Journal of Big Data

SURVEY Open Access

Engineering the advances of the artificial neural networks (ANNs) for the security requirements of Internet of Things: a systematic review

Yasir Ali[1], Habib Ullah Khan[2*] and Muhammad Khalid[3]

*Correspondence:
habib.khan@qu.edu.qa

[1] Shahzeb Shaheed Government Degree College Razzar, Swabi, Higher Education Department, Peshawar, Khyber Pakhtunkhwa, Pakistan
[2] Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar
[3] School of Computer Science, University of Hull, Hull, UK HU5 2BQ

Abstract

Internet of Things (IoT) driven systems have been sharply growing in the recent times but this evolution is hampered by cybersecurity threats like spoofing, denial of service (DoS), distributed denial of service (DDoS) attacks, intrusions, malwares, authentication problems or other fatal attacks. The impacts of these security threats can be diminished by providing protection towards the different IoT security features. Different technological solutions have been presented to cope with the vulnerabilities and providing overall security towards IoT systems operating in numerous environments. In order to attain the full-pledged security of any IoT-driven system the significant contribution presented by artificial neural networks (ANNs) is worthy to be highlighted. Therefore, a systematic approach is presented to unfold the efforts and approaches of ANNs towards the security challenges of IoT. This systematic literature review (SLR) is composed of three (3) research questions (RQs) such that in RQ1, the major focus is to identify security requirements or criteria that defines a full-pledge IoT system. This question also focusses on pinpointing the different types of ANNs approaches that are contributing towards IoT security. In RQ2, we highlighted and discussed the contributions of ANNs approaches for individual security requirement/feature in comprehensive and detailed fashion. In this question, we also determined the various models, frameworks, techniques and algorithms suggested by ANNs for the security advancements of IoT. In RQ3, different security mechanisms presented by ANNs especially towards intrusion detection system (IDS) in IoT along with their performances are comparatively discussed. In this research, 143 research papers have been used for analysis which are providing security solutions towards IoT security issues. A comprehensive and in-depth analysis of selected studies have been made to understand the current research gaps and future research works in this domain.

Keywords: Internet of Things, Artificial neural network, Network, Security requirements, Internet security

Introduction

The security of Internet of Things (IoT) has become burning issue since last couple of years as the IoT devices are not equipped with sufficient security due to low memory, storage, bandwidth and computational power which makes these devices susceptible to many attacks like denial of service (DoS), distributed denial of service (DDoS), botnet, spoofing, snipping and some other serious type of attacks. Therefore, it is indispensable to provide complete vigorous security solutions for IoT-equipped systems. Such security solutions can only be provided by covering all the aspects related to IoT security. To provide a complete package of security in IoT, it is better to understand the building blocks of IoT security. These building blocks not only cover all the aspects related to security issues in IoT but are also known as security requirements or security criteria or security characteristics of IoT. IoT security in terms of security criteria is described by different authors in the literature. For example, Hameed et al. [1] defined the security of IoT by requirements like privacy, confidentiality, attack detection and secure routing. Similarly, the security criteria for IoT defined by some authors in terms of confidentially, integrity and availability which is also known as CIA model [2]. Different approaches and research works have been presented to safeguard IoT based systems by fulfilling the IoT security requirements. This research work is also intended to highlight the significant role of ANNs technologies towards fulfilling the security requirements. These security requirements are discussed in detailed fashion in later part of this research in light of ANNs.

ANNs are the networking models, which mimic the human brain in terms of processing information [3]. They are applied to find patterns in data by building the complex relationship among the data for the entry in inputs to corresponding outputs [4]. Before using ANNs in any environment, the most vital thing is to train it by inputting a huge amount of data and rules in order to obtain the desirable output [5]. ANNs has wide spectrum of applications in various domains like engineering fields, Mathematics, Pharmacy, transportation, theft and fraud detection, Computer vision, pattern recognition and network security [6]. However, the main focus of this study is to highlight the efforts and approaches of ANNs for the IoT security domain. In this regard, different machine learning approaches have been taken in context of IoT security but ANNs have addressed the security of IoT in marvellous fashion and covered all the aspects of IoT network. ANNs have presented many approaches to address the security issues in IoT.

ANN furnishes security solutions towards IoT by using different approaches, its types and sub-types such as convolutional neural network (CNN), recurrent neural network (RNN), feed forward neural network (FF-NN), deep neural network (DNN), long short-term memory (LSTM), radial basis function (RBF), multi-layer perception (MLP), autoencoders, back propagation neural network (BP NN), probabilistic neural network (PNN) and so on. Our focus in this work is to discuss the security requirements of IoT in light of approaches and modelling techniques provided by ANN. In first attempt the security criteria for IoT has been identified from various sources of literature then ANNs contributions towards the underlying security requirements like authentication, network monitoring [7], attack detection privacy [8], secure routing [9], encryption [10], access control [11, 12], privacy [13, 14], theft resistance [14, 15] and authorization [16] have been completely discussed. ANNs not only contribute towards the security requirements

but they also leverage the security of IoT to deliver a robust IDS for detecting attacks, threats and anomalies. The role of ANNs in detection of DoS/DDoS attacks in IoT is significantly conspicuous. In this regards, numerous ANNs approaches and techniques for detection and classification of DoS/DDoS attacks in IoT network have been presented [17–21]. ANN-based approaches and methods provide highest precision and accuracy for classification and detection of unusual traffic related to IoT. Besides, handling the DoS/DDoS threats, ANNs also provide a wide range of security solutions for other IoT security aspects. They can be applied for different purposes in IoT systems such as detection of malicious nodes [22], facial recognition services [23], anomalies detections [24, 25], routing attacks [26] and face recognition system for blind people [27].

a. Motivation

Following are the major motivations for conducing this SLR.

- The security of IoT has become the most intriguing and trending research topic over the last few years. Different modern technologies have been adopted to deal with the security scenarios related to IoT-based systems.
- The security of IoT is main concern for all the stakeholders such as researchers, network administrators, engineers and IoT platform companies. Exorbitant research works have been conducted in this domain but still there are a lot of potential opportunities available for the researcher to get deep dive into the security aspects of IoT.
- The major focus of this study is to highlight the security requirements of IoT based on the application of ANNs, this research investigates all the important features of IoT that were not addressed by researchers, previously.

b. Contribution

The major contributions of this systematic literature review are given below as:

- This is the first attempt systematic literature review (SLR) to spotlight the efforts and approaches presented by ANN for the security of IoT. To the best of our knowledge, there does not exist any related work that discusses the security requirements of IoT in light of ANNs approaches. Although, there exists a lot of works done by machine learning to address the security issues related to IoT.
- This SLR collects the latest research articles in the field of to IoT security that are leveraging different approaches and techniques of ANNs in this domain. Research articles from 2002 up to 2021 are included in this literature study.
- Security requirements of IoT are identified after extensive literature study and different type of ANNs approaches have been identified as well. This is novel effort to illustrate the underlying IoT security requirements such as authentication, authorization, encryption, secure routing, network monitoring, confidentially, integrity, availability, IDS and access control in light of different ANN-based solutions. The overall security requirements have never been addressed in light of engineering the security solutions of ANNs.

- Two major areas of IoT security such as authentication and IDS have been extensively studied and state-of-the-art review has presented to address the underlying security issues in these two IoT security areas more importantly.
- This SLR compares different ANNs approaches which are intended towards detection of DoS/DDoS attacks in IoT network. The performances of different ANNs methods for security solutions of IoT are discussed based on performance evaluation criteria to judge the best model.
- Complete in-depth analysis of research studies is performed to know about the current research trend and research gaps in this domain. This research provides a basic foundation for the researchers and security experts related to IoT security in this area.

The remaining paper is organized as: Sect. "Related work" is consisted of similar works presented by authors related to the security of IoT. Section "SLR method" describes the overall procedure taken for the completion of SLR. The overview of selected studies or answering to the research questions is discussed in Sect. "Results". Section "Threats to validity" includes the different types of threats to validity and finally Sect. "Conclusion" ends with conclusion part of this research work.

Related work

According to our literature study, a lot surveys, reviews and systematic literature reviews on the security in IoT by using both machine and deep learning approaches are available. The previous works discussed the security issues of IoT in broader sense like machine learning or deep learning based solutions have been applied. But, our work mainly focused to address the security aspects of IoT based on ANNs. According to our literature study, we did not find any related work that uses ANN approaches to address the security of IoT in terms of highlighting the security requirements. Therefore, in this section, we are discussing the different related works that are focusing the security of IoT in light of machine learning and deep learning methods.

Al-Garadi et al. [28] presented a survey of highlighting the various methods presented by machine learning and deep learning for security of IoT. Tahsien et al. [29] put forward the machine based solutions of for security of IoT. Mohanta et al. [30] performed a survey to address the issues related to CIA addressing different IoT layers by using Block chain, artificial intelligence and machine learning approaches. Restuccia et al. [31] surveyed the security issues and threats of IoT devices by using machine learning and software-defined networking. Andročec et al. [32] briefly discussed the security of IoT in light of machine learning techniques and approaches in SLR. The main focus of this work is to discuss authentication procedures and intrusion detection system in IoT based system with the support of machine learning methods. Rana et al. [33] highlighted different machine learning methods and their applications in IoT. Amanullah et al. [34] illustrated the relationship between IoT security, deep learning and big data technologies. They discussed the security of IoT in terms of security requirements such as CIA, authentication and access control using big data technologies. Cui et al. [35] focused on traffic profiling, IoT device authentication and other issues related to IoT security by using machine learning. Similarly, machine learning has become a powerful tool for

detection of abnormal network behaviour and threats in IoT environment, therefore different surveys, reviews, and SLR are presented in this domain. In this regard Chaabouni et al. [36] presented a survey focusing on discussing the Network Intrusion Detection System (NIDS) deployed through machine learning. The main theme of their work is to discuss in detail NIDS implementations, threat detection methodologies, comparing different free datasets and various deployed machine learning strategies and algorithms in context of IoT security. Fahim et al. [37] highlighted various techniques of intrusion detection, prediction and analysis by using statistical and machine learning towards the security of IoT. They also highlighted the areas of application and performance of machine learning methods employed for IoT security. Elrawy et al. [38] surveyed all the previous works to demystify the IDS based on machine learning intended for IoT paradigm. They also provided a deep insight into the different attacks and vulnerabilities pertaining to IoT security. Costa et al. [39] also made an extensive survey and studied different intrusion detection techniques for IoT security by using machine learning approaches. Alsamiri et al. [40] evaluated different machine learning algorithms, which are used for detection of different attacks in IoT network. Albalawi [41] also discussed different machine learning algorithms for security of IoT. Albalawi discussed various machine learning approaches for IDS and authentication in IoT. Hussain et al. [42] highlighted machine learning and deep learning approaches to address the security issues in IoT network. They also identified challenges and existing gaps in current works for machine learning-based IoT security. Moh et al. [43] also focused on surveying of different machine learning techniques for IoT and fog computing security. They illustrated different machine learning techniques to identify threats and attacks in IoT network and also presented machine learning based solutions. Deorankar et al. [44] also studied machine learning approaches for detection of anomalies and cyberattacks. The work presented by Podder et al. [45] is utilizing the different types of ANNs such as deep belief network, RNNs, generative adversarial network and many others towards the cybersecurity of IoT. They discuss the various IoT attacks and the effectiveness of these approaches in managing different attacks.

We categorized the related works based upon the area of security in IoT. According to our literature study, machine learning or deep learning approaches contribute towards the security of IoT in three different areas such as IDS, authentication and general security. The majority section of related works is related to the intrusion detection of IoT. Some of authors also used machine learning or deep learning for authentication purposes and some authors focused upon general security of IoT. The general security describes network monitoring, access control, encryption, authorization, routing attack, detection of malicious nodes, theft resistance and privacy. Summary of literature work is given in Table 1. This table shows the approaches presented by different authors to address the security of IoT by considering different security requirement of IoT.

SLR method

The proposed SLR method is inspired by the work presented by Liao et al. [35]. Thus, the proposed SLR design is composed of seven (7) major steps. In step (1), the Research Questions (RQs) are defined along with their objectives. In step (2), the planning procedure for this search is discussed. In step (3), the search activity is performed on different

Table 1 Comparative study of proposed SRL with existing literature work

Refs.	Research method	IoT security requirements			Machine learning technology	Year
		IDS	Authentication	General security (encryption, privacy, integrity DoS/DDoS, authorization, secure routing, confidentiality, access control, theft detection secure routing, availability, etc.)		
[46]	Survey	×	×	✓	Deep learning	2020
[47]	Survey	✓	×	✓	Machine learning	2020
[48]	Survey	×	×	✓	Machine learning and artificial intelligence	2020
[49]	Literature review	×	✓	✓	Machine learning	2018
[50]	SLR	✓	✓	×	Machine learning	2018
[51]	Literature review	×	×	✓	Machine learning	2018
[52]	Review	✓	×	✓	Deep learning	2020
[53]	Survey	✓	×	✓	Machine learning	2018
[54]	Survey	✓	×	×	Machine learning	2019
[55]	Literature review	✓	×	×	Machine learning	2019
[56]	Survey	✓	×	×	Machine learning	2018
[57]	Survey	✓	×	×	Machine learning	2019
[28]	Review	✓	×	×	Machine learning	2019
[29]	Review	✓	✓	×	Machine learning	2020
[30]	Review	×	×	✓	Deep learning and machine learning	2020
[31]	Survey	✓	×	✓	Machine learning	2018
[32]	Survey	✓	×	×	Machine learning	2020
[33]	Review	×	×	✓	Machine learning	2018
[34]	SLR	✓	×	×	Machine learning	2020
Proposed work	SLR	✓	✓	✓	Artificial neural networks (ANNs)	2020

online libraries. Inclusion–exclusion criteria and snowballing are discussed in step (4) and step (5) respectively. The quality assessment procedure is carried out in step (6) and quantitative meta-data analysis is the final step of this SLR protocol. The step-wise detail and complete structure of the proposed SLR is given is depicted in Fig. 1. All steps involved in SLR protocol are discussed in concrete and detailed manner as below.

Defining research questions (RQs)

In first step of SLR, the research questions are formulated by focusing upon their objectives. In this systematic study, four RQs are defined such as RQ1, RQ2 and RQ3. The major focus is to define questions in such manner that each question can describe the efforts and approaches of ANNs towards the security of IoT. The detail of RQs along with motivation and objectives is given in Table 2.

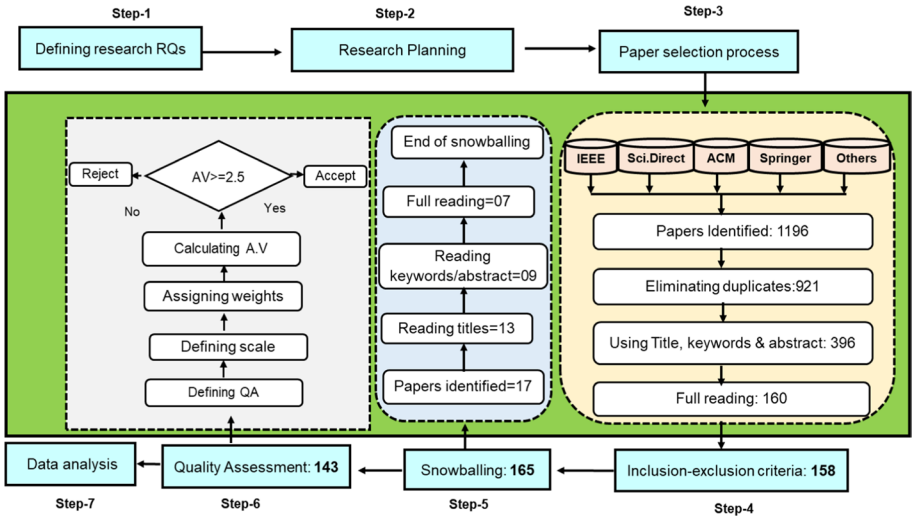

Fig. 1 SLR Protocol design

Table 2 Research questions detail

No.	RQs	Objectives and motivation
RQ1	Identify security requirements that define a full pledge secure IoT based system. What are the different types of ANNs contributing towards IoT security in the literature?	The main idea and purpose of formulating RQ1 is to identify the various security requirements of IoT network, which provide a complete package of security for IoT based systems. This question is also intended to identify the various ANN types and techniques/approaches that affect the security requirements of IoT. This question provides a solid foundation for RQ2
RQ2	What is the role of ANNs approaches towards the identified underlying security requirements/criteria of IoT? Identify the different approaches contributing towards overall IoT security	The major motivation of this question is to highlight the prime contributions made by ANN based solution towards the individual security requirements of IoT. Every security requirement or feature related to IoT security is illustrated based on the application of ANN. Different types of security models, frameworks, methods, techniques, algorithms and approaches intended to address the security issues and challenges in IoT
RQ3	How ANNs can be used to detect and analyze DoS/DDoS attacks in IoT network; and also compare the performances of ANNs approaches targeted towards the IoT security?	The main theme of this question is to discuss the major role of ANNs for detection and analysis of DoS/DDoS attacks briefly. ANN significant contributions towards the security of IoT exists in the form handling these threats and abnormal behaviors of network. A comparative analysis of different ANNs approaches have been performed in context of handling DoS/DDoS attacks

Search planning

In this step of SLR design, a proper search strategy is made to complete the search process in vigorous and complete manner. First step of search planning is to define keywords for individual RQs. Then, these keywords have been used for forming search string as well. The detail of keywords related to each RQ is given in Table 3.

After searching individual questions with defined keywords, it was observed that some important papers were skipped and were not retrieved from some online search libraries due to the reason that some libraries do not support quotation marks for searching.

Table 3 Keywords and research questions

RQs ID	Research questions Keywords
RQ1	"Security criteria" OR "security requirements" OR "security attributes" AND "IoT" OR "Internet of Things" AND "Artificial neural network types" OR "ANN types"
RQ2	"Artificial neural network methods" OR "ANNs method" OR "artificial neural network techniques" or "ANN techniques" OR "artificial neural network approaches" OR "ANNs approaches" OR "artificial neural network algorithms" OR "ANNs algorithms" AND "IoT security requirements" OR "IoT security criteria" AND "Internet of thing security" OR "IoT security"
RQ3	"Denial of Survive attack" OR "DoS" AND "Distributed Denial of Service attack" OR "DdoS attack" AND "Artificial neural network techniques" or "ANN techniques" OR "artificial neural network approaches" OR "ANNs approaches" AND "Internet of Things" OR "IoT"

So, quotation marks were expunged for those libraries that do not support. According to Kitchenham et al. [36] keywords are not enough for searching purposes and they need to be combined in form of string such as search string. For this purpose, a search string was formed based upon title of the research work to get the best results out of the search activity. Search string is derived from the keywords defined for RQs. Search string was formed by observing some steps as suggested in [37] and following steps were taken to form search string.

- Major or key terms are derived from main research topic
- Identification of keywords
- "OR" operator is used for similar words and alternative spellings
- Different terms are linked by using AND operator

In likes of this procedure, following search string is created from the research topic.

(Internet of Things security OR IoT security) AND (Artificial neural networks OR ANNs) AND (Approaches OR Techniques OR Methods OR Algorithms OR Frameworks).

There are two parts of search string: the first part is related to the security of IoT and second part is focused on ANNs approaches, methods, techniques or algorithms which are applied in the context of IoT security. Search string is applied on all database sources and it fetches the desired results related to this research work. Searching process is improved by using advance search options available in online search libraries. A pilot search is conducted to know about the results and to refine the search string for obtaining the required results related to this study. ACM, Science Direct, Springer and IEEE Xplore are the main online libraries that are selected for search purpose. While MDPI, Taylor and Francis, Hindawi and Wiley are included in other category. According to Mahdavi-Hezavehi et al. [38] these online libraries have more powerful search engines and are more ideal for automatic searching as well.

Searching process

According to 3rd step of SLR protocol, both automatic and manual searches were performed to get the most desirable primary studies related to this research work. Automatic search produces better results than manual search [39]. But, still manual search has been carried out to validate our the search string. The procedure for selection of papers from different online sources is depicted in Fig. 2.

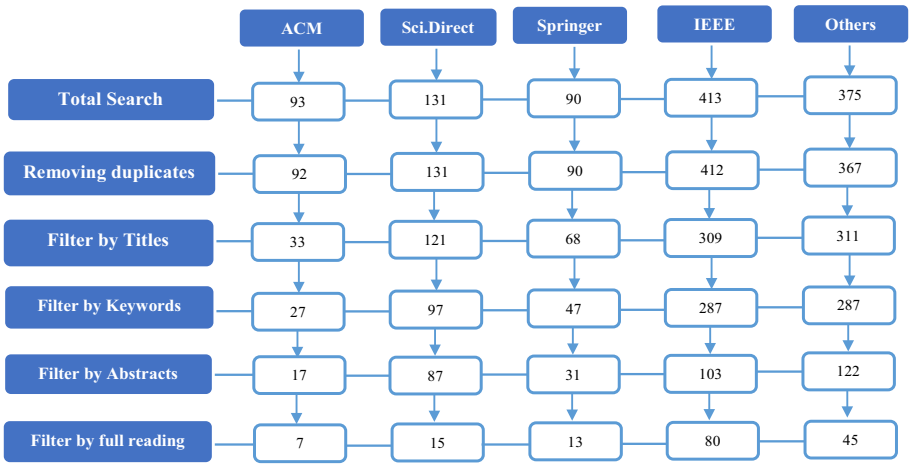

Fig. 2 Paper selection procedure

Table 4 Detail of included and excluded papers

Journal name	Included	Excluded	Total
ACM	4	89	93
IEEE	66	364	428
Science Direct	18	120	135
Springer	14	81	93
Others (Wiley, MDPI, Hindawi etc	41	407	447
Total	143	1061	1196

Online sources are ACM, Science direct, Springer and IEEE. The other category comprised of sources like Wiley, Hindawi, MDPI, Taylor and Frances etc. Initially keywords and search string were applied to identify the relevant studies. After the collection of papers, repeated papers are removed. Title of each paper is thoroughly checked against the collected papers from each online sources. Papers collected from online libraries were also checked against the keywords. Abstracts were studied to find out the most relevant studies. Finally, after full reading 160 papers were tentatively selected to address the RQs. The detail of searching process is documented and is shown in Table 4. In this table, the final list of included and excluded papers are identified. Included papers are those papers which are used for answering the research questions. These papers are selected after quality assessment (discussed in Sect. "Quality Assessment").

Inclusion–exclusion criteria

It is important to have mechanism for inclusion and exclusion of research articles based on certain criteria. Papers inclusion and exclusion in this research work is based on the criteria which is defined in Table 5.

Snowballing

Snowballing is basically the most important mechanism for inclusion of papers. Its working begins from relevant studies and it expands the number of relevant papers

Table 5 Inclusion-exclusion criteria

Inclusion criteria	Exclusion criteria
Research articles written in English language are included	Papers published except than English language are excluded
The focus is to include primary studies such as original research papers	Papers failed to provide answer to the RQs or failed to answer the topic are not included
Workshops, thesis, book chapters and magazines related to our studies are selected	Papers identifies as "Grey" are excluded from our studies
Research papers from 2002 to 2020 have been included for answering the questions	Redundant papers are excluded
Research papers from reliable and authentic source selected	Research articles comprised of three or less than three pages are also eliminated from our studies

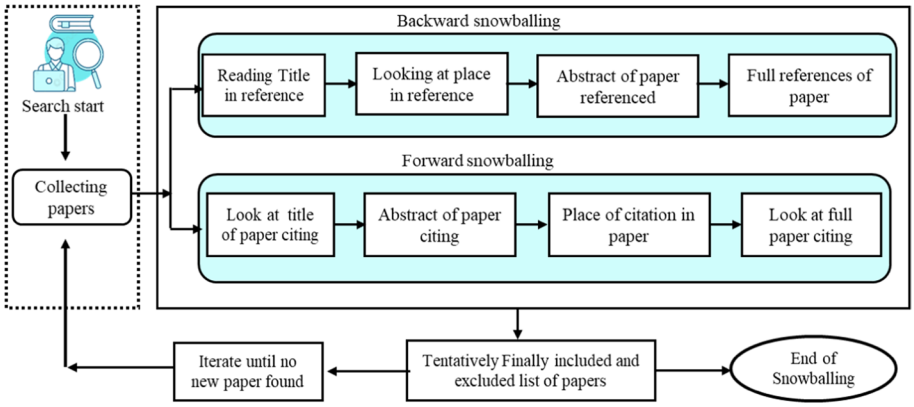

Fig. 3 Forward and backward snowballing approaches steps

by deriving more relevant papers related to research studies [39]. Snowballing works in two methods such as forward snowballing[1] and backward snowballing.[2] The procedure adopted by snowballing is iterative in nature. The stepwise procedures of both approaches is given in Fig. 3. In this research, both types of snowballing have been used to get the most relevant and desired studies related to our work. Snowballing is applied in such way that initially 17 papers identified and after reading titles the number of papers diminished to 13. After reading abstracts and full reading, finally 7 research papers were selected through this procedure. These papers were also subjected to the quality assessment procedure. The working of snowballing procedure of both approaches during the 5th step of SLR is graphically in Fig. 1.

Quality assessment

This is the most significant step of our SLR protocol design as it defines a criteria for inclusion of most relevant and important papers related to research study. This criteria helps in selection of studies and improves the decision making about selection of papers. The quality assessment procedure is done in step-wise fashion such as initially quality

[1] Forward snowballing procedure starts with looking at title of paper citing then abstract of paper citing followed by place of citation in paper and finally look at full paper citing.

[2] Backward snowballing follows procedure of looking at title in reference list, followed by looking a place of reference then looking at abstract of paper referenced and finally looking at the full references.

Table 6 Quality assessment questions

Q.ID	Questions for assessment of quality
QA1	Are the objectives of research achieved?
QA2	Is there any security feature of IoT reported?
QA3	Is any type of ANN technique method or approach reported?
QA4	Is any security aspects of IoT in light of ANNs reported?
QA5	Is any intrusion detection mechanism supported by ANNs reported?
QA6	Does it answer to the formulated research questions?
QA7	Are the results mentioned by authors empirically tested?

assessment questions are defined. These questions are QA1, QA2, QA3, QA4, QA5 QA6 and QA7. The detail of these questions is given in Table 6. During the quality assessment procedure, we collected all the included research articles in excel sheet. A criteria/condition is defined for inclusion and exculsion of particular study during this process and it is given mathematically it can be written in the following equations.

$$A.V(P_n) = \sum_{i}^{n} QA_i \tag{1}$$

In Eq. (1), aggregated value *(A.V)* is calculated for each paper, where the values of "i" to "n" and "P_n" can be any paper for which A.V is calculated. The instance or case of nth paper, accepted in quality assessment procedure by using Eq. (1) is given as follows as.

$$IfA.V(P_n) = \sum_{i=1}^{n} QA_i \geq 2.5 \rightarrow Paper\ accepted \tag{2}$$

Similarly, the case of nth paper (any paper) rejected by using Eq. (1) is given below as.

$$IfA.V(P_n) = \sum_{i=1}^{n} QA_i < 2.5 \rightarrow Paper\ rejected \tag{3}$$

A.V is aggregated value and P_n is any paper, which is subjected to quality assessment procedure. The value of "i" starts from 1 and ends with "n", the maximum value of n is "7" as there are 7 quality assessment questions. QA_i is ith quality assessment question. For the acceptance and rejection of papers a proper scale is defined, which shows the aggregate value. This scale ranges from 1 to 7. The conversion of linguistic terms into numbers and defined scale for aggregate value is shown in Fig. 4.

All the collected articles for this research work are checked against the quality assessment questions and numeric scores are assigned to the research papers based upon answering the quality assessment questions. If a particular paper provides enough answer to the quality assessment question then it is marked as "Yes"; and if it fails to answer the quality assessment question then it is marked as "No". Then, to resolve this issue, we convert these linguistic terms into numeric form. Score or integer values are assigned to the research papers based upon their answers to the quality assessment questions. If a paper answered the QA question properly and completely then it is interpreted as "Yes" and value of 1 is assigned to the paper. If,

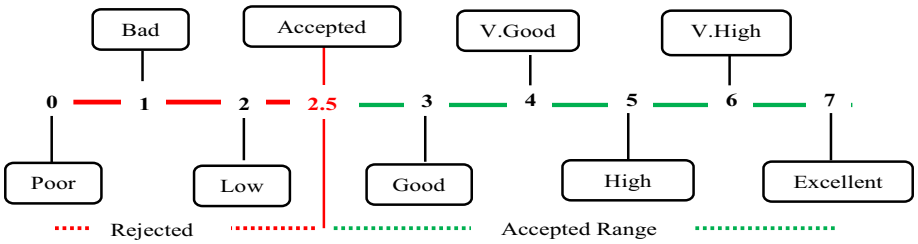

Fig. 4 Scale and converting linguistic terms in numeric form

it failed to answer the quality assessment question then it is considered as "No" and value of 0 is assigned to that research paper. For partially answered papers the value of 0.5 is assigned. Each paper is thoroughly checked against all quality assessment questions and corresponding numbers are assigned to each answer of question. Now, aggregate of all scores for individual paper is calculated. If the value is greater than or equal to 2.5 then it is accepted for inclusion in studies and if it is less than 2.5 then it is rejected and excluded from research studies. The outcomes derived from this assessment procedure are given in Fig. 5.

Quantitative meta-data analysis

This is the last step SLR protocol, which is focused upon performing various analysis of research data from different perspectives. The core purpose of this section is to perform statistical and in-depth analysis of collated research articles in order to get a deep insight about the existing research trend in the field of IoT security via ANNs. The selected collated studies in this SLR to address the questions are derived from journal, conference proceedings, books and workshops. We selected 96 papers from different journals, 34 papers are chosen from conference proceedings, 3 from book extracts and 2 from workshops. The overall primary study for this research work is composed of 143 articles. The detail about source distribution of selected studies is given in Fig. 6. In this study, we collected research articles from 2002 to 2021. The research trend is investigated based on collated studies. According to our collected studies, it has been observed that exorbitant research work has taken placed during 2018, 2019 and 2020. The research in 2021 is underway. The complete research trend of security of IoT-based system using ANN techniques is given in Fig. 7.

Results

In this section our focus is to provide answer to the formulated RQs in light of collected research articles. The comprehensive solutions are provided to the RQs (RQ1, RQ2 and RQ3). In first question (RQ1), we focus on to find out the security requirements that define a complete secure IoT network. We also identified the different types of ANNs. The main idea of this question is to collect security requirements of IoT and Types of ANNs, which are to be discussed in next research question i.e. RQ2. In second question (RQ2), we discussed and analyzed the security requirements of IoT by using ANNs types or different approaches. In this question, we highlighted the every security requirement with respect

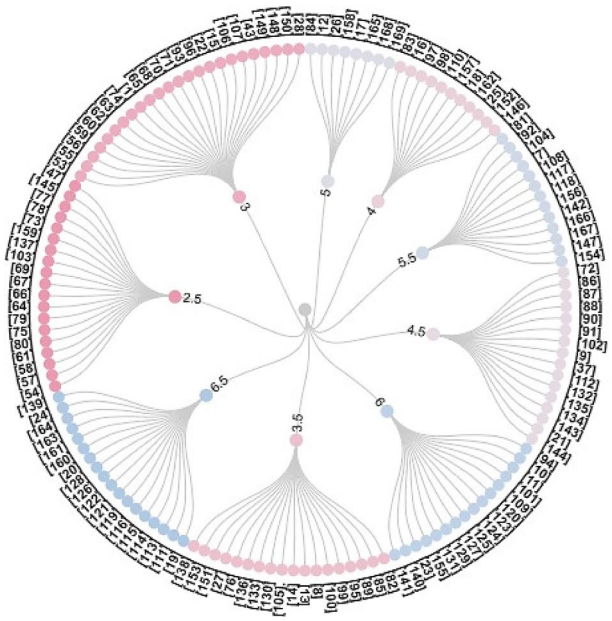

Fig. 5 Quality assessment detail

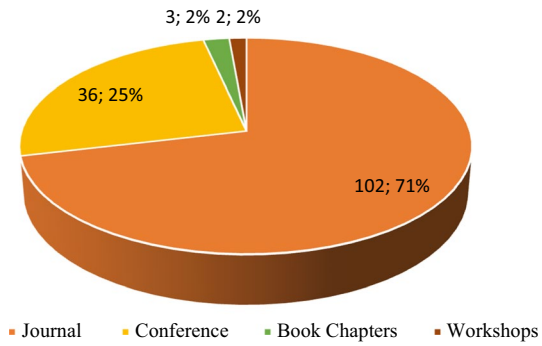

Fig. 6 Categories of studies

different approaches or methods presented by ANNs. We also highlighted the different frameworks, models, techniques and algorithms presented by ANN for overall security of IoT. In 3rd question (RQ3), we discussed the DoS/DDoS attacks and theirs solutions provided by ANNs to the IoT-based systems. In this question, we also comprehensively

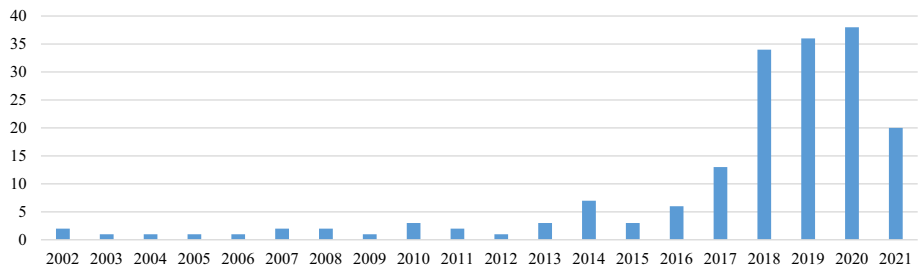

Fig. 7 Year-wise breakup of studies

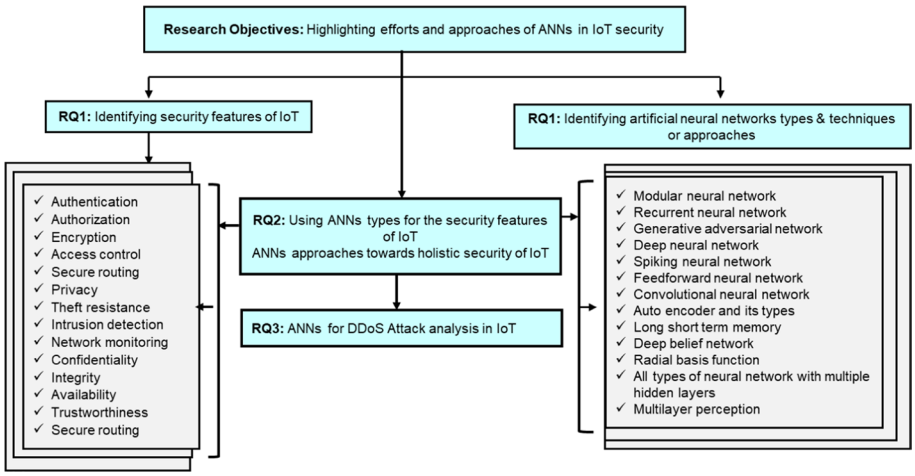

Fig. 8 Overall research framework

compared different ANN approaches in terms of performance for detection of DoS/DDoS attacks. The complete picture of entire research framework in hierarchical structure is depicted in Fig. 8. Similarly, the break–up of all papers in terms of providing answers to the related research questions is given in Table 7. The most number of papers are used for answering the RQ2.

RQ1: Identify security requirements that define a full pledge secure IoT based system. What are the different types of ANNs contributing towards IoT security in the literature?

This questions consists of two sections i.e. in first section of question, we identified the security requirements of IoT from the existing literature while in second section we reported the different type of neural networks that have contributed towards the IoT security requirements. These two sections are fully explained as below.

Identifying IoT security requirements/features

In this question, the security criteria or requirements for IoT security are identified from the literature study. The main focus of this question is to identify and collect the security features/requirements that completely describe a full-pledged IoT system with the robust security. These features will be discussed for IoT security by using ANNs (will be discussed in next question). The overall procedure for selection of security features consists of two steps: in step one, 119 security features are identified from literature and

Table 7 Detail of studies for RQs

RQ ID	No. of studies	Paper citation
RQ1	30	[1, 40–44, 44, 58–80]
RQ2	93	[7–16, 19, 22, 26, 54, 73, 76–78, 81–155]
RQ3	38	[17–21, 30, 106, 108, 109, 111, 114, 116–118, 120, 122–124, 129, 139, 141–143, 156–162]

Table 8 All attributes identified from various sources of literature

Ref#	Security features
[40]	Confidentiality, Authentication, Access Control, Availability, Authorization, Auditing, Trustworthiness, Integrity
[64]	Authentication, Key agreement, Privacy protection, Anti DDOS, Privacy, Encryption, Platform protection, User access control
[79]	Resilience to attacks, Confidentiality, Availability, Authentication, Auditing, Access control, Non-repudiation, Anonymity, Reply protection, Integrity, Authorization, Privacy, Trust
[1]	Attack detection, Privacy, Confidentiality, R.R management, Secure routing
[74]	Confidentiality, Availability, Authorization, Identification, Integrity
[65]	Confidentiality, Availability, Integrity, Non repudiation, Continuity, Physical Security
[60]	Confidentiality, Integrity, Availability
[42]	Anonymity, Integrity, Availability, Non-repudiation, Authorization, Access control, Resiliency, Self-organization, Information Protection, Exception Handling
[43]	Identification, Lightweight Protocol, Permission, Cryptography, Data protection, Communication Security, Physical protection
[44]	Authentication, Access Control, Attack resilience,
[58]	Non Repudiation, Intrusion Detection Contextual integrity, Authentication, Access control, Authorization, Integrity,
[59]	Privacy, Tracking, Integrity, Authentication, Digital forgetting, Mutual trust
[61]	Resilience to attack, Client Privacy, Authentication, Access Control
[62]	Physical protection, User authentication, Network Monitoring, Secure key management Device authentication
[63]	Key Management, Policies, Confidentiality, Authentication, Light weight algorithm, Heterogeneity, Integrity, Availability,
[80]	Identity management, Resilience to attack, Data authentication, Access control, Secure data communication, Temper resistance, Availability, Secure storage, Secure content, Secure environment execution, Secure N/W Access, User identification, Client privacy
[75]	Theft resistance, Authorization, Cloud federated authentication
[41]	Access control, End to End security, Authorization, Authentication,

in second step, duplicates or repetitive features are removed. The sources of all security features selected from literature study are given in Table 8.

The final features have been collected from the pool of security attributes as identified in Table 8. These security attributes will be used as IoT security requirements. According to our literature study the most significant IoT security requirements are confidentiality (F_1), integrity (F_2), availability (F_3) Authorization (F_4), Trustworthiness (F_5), Network monitoring (F_6) Access Control (F_7), Anti-DDoS (F_8), Authentication (F_9) Secure routing (F_{10}) Encryption (F_{11}), Privacy(F_{12}) Theft resistance (F_{13}), Intrusion detection (F_{14}). We collected 14 security requirements, which are the building blocks of any IoT network. The number of studies focusing on IoT security requirement features are given in Fig. 9.

Description or definitions of 14 security requirements of IoT are given Table 9.

Frequency of attributes citation based on number of papers in literature is depicted in Fig. 9. This figure shows the number occurrence of each security attribute in literature. The detail of finally identified security attributes along with the sources are given in Table 10.

Now, we will discuss and analyse the security of IoT by using ANNs in light of the finally selected security requirements. The impact of ANNs approaches for IoT security requirements will be completely discussed in next RQ.

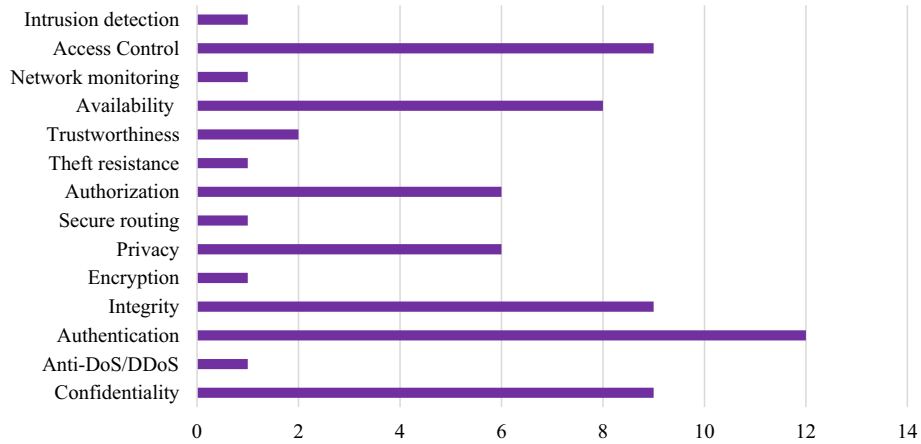

Fig. 9 Number of studies focusing on individual IoT security requirement

Types of artificial neural networks

The types and applications of ANNs exist in good numbers and in multiple domains. ANNs types are used for variety purposes such as data compression, prediction and pattern recognition [70]. Pattern recognition is the most important one and it is the form of classification [72]. ANNs use pattern recognition to address the security issues in IoT. For pattern recognition ANNs use different set of various algorithms, techniques, methods or types, which provide a reliable and secure options to IoT. Different types of ANNs are given in Fig. 10 [54, 71].

RQ2. What is the role of ANNs towards the identified underlying security requirements/criteria of IoT? Identify the different approaches contributing towards overall IoT security

In this question, the security requirements/criteria for IoT as previously defined in RQ1 has been briefly explained in light of contributions provided by ANNs. As, ANNs provide a holistic approach towards the security of IoT but in this question, we are going to discuss the security of IoT with respect to the individual security requirements by using different ANN approaches or models. After, identifying the security requirements in the previous question, our focus is to discuss the significant role of ANNs to deal with the security issues and challenges related to IoT. In this question, we broadly address the security of IoT network in light of different frameworks, models, algorithms and techniques employed with the support of ANNs. The role of different approaches presented by ANNs for the overall security of IoT devices is highlighted. As, the number of IoT devices are drastically elevating due to their ubiquitous and pervasive nature. This significant rise has led towards the implementation issues related to the enforcement of security standards and procedures in IoT environment. Major challenges for implementing the security in IoT devices are: first, these devices are heterogeneous in nature and secondly these devices are bulky in numbers and third, these devices have less computational power, memory and processing abilities. The security of IoT devices is not only limited to the network where they are operating but it is also mandatory to inject the security in IoT devices which are using services, products and applications.

Table 9 Detail of IoT security requirements

IoT security requirements	Description/detail
Authorization [58, 66, 69]	It is about giving or denying limited access to the data, resources and applications within the system. It is the procedure of allowing, denying, and restricting access to entities
Authentication [58, 66]	Defines the rights or privileges given to the users based upon the identity to access the system. It verifies and differentiates the identities of users or entities that are entitled for accessing the data or system resources
Access control [65]	Access will be granted or denied to the network assets based on security and business requirements related to security
Network monitoring [62]	It is the procedure of detecting and reporting anomalies and DoS attacks in IoT network
Trustworthiness [40, 68]	According to trustworthiness security property any untrusted and malicious data can come from trusted node or sensor. Trustworthiness is described by privacy and security features
Availability [66, 67]	Data and services of network must be used by legitimate user must be available to them
Secure routing [73]	It is procedure of mitigating the impacts of routing attacks, alteration, and packet dropping during the routing operation
Theft resistance [75]	It is detecting of removing IoT devices in network
Intrusion detection [76]	Software or hardware systems which monitor the events occurring in network or computer system and make analysis of such events to analysing them for symbols of problems related to security
Anti-DoS/DDoS [77]	It is the attack which attempts to make the services or resources unavailable or partially inaccessible for using. This security feature is protecting such attacks which forfeits the system resources fully or partially
Confidentiality[66]	Protection of user's privacy and hiding data from illegal user or entity
Integrity [67]	Integrity is about keeping the sensitive data away from modification and destruction. Data must be in complete, correct and reliable form
Privacy [78]	It is the ability or rights to manage information itself. It means protecting information from the public exposure
Encryption	A step-wise procedure to convert the message in unreadable format

Authentication

Authentication of IoT device is mandatory before it participates in any network or login activity. For this purpose, ANNs have significant impact upon the authentication feature of IoT-based systems. ANNs based approaches provide a smart and secure authentication schemes by eliminating the traditional methods of authentication such as pins, passwords, username etc. Introducing ANNs as feature extractor for modern procedures of authentication such as biometric authentication, iris recognition, Wi-Fi signals and keystroke can be proven to provide good options for identification and authentication of IoT devices. ANNs with the support of deep learning provide strong security solution towards the authentication of IoT devices. Deep learning has major application as it is ideal for authentication of low power IoT devices [81]. In this regards, Chatterjee et al. [82] proposed authentication scheme leveraging ANNs for enhancing the security of IoT. They presented physical unclonable functions (PUF) based method which can be used for easy and secure identification of IoT devices. Similarly, the another main advantage of this method is, it does not require addition hardware cost and provides a secure way of identification. During the authentication procedure it is imperative to analyze the behavior or pattern to detect malicious activity. In this regard, to strengthen the security of IoT

Table 10 Final list of selected attribute in this study

Req	Citation																	
	[40]	[41]	[42]	[43]	[44]	[58]	[59]	[60]	[61]	[62]	[63]	[74]	[80]	[75]	[79]	[1]	[64]	[65]
F_1	✓	×	✓	✓	×	×	×	✓	×	×	✓	✓	×	×	✓	✓	×	✓
F_2	✓	×	✓	×	×	✓	✓	✓		×	✓	✓	×	×	✓	×	×	✓
F_3	✓	×	✓	×	×	×	×	✓	×	×	✓	✓	✓	×	✓	×	×	✓
F_4	×	✓	✓	×	×	✓	×	×	×	×	×	✓	×	✓	✓	×	×	×
F_5	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
F_6	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
F_7	✓	✓	×	×	✓	✓	×	×	✓	×	×	×	✓	×	✓	✓	✓	×
F_8	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓		×
F_9	✓	✓	×	×	✓	✓	✓	×	✓	✓	✓	×	✓	×	✓	✓	✓	×
F_{10}	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
F_{11}	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×
F_{12}	×	×	×	×	×	×	✓	×	✓	×	×	×	✓	×	✓	✓	✓	×
F_{13}	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×		×	×
F_{14}	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	✓	×	×

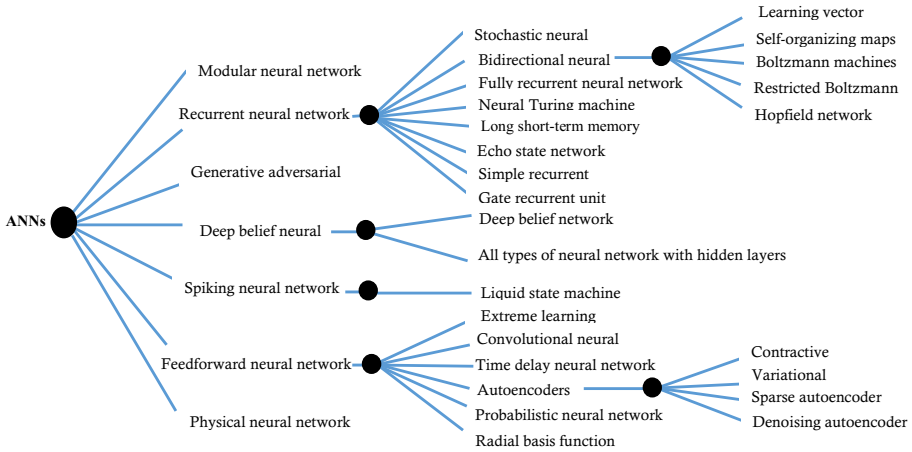

Fig. 10 Summary of All ANNs types

devices, ANNs along with support Counter Propagation ANN (CPANN) as classification models can be employed for continuous authentication to prohibit the attacker by analyzing behavior pattern of mouse and keystroke [81, 83]. Similarly, another authentication method for keystroking is introduced by Huang et al. [88]. This keystroke authentication method is using force information and touch time on piezoelectric touch panel for authentication in IoT. The signal authentication of IoT devices is also a major concern. For signal authentication of IoT devices, a deep learning based long short-term memory (LSTM) watermarking scheme is suggested by Ferdowsi et al. [84]. This approach can be used to collect data from IoT devices and authenticating the reliability of signals. This scheme is also helpful in detection of cyberattacks such as eavesdropping, man-in-the-middle and data injection. As, IoT devices have limited power options so secure authentication becomes a challenging task. In this regard, Das et al. [86] presented LSTM based framework to solve the authentication problems of low power IoT devices. This framework uses deep neural networks for classification of impairments in the signal received. For sufficient computation and memory power of IoT devices, Shi et al. [87] suggested an authentication mechanism based on Channel State Information (CSI) features of Wi-Fi signals extracted through the deep neural networks for identification.

ANNs also contributes towards biometric authentication in IoT environment. Biometric authentication does not require passwords or any other credentials so comparatively it is more convenient way of authentication. In this regards, the proposed model suggested by Meena et al. [85] has been used for biometric authentication in IoT. The proposed model uses ANNs as a classification of iris templates cells for authentication purposes of a person. ANNs are used for feature extraction in order to improve the accuracy and feasibility for deployment in IoT based system. McGinthy et al. [89] presented neural network based specific emitter identification (SEI) approach for secure authentication of IoT devices. Similarly, authentication method suggested by Reyhani et al. [90] uses encryption algorithms learned by neural networks for storing the encrypted passwords for authentication and access control. Bazrafkan et al. [91] presented segmentation algorithms derived from deep learning for iris based authentication for handheld

devices in IoT environment. Chauhane et al. [138] presented end to end authentication based on breathing acoustics using RNN. Agrawal et al. [140] applied crypto token for authentication without intervention of user by using LSTM model and Blockchain technology.

Authorization

In IoT environment authorization is important security feature as it ensures that only authorized entity will get access to the applications, services or network resources. ANN with the support of deep learning has made a good influence on authorization security feature of IoT. There are various studies available in the literature, that describe the significant role of ANNs. To completely understand the authentication and authorization, Ferrag et al. [81] in their study provided a comprehensive overview of all machine learning approaches. For authorization in IoT, a trust authorization model is suggested by Du et al. [16] is using ANNs along with Back Propagation (BP) algorithm. This proposed method is used for detection of attacked node, monitoring the interactive data stream, periodically and urgently implementing the response measures. Similarly, proposed authorization technique based on behavioral characteristics extracted from the captured data by using ANN is also applicable as given in [81, 92]. Another study forwarded by Ahmed et al. [93] presented an approach for analyzing the free text of keystrokes by using neural network approach.

Encryption and decryption

Encryption is the most important security feature of IoT. ANNs also played an important role in encryption and decryption of images and data. The major reason of the applying ANNs for the encryption and decryption is that such cryptosystems are extremely hard to break but still key factors remain are the weight and architecture of the network [94]. However, neural networks are applied to build an efficient encryption systems by changing key permanently [136]. This is the main reason that the modern encryption schemes are using ANNs for cryptography. In the existing literature some studies are available, where ANNs have been applied for chaotic cryptography. Like, the study forwarded by Chauhan et al. [10] is using chaotic based artificial neural network for encryption of images. Similarly, Rarhi et al. [95] designed encryption scheme which combines the DNA encoding scheme by using Hyperchaotic Neural Network for encryption of images in IoT devices. Application of neural network in this approach, makes it hard to break. Similarly, for encryption of data different encryption and decryption schemes have been proposed for IoT devices using neural network concepts. In this regard, the Khari et al. [96] presented elliptic Galois cryptography protocol which is using chaotic artificial neural network for encryption and decryption of data. Another approach suggested by Saraswat et al. [97] is based upon auto associative neural network with the support of encryption techniques which is designed for transmission and receiving of data securely. This approach is very simple and exhibits fast encryption and decryption of data. ANNs can also be employed to provide cost effective and highly processing cryptographic algorithms that are ideal for the deployment for resource-constrained devices in the embedded systems [147].

Access control

It is another important feature of IoT that takes decision about which entity is allowed to access the network resources and which one is to be restricted. ANNs can also be used to provide a secure access control in IoT environment. The framework presented by Pacheco et al. [98] introduces ANNs as parametric model to provide access techniques for IoT end nodes. Modern authentication and access control methods like biometric access control system are based upon voice authentication, they use ANNs for identification of user voice [11]. For secure access control and offloading in IoT environment, Nguyen et al. [12] combined deep reinforcement learning (mixture of ANNs and reinforcement learning) by using block chain technology for mobile edge-cloud computation offloading system. Similarly, the block chain technology combines with machine learning approach such as reinforcement learning to define dynamic access control for IoT devices [99]. The reinforcement learning can also be used for access control and battery predication in IoT [100]. Artificial neural network has been used for collision detection and prediction mechanism for wireless network on media access control [101]. The application of ANNs approaches for access control can provide a secure access based on biometric for the network resources. In this regard, MultiLayer Perception (MLP) neural network presented by Bryliuk et al. [102] can be reckoned as good approach for nullifying the unauthorized access towards the IoT based systems.

Secure routing

Secure routing in IoT-based networks is considered as the fundamental security requirement. ANNs offer variety of approaches for the routing in IoT network. ANNs with the support of routing protocol known as SAEER [22], provides secure and energy efficient routing from one IoT device to other. Similarly, ANNs can also be applied for prediction of traffic or packet loss during the routing or congestion control [9]. In this approach ANNs combine with multi step ahead predication time series to predict the loss of packets. For efficient routing, energy utilization, ratio of packet delivery and network lifetime a routing protocol suggested by Thangaramya et al. [103]. This protocol uses CNNs in IoT based wireless sensors networks.

Privacy and trustworthiness

Privacy is also important feature of IoT and ANNs have also impacts on the privacy of IoT system. ANNs work as add-ons to provide privacy and element of trustworthy to the IoT networks. Data related to IoT devices can be locally processed in IoT network by using ANN's components known as neurons and theirs's interconnectivity [8]. These component allow to minimize the latency and preserves the privacy without sending data to the remote sites for the purpose of processing. Similarly, preserving the privacy of multimedia data of IoMT applications, ANNs can be applied at cloud server by segmentation techniques to extract the meaningful data generated from multimedia sensor nodes [13]. Type of ANN known as CNNs [15] can be leveraged for privacy in IoT for the energy preservation [14]. Trustworthiness of IoT can be achieved by two features such as security and privacy [68]. ANNs also provide different methods for trustworthiness security feature of IoT. In this regard, Abbas et al.

[143] presented a trustworthy privacy framework known as "PriModChain" for IoT which is using deep neural networks. This framework is intended to provide trustworthy based on five security pillars such as safety, security, resilience, reliability and privacy in industrial IoT environment. Utilizing the ANNs, Banerjee et al. [144] forwarded a framework for the cyber trustworthiness in IoT environment. Although, the proposed framework has certain limitations, however it can be improved by using autoencoder and deep neural networks.

Theft resistance

Artificial neural networks are also helpful for theft detection IoT based system. Neural Networks have major applications in IoT with respect to theft resistance. The major role of neural networks can be seen in energy theft detection is inside the smart grid systems [14]. A similar model known as Smart Energy Theft System (SETS) was presented by Li et al. [15] incorporating CNNs for detection of theft. This approach provides very high accuracy of 99.96%; and it ensures the security of IoT based smart home systems. Similarly, neural networks were also applied in the approach for smart energy meter, where the role of neural networks is to analyze the trend of energy consumption in the household [104].

Network monitoring

The network monitoring and decision making about the entities involved in network are important considerations for the better and smooth running of IoT network. A proper network monitoring can be achieved by deploying a smart Intrusion Detection System (IDS). IDS is software program, which regularly monitors the network traffic and informs the network administrator about the anomalies encountered during the network traffic [105]. ANNs based intrusion detection mechanism bring forecasting approach which tends to predict the network elements in IoT environment [7]. This approach has the ability to reduces the human intervention and labor administration inside the network. The complete IDS approaches leveraging ANNs are discussed in the next section in detail.

Intrusion detection

It can be defined as "software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analysing those events for signs of the security problems" [76]. One of the most challenges faced by IoT is to detect and prevent intruders in IoT devices and networks [146]. As, security of data is important, for this purpose different IDSs have been designed to keep security of IoT device in mind. IoT devices suffer from various threats and vulnerabilities, therefore, it is necessary to detect these cyberattacks and intrusions before they exploit the vital network resources. Different approaches and attempts have been made to address the security issues and challenges related to threat detection. But, more importantly, the contribution of ANNs is noticeable in this respect. ANNs have been applied by different models related to intrusion detection in IoT environment over the years. But, the most common

are two types of models such as misuse IDS and anomaly. The former model searches for activity against the well-known signatures of intrusions while anomaly based IDS detects abnormal activity [137]. Misuse IDSs normally have shortcoming, when the attacks characteristics change from built-in signatures but this problem can be solved by ANNs [137]. One of the most applications of ANNs is intrusion detection in IoT network. There is a sharp rise in intrusion detection technologies specifically in distributed and intelligent system [135]. In this survey, we collected different approaches for intrusion detection mechanisms using ANNs. The complete detail of ANNs approaches for IoT intrusion detection/attacks along with limitations are given in Table 11.

From above discussion it becomes significantly clear that the ANN approaches have significand contributions towards the intrusion detection security requirement of IoT.

Confidentiality integrity and availability (CIA) security requirements

Confidentiality is about keeping secret or preventing data disclosure to the unauthorized access. The confidentiality of data can be achieved via various security mechanisms but one of them is encryption. Encryption is a good solution in order to maintain the confidentiality and privacy of data [54]. ANNs provide confidentiality of data in IoT networks by converting it into unreadable format through different encryption approaches like [10, 94, 95]. Similarly, the most common method for confidentiality of data is biometric verification [130]. ANN has also been used to provide biometric authentication through the iris recognition [85]. ANNs are also helpful in providing biometric based verification scheme known as "gait-based security" scheme intended for the security of IoT devices operating in healthcare system [131]. To ensure the confidentiality of data in IoT network, the Usman et al. [13] presented privacy preserving framework by using counter-propagation ANNs. Similarly, Yao et al. [14] presented CNNs based scheme for detection of energy theft in smart grid. Another approach using Multilayer Perceptron (MLP) ANNs supposed by Barros et al. [132] performs biometric authentication by using ECG (electrocardiography). It uses MLP ANN for extraction of features in IoT network. The confidentiality, availability and integrity (CIA) features of systems are dependent on persistent security and robustness against routing attacks [26]. The availably of data is affected by catastrophic situations like storm, earthquake and flooding. Data can also be harmed by human activities that are done accidently or deliberately. Firewall, redundancy methods and IDS are the best possible ways of protecting the availability of data. CIA features related to IoT can be protected by using intrusion detection mechanisms [133]. Intrusion detection is mechanism of detecting any attempt which leads towards the compromising of confidentiality, integrity and availability of network resources [134]. The most significant application of ANNs is intrusion detection mechanisms as available in [19, 108–111]. The complete detail of all ANN-based approaches, which contributed towards the security requirements of IoT are given in summarized form in Table 12.

Different approaches, frameworks, models, techniques and algorithms have been presented to cope with the threats and attacks related to IoT systems. But, ANN approaches encompassing the concepts of brains and neurons can be reckoned as best security

Table 11 IDS in IoT using ANN approaches/techniques

Ref#	ANNs approach	Intrusion targets in IoT	Limitations
[106]	Feed forward NNs	DoS, DDoS, Reconnaissance, Information theft	✓ The precision drops for binary and multi-class classification
[107]	Gated RNNs	All IoT layers attacks	✓ This work is only applicable to low power IoT devices and low dataset
[108]	ANNs	Worms, Shellcode, DoS, Backdoors, Reconnaissance	✓ More complex dataset due to similar behaviour of normal network traffic and modern attacks [54] ✓ Real time network traffic is not addressed (Future focus)
[109]	ANNs	DoS, DDoS	✓ Other major type of attacks are not addressed by this approach
[19]	ANNs	DDoS	✓ Not appropriate for encrypted packets ✓ Accuracy is less for very old dataset ✓ Algorithm requires re-training after 5 to 6 years ✓ This approach is not tested in simulated environment ✓ Targets only DDoS
[110]	ANNs	Anomalies in IoT data	✓ Applicable for limited dataset and small scale system
[111]	ANNs	Malicious shellcode pattern	✓ It uses offline approaches of detecting shellcode ✓ Focus is only on shellcode patterns
[112]	Deep RNN	DoS, Probe, R2L, U2R	✓ NSL-KDD data set used which is not ideal dataset for IoT [54] ✓ It lacks modern footprint attacks scenarios [54]
[113]	Conditional variant autoencoder	DoS, Probe, R2L, U2R	✓ NSL-KDD data set used which is not ideal dataset for IoT [54] ✓ It lacks modern footprint attacks scenarios [54]
[114]	Auto encoded DNN	DoS, Injection, Impersonation	✓ Covers limited range of attacks ✓ Algorithm is trained offline ✓ Dataset in this approach is valid small networks
[115]	ANN based IDS	DIS attack, Version attack	✓ Simulated dataset ✓ Limited range of attacks
[116]	Bi-directional LSTM RNN	Worms, Backdoor, DoS, Reconnaissance, Analysis	✓ Small network dataset used ✓ Some attacks available in dataset were left unaddressed
[117]	ANNs	DoS, Probe, Remote to Local (R2L), User to Root (U2R)	✓ Dataset contain large amount of redundancy ✓ Dataset used by approach applicable to small network
[118]	Fuzzy Clustering FC-ANN	DoS, Probe, R2L, U2R	✓ More suitable for low frequent attacks such as R2L and U2R attacks but for high frequent attacks the accuracy drops a bit ✓ Determining the appropriate number of clustering is an issue
[119]	LSTM & RNN	■ DoS, SYN flood attack	✓ Very limited dataset used by this approach ✓ This approach is applicable to small network ✓ Limited number of attacks addressed

Table 11 (continued)

Ref#	ANNs approach	Intrusion targets in IoT	Limitations
[120]	Random neural network (RNN)	DoS, Malicious operation, Malicious control, Data type probing, Spying, Scan, Wrong setup attack	✓ Method is checked against dataset which contains less features ✓ Not efficient for noisy and low quality data ✓ Implementation on different IoT devices will create complexity issue
[121]	Dense RNN	DoS, Denial of sleep attacks	✓ Probabilistic approach towards attack detection ✓ Applicable to small network
[122]	Back propagation (BP) NN, and Radial basis function (RBF) NN	DoS, Probe, R2L, U2R	✓ Dataset used by approach is redundant ✓ Can be applied to small network
[123]	BP ANNs	DDoS, DoS	✓ Detection rate drastically drops at second stage ✓ Detection rate is affected by time out values
[124]	ANNs	DoS, Spoofing. Sniffing, Impersonation, Malware	✓ Applied on limited number of IoT devices ✓ Test on Wi-Fi network only, not applicable to other networks like ZigBee ✓ A hypothetical approach towards detection
[125]	CNN + RNN	Network traffic classification	✓ Dependency of detection model on TCP window size and TIMESTAMP ✓ Results get worst by TIMESTAMP factor
[126]	Autoencoder	Mirai attacks, BASHLITE attacks	✓ More hypothetical approach ✓ Method applied to very small network
[127]	RNN + LSTM	IoT malwares detection	✓ Dataset used in this approach is small ✓ Improvements are required for real life environment implementation
[128]	Feed forward (FF) ANN	DoS, Backdoors, Shellcode, Worms, Spams, Reconnaissance, Port scan, Generic	✓ UNSW-NB15 data set is valid only for emulated and small networks
[129]	LSTM-RNN	DoS, Probe, R2L, U2R	✓ False Alarm Rate (FAR) requires more improvement ✓ Dataset suffers from redundancy ✓ Dataset used by model is for small network
[139]	Deep Belief network DBN-IDS	Botnet, Brute force, DoS/DDoS, Infiltration, Port scan, Web attacks	✓ Some other class of attacks needs to be included ✓ Dataset used by this model is emulated and valid for small traffic
[141]	Multi CNN	DoS, Probe, R2L, U2R	✓ This is offline learning ✓ Dataset is not ideal for IoT
[142]	Bidirectional Long Short Term Memory based Recurrent Neural Network (BLSTM-RNN)	UDP, ACK, DNS, SYN	✓ Some attacks in the Mirai botnet dataset are skipped

option to monitor the network and make timely decisions related to the security of IoT. ANNs also provide the features of self-organization and self-feedback network [148]. Deep neural network-a type of feed-forward ANN constructed from deep belief network but with more detail included, can be more effective towards IoT security [163].

According to different research studies, it becomes clear that ANN approaches provided better accuracy and detection rate as compared to the other approaches [115]. The detail of different types of ANNs-based methods, frameworks, models, techniques and algorithms contributing towards IoT security are given in Table 13.

RQ3: How artificial neural networks (ANNs) can be used to detect and analyze DoS/DDoS attacks in IoT network; and also compare the performances of ANNs approaches targeted towards the IoT security?

Our main motivation in this question is to discuss the security solutions provided by ANNs for IoT against DDoS or DoS attacks. In response to this question, the different types of ANN approaches that are fruitful for threat detection in IoT along with their performances evaluation are reported. We collected different studies that are reporting various attacks addressed by IoT based systems. In the literature review, it has been observed that majority of studies were focused on leveraging ANNs techniques for DoS attacks in IoT networks. The number of studies focusing on using ANNs for DoS attacks are given in Fig. 11.

IoT-based systems are susceptible to many security threats and attacks such that even a single attack can compromise the entire network system. Therefore, it is mandatory to identify and assess the gravity of such attacks which could halt the system. Like, back in 2016, Dyns security cameras were hacked, ultimately it not only led towards breaching of data but Twitter and Netix also went under DDOS attacks [143]. Similarly in 2016, IoT infrastructure suffered from Mirai attack—a family of malware attacks which halted the internet by using webcams and printers as botnet for DDoS attacks [30]. DDoS attacks spawn a conspicuous security threats to Internet in modern world. But, these attacks have more dominant impacts in IoT environment because devices operating in this environment come up with minimum memory, computation power and less security. DDoS attacks degrade the performance of IoT system by misusing the resources such as memory, CPU or network bandwidth [156]. DDoS attacks are arising at the 2.5 rate in last 3 years [164]. In response to these attacks, ANNs furnish the services for detection and classification of DoS/DDoS attacks then identifies and analyses their impacts in IoT network. For the classification of such attacks various attempts have been made that are using ANNs as identifier and classifier [117, 118]. Because, ANNs based approaches for the detection, classification and prevention of DDoS attacks produce higher accuracy than other machine learning approaches. The major reason behind the application of ANNs-based algorithms for unsupervised learning is due to theirs effectiveness in detection of DDoS [165]. We collected different approaches using ANNs algorithm for the detection of DoS/DDoS attacks in IoT as detail given in Table 14. In this table, all the ANNs algorithms and approaches that have been applied alone or with the support of other methods for the security purpose of IoT are reported. We also highlighted the existing limitations and improvements of these approaches based on our literature study. We also studied these research studies for different types of datasets that have been applied for detecting of DoS/DDoS attacks.

It is indispensable to select a robust and efficient ANN-based architecture/approach which can provide answers to the security questions related to the IoT network. This ANN architecture/approach can be selected based upon certain performance evaluation

Table 12 Summary of ANN approaches for IoT security requirements

Security attribute	ANN	RNN	MNN	CNN	DBN	LSTM	FF NN	Autoencoder	MLP	CPANN	ANN BP
Authentication	✓	✓	✓	×	✓	✓	×	×	✓	✓	×
Authorization	✓	×	×	×	×	×	×	×	×	×	✓
Encryption	✓	×	×	×	×	×	✓	×	×	×	×
Access control	✓	×	×	×	×	×	×	×	×	×	×
Secure routing	✓	×	×	×	×	×	✓	×	×	×	×
Privacy	✓	×	×	×	×	×	✓	×	×	×	×
Theft resistance	×	×	×	×	×	×	✓	×	×	×	×
Network monitoring	✓	✓	×	×	×	×	×	✓	×	×	×
Intrusion detection	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓
Trustworthiness	✓	×	×		✓	×	×	×	×	×	×
CIA features	✓	✓	×	✓	✓	×	✓	×	×	×	×

Table 13 ANNs based frameworks, models and techniques for overall IoT security

Ref.	Framework/technique/model	Contributions towards IoT security
Anitha et al. [115]	ANNIDS technique based on Multilayer Perceptron (MLP)	Using MLP for detection of attacks in IoT environment and can be used combined with IDS for better performance
Pacheco et al. [98]	ANNs based IoT security framework	An IoT framework for security of application and services is presented to address all the issues at IoT layers and ANNs is used as parametric model
Lee et al. [133]	ANNs model	ANNs based model to detect the anomalies in IoT network and provide the required solution,
Choi et al. [149]	ANNs model	A model for fraud detection and using ANNs for comparing results with other machine learning method for IoT devices
Canedo et al. [110]	ANNs approach	Securing IoT network by detecting anomalies in IoT gateway
Wu et al. [122]	Back propagation (BP) and Radial basis function (RBF)	Detection of abnormality and multi attack in IoT environment. RBP is the special class of ANN [150]
Hwang et al. [155]	Autoencoder	Autoencoder (Type of neural network) for detection of malicious traffic based on fewer packets
Luo et al. [24]	Autoencoder neural network	Autoencoder neural network mechanism for anomaly detection in wireless sensor network for IoT
Martin et al. [113]	Intrusion Detection CVAE (ID-CVAE) method	Introduction detection mechanism based on ANNs for IoT with best classification results
Kotenko et al. [7]	MLP and neural network probabilistic approach	An approach intended to monitor, forecast and make decisions about the state of elements of IoT using an artificial neural network
Cowdrey et al. [23]	ANNs based system	Uses ANNs as optical character recognition for characters on plate to open the security gates of home based IoT system
Chatterjee et al. [82]	RF-PUF framework	A framework to enhance the security of IoT through authentication of nodes by using ANNs
Alhajri, et. al. [25]	Autoencoder	A method for detection of IoT botnet and security threat detection
Kaur et al. [22]	SAEER protocol based on ANN	A proposed method for secure routing and detection of malicious nodes in IoT network
Yavuz et al. [26]	Deep learning based method	A deep learning based machine learning method for detection of IoT routing attacks
Kumar et al. [27]	Face recognition using neural network	A smart and intelligent face recognition and navigation system for blind people in IoT for smart security
Bhavani et al. [151]	Back propagation with Ant colony algorithm	BPA is used for image flame classification in sensor based IoT system
Chiuchisan et al. [152]	ANNs (Multilayer Perceptron & Radial Basis Functions Network)	This work uses ANNs for identifying normal or Parkinson disease objects in healthcare environment
Wu et al. [153]	ANN-BP	This method uses back propagation algorithm for detection of ambiguous situation and provides disposal processes in IoT environment

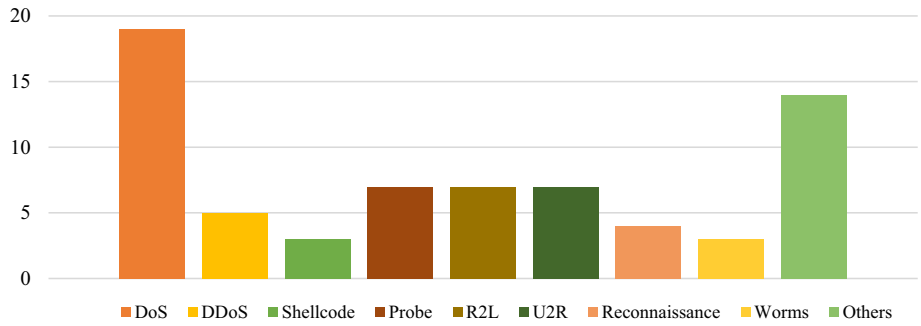

Fig. 11 Number of studies focusing on IoT attacks

criteria or parameters. This performance evaluation metrics of ANN methods intended towards the IoT security can be determined by detection of accuracy, precision, recall and F1-score. But, among these evaluation parameters, the most significant one is accuracy. Accuracy determines the true detection in terms of percentage over total data instances. It is very important performance evaluation parameter for ANN approach intended towards the DDoS or other threat detection. Accuracy, precision, recall and F1-score can be calculated by using following equations.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FP} \tag{4}$$

$$Precison = \frac{TP}{TP + FP} \tag{5}$$

$$Recall = \frac{TP}{TP + FN} \tag{6}$$

$$F1 - Score = \frac{2 \times (Precision + Recall)}{Precision + Recall} \tag{7}$$

where, TP, FP, TN and FN represents the true positive, false positive, true negative and false negative respectively. These are the performance metrics of any ANN based detection method. There are many performance evaluation parameters for measuring the efficiency of ANN method for detection of DoS/DDoS attack but the most prominent and significant parameters, which can be used as metric for selection of best approach are accuracy, precision, recall and F1-value.

The accuracy, precision, F1 value and recall of different ANN approaches along with dataset for the DoS/DDoS attack detection in IoT-based systems are given in Table 15.

Accuracy is important parameter for assessment of the performances of ANNs approaches. Similarly, precision, F1-score and recall are the most commonly used evaluation parameters that are also used to assess the performance of different ANN-based security techniques towards the security threats in IoT-driven systems. The number of studies measuring the performance of ANNs approaches with respect to IoT security are given in Fig. 12.

Table 14 ANNs-based approaches of detection of DoS/DDoS threats in IoT-driven systems

Methodology	Data set	Study limitations	Improvement
ANN + FF and Backward algorithm [117]	NSL-KDD dataset	(−) Insufficient parameters for performance evaluation	(+) Requires other parameters for better performance
Fuzzy clustering (FC)-ANN [118]	KDD CUP 1999	(−) Effective only for low-frequent attacks i.e. R2L and U2R (-) Determining number of clustering can be issue	(+) The clustering techniques can be improved through advanced data mining techniques i.e. outlier detection, evolutionary computing etc
Deep learning model [18]	CICIDS2017 datasets	(−) Data set adopted is redundant (−) Data set requires extra computing and processing	(+) Implementation required for fog to node testing (+) Data set can be filtered through labelling
ANN with pattern analysis [19]	Multiple datasets related to DDoS attack	(−) Detecting encrypted DDoS attacks is concern	(+) Updating dataset for new information regarding encrypted DDoS attacks (−) Training of ANNs algorithm after some time
ANNs with Synthetic Minority Over-sampling Technique (SMOTE) [20]	Bot-IoT	(−) Proposed approach targets only Mirai IoT attack	(+) Extending same approach for other types of attack
Deep belief network learning model[21]	IoT benign network traffic	(−) Some other attacks Sybil and spoofing attacks like requires consideration	(+) Model can be optimized for zero-day attacks
ANN-based IDS [111]	IoT benign network traffic (Test dataset)	(−) Offline approach for detecting shellcode pattern (−) Not applicable to SQL injection attack and cross-site scripting (−) Implementation on real-world network traffic	(+) False positive rate should be reduced (+) Live network optimization is required
Multi-level perception approach (MLP) [109]	IoT network traffic collected from sensor nodes	(−) Testing model in real world	(+) Accuracy and reliability can be improved by adding recurrent and CNNs
Neural network approach [157]	Consumer IoT local network traffic	(−) Limited features and dataset (−) Hypothetical approach (−) Real DDoS traffic can be a challenge	(+) Requires more sophisticated approach for building model by adding more features set and ML approaches

Table 14 (continued)

Methodology	Data set	Study limitations	Improvement
ANNs based IDS [124]	Raw traffic captured from IoT devices (Bulbs)	(−) Hypothetical proposed model (−) Tested only on Wi-Fi network (−) Experiment is limited to only specific class of IoT devices such as bulbs	(+) Devices diversification issue should be resolved (+) It should be tested on other networks like Zigbee, or Zwabe etc
IoTDePT [166]	Local IoT network traffic	(−) Limited dataset and features	(+) Advanced approach for enhancing the behaviour pattern analysis
ANN approach [108]	UNSW-NB15 Dataset	(−) Threat identification can be issues due to class imbalance and overlapping (−) Accuracy can be improved	(+) More techniques are required for real time traffic
MLP architecture [167]	IoT benign network traffic	(−) Reliability issues against the latest type of threats (−) Limited data set and features (−) Tested in simulated IoT environment	(+) More training required by adding latest threats definitions
ANN based prediction model [120]	DS2OS dataset	(−) This model is tested for single data set (−) Limited features in dataset	(+) More experiments are required for model implementation in real time setup
Bi-directional LSTM RNN approach [116]	UNSW-NB15 Dataset	(−) Class imbalance and overlapping issue in dataset	(+) Data processing and clustering techniques should be employed for building efficient model
Back propagation (BP) Radial basis function (RBF) neural networks [122]	KDD99 dataset	(−) Limited number of attacks are available in dataset	(+) Extension is required for addressing issues in mobile edge servers
Adaptive Particle Swarm Optimization (CNN) [154]	Data collected from Nine IoT devices	(−) Large number of features may affect the model training time (−) More work is required to reduce the heuristic time complexity	(+) Upgrading of proposed framework for including effective features for testing in heterogeneous platforms

Table 15 List of studies using ANNs approaches, dataset and performance metric for IoT DoS/DDoS detection

Ref.	Dataset	Performance evaluation parameters
[117]	NSL-KDD	Accuracy, Recall, No of features
[118]	KDD CUP 1999	Precision, Accuracy, Recall and F_1-score
[17]	DS2OS traffic traces	Accuracy, Precision, Recall and F1-score
[18]	CICIDS2017	Precision, Accuracy and Recall
[19]	Data collected from local network	Accuracy, Specificity, Sensitivity/Recall and Precision
[20]	Bot-IoT	TPR (True Positive Rate), FPR (False positive Rate), Precision, Recall, Accuracy, F1-score
[21]	IoT network-traffic	Precision, Recall, Accuracy, F1-score
[168]	Own	Sensitivity/Recall, Specificity, FPR, FNR, Precision
[111]	Network traffic file	Accuracy, Precision, Sensitivity
[169]	CIDDS-001	Accuracy, Precision, Recall, FPR
[120]	DS2OS traffic traces	Accuracy, Precision, Recall F1-score
[116]	UNSW-NB15 dataset	Accuracy, Precision, Recall, F1-score, Miscalculation rate
[157]	Consumer IoT DoS attack traffic	Accuracy, Precision, Recall, F1-score
[108]	UNSW-15 dataset	Accuracy, Precision, Detection rate, Dataset size, No of attacks
[123]	UCLA Dataset	Accuracy, Detection rate, FPR,FNR, TNR, TPR
[114]	Aegean Wi-Fi Intrusion dataset	Accuracy, Precision, Recall, F-measure
[163]	Own dataset	Accuracy, Precision, Recall, F-measure
[106]	IoT generated dataset	Accuracy, Precision, Recall, F-measure
[170]	Own dataset	Accuracy, Precision, Recall, F-measure
[139]	CICIDS dataset	Accuracy, Precision, Recall, F-measure
[141]	NSL-KDD dataset	Accuracy, Precision, Recall, F-measure, False alarm
[129]	KDD Cup 1999	Accuracy, Detection rate, False alarm rate
[158]	NSL-KDD dataset	Accuracy, Precision, Detection rate, True positive rate, True negative rate, False positive rate, False negative rate
[159]	KDDCUP99 dataset	Precision, Recall, Accuracy, Detection rate, FAR (False alarm rate)
[160]	CICDDoS2019	Accuracy, FAR, Detection rate, Precision
[45]	KDDCUP99 dataset and custom dataset	Accuracy
[161]	VeReMi Extension dataset	Precision, Accuracy, Recall, F1-score
[162]	IoT-Botnet 2020	Precision, Recall, Accuracy, F1-score, True-negative rate (TNR), False alarm rate (FAR), False-negative rate (FNR)

From literature study we have collected the values of accuracy, precision, recall and F1-score for each ANN methods as discussed in Table 15 and the detail is given in Fig. 13.

Among the ANNs methods of detection of threats, that method having higher value of accuracy, precision, recall and F1-score is said to be the best method of detecting DoS/DDoS attacks in IoT-based systems. According to the findings of this study, the architecture presented by Soe et al. [20] is more ideal for detection of DDoS attacks due its higher accuracy, detection rate and precision. This architecture has the advantages over other detection methods like (i) it resolves the issue of data imbalance by using Synthetic Minority Over-Sampling Technique (SMOTE), (ii) it requires very less configuration with ANN and (iii) its resampling techniques enable to extend the detection rate by 100%.

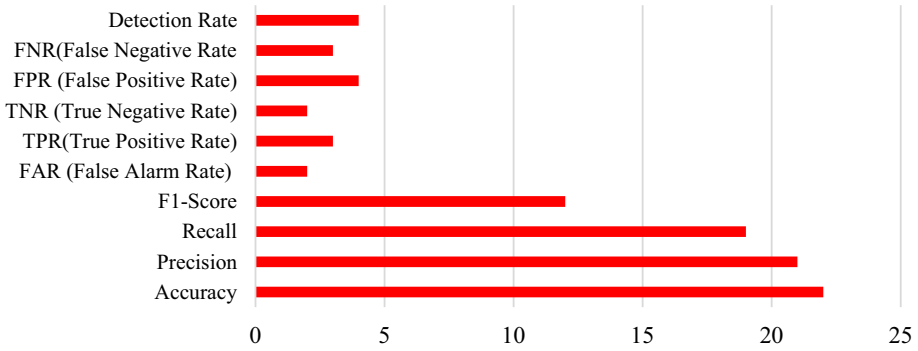

Fig. 12 Number of studies focusing on performance evaluation parameters

Threats to validity

In this section, we have classified the different types of threats related to validity. Validity threats affected the procedure of data extraction and quality assessment of selected studies in this SLR. According to Wohlin et al. [39], there are four categories of validity such as construct validity, internal validity, external validity and conclusion validity. Threats to the different types of validities are discussed below as.

Construct validity

Threats related to forming keywords and search string, formulating research questions, decision regarding the selection of online data sources, building inclusion–exclusion criteria and selection of primary studies towards the validity are discussed. In context of this SLR approach, these threats were diminished such as keywords and search string were formed carefully under the supervision of experts. A pilot search was conducted to refine the search string and check its validity. Research questions were thoroughly checked against the individual search string which were formed for the questions. Online data sources for searching purposes were selected based upon the reliability, authenticity, well-reputation and trust. Inclusion exclusion criteria was thoroughly checked and applied for selection of primary studies. Snowballing and pilot study mitigated the impacts of threats related to construct validity to much extent.

Internal validity

This type of validity is related to the implementation part of SLR design such as data extraction, quality assessment, search terms and search method. Threats related to internal validity were mitigated by performing manual search to validate the search terms and search method. Different versions of search string were formed to get the most desired and relevant results. Threats related to quality assessment were lessened by defining a quality assessment criteria and strictly following criteria for inclusion and exclusion of papers. Based upon a defined scale, each paper was checked against the aggregated value obtained after summation of score for each paper. If, for a particular paper the aggregated score is greater than 2.5 then it was accepted for inclusion in primary studies, otherwise, it was rejected and excluded. After the completion

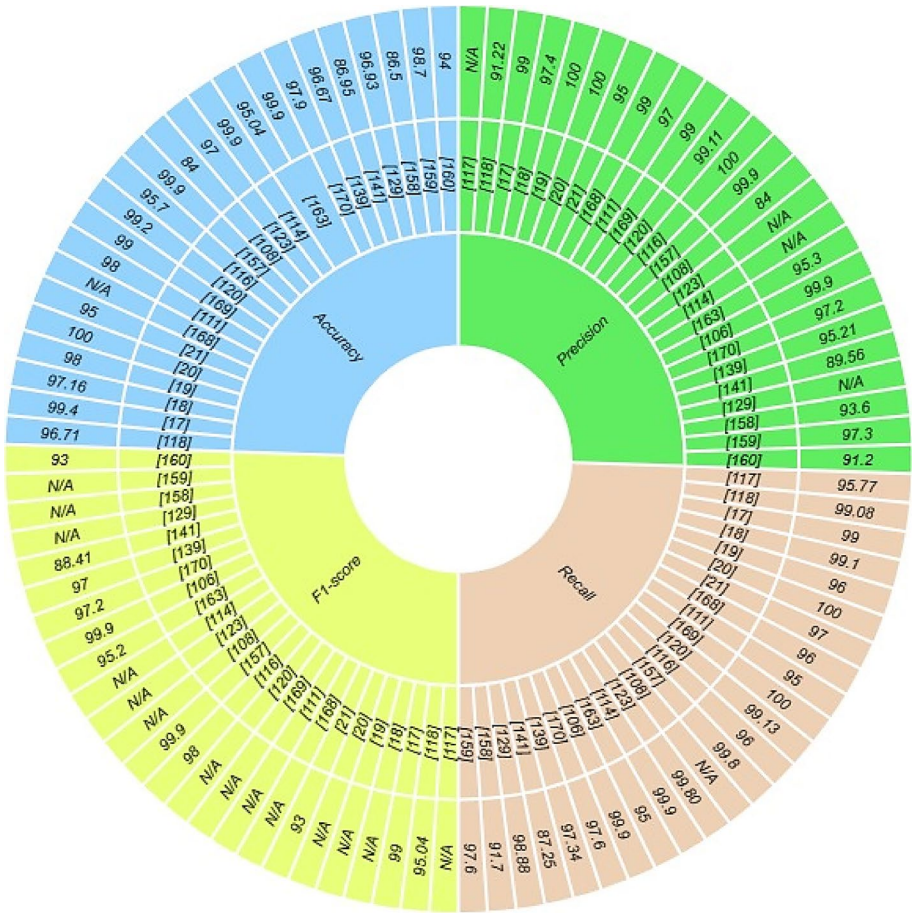

Fig. 13 Performance evaluation parameters comparison of different ANN methods

of quality assessment, those papers were selected in primary studies which answered the research questions.

External validity

External validity is related to the generalization of SLR results, accessibility and database. This validity describes to which level of degree the primary studies are related to the research topic. In context of our research, threats related to external validity are mitigated by running the search query on multiple database sources to refine the search query and reduce the error of subjectivity. The main focus was to remove the redundant and outdated papers. In this way, 143 papers were selected as primary studies to address the research questions.

Conclusion validity

Conclusion validity is about generalizing the finding of our primary studies to the entire literature. It is not possible that all the primary studies are included, there is chance of skipping some papers during the phase of exclusion or failing to identify

such papers relevant to our research questions. To mitigate threats related to this validity, we aimed to focus upon the paper selection process, inclusion–exclusion criteria, quality assessment and snowballing. These steps were performed very carefully and meticulously. Expert's opinions were properly utilized in defining the inclusion exclusion criteria. The main focus was to avoid the element of subjectivity and biasness in the inclusion and exclusion of papers.

Conclusion

The security of IoT is getting a burning topic due to the significant rise of research in this area. The security of IoT is important due to many reasons such as: IoT based systems are vulnerable to various cyber threats due to the nature of devices as they have limited storage, memory, processing and bandwidth capabilities. Therefore, it is important to identify and highlight those security solutions, which provide appropriate and robust ways of handling issues related to IoT. In this regard, machine learning has played an anchor role to uplift IoT security. In the existing literature, IoT security has been analysed by different authors using different machine learning methods. In this paper, we also made effort to elaborate the security of IoT by identifying the approaches and efforts of ANNs. As a compared to the previous works, the security of IoT is investigated in broader sense such as using machine learning but this research work made first attempt to bring upfront the contribution of ANNs towards the security of IoT. The starring role of ANNs for the enhancing the security of IoT has been thoroughly discussed. A complete and in-depth analysis were performed to understand the difference of research gaps between current work and future work The plus side of this work is, it made in-depth analysis by collecting 143 research articles to address the formulated research questions. All these articles were filtered and went through a systematic and organized procedure of quality assessment. All questions were answered in detailed and comprehensive manner. Different approaches, frameworks, techniques, models and methods presented by ANNs were discussed with respect to identified security requirements of IoT. This research identifies the limitations, contributions and suggest improvements for the existing ANNs approaches that are targeted towards IoT security. The ANNs intrusion detection methods for DoS/DDoS attacks in IoT were thoroughly discussed along with the comparative performance analysis of different methods.

The major limitations of this study are that the security requirements or criteria defined in this manuscript are not absolute. It significantly changes from one study to another. Similarly, there is possibility that some of ANNs approaches might be reported by this SLR. In future we are looking forward to identify more security requirements of IoT-based systems operating in different environment. Our future work is also aimed to identify the efforts of other machine learning approaches to address the security requirements of IoT.

Acknowledgements
Not applicable.

Author contributions
YA and HUK wrote manuscript. HUK analyzed and organized the content. MK reviewed the manuscript.

Funding
Open Access funding provided by the Qatar National Library. Qatar National Library, IR CC 2021-001.

Availability of data and materials
All the supporting data and files are shown in this manuscript.

Declarations

Ethics approval and consent to participate
Ethical approval obtained from Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha Qatar. All the authors are providing consent for participating.

Consent for publication
All authors are providing consent for publishing.

Competing interests
The authors declare no competing interests.

Received: 4 February 2023 Accepted: 18 July 2023
Published online: 14 August 2023

References

1. Hameed S, Khan FI, Hameed B. Understanding security requirements and challenges in Internet of Things (IoT): a review. J Comput Netw Commun. 2019. https://doi.org/10.1155/2019/9629381.
2. Gulzar M, Abbas G. Internet of things security: a survey and taxonomy. In 2019 International Conference on Engineering and Emerging Technologies (ICEET), 2019, pp. 1–6.
3. Agatonovic-Kustrin S, Beresford R. Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research. J Pharm Biomed Anal. 2000;22:717–27.
4. Runehov AL, Oviedo L, Azari NP. Encyclopedia of sciences and religions. Dordrecht: Springer Netherlands; 2013.
5. Agarwal N, Agarwal P. Use of artificial neural network in the field of security. MIT Int J Comput Sci Inf Technol. 2013;3:42–4.
6. Abiodun OI, Jantan A, Omolara AE, Dada KV, Mohamed NA, Arshad H. State-of-the-art in artificial neural network applications: a survey. Heliyon. 2018;4: e00938.
7. Kotenko I, Saenko I, Skorik F, Bushuev S. Neural network approach to forecast the state of the internet of things elements. In 2015 XVIII international conference on soft computing and measurements (SCM), 2015, pp. 133–135.
8. Kaminski N, Macaluso I, Di Pascale E, Nag A, Brady J, Kelly M et al. A neural-network-based realization of in-network computation for the Internet of Things. In 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–6.
9. Abdellah AR, Mahmood OAK, Paramonov A, Koucheryavy A. IoT traffic prediction using multi-step ahead prediction with neural network. In 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2019, pp. 1–4.
10. Chauhan M, Prajapati R. Image encryption using chaotic based artificial neural network. Int J Sci Eng Res. 2014;5(6):351. ISSN 2229-5518
11. Belova YP, Mashkina I. Access control system with the authentication mechanism implementation using artificial neural network. J Phys Conf Ser. 2020. https://doi.org/10.1088/1742-6596/1488/1/012025.
12. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Secure computation offloading in blockchain based IoT networks with deep reinforcement learning. arXiv preprint arXiv:1908.07466, 2019.
13. Usman M, Jan MA, He X, Chen J. P2DCA: a privacy-preserving-based data collection and analysis framework for IoMT applications. IEEE J Sel Areas Commun. 2019;37:1222–30.
14. Yao D, Wen M, Liang X, Fu Z, Zhang K, Yang B. Energy theft detection with energy privacy preservation in the smart grid. IEEE Internet Things J. 2019;6:7659–69.
15. Li W, Logenthiran T, Phan V-T, Woo WL. A novel smart energy theft system (SETS) for IoT-based smart home. IEEE Internet Things J. 2019;6:5531–9.
16. Du R, Liu C, Liu F. Trust authorization monitoring model in IoT. Int J Perform Eng. 2018. https://doi.org/10.23940/ijpe.18.03.p6.453462.
17. Hasan M, Islam MM, Zarif MII, Hashem M. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet Things. 2019;7: 100059.
18. Roopak M, Tian GY, Chambers J. Deep learning models for cyber security in IoT networks. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0452–0457.
19. Saied A, Overill RE, Radzik T. Detection of known and unknown DDoS attacks using artificial neural networks. Neurocomputing. 2016;172:385–93.
20. Soe YN, Santosa PI, Hartanto R. DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment. In 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019, pp. 1–5.
21. Thamilarasu G, Chawla S. Towards deep-learning-driven intrusion detection for the internet of things. Sensors. 2019;19:1977.
22. Kaur H, Kang SS, Kapoor N. Optimized artificial intelligence approach based spectrum aware energy efficient routing (SAEER) for device-to-device IoT communication. ISSN: 2277-3878 (Online), 2019;8(1).
23. Cowdrey KWG, Malekian R. Home automation-an IoT based system to open security gates using number plate recognition and artificial neural networks. Multimed Tools Appl. 2018;77:20325–54.
24. Luo T, Nagarajan SG. Distributed anomaly detection using autoencoder neural networks in WSN for IoT. In 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6.

25. Alhajri R, Zagrouba R, Al-Haidari F. Survey for anomaly detection of IoT botnets using machine learning autoencoders. Int J Appl Eng Res. 2019;14:2417–21.
26. Yavuz FY, Devrim Ü, Ensar G. Deep learning for detection of routing attacks in the internet of things. Int J Comput Intell Syst. 2018;12:39–58.
27. Kumar PM, Gandhi U, Varatharajan R, Manogaran G, Jidhesh R, Vadivel T. Intelligent face recognition and navigation system using neural learning for smart security in Internet of Things. Clust Comput. 2019;22:7733–44.
28. Jadel Alsamiri KA. Internet of Things cyber attacks detection using machine learning. Int J Adv Comput Sci Appl. 2019;10:627–34.
29. Albalawi U. A comprehensive analysis on intrusion detection in IoT based smart environments using machine learning approaches. Int J Sci Technol Res. 2020;09:1646–52.
30. Hussain F, Hussain R, Hassan SA, Hossain E. Machine learning in IoT security: current solutions and future challenges. IEEE Commun Surv Tutor. 2020. https://doi.org/10.1109/COMST.2020.2986444.
31. Moh M, Raju R. Machine learning techniques for security of Internet of Things (IoT) and fog computing systems. In 2018 International Conference on High Performance Computing & Simulation (HPCS), 2018, pp. 709–715.
32. Deorankar AV, Thakare SS. Survey on Anomaly Detection of (IoT)-Internet of Things cyberattacks using machine learning. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 115–117.
33. Mahdavinejad MS, Rezvan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP. Machine learning for Internet of Things data analysis: a survey. Digit Commun Netw. 2018;4:161–75.
34. Rasheed Ahmad, Izzat Alsmadi, Machine learning approaches to IoT security: A systematic literature review. Internet of Things 2021;14:100365, ISSN 2542-6605. https://doi.org/10.1016/j.iot.2021.100365.
35. Liao B, Ali Y, Nazir S, He L, Khan HU. Security analysis of IoT devices by using mobile computing: a systematic literature review. IEEE Access. 2020;8:120331–50.
36. Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M. Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw. 2007;80:571–83.
37. Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th international conference on evaluation and assessment in software engineering, 2014, pp. 1–10.
38. Mahdavi-Hezavehi S, Durelli VH, Weyns D, Avgeriou P. A systematic literature review on methods that handle multiple quality attributes in architecture-based self-adaptive systems. Inf Softw Technol. 2017;90:1–26.
39. Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th international conference on evaluation and assessment in software engineering, 2014, p. 38.
40. Alam S, Chowdhury MM, Noll J. Interoperability of security-enabled internet of things. Wireless Pers Commun. 2011;61:567–86.
41. Ammar M, Russello G, Crispo B. Internet of Things: a survey on the security of IoT frameworks. J Inf Secur Appl. 2018;38:8–27.
42. Hossain MM, Fotouhi M, Hasan R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In 2015 IEEE World Congress on Services, 2015, pp. 21–28.
43. Kim H-J, Chang H-S, Suh JJ, Shon T-S. A study on device security in IoT convergence. In 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA), 2016, pp. 1–4.
44. Tarouco LMR, Bertholdo LM, Granville LZ, Arbiza LMR, Carbone F, Marotta M et al. Internet of Things in healthcare: interoperatibility and security issues. In 2012 IEEE international conference on communications (ICC), 2012, pp. 6121–6125.
45. Podder P, Bharati S, Mondal M, Paul PK, Kose U. Artificial neural network for cybersecurity: a comprehensive review. arXiv preprint arXiv:2107.01185, 2021.
46. Al-Garadi MA, Mohamed A, Al-Ali A, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun Surv Tutor. 2020. https://doi.org/10.1109/COMST.2020.2988293.
47. Tahsien SM, Karimipour H, Spachos P. Machine learning based solutions for security of Internet of Things (IoT): A survey. J Netw Computer Appl. 2020;161:102630.
48. Mohanta B, Jena D, Satapathy U, Patnaik S. Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology. Internet of Things 2020;11:100227. https://doi.org/10.1016/j.iot.2020.100227.
49. Restuccia F, D'Oro S, Melodia T. Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet Things J. 2018;5:4829–42.
50. Andročec D, Vrček N. Machine learning for the Internet of Things Security: a systematic. In 13th International conference on software technologies. 2018; 97060. https://doi.org/10.5220/00068.
51. Rana AK, Salau AO, Gupta S, Arora S. A Survey of Machine Learning Methods for IoT and their Future Applications. Amity J Comput Sci. 2018;2(2):1–5. ffhal-01983429.
52. Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, et al. Deep learning and big data technologies for IoT security. Comput Commun. 2020;151:495–517.
53. Cui L, Yang S, Chen F, Ming Z, Lu N, Qin J. A survey on application of machine learning for Internet of Things. Int J Mach Learn Cybern. 2018;9:1399–417.
54. Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P. Network intrusion detection for IoT security based on learning techniques. IEEE Commun Surv Tutor. 2019;21:2671–701.
55. Fahim M, Sillitti A. Anomaly detection, analysis and prediction techniques in iot environment: a systematic literature review. IEEE Access. 2019;7:81664–81.
56. Elrawy MF, Awad AI, Hamed HF. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comput. 2018;7:21.
57. da Costa KA, Papa JP, Lisboa CO, Munoz R, de Albuquerque VHC. Internet of Things: a survey on machine learning-based intrusion detection approaches. Comput Netw. 2019;151:147–57.

58. Alqassem I, Svetinovic D. A taxonomy of security and privacy requirements for the Internet of Things (IoT). In 2014 IEEE International Conference on Industrial Engineering and Engineering Management, 2014, pp. 1244–1248.
59. Xu R, Wendt JB, Potkonjak M. Security of IoT systems: Design challenges and opportunities. In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2014, pp. 417–423.
60. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017, pp. 618–623.
61. Razzaq MA, Gill SH, Qureshi MA, Ullah S. Security issues in the Internet of Things (IoT): a comprehensive study. Int J Adv Comput Sci Appl (IJACSA). 2017;8:383–8.
62. Lee C, Zappaterra L, Choi K, Choi H-A. Securing smart home: Technologies, security challenges, and security requirements. In 2014 IEEE Conference on Communications and Network Security, 2014, pp. 67–72.
63. Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 336–341.
64. Hinduja A, Pandey M. An ANP-GRA-Based Evaluation Model for Security Features of IoT Systems. In Intelligent Communication, Control and Devices, ed: Springer, 2020, pp. 243–253.
65. Diesch R, Pfaff M, Krcmar H. A comprehensive model of information security factors for decision-makers. Comput Secur. 2020; 101747.
66. Chen K, Zhang S, Li Z, Zhang Y, Deng Q, Ray S, et al. Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J Hardw Syst Secur. 2018;2:97–110.
67. Samaila MG, Neto M, Fernandes DA, Freire MM, Inácio PR. Challenges of securing Internet of Things devices: a survey. Secur Privacy. 2018;1: e20.
68. Ziegler S, Crettaz C, Kim E, Skarmeta A, Bernabe JB, Trapero R, et al. Privacy and security threats on the Internet of Things. In: Ziegler S, editor., et al., Internet of Things security and data protection. Cham: Springer International Publishing; 2019. p. 9–43. https://doi.org/10.1007/978-3-030-04984-3_2.
69. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019. https://doi.org/10.1109/JIOT.2019.2935189.
70. Gershenson C. Artificial neural networks for beginners. arXiv preprint cs/0308031, 2003.
71. Chen M, Challita U, Saad W, Yin C, Debbah M. Artificial neural networks-based machine learning for wireless networks: a tutorial. IEEE Commun Surv Tutor. 2019;21:3039–71.
72. Rahman MZ. NeuDetect: A neural network data mining system for wireless network intrusion detection. Electronic Theses and Dissertations. 2009. 8248. https://scholar.uwindsor.ca/etd/8248.
73. Jajodia S, van Tilborg HC. Encyclopedia of cryptography and security. A-K: Springer; 2011.
74. Atamli AW, Martin A. Threat-based security analysis for the internet of things. In 2014 International Workshop on Secure Internet of Things, 2014, pp. 35–43.
75. Chifor B-C, Bica I, Patriciu V-V, Pop F. A security authorization scheme for smart home Internet of Things devices. Futur Gener Comput Syst. 2018;86:740–9.
76. Liu G, Wang X. An integrated intrusion detection system by using multiple neural networks. In 2008 IEEE Conference on Cybernetics and Intelligent Systems, 2008, pp. 22–27.
77. Roohi A, Adeel M, Shah MA. DDoS in IoT: A Roadmap Towards Security & Countermeasures. In 2019 25th International Conference on Automation and Computing (ICAC), 2019, pp. 1–6.
78. Belanger F, Hiller JS, Smith WJ. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. J Strateg Inf Syst. 2002;11:245–70.
79. Park KC, Shin D-H. Security assessment framework for IoT service. Telecommun Syst. 2017;64:193–209.
80. Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the Internet of Things (IoT). In International Conference on Network Security and Applications, 2010, pp. 420–429.
81. Ferrag MA, Maglaras L, Derhab A. Authentication and authorization for mobile IoT devices using biofeatures: recent advances and future trends. Secur Commun Netw. 2019. https://doi.org/10.1155/2019/5452870.
82. Chatterjee B, Das D, Sen S. RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. In 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2018, pp. 205–208.
83. Mondal S, Bours P. A study on continuous authentication using a combination of keystroke and mouse biometrics. Neurocomputing. 2017;230:1–22.
84. Ferdowsi A, Saad W. Deep learning-based dynamic watermarking for secure signal authentication in the Internet of Things. In 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6.
85. Meena G, Choudhary S. Biometric authentication in internet of things: a conceptual view. J Stat Manag Syst. 2019;22:643–52.
86. Das R, Gadre A, Zhang S, Kumar S, Moura JM. A deep learning approach to IoT authentication. In 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6.
87. Shi C, Liu J, Liu H, Chen Y. Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. In Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2017, pp. 1–10.
88. Huang A, Gao S, Nathan A. A user authentication enabled piezoelectric force touch system for the Internet of Things. In: 2020 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS). IEEE; 2020. p. 1–4.
89. McGinthy JM, Wong LJ, Michaels AJ. Groundwork for neural network-based specific emitter identification authentication for IoT. IEEE Internet Things J. 2019;6:6429–40.
90. Reyhani SZ, Mahdavi M. User authentication using neural network in smart home networks. Int J Smart Home. 2007;1:147–54.
91. Bazrafkan S, Corcoran P. Enhancing iris authentication on handheld devices using deep learning derived segmentation techniques. In 2018 IEEE international conference on consumer electronics (ICCE), 2018, pp. 1–2.

92. Ahmed AAE, Traore I. A new biometric technology based on mouse dynamics. IEEE Trans Depend Secure Comput. 2007;4:165–79.
93. Ahmed AA, Traore I. Biometric recognition based on free-text keystroke dynamics. IEEE Trans Cybern. 2013;44:458–72.
94. Chauhan M, Prajapati R. Image encryption using chaotic cryptosystems and artificial neural network cryptosystems: a review. Int J Sci Eng Res. 2014;5(5):52 ISSN 2229-5518
95. Rarhi K, Saha S. Image encryption in IoT devices using DNA and hyperchaotic neural network. In: Das SK, Samanta S, Dey N, Kumar R, editors. Design frameworks for wireless networks. Singapore: Springer Singapore; 2020. p. 347–75. https://doi.org/10.1007/978-981-13-9574-1_15.
96. Khari M, Garg AK, Gandomi AH, Gupta R, Patan R, Balusamy B. Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Trans Syst Man Cybern Syst. 2019;50:73–80.
97. Saraswat P, Garg K, Tripathi R, Agarwal A. Encryption algorithm based on neural network. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1–5.
98. Pacheco J, Benitez VH, Pan Z. Security framework for IoT end nodes with neural networks. Int J Mach Learn Comput. 2019;9:381–6.
99. Outchakoucht A, Hamza E, Leroy JP. Dynamic access control policy based on blockchain and machine learning for the internet of things. Int J Adv Comput Sci Appl. 2017;8:417–24.
100. Chu M, Li H, Liao X, Cui S. Reinforcement learning-based multiaccess control and battery prediction with energy harvesting in IoT systems. IEEE Internet Things J. 2018;6:2009–20.
101. Murugesan R. "Artificial Neural Network Based Prediction Mechanism for Wireless Network on Chips Medium Access Control". Thesis. Rochester Institute of Technology. 2017.
102. Bryliuk D, Starovoitov V. Access control by face recognition using neural networks. Institute of Engineering Cybernetics, Laboratory of Image Processing and Recognition. 2002; 4.
103. Thangaramya K, Kulothungan K, Logambigai R, Selvi M, Ganapathy S, Kannan A. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. Comput Netw. 2019;151:211–23.
104. Priya S, Srivastava A, Jindal SK, Sahoo SK. Design and implementation of a smart energy meter based on Internet of Things and neural network approach. In Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018, pp. 26–27.
105. Kamat SS. Analyzing Radial Basis Function Neural Networks for predicting anomalies in Intrusion Detection Systems (Dissertation). 2019, Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-259187.
106. Ge M, Fu X, Syed N, Baig Z, Teo G, Robles-Kelly A. Deep Learning-Based Intrusion Detection for IoT Networks. In 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 2019, pp. 256–25609.
107. Putchala MK. "Deep Learning Approach for Intrusion Detection System (IDS) in the Internet of Things (IoT) Network using Gated Recurrent Neural Networks (GRU)" (2017). Browse all Theses and Dissertations. 1848. https://corescholar.libraries.wright.edu/etd_all/1848.
108. Hanif S, Ilyas T, Zeeshan M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. In 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), 2019, pp. 152–156.
109. Hodo E, Bellekens X, Hamilton A, Dubouilh P-L, Iorkyase E, Tachtatzis C et al. Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC), 2016, pp. 1–6.
110. Canedo J, Skjellum A. Using machine learning to secure IoT systems. In 2016 14th annual conference on privacy, security and trust (PST), 2016, pp. 219–222.
111. Shenfield A, Day D, Ayesh A. Intelligent intrusion detection systems using artificial neural networks. ICT Express. 2018;4:95–9.
112. Almiani M, AbuGhazleh A, Al-Rahayfeh A, Atiewi S, Razaque A. Deep recurrent neural network for IoT intrusion detection system. Simul Model Pract Theory. 2020;101: 102031.
113. Lopez-Martin M, Carro B, Sanchez-Esguevillas A, Lloret J. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot. Sensors. 2017;17:1967.
114. Rezvy S, Luo Y, Petridis M, Lasebae A, Zebin T. An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks. In 2019 53rd Annual Conference on Information Sciences and Systems (CISS), 2019, pp. 1–6.
115. Anitha AA, Arockiam L. ANNIDS: artificial neural network based intrusion detection system for Internet of Things. Int J Innov Technol Explor Eng IJITEE. 2019. https://doi.org/10.35940/ijitee.K1875.0981119.
116. Roy B, Cheung H. A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018, pp. 1–6.
117. Subba B, Biswas S, Karmakar S. A neural network based system for intrusion detection and attack classification. In 2016 Twenty Second National Conference on Communication (NCC), 2016, pp. 1–6.
118. Wang G, Hao J, Ma J, Huang L. A new approach to intrusion detection using artificial neural networks and fuzzy clustering. Expert Syst Appl. 2010;37:6225–32.
119. Evmorfos S, Vlachodimitropoulos G, Bakalos N, Gelenbe E. Neural network architectures for the detection of SYN flood attacks in IoT systems. In Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments, 2020, pp. 1–4.
120. Latif S, Zou Z, Idrees Z, Ahmad J. A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network. IEEE Access. 2020;8:89337–50.
121. Brun O, Yin Y, Gelenbe E, Kadioglu YM, Augusto-Gonzalez J, Ramos M. Deep learning with dense random neural networks for detecting attacks against iot-connected home environments. In International ISCIS Security Workshop, 2018, pp. 79–89.
122. Wu D, Yan J, Wang H, Wang R. Multiattack Intrusion Detection Algorithm for Edge-Assisted Internet of Things. In 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 210–218.

123. Chang T-Y, Hsieh C-J. Detection and analysis of distributed denial-of-service in internet of things—employing artificial neural network and Apache spark platform. Sens Mater. 2018;30:857–67.
124. Khatun MA, Chowdhury N, Uddin MN. Malicious Nodes Detection based on Artificial Neural Network in IoT Environments. In 2019 22nd International Conference on Computer and Information Technology (ICCIT), 2019, pp. 1–6.
125. Lopez-Martin M, Carro B, Sanchez-Esguevillas A, Lloret J. Network traffic classifier with convolutional and recurrent neural networks for Internet of Things. IEEE Access. 2017;5:18042–50.
126. Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, et al. N-baiot—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018;17:12–22.
127. HaddadPajouh H, Dehghantanha A, Khayami R, Choo K-KR. A deep recurrent neural network based approach for internet of things malware threat hunting. Futur Gener Comput Syst. 2018;85:88–96.
128. Al-Zewairi M, Almajali S, Awajan A. Experimental evaluation of a multi-layer feed-forward artificial neural network classifier for network intrusion detection system. In 2017 International Conference on New Trends in Computing Sciences (ICTCS), 2017, pp. 167–172.
129. Kim J, Kim J, Thu HLT, Kim H. Long short term memory recurrent neural network classifier for intrusion detection. In 2016 International Conference on Platform Technology and Service (PlatCon), 2016, pp. 1–5.
130. Khamidov B, Urmanov S, Abdukhamidov E, Bakhodirov J. Internet of Things: A security overview. 2019. https://doi.org/10.13140/RG.2.2.29288.72963/1.
131. Sun Y, Lo B. An artificial neural network framework for gait-based biometrics. IEEE J Biomed Health Inform. 2018;23:987–98.
132. Barros A, Rosário D, Resque P, Cerqueira E. Heart of IoT: ECG as biometric sign for authentication and identification. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 307–312.
133. Lee S, Mun C, Lee O. A study of neural network based IoT device information security system. J Theor Appl Inf Technol. 2018;96:7406–14.
134. Osueke TT. Detecting Brute-Force Attack in IoT Device using Network Flow Data. Dublin, National College of Ireland, 2018.
135. Wang Y, Yang H, Wang X, Zhang R. Distributed intrusion detection system based on data fusion method. In Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No. 04EX788), 2004, pp. 4331–4334.
136. Noaman KM, Jalab HA. Data security based on neural networks. Task Q. 2005;9:409–14.
137. Singh A, Sharma G. Intrusion detection using neural network techniques. Int J IT Knowl Manag. 2008;1:79–84.
138. Chauhan J, Seneviratne S, Hu Y, Misra A, Seneviratne A, Lee Y. Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks. Computer. 2018;51:60–7.
139. Manimurugan S, Al-Mutairi S, Aborokbah MM, Chilamkurti N, Ganesan S, Patan R. Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network. IEEE Access. 2020;8:77396–404.
140. Agrawal R, Verma P, Sonanis R, Goel U, De A, Kondaveeti SA et al. Continuous security in IoT using Blockchain. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 6423–6427.
141. Li Y, Xu Y, Liu Z, Hou H, Zheng Y, Xin Y, et al. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. Measurement. 2020;154: 107450.
142. McDermott CD, Majdani F, Petrovski AV. Botnet detection in the internet of things using deep learning approaches. In 2018 international joint conference on neural networks (IJCNN), 2018, pp. 1–8.
143. Abbass W, Bakraouy Z, Baïna A, Bellafkih M. Classifying IoT security risks using deep learning algorithms. In 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), 2018, pp. 1–6.
144. Banerjee N, Giannetsos T, Panaousis E, Took CC. Unsupervised learning for trustworthy IoT. In 2018 IEEE international conference on fuzzy systems (FUZZ-IEEE), 2018, pp. 1–8.
145. Aversano L, Bernardi ML, Cimitile M, Pecori R. A systematic review on deep learning approaches for IoT security. Comput Sci Rev. 2021;40: 100389.
146. Abbasi F, Naderan M, Alavi SE. Anomaly detection in Internet of Things using feature selection and classification based on logistic regression and artificial neural network on N-BaIoT dataset. In 2021 5th International Conference on Internet of Things and Applications (IoT), 2021, pp. 1–7.
147. Teodoro AA, Gomes OS, Saadi M, Silva BA, Rosa RL, Rodríguez DZ. An FPGA-based performance evaluation of artificial neural network architecture algorithm for IoT. Wirel Pers Commun. 2021. https://doi.org/10.1007/s11277-021-08566-1.
148. Liu Y, Wang K. Trust control in heterogeneous networks for Internet of Things. In 2010 International conference on computer application and system modeling (ICCASM 2010), 2010, pp. V1-632–V1-636.
149. Choi D, Lee K. An artificial intelligence approach to financial fraud detection under IoT environment: a survey and implementation. Secur Commun Netw. 2018;2018:15.
150. Moreno-Cano M, Zamora-Izquierdo MA, Santa J, Skarmeta AF. An indoor localization system based on artificial neural networks and particle filters applied to intelligent buildings. Neurocomputing. 2013;122:116–25.
151. Bhavani N, Sujatha K. Intelligent estimation of NO emissions by flame monitoring in power x station using Internet of Things. ARPN J Eng Appl Sci. 2006;12:6677–88.
152. Chiuchisan I, Geman O. An approach of a decision support and home monitoring system for patients with neurological disorders using internet of things concepts. WSEAS Trans Syst. 2014;13:460–9.
153. Wu X, Wu J, Cheng B, Chen J. Neural network based situation detection and service provision in the environment of IoT. In 2013 IEEE 78th Vehicular Technology Conference (VTC Fall), 2013, pp. 1–5.
154. Kan X, Fan Y, Fang Z, Cao L, Xiong NN, Yang D, et al. A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network. Inf Sci. 2021;568:147–62.
155. Hwang R-H, Peng M-C, Huang C-W. Detecting IoT malicious traffic based on autoencoder and convolutional neural network. In 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–6.
156. Irum A, Khan MA, Noor A, Shabir B. DDoS detection and prevention in internet of things. EasyChair. 2020 Jan 29(2486):1–7. https://easychair.org/publications/preprint/kPlm.

157. Doshi R, Apthorpe N, Feamster N. Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE Security and Privacy Workshops (SPW). 2018. IEEE. https://doi.org/10.1109/spw. pp. 29–35.
158. Huda S, Miah S, Yearwood J, Alyahya S, Al-Dossari H, Doss R. A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. J Parallel Distrib Comput. 2018;120:23–31.
159. Zhang Y, Li P, Wang X. Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access. 2019;7:31711–22.
160. Almiani M, AbuGhazleh A, Jararweh Y, Razaque A. DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. Int J Mach Learn Cybern. 2021;12:3337–49.
161. Alladi T, Agrawal A, Gera B, Chamola V, Sikdar B, Guizani M. Deep neural networks for securing IoT enabled vehicular ad-hoc networks. In ICC 2021-IEEE International Conference on Communications, 2021, pp. 1–6.
162. Ahmad Z, Shahid Khan A, Nisar K, Haider I, Hassan R, Haque MR, et al. Anomaly detection using deep neural network for IoT architecture. Appl Sci. 2021;11(15):7050. https://doi.org/10.3390/app11157050.
163. Chawla S. Deep learning based intrusion detection system for Internet of Things. 2017. Thesis (Master's)--University of Washington, 2017-06. retrieved from http://hdl.handle.net/1773/39829.
164. Vishwakarma R, Jain AK. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst. 2020;73:3–25.
165. Gao Y, Wu H, Song B, Jin Y, Luo X, Zeng X. A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. IEEE Access. 2019;7:154560–71.
166. Rattanalerdnusorn E, Pattaranantakul M, Thaenkaew P, Vorakulpipat C. IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT environment. In Proceedings of the 2020 9th International Conference on Software and Computer Applications, 2020, pp. 232–236.
167. Ahanger TA. Defense scheme to protect IoT from cyber attacks using AI principles. Int J Comput Commun Control. 2018;13:915–26.
168. Wani A, Revathi S. DDoS detection and alleviation in IoT using SDN (SDIoT-DDoS-DA). J Inst Eng Ser B. 2020;101(2):117–28. https://doi.org/10.1007/s40031-020-00442-z.
169. Tama BA, Rhee K-H. Attack classification analysis of IoT network via deep learning approach. Res Briefs Inf Commun Technol Evol (ReBICTE). 2017;3:1–9.
170. Ravi N, Shalinie SM. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet Things J. 2020;7:3559–70.

Publisher's Note