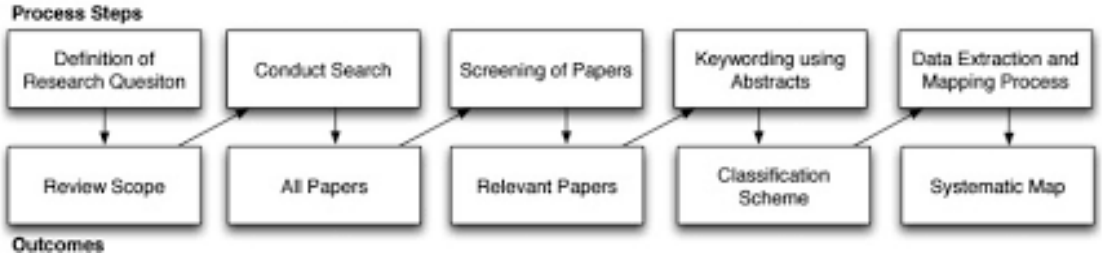

Fig 1: Systematic Mapping Study stages[5]

The figures, as mentioned earlier, show the stage of SMS. For the first stage, research questions are determined that will be presented in this section. The next stage of SMS is conducting a survey; this survey will be based on a research paper search from authenticated resources such as IEEE Xplorer, web of science, Scopus, and Nature. Papers will be searched according to the defined search string. Afterward, final data will be collected in an MS Excel spreadsheet. This data will be further processed according to the defined research question. The output charts and graphs will be available for discussion on the result.

Research Questions:

The research question will be designed in this section. Following are some supposed research questions that are going to be presented:

RQ1: Trend of IoT IDS development years wise

RQ2: The proportion of research types in IoT IDS

RQ3. Worth of research papers in IoT IDS

RQ2: Which Artificial Intelligence approach is frequently used for IoT IDS

IV. RESULT OF EXPERIMENT

This section will discuss our experiment's results to discover answers to our proposed research questions. The result will be in graphs and charts prepared in MS Excel; the following figures are the survey's expected output.

RQ1: Research question one is related to rising trends of IoT IDS development. From our experiment, we find that trend of using AI in IoT IDS is gradually increasing year-wise. Fig 2 shows the chart of years was research work that involved AI in IoT IDS. As shown in figure 2, in 2021, a majority of research happened using computer vision in IoT IDS tools. Object tracking is also rising in the use of IoT IDS research area. Afterward, machine learning comes in AI techniques in IoT IDS

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:07/July-2022 Impact Factor- 6.752 www.irjmets.com

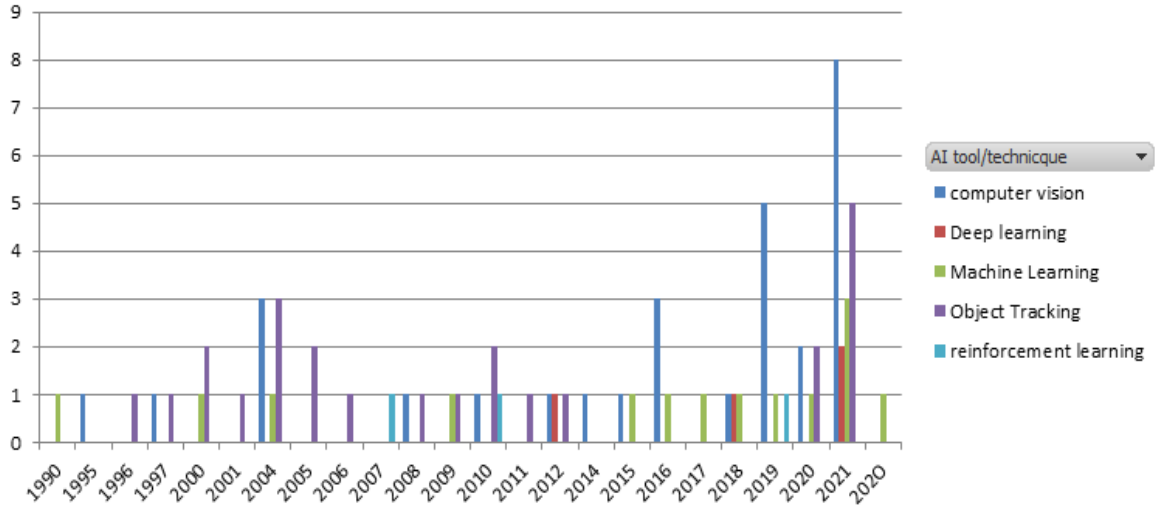

Fig 2: Year wise growth rate of using AI techniques in IoT IDS

RQ 2: Research question 2 deals with typical AI techniques used in the IoT IDS research areas. From figure 3, we can see that most solutions have been provided in IoT IDS research, showing that new solutions and framework are being proposed drastically in the research mentioned above.

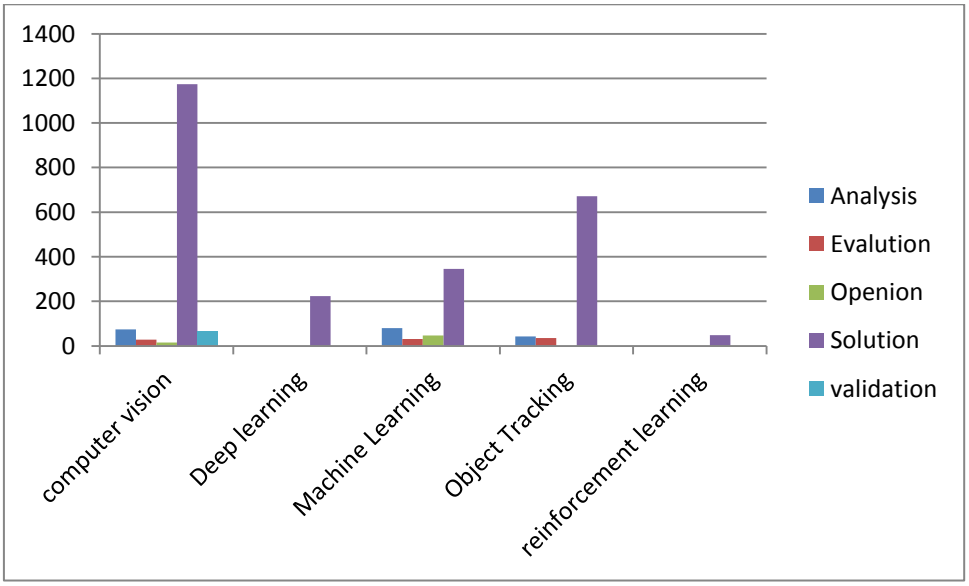

Fig 3: AI technique in IoT IDS

RQ 3: Our research question deals with the worth of IoT IDS research. We assume the journal paper is more worthy from all kinds of research venues. Afterward, conferences have a good worth of research publications. We assume workshop and symposium papers are the most negligible contribution to the knowledge areas. Figure 4 shows that in 2021, most papers will be published in journals, and most of the others will be presented in conference proceedings. A very few propositions of papers are presented in workshops. The facts mentioned above prove that IoT IDS research is increasing its value.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:07/July-2022 Impact Factor- 6.752 www.irjmets.com

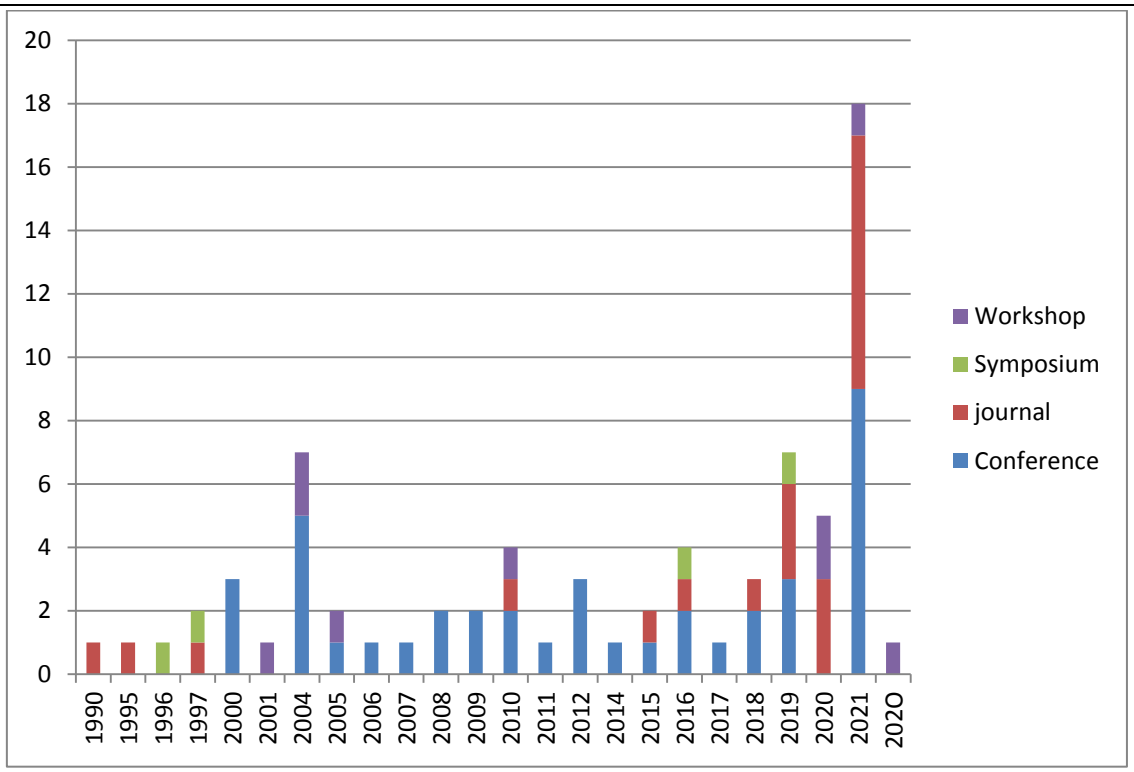

Fig 4: Year-wise research work in IoT IDS according to venue

RQ 4: Our final research question is aimed to explore gaps in our targeted research domain. To explore the answer to research question 4, we designed a bubble chart showing each area's frequency to be used in IoT IDS research. This bubble chart shows that 19.2 % of researchers used computer vision as an AI tool in IoT IDS. Afterward, ANN and reinforcement learning played a significant part in IoT IDS.

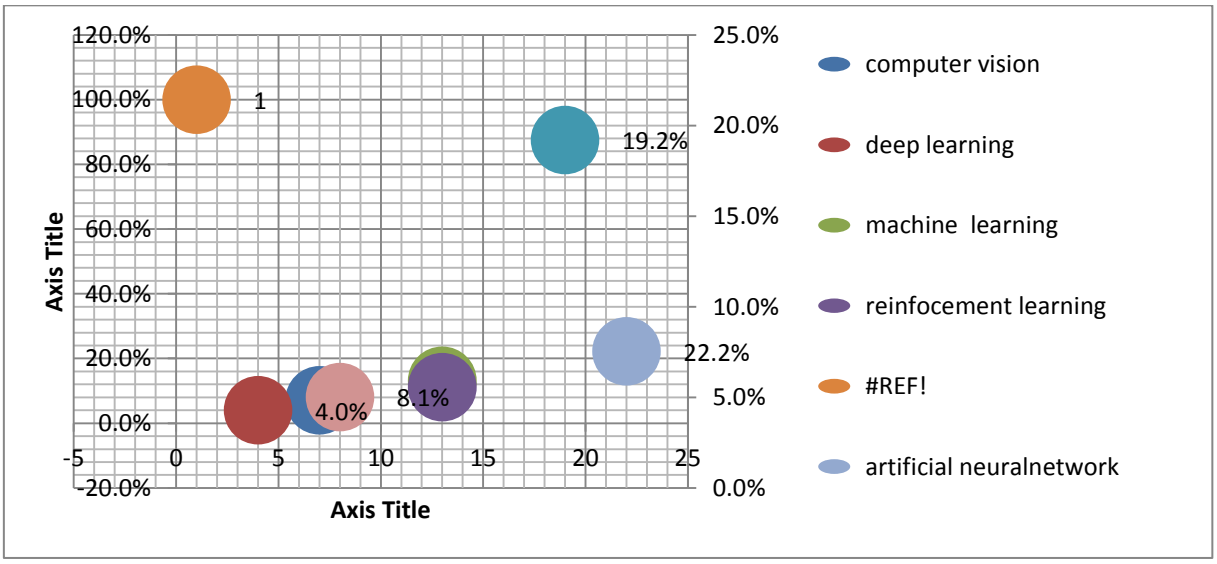

Fig 5: Frequency of using AI technique in IoT IDS

V. CONCLUSION

With the increasing trend of IoT, security is needed to improve in notable proportion. Different security measures for IoT devices and software have been proposed. Intrusion detection systems are typically a tool to secure any network from intruders. With the involvement of AI in all areas of life, IoT intrusion detection systems are also leveraged. Because of various standards and aspects, there is a need to analyze the use of AI techniques in IoT IDS comprehensively. We performed a systematic mapping study on the area of use of AI in IoT IDS. From our systematic literature review, we statistically explore how much AI is involved in IoT IDS. We

believe that our research can be a milestone for new researchers to find the gap in this area and choose their research direction.

VI. REFERENCES

[1] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," Internet of Things, vol. 14, p. 100365, 2021.

[2] M. Asadullah and A. R. Celik, "An Effective Approach to Build Smart Building Based on Internet of Things (IoT)," 2016.

[3] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," International Journal of Advanced Computer Research, vol. 9, no. 45, pp. 325-350, 2019.

[4] S. A. Shah and N. Mazher, "A review on security on internet of things," in November 2018 Conference: 1st International Multi-Disciplinary Research Conference (IMDRC 2017).

[5] N. Mazher and I. Ashraf, "A Systematic Mapping Study on Cloud Computing Security," International Journal of Computer Applications, vol. 89, no. 16, pp. 6-9, 2014.

[6] M. Ahmadi and B. S. Ghahfarokhi, "Preserving privacy in location based mobile coupon systems using anonymous authentication scheme," in 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), 2016: IEEE, pp. 60-65.

[7] M. Ahmadi, "Hidden fear: Evaluating the effectiveness of messages on social media," Arizona State University, 2020.

[8] M. Ahmadi, K. Leach, R. Dougherty, S. Forrest, and W. Weimer, "Mimosa: Reducing malware analysis overhead with coverings," arXiv preprint arXiv:2101.07328, 2021.

[9] M. Ahmadi, P. Kiaei, and N. Emamdoost, "SN4KE: Practical Mutation Testing at Binary Level," arXiv preprint arXiv:2102.05709, 2021.

[10] P. Kiaei, C.-B. Breunesse, M. Ahmadi, P. Schaumont, and J. Van Woudenberg, "Rewrite to reinforce: Rewriting the binary to apply countermeasures against fault injection," in 2021 58th ACM/IEEE Design Automation Conference (DAC), 2021: IEEE, pp. 319-324.

[11] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.