Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 7, 2025

A DEEP LEARNING APPROACH FOR SECURING IOT SYSTEMS WITH CNN-BASED PREDICTION OF WORST-CASE RESPONSE TIME

Muhammad Usman Javeed[*1], Hafiza Ayesha Sadiqa[2], Mahrukh Jaffar[3], Shafqat Maria Aslam[4], Muhammad Khadim Hussain[5], Zeeshan Raza[6], Muhammad Azhar[7]

[*1,2,5,6]*Department of Computer Science, COMSATS University of Islamabad, Sahiwal, Pakistan*
[3]*Department of Computer Science, Superior University Lahore, Lahore, Pakistan*
[4]*School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi, China*
[7]*Department of Applied Data Science, Hong Kong Shue Yan University, SAR, China*

[*1]usmanjavveed@gmail.com

DOI: https://doi.org/10.5281/zenodo.15844934

Keywords
IoT, Deep learning, Convolutional Neural Network, Security, Response Time

Article History
Received: 02 April, 2025
Accepted: 23 June, 2025
Published: 09 July, 2025

Corresponding Author: *
Muhammad Usman Javeed

Abstract

The global industry and AI have promoted the development of the diversified intelligent applications. Because of large number of devices getting associated and controlled with remote framework, there is a lot massive safety concerns are rising. In order to maximize real-time intrusion detection in the context of the Internet of Things, this article suggests an advanced CNN secure framework. This paper concentrated on the security of web of things, security in term of our IOT gadgets framework usage, for mapping our framework in this study we used a Convolutional Neural Network which help us to characterize our framework. In order to enhance the security and functionality of Internet of Things (IoT) systems, this study proposes a unique framework that blends real-time task modeling with a Convolutional Neural Network (CNN). In a distributed networked control environment, we evaluate system behavior by looking at CPU usage, job scheduling, and execution time. For reliable data transfer, tasks are evaluated in terms of their worst-case execution time (WCET), deadline restrictions, and release jitter. In order to detect any deadline breaches early on, a CNN is used to estimate the worst-case response time (WCRT) of tasks before they are executed. Experimental findings show that the CNN achieved an average prediction error of less than 3% and that all jobs were completed within the deadline. The suggested architecture provides a dependable, clever method to improve task stability and predictability in time-sensitive Internet of Things applications.

INTRODUCTION

Deep learning also known as deep structure learning is a subfield of AI. Its utilization deep neural system, because of the utilization of deep neural system its known as deep learning[1]. The calculation utilized for deep learning process follow the structure of mind and furthermore adjust the usefulness of cerebrum which is known as counterfeit neural network [2].Different sort of deep learning models can be applied in various fields for various purposes[3].The innovation of deep learning follow the fake neural system, these fake neural system utilize huge informational index for preparing reason to upgrade the procedure of training[4].

Development of deep learning calculation comprise on association of layers[1].

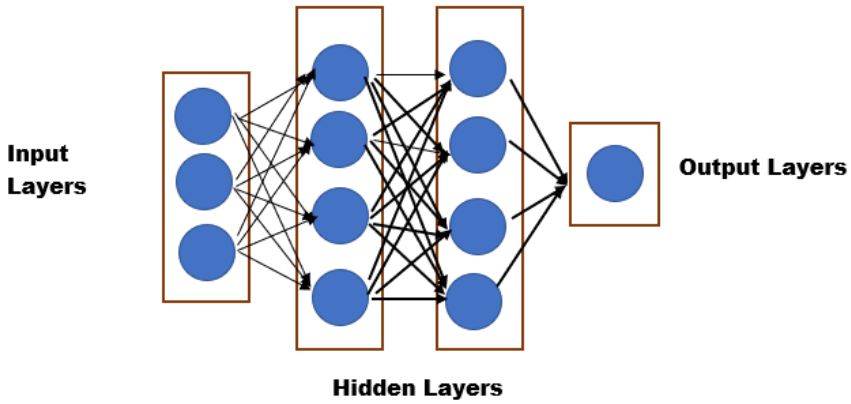

Figure 1. Layers of Neural Network

As Shown in figure 1, there are three layers input layer, hidden layer and output layer which are used to make the algorithms of deep learning. Layers among info and yield layer which known as concealed layer comprise on assortment of neurons, that neurons in shrouded layers associated with each other[1]. Ongoing examination in the field of deep learning show that the utilization of deep learning increment step by step like its utilization in various field, for example, its utilization for instructive reason, utilized in the field of medicinal services, utilized in industry and so on [5].

Deep learning use for various purposes like its utilization ongoing include show, utilized for recognizing companions tag in photographs, utilized for deciphering content on a site page. Its additionally utilized by organizations like deep learning use for extortion identification in charge card organizations, so we can said that now days we have boundless utilization of deep learning[6].Deep learning use for a huge scope for design location, for forms robotization, and for comprehending diverse problems[6]. Later an enormous an improvement in the field of data innovation, wherein web of things have to a great extent surpassed the customary view of encompassing condition, the innovation of IoT upgrading step by step and assume a significant job today in each individual life[7]. The innovation of correspondence and web innovation driving people towards virtual world. Innovation of Web of thing is currently one of the most famous innovation which help people from multiple points of view to make their life simple as far as playing out their every day task in productive way, IoT changes the human life ways. IoT innovation equipped for evaluating, gathering and understanding natural elements. So its play an imperative to make a correspondence among people and things, So it make workable for brilliant urban communities implementation[8]. In PC history IoT is quickest developing innovation. Figure 2 shows that the expected number of IoT devices in 2030 is over 40 million [9].

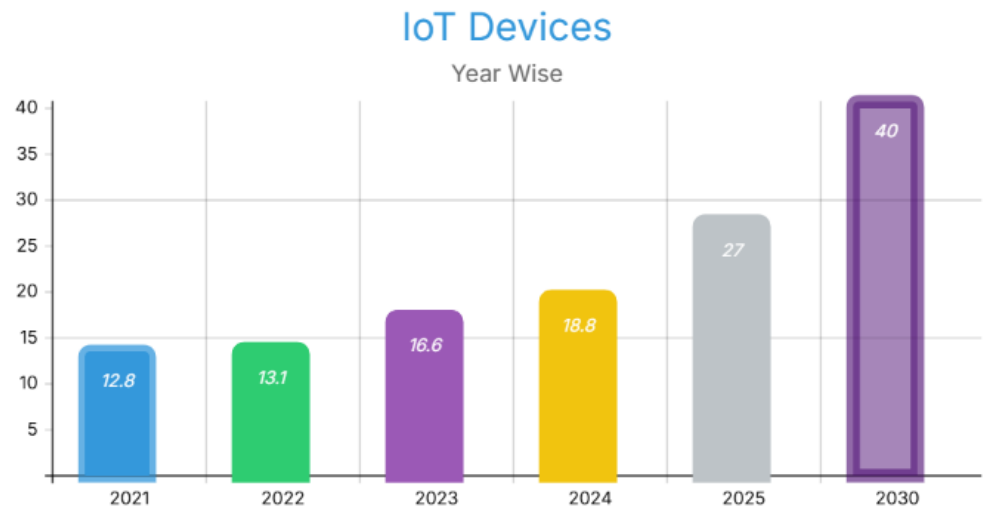

Figure 2. IoT Devices breakdown year wise

Figure 3 shows the engineering of web of things. which comprise on four layers observation , arrange backing and application layer, and show the security dangers in square, and in other square show the arrangement of security dangers

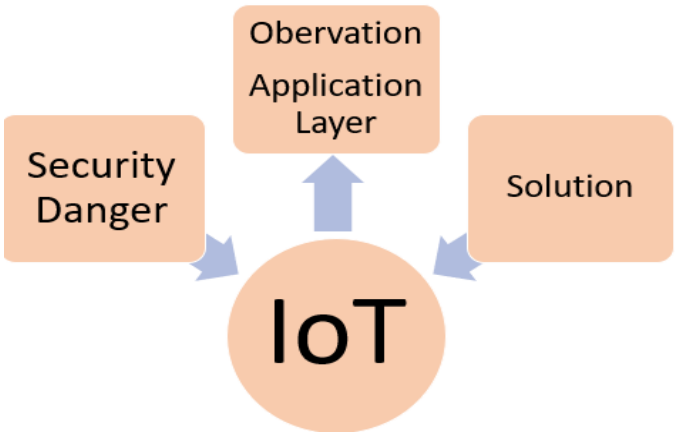

Figure 3. IOT Design

Web of things assess with the progression of time and how they associated with one another, Fig 3 comprise on an alternate kind of web of things , which utilized in various fields to satisfy their particular prerequisite. The innovation of IoT assume a significant job in term of expanding shrewd application for down to earth life, as give a savvy application to instructive reason, give brilliant application in the field of medicinal services , give keen application to transportation and brilliant home. Because of expansive quintessence of IoT innovation new security challenges developed among these frameworks.

Its difficult to dealing with the security prerequisites for IoT frameworks on a more extensive scale because of the multifaceted nature of IoT framework. Web of things gadgets face terrible inherent security because of impediment on capacity of calculation and furthermore because of littler limit. There is more odds of assaults when association between web of things gadgets increment step by step. Update oftentimes old or customary framework is troublesome that requires a great deal

of time to perform such activities, because of these reasons it's hard to execute conventional framework on implanted frameworks[34-35]. For fulfilling security necessities arrangement should comprise on thorough issues. In IoT innovation gadgets associated through remote system, so there is an odds that an unapproved individual can get to individual data. Because of constrained force supplies and restricted capacity of calculation IoT gadgets can't bolster complex structure of security[10]. Higher security hazard in IoT framework when contrasted with different frameworks of figuring, and existing strategy not productive for IoT systems[11]. Gigantic measure of significant information produced through IoT stage, if the information not dissected and transmitted in a safe manner so there is an odds of inconvenience may happen due protection understanding. Existing technique utilized for IoT framework security need to alter , on the grounds that the arrangement of IoT are congenial globally[12] , so its basic to give effective strategy to IoT Security. For checking the security of web of things models can be structured which help us in term of anticipating the conduct of framework security is it ordinary or irregular, For IoT security learning base strategy created by Al-Garadi [36], he made point by point overview on this technique. Web of things gadgets are planned in genuine application, for example, adaption of independent framework when for certain time length it's unnoticed, during preparing of the model these procedures considered. At the point when peculiarities conduct perceived then organization of framework can be refreshed. For web of things security inconsistency location assume a significant job, since it's not interest for any uncommon gadgets establishment in organize and furthermore not interest for whatever else which consider as an overwhelming. Insights of framework can be gathered utilizing Programming interface which is associated with gadgets of IoT. There is a wide application accessible for irregularity which depends on insights of the framework.

I. LITERATURE REVIEW:

The best test for web of things is accomplishing security. Web of things equipped for giving the incredible future in term of giving progressively most prominent innovation, and yet there is additionally a couple of impediment of gadgets which is associated with web and the measure of associated gadgets to web step by step, so there is emerge a significant issue for information security, if there is no security of information, there is nothing remain beneficial.Various overviews led by barely any analysts on web of things security in term of giving helpful manual for fathoming the issue of poor existing security strategies, and furthermore give likely arrangement to web of things security[13]. Various studies results call attention to various sort of security challenges for web of things[14], similar to challenges in get to control, challenges in encryption, challenges in validation, challenges in application security and system security[15]. Overview sorted out on recognition of interruption in web of things by [16]. Specialists center around Security of web of things subsequent to surveying the issues and the arrangement of the correspondence arrangement of web of things[17].Weber underline on Web of things security system, in term of is that structure satisfy the ideal prerequisites of security and protection for web of things[18]. In the wake of leading studies specialists discover distinctive sort of issues in IoT framework like security issues and assaults of payoff aware[18]. Lopez, Roman and Zhou concentrated on appropriated web of things frameworks security and protection, and furthermore these analysts center around advantages of circulated framework in term of settling protection and security issues of web of things[19]. Various analysts direct studies and stress on AI and information mining systems in term of giving cybersecurity[33]. These reviews principally center around digital space security. Creators of this paper [20] center around the executives of security for web of things, creator give the insight concerning the correspondence of machine to machine in term of utilizing object traits which known as powerful or static, sensors distinguished by the dynamic and static really put away in the name, focal point of this paper is to machine to machine transmission, security and sensor. Creators center around right now [21]about security and protection issue of IoT, through system and detecting gadgets people groups can interface with web at whatever point they need, and any place they need, and furthermore characterize IoT application and its engineering.

Creators [22]right now on coming ideas in the market for security. Most significant play in the arrangement of security is tactile. Most easiest procedure is remote security since its establishment is simple, its assume significant job for the security arrangement of home. Be that as it may, its additionally have weakness ,its costly, its execution is troublesome, and its likewise extremely mind boggling.

Cryptography use for low force sensor arrange security there is a great deal of research on it. Barely any specialist center around this issue through helpful figure content implementation[23], there is additionally extraordinary term use for this like best in class cryptographic calculation usage use FPGA and ASIC for improvement of security. Be that as it may, these procedures likewise have two kind of problems.one is during conveyance key and transmission face overhead and also high force adversaries vulnerabilities. For guaranteeing that the correspondence between IoT gadgets approved and solid or not , conventions characterize for the Pile of web of things characterize which comprise on different layers, it's a procedure which use for the various conventions usage on transmission control convention or web convention stack at each layer. However, it's insufficient utilizing convention for correspondence alone to ensure gadgets on organize.

Definite review on web of things made by Abdul-Ghani in which he additionally portrayed about physical assaults and digital assaults . Insights of framework affected by digital assaults, similar to arrange traffic create variation from the norm when sestive information got to by unapproved way, strange properties when aggressor use devices to discover port which is feeble on organize.

For arrange which is remote sensor a framework proposed by Da silva which depends on interruption discovery, however to cover assaults which is various it's a test to pick this framework, on the grounds that quite possibly assaults not weel sum up. For IoT a framework exceptionally structured which is utilized for interruption identification ,this light weight framework proposed by Raza, for IoT organize a firewall planned which is appropriated and furthermore light weight. Proposed framework by them use for explicit sort assault identification on the layer of system.

II. METHODOLOGY:

A. CPU Use Model:

Use of CPU known as the total work oversaw by focal handling unit, CPU usage model additionally utilized for checking the exhibition of our framework, CPU use can be distinctive use of CPU rely upon the amount of processing task, since hardly any errand require gigantic CPU time, and barely any require less time of CPU. CPU usage otherwise called handling time, mean CPU required a period for preparing PC program directions [24].

Scarcely any specialist utilize composite model method for forecast of use of CPU base on investigation of time arrangement. Scientist center around framework productivity in term of weighting. Effectiveness of framework in term of weighting mean forecast result is precise, yet because of a ton issues its hard to plan such framework [25]. Table 1. explains the symbols used in this model with their descriptions.

Table 1. Symbol Descriptions

Symbol	Description
BL	Worst-case blocking time
W	WCET (Worst-case execution time)
DL	Deadline of the task
T	Interference time
RJ	Release jitter
No	Number of tasks in the system
PA	Task priority
RT	Worst-case response time
MT	Minimum time between task releases (task period)
UT	Task utilization (C/T)

We used a topographically spread colossal control framework with a great deal of actuators and sensors, actuators and sensors not associated with one another legitimately rather than that sensors and actuators are put on areas that are genuinely extraordinary. Control signal spoke to by "w" and estimation spoke to by "z" .control signs and estimation are gotten after gone over the system. State gauge "y" produce when estimation are passed to state estimator. We adhere to IEEE standard 802.15.4 to confirm that our transmission is fruitful transmission towards the actuator. Result of transmission is "u" and the state estimator and controller mindful of the results. Different superframes are upheld by IEEE standard 802.15.4. Controller figure the actuator flags that at time "ti" quantifies so its applied fundamentally to our errand at time "ti+1" when we taken next estimation. Control inputs are determined at time "ti" by the controller that we applied to our assignment at time "ti+1". In the event that at time "ti" estimator doesn't have any data , controller get expectations rather at time "ti+1" that rely upon the state at time ti, y(ti+1|ti). For fruitful transmission we use endorsement so its vital for estimator to mindful of the transmission effective rate in term of that control signals are transmitted effectively or not. We have a partition principal[24]. By anticipating that we have state criticism we can plan controller and afterward dislodge it with the express that evaluated y(ti|ti-1). We expect actuator planning just, so we consider all sensors esteems are transmitted in each instance[26]. The state of our task is given by Eq (1) and the output is given by Eq (2).

$y(ti+ 1) = Ay(ti) + B \hat{} w(ti) + \omega(ti), ti \in N$ (1)

$z(ti) = Wy(ti) + \nu(ti)$ (2)

B. Undertaking Model:

In task model we define variables of task , mean the variable we use to perform our task, we give complete description about each task in term of it's working. So here is task model value: BL denote Worst-case blocking time for the task ,W denote Worst-case computation time (WCET) of the task, DL denote Deadline of the task, T denote The interference time of the task, RJ denote Release jitter of the task ,No denote Number of tasks in the system, PA denote Priority assigned to the task (if applicable), RT denote Worst-case response time of the task, MT denote Minimum time between task releases, jobs, (task period), UT denote The utilization of each task (equal to C/T), a-z denote The name of a task. Each task have its own worst-case execution time. Based on task period assign each task a unique priority, priority of task is high when the task period is shorter. For k and l task

MTk < MTl => PAk> PAl

(3)

We are breaking down reaction time, here we have condition, where "I" is a most pessimistic scenario reaction time, right off the bat we determined R and afterward check with its cutoff time, and I is the impedance [27].

$RT_k \leq DL_k$ (4)

$RT_k = W_k + T_k$ (5)

Each higher need task l will execute ordinarily during RT:

Number of release=$\lceil \frac{RTk}{MTl} \rceil$ (6)

Total interference is:

$\lceil \frac{RTk}{MTl} \rceil C_j$ (7)

Condition of reaction time: right now) is the assignments set that have higher need as contrast with task I. $RT_k = W_{k+} \sum_{l \epsilon hpa(k)} \lceil \frac{RTk}{MTl} \rceil W_l$ (8)

Set tasks with DL<MT:

If DL=MT, so rate monotonic order of priority is optimal.

If DL<MT, monotonic deadline order of priority is optimal.

DLk < DLl => PAk >PAl (9)

Examination dependent on usage just for DL=MT sets of undertaking. On the off chance that the errand set is comply with its time constraint so's mean its breeze through usage assessment.

$$UT = \sum_{k=1}^{N} \frac{Wk}{MTk} \leq No(21/No - 1) \quad (10)$$

C. Convolutional neural network:

Convolutional Neural Network system is a calculation of deep learning [31-32]. Much lower preprocessing required for CNN system as contrast

with different calculations that utilized for arrangement [28]. CNN learn highlights of pictures and afterward work with pixels and utilize little square as contribution for this reason [29-30]. At the point when our errand run for first time so we compute most pessimistic scenario execution time of our assignment , our target of utilizing CNN system to foresee the most pessimistic scenario execution time of our undertaking, its mean we need to think about the execution of our assignment before it's execution, if the CNN help us for expectation so its mean we accomplish our goal.

Right now use CNN system for playing out our undertaking, we need to think about cost condition of our assignment, really cost is a normal contrast b/w yield of real right yield and yield of neuron. In this study input and output is shown as Figure 4.

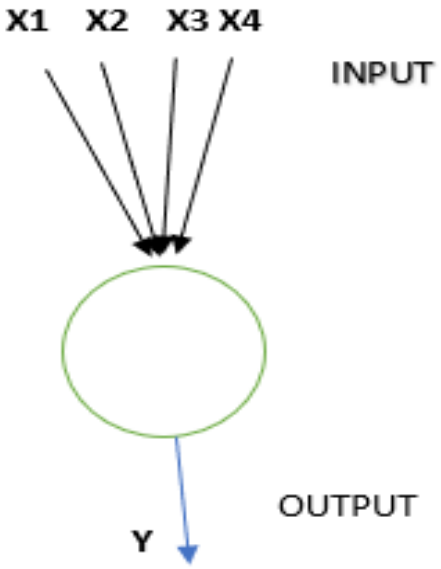

Figure 4 Input and output of model

Procedure of learning: here x, y realized qualities mean info esteems for learning, and p, j obscure qualities which indicate the educated parameter of yield**.**

$z=\sigma(\sum k + pak.yk+l)$ (11)

Here we have cost condition, cost is a normal contrast b/w yield of real right yield and yield of neuron. P speak to need of our undertaking, T speak to jitter, jitter mean the varieties between one time cut of our assignment to some other time cut of our errand, we will likely limit jitter. Zn speak to current most pessimistic scenario reaction time and Z′n speak to next most pessimistic scenario reaction time, we can anticipate next most pessimistic scenario reaction time base on the past most pessimistic scenario reaction time. N speak to add up to number of task[30].Solution is best when the expense is most minimal, that is the reason our objective is insignificant (pa,l).

$$W(pa,l) = \frac{1}{2N}\sum_{n} ||Zn - Z'n||2 \quad (12)$$

When the derivative is zero , function is at minimal point.

$$aW(pa,l) = \frac{2}{2N}\sum_{n} ||Zn - Z'n||.(azn) \quad (13)$$

Method to discover subordinate zero, as scientifically need N> num(p)but when stacked its unrealistic and furthermore utilized credulous iterative methodology, in which we start from an arbitrary position and attempt to make sense of little blend of Δp to min c,and if num(p) huge so an excess of mix and checks, and furthermore use angle plunge.

III. RESULTS

Before starting task execution, we used a Convolutional Neural Network (CNN) to forecast the tasks' worst-case reaction time (WCRT). The

CNN model effectively generalized to unseen task inputs after being trained on historical execution time data. There was very little prediction error when comparing the anticipated values to the worst-case real values. Table 2 and Figure 5 shows the comparison of actual and predicted WCRT in ms (milliseconds) over three different tasks.

Table 2. Comparison of predicted vs actual WCRT

Task	Actual WCRT (ms)	Predicted WCRT (ms)	Error (%)
1	14	13.6	2.85%
2	10.8	11	1.85%
3	17.2	17.6	2.33%

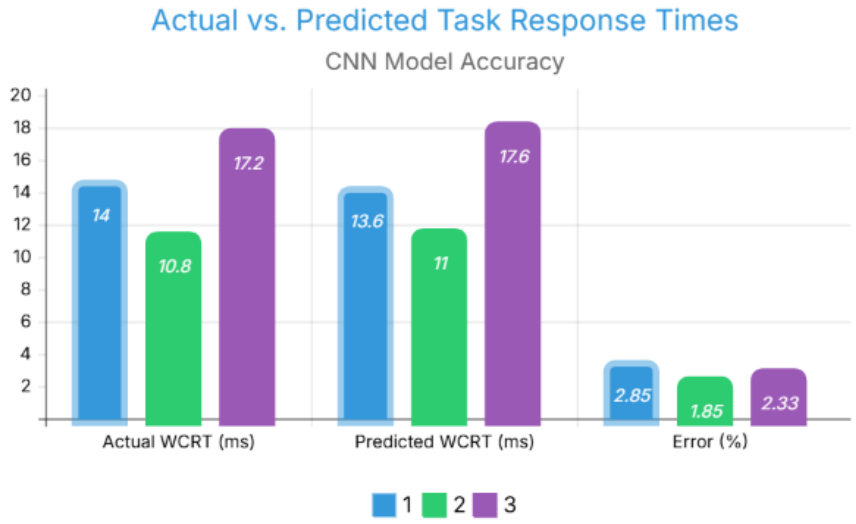

Figure 2. Performance Comparison of CNN in the term of Actual vs Predicted Response Time

The CNN's ability to accurately anticipate timing performance was demonstrated by the average prediction error across all tasks, which was less than 3%. During training, the cost function, which was reduced via gradient descent, effectively converged to an ideal solution.

IV. CONCLUSION

To improve security of IOT gadgets in term of their usage, we use Convolutional Neural Network system for mapping and lead a test to confirm that our all errand meet their dead line or not. So in the wake of directing a trials, we come to realize that all errand fulfill their time constraint so our outcomes are right, and there is likewise dependability in our outcomes. So our framework is legitimate and satisfy every one of our necessities. We are utilizing CNN system for mapping and concentrate wanted outcomes. However, we also experience very little problem in that occasionally we have more jitter and occasionally there is less jitter, which indicates that there is also a soundness issue. So we can take care of this issue in future by utilizing some other neural system for mapping however then we have to portray factors as per that neural system , so all things considered might be we can accomplish security, and there is additionally risks we get CNN system.

REFERENCE:

[1] "Deep Learning Tutorial for Beginners: Neural Network Classification." [Online]. Available: https://www.guru99.com/deep-learning-tutorial.html. [Accessed: 27-May-2019].

[2] J. Brownlee, "What is Deep Learning?," Machine Learning Mastery, 1 Nov. 2023. [Online]. Available: https://www.machinelearningmastery.com/what-is-deep-learning/ . [Accessed: 27-May-2025].
[3] "Deep learning," Wikipedia, 18-May-2019. [Online]. Available: https://en.wikipedia.org/wiki/Deep_learning. [Accessed: 27-May-2025].
[4] stfalcon.com, "What is Deep Learning? A Look at Its Definition, Benefits, and Challenges," Upwork, 13-Dec-2017. [Online]. Available: https://www.upwork.com/hiring/for-clients/deep-learning-definition-benefits-challenges/. [Accessed: 27-May-2025].
[5] "30 amazing applications of deep learning - Yaron Hadad." [Online]. Available: http://www.yaronhadad.com/deep-learning-most-amazing-applications/. [Accessed: 27-May-2025].
[6] H. H. Eckerson, "Deep Learning – Past, Present, and Future," KDnuggets, May 2017. [Online]. Available: https://www.kdnuggets.com/2017/05/deep-learning-big-deal.html. [Accessed: 27-May-2025].
[7] A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," Computer, vol. 49, no. 8, pp. 112–116, Aug. 2016.
[8] "A Survey on Trust Management for Internet of Things." [Online]. Available: https://www.researchgate.net/publication/261104622_A_Survey_on_Trust_Management_for_Internet_of_Things. [Accessed: 27-May-2025].
[9] D. Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco Internet Business Solutions Group (IBSG), vol. 1, pp. 1–11, Jan. 2011.
[10] M. Abomhara, G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," J. Cyber Secur. Mobil., vol. 4, no. 1, pp. 65–88, 2015.
[11] "Botnets and Internet of Things Security," IEEE Journals & Magazine. [Online]. Available: https://ieeexplore.ieee.org/document/7842850. [Accessed: 27-May-2025].
[12] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time Intrusion Detection in the Internet of Things," Ad Hoc Netw., vol. 11, no. 8, pp. 2661–2674, Nov. 2013.
[13] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digit. Commun. Netw., vol. 4, no. 2, pp. 118–137, Apr. 2018.
[14] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, Jan. 2015.
[15] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Comput. Netw., vol. 141, pp. 199–221, Mar. 2018.
[16] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," J. Netw. Comput. Appl., vol. 84, pp. 25–37, 2017.
[17] R. H. Weber, "Internet of Things – New security and privacy challenges," Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30.
[18] W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, and A. F. M. Ariffin, "The Rise of Ransomware," in Proc. 2017 Int. Conf. Softw. e-Business, New York, USA, 2017, pp. 66–70.
[19] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Comput. Netw., vol. 57, pp. 2266–2279, 2013.
[20] K. Wang, J. Bao, M. Wu, and W. Lu, "Research on security management for Internet of Things," in 2010 Int. Conf. Comput. Appl. Syst. Model. (ICCASM), 2010, vol. 15, pp. V15-133–V15-137.
[21] J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," 2014.
[22] "An Internet of Things (IoT) Based Security Alert System Using Raspberry Pi." [Online]. Available: https://docplayer.net/19093876-An-internet-of-things-iot-based-security-alert-system-using-raspberry-pi.html. [Accessed: 29-May-2025].

[23] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," in Int. Conf. Advanced Networking, Distributed Systems and Applications, Béjaia, Algeria, 2014, pp. 64–69.

[24] "What is CPU utilization and how can it be calculated?," eUKhost Official Web Hosting Forum. [Online]. Available: https://www.eukhost.com/forums/forum/general/technology-forum/22321-what-is-cpu-utilization-and-how-can-it-be-calculated. [Accessed: 25-Jun-2025].

[25] J. Wang, Y. Yan, and J. Guo, Research on the Prediction Model of CPU Utilization Based on ARIMA-BP Neural Network, vol. 65, 2016.

[26] E. G. Peters, D. E. Quevedo, and M. Fu, "Controller and scheduler codesign for feedback control over IEEE 802.15.4 networks," IEEE Trans. Control Syst. Technol., vol. 24, no. 6, 2016.

[27] A. Burns and A. J. Wellings, Real-Time Systems and Programming Languages, 3rd ed. Pearson Education, 2001.

[28] S. Saha, "A Comprehensive Guide to Convolutional Neural Networks — the ELI5 way," Towards Data Science, 15-Dec-2018. [Online]. Available: https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53. [Accessed: 25-Jun-2025].

[29] H. Srivastava, "Convolutional Neural Networks Explained," Magoosh Data Science Blog, 25-Apr-2018.

[30] "Understanding Convolutional Neural Networks for Object Recognition - ppt video online download." [Online]. Available: https://slideplayer.com/slide/10983919/. [Accessed: 25-Jun-2025].

[31] Raza, A., Zongxin, S., Qiao, G., Javed, M., Bilal, M., Zuberi, H. H., & Mohsin, M. (2025). Automated classification of humpback whale calls in four regions using convolutional neural networks and multi scale deep feature aggregation (MSDFA). Measurement, 118038.

[32] S. Aslam, M. . Usman Javeed, S. . Maria Aslam, M. M. Iqbal, H. . Ahmad, and A. . Tariq, "Personality Prediction of the Users Based on Tweets through Machine Learning Techniques", JCBI, vol. 8, no. 02, Mar. 2025.

[33] M. U. Javeed, Shafqat Maria Aslam, Hafiza Ayesha Sadiqa, Ali Raza, Muhammad Munawar Iqbal, and Misbah Akram, "Phishing Website URL Detection Using a Hybrid Machine Learning Approach", JCBI, vol. 9, no. 01, Jun. 2025.

[34] H. . Shakeel, "LncRNAs Disease: A text mining Approach to Find the role of lncRNA in Aging", JCBI, vol. 9, no. 01, Jun. 2025.

[35] M. U. Javeed, M. S. Ali, A. Iqbal, M. Azhar, S. M. Aslam and I. Shabbir, "Transforming Heart Disease Detection with BERT: Novel Architectures and Fine-Tuning Techniques," 2024 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 2024, pp. 1-6, doi: 10.1109/FIT63703.2024.10838424.

[36] M. Javeed, S. Aslam, M. Farhan, M. Aslam, and M. Khan, "An Enhanced Predictive Model for Heart Disease Diagnoses Using Machine Learning Algorithms", TJ, vol. 28, no. 04, pp. 64-73, Dec. 2023.