International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A NOVEL EXTENDED INTERNET OF THINGS (IOT) CYBER SECURITY PROTECTION BASED ON ADAPTIVE DEEP LEARNING PREDICTION FOR INDUSTRIAL MANUFACTURING APPLICATIONS

***Mohammed Mohideen[1], Kalakumari. T[2], Mohammad Abdul Basith[3], Narayanasamy Rajendran[4] Sivaramu.T[5], Jehan Murugadhas[6], Mary Amirtha Sagayee. G[7]**

[1]Lecturer, Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Science – Nizwa, Sultanate of Oman, mohammed.kani@utas.edu.om

[2]Associate Professor, Department of Commerce IT & E-Commerce, Sri Krishna Arts & Science College, Coimbatore, Tamilnadu, India, kalakumarit@skasc.ac.in

[3]Lecturer, Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Science – Nizwa, Sultanate of Oman, mohammad.basith@utas.edu.om

[4]Lecturer, Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Science – Nizwa, Sultanate of Oman, naren.rajendran@utas.edu.om

[5]Lecturer, Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Science – Nizwa, Sultanate of Oman, tsiva.ramu@utas.edu.om

[6]Lecturer, Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Science – Nizwa, Sultanate of Oman, jehan.murugadhas@utas.edu.om

[7]Senior Lecturer, Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Science – Nizwa, Sultanate of Oman, mary.sagayee@utas.edu.om

Abstract

The emerging technology Internet of Things (IoT) has fundamentally changed the way people, smart objects, smart devices, information, and data are connected around the world. While the Internet of Things is still in its infancy, many directly related issues need to be resolved. IoT is the overarching idea of embedding everything. Thanks to IoT, higher levels of accessibility, integrity, availability, scalability, confidentiality, and interoperability can be achieved around the world. The use of Internet of Things (IoT) devices is growing rapidly in modern industrial sectors. The IoT technology market is at risk as the integration of these devices into the network infrastructure exposes information to cybersecurity

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

attacks. For this reason, it is necessary to create accurate protection algorithms and effective monitoring systems. This research will help create algorithms that can reduce traffic accidents, improve traffic flow, reduce energy waste, and reduce traffic control costs. The results show that this new algorithm is 100x more curated, making it the best option for bug and threat detection. The purpose of this essay is to provide important information about Federated Deep his learning methodologies and upcoming cybersecurity technologies. For this reason, it is necessary to create accurate protection algorithms and effective monitoring systems. This research provides a new framework design for industrial manufacturing, including: B. Transport and energy based on probabilistic measurements of key parameters using state-of-the-art adaptive deep learning (ADL) methods.The new framework will be designed to include an element of randomness, as opposed to deterministic frameworks. The implemented method considered network forensic systems and intruder detection (ID). Therefore, predictive models are set up to inform administrators of the state of the system. The results demonstrated the ability to simulate IoT network traffic along with risk assessment against various types of attacks using ADL algorithms. The new framework aims to improve computational efficiency by allowing the structure to be adjusted based on the input.

Keywords: IoT security, Intrusion detection, Deep learning, Industrial manufacturing, Transportation,Security prediction

Introduction

The Internet of Things (IoT) aims to integrate the physical and digital worlds into a single, coherent format, thereby bringing great commercial potential to various sectors such as energy, tourism and industry. Perspectives are open. It has created a new paradigm where new processes are driven by a network of machines and devices that can work together and interact. However, due to its complex environment and the multitude of tools that expose resource flows, IoT exposes it to a variety of security vulnerabilities, often very sophisticated [1]. The Internet of Things (IoT) is a system that uses sensors to connect the Internet to the real world [2]. Cybersecurity deals with the methods used to access systems and the protection of hardware, software and data. Security goals usually include privacy. This relates to detecting unwanted devices or individuals accessing, modifying, or destroying information [3, 4]. Today's society is also vulnerable to cyber-attacks due to the multitude of connected devices that are powered by IoT. B. Denial of service attacks by insiders and hackers [5]. Directly interfere with access to devices, etc. [6,7]. As technology plays a greater role in our daily lives, both cybercrime and cybersecurity tools are evolving at the same time [8,9], investment in cybersecurity measures from across the industry [10] and There is a need for the development of new IoT cybersecurity management solutions [11]. A DL-based architecture and its impact on IIoT is shown in Figure 1. The following section describes various DL methods for IIoT networks.

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Apart from that, cyberattacks on smart grids have a significant negative impact on public safety due to the sensitive and costly nature of compromising critical infrastructure [5]. More and more people are concerned about cybersecurity and the lack of strong defense mechanisms such as:

Cybersecurity expert [12]. For example, China is creating new regulations and rules on cybersecurity [13]. Hospitals generally have weak cybersecurity due to the availability of critical data, putting patients' lives and trust at risk[14], but healthcare is now a top priority.

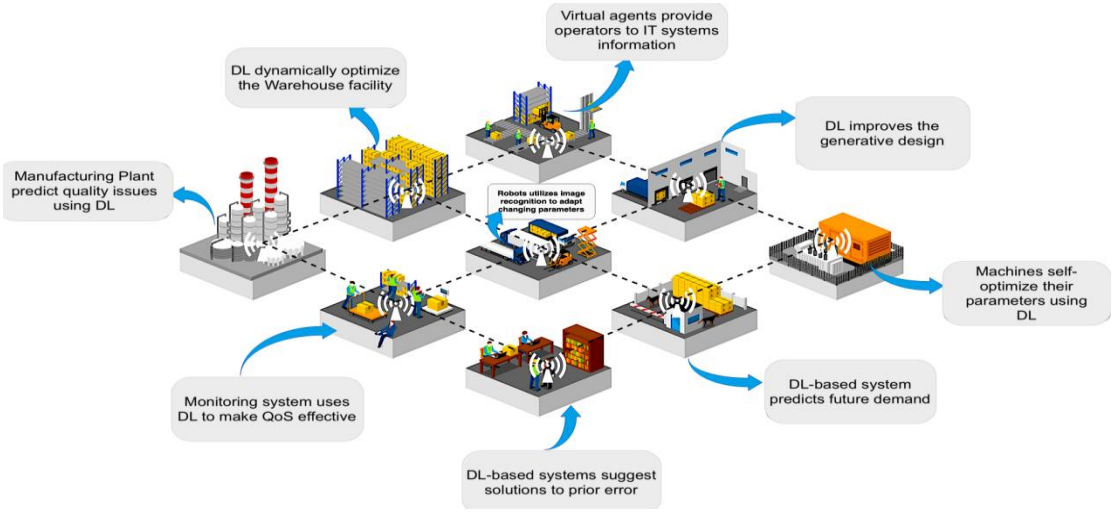

Fig. 1. Deep learning in future Industrial Internet of Things.

The most important requirement for IoT networks is the security of all connected systems, applications and devices. Device, data, computer, security, and privacy management are just a few of the many areas where large-scale IoT networks pose significant challenges. As the IoT grows, many security concerns have been identified as potential hazards. Without a solid structure, new IoT applications like the one above run the risk of losing all their potential and being unable to meet not only the demands of individual users, but also the needs of society as a whole. Most IoT systems operate at layers such as application layer, middleware or support layer, network and data link layer, perception or acquisition layer. Each of these layers in an IoT application has a unique set of tasks and associated technologies that need to be performed, and each layer introduces a new set of issues and security risks. For example, the most common IoT risks include denial of service (DoS) attacks, spoofing attacks, jamming, eavesdropping, data tampering, man-in-the-middle attacks, and malicious attacks.

Related Work

Some authors have shown that deep learning outperforms machine learning in industrial manufacturing applications. According to the authors, deep learning algorithms perform better on GPUs, but require more training time. In contrast, Hassanalieragh et al. Using the support vector machine (SVM) machine learning technique, he achieved an accuracy of 89.85 with weak generalization against unproven attacks.

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

According to Thiesse et al. [15] The Internet of Things consists of “hardware components and digital information flows based on RFID tags”. The Internet of Things (IoT) has been described by the Institute of Electrical and Electronics Engineers (IEEE) as “a collection of devices with sensors that represent an Internet-connected network” [16]. According to the European Telecommunications Standards Institute (ETSI) [17], machine-to-machine (M2M) communications are automated communication systems that make decisions and handle data manipulation without overt human involvement.

The Internet-of-Everything (IoE) concept is defined by Cisco (San Francisco), a global leader in IT, network, and cybersecurity solutions, as "a network made up of people, data, things, and processes." . [18].

According to Gubbi et al. [19], the Internet of Things (IoT) is the connectivity of sensing and actuating devices that enables the sharing of information across platforms through a uniform framework and creates a common operational picture for enabling creative applications.

Phosphorus et al. It examines cyber threat detection in mobile cloud computing and shows an accuracy of 99.65% [20]. Al-Qatf and co-authors achieved an accuracy of 84.96 in intruder detection using a sparse autoencoder. For online intrusion detection, Mirksy et al. used a group of autoencoders in incremental training [21].

The Industrial Internet of Things (IIoT)

The IIoT offers a number of characteristics that set it apart from traditional IoT. IIoT works in industrial environments and IoT works in home environments. This approach includes things like supply chain optimization. Industry 4.0 is a term that refers to technologies and ideas for organizing value chains, the same as IIoT. Computers use the modular framework of Industry 4.0 to drive smart factories and the resulting physical processes, decentralizing decision-making while creating digital copies of these operations. Computer-human interactions occur along the route. Aspects of the supply chain can receive organizational and super-organizational services. Interconnected elements managed and accessed by data mining techniques such as blockchain are partially accessible, acting as sensors and communicating with other devices. These IoT systems of smart objects rely heavily on artificial intelligence algorithms to share and generate data with little to no human involvement. Reduced material and energy consumption, better management of the temporal aspects of security related to "intrusion detection", cloud computing, interfaces between supply chain management and marketing processes, infrastructure complexity in terms of number of entry points In summary, the interface between supply chain management and marketing processes is a major concern of the IIoT.

Common IoT and cybersecurity concerns are both unique to the IIoT. Data integrity to ensure that data cannot be changed by unauthorized persons, authentication to ensure that the data originates from the claimed identity, and unauthorized persons to track a user's identity through their actions Emphasizes privacy, which prevents information from being understood, and confidentiality. Restrict access to system services to authorized users.However, IIoT faces major challenges, especially when working in

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

distributed environments such as blockchain systems and various intelligent artifacts. It must also be emphasized that the processing power and performance of various sensors are limited, making traditional security measures ineffective. The above issues increase the risk of cyberattacks on IoT systems such as transportation, consumer electronics, and manufacturing facilities, requiring significant advances in remote system authentication, new sensor encryption, web interface designs, and intruder detection software. Also, with the development of IoT, wireless technology is becoming more and more sophisticated. B. His 5G that offers more possibilities than just voice and data.

In particular, decentralized architectures consisting of many objects, such as blockchains and cloud computing systems, make networks easier to manage and configure. It also improves his IoT security with sensors that optimize data transmission and prevent radio channel redundancy with network systems such as big data. Preliminary Scopus searches using the terms "Internet of Things" and "cybersecurity" yielded a draft of the conceptual and technical framework for this white paper. Cybersecurity experts often emphasize this point when they claim that the IoT will expand the attack surface that criminals can exploit.

Edge includes ICS and IoT devices. In other words, they are the final link in a communication chain that begins with a human or robotic device and ends with cloud platforms and data centers. IoT and ICS devices do not emerge out of thin air. Like any computer, they are created, developed and controlled. Figure 2 shows an overview of the components of a typical IoT device.

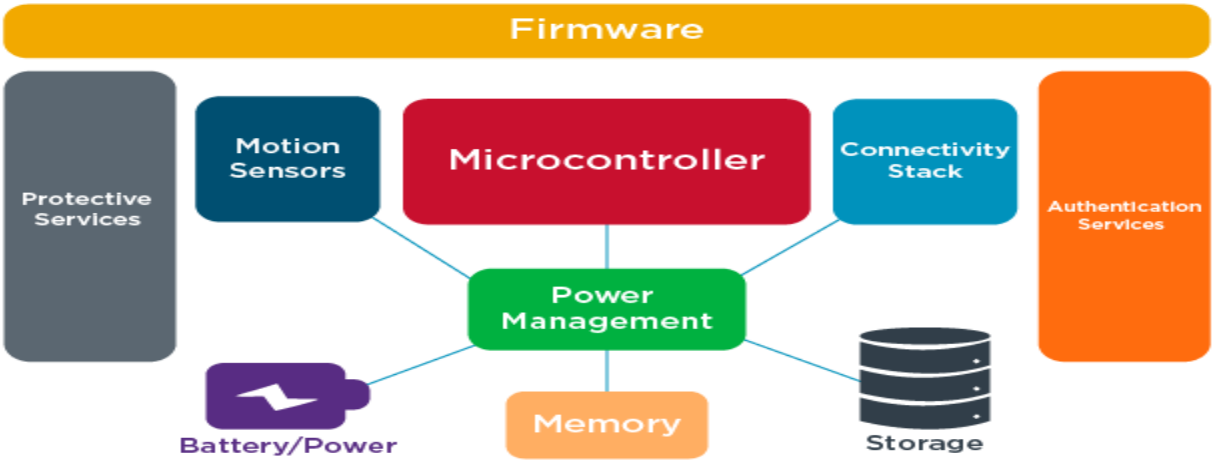

Figure 2 Typical IoT device

As shown in the image above, every IoT device contains each of the following components:

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- **Firmware:** Read-only memory that is built into the system and provides low-level control over hardware. Usually not coded, but can be changed. It communicates with all components of the device as well as other network devices.
- **Protective services:** A section of a device's operating system or firmware that provides security features such as encryption or the ability to isolate programs so that they cannot be used to bypass security.
- **Motion sensors:** Motion sensors are the hardware and software that work together to monitor how a gadget is moved. Included in this are either satellite connectivity or the detection of simple movement (such as moving the device up and down or back and forth) (e.g., Global Positioning System or GLONASS).
- **Microcontroller:** The "brains" of the device are provided by the microcontroller, which is the processor needed to operate the software.
- **Connectivity stack:** Network connectivity is provided via the connectivity stack. Bluetooth, mobile (such as 3G, 4G, or 5G), Zigbee, LoRA, SigFox, or WiFi are all forms of networking.
- **Authentication services:** When used, authentication services give IoT devices the ability to confirm and validate people, network activity, or processes.
- **Power management:**Power management refers to features that control both the device's charging and power usage if the gadget uses a lot of power.
- **Battery/power:** The ability to physically store electricity as well as receive power from a distant source.
- **Memory:** Memory is the "muscle" of the Internet of Things device, allowing it to store data that is currently in use, programme code, and other data that the processor will later use.
- **Storage:** Storage enables the collection and preservation of data for comparatively lengthy stretches of time. Such data may comprise the location(s) the wearer or operator of the IoT device travelled with the device, details about other devices linked to it, and data input by the user. Such data can be added actively (e.g., by purposefully programming an IoT/OT device) or passively (e.g., by the device collecting the wearer's or user's movements and actions).

DEEP LEARNING FOR IIOT

The use of smart manufacturing is essential for making production and manufacturing smarter, and could benefit the IIoT. Since then, IIoT solutions have grown tremendously, especially for sensor-based data of various shapes, formats, and semantics. The data provided by IIoT technology comes from various manufacturing-related resources such as product lines, machines and processes, workflows, and environmental variables. Modeling, labeling and analyzing data is essential to making production much smarter. They provide real-time data processing and play an important role in managing large amounts of data. Due to its multi-layered structure, deep learning (DL), one of the most powerful machine learning (ML) techniques, can transform manufacturing into highly optimized intelligent devices. By extracting computational intelligence from ambiguous sensor data, DL technology enables intelligent

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

manufacturing. DL approaches are beneficial because they automatically learn from data, find underlying patterns, and draw intelligent conclusions. The advantage of DL over traditional machine learning techniques is that feature learning is performed automatically without the need for a separate algorithm. Figure 3 analyzes the contrast between DL and traditional approaches in IIoT.

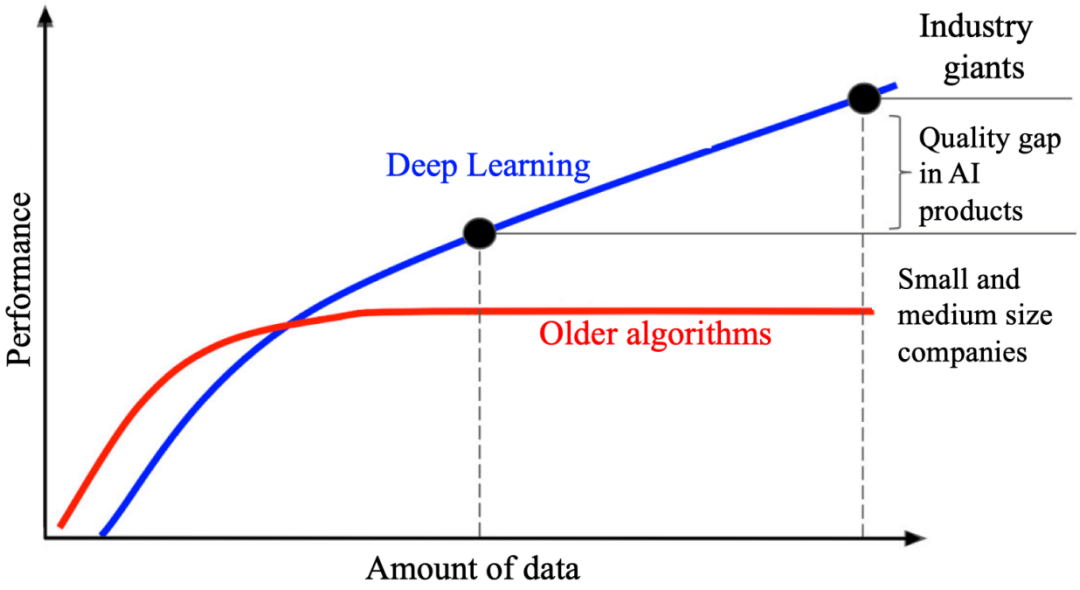

Fig. 3. Comparison of DL with traditional algorithms for IIoT

DL algorithms for rul prediction formulated as

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \quad (1)$$

$$f_t = \sigma(W_f.[h_{t-1}, x_t] + b_f) \quad (2)$$

$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o) \quad (3)$$

$$\tilde{c}_t = act(W_c.[h_{t-1}, x_t] + b_c) \quad (4)$$

$$c_t = f_t * c_{t-1} + i_t * \tilde{c}_t \quad (5)$$

$$h_t = o_t * act(c_t) \quad (6)$$

Where σ is the sigmoid layer. $c_t$and e $c_t$are each internal memory cell and temporary value to make a new internal memory cell at time t. $*$ is element-wise multiplication of two vectors.

$$z_t = \sigma(W_z.[h_{t-1}, x_t] + b_z)\,, \quad (7)$$

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$r_t = \sigma(W_r.[h_{t-1}, x_t] + b_r)\ , \quad (8)$$

$$\tilde{c}_t = act(W.[r_t * h_{t-1}, x_t] + b_h)\ , \quad (9)$$

$$c_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \quad (10)$$

where $z_t$and $r_t$are the update gate and reset gate at time t, respectively. e $h_t$is a temporary value to make new hidden state at time t.

KEY CHALLENGES IN DL-IIOT

We've described the value of DL in various industries, but it isn't easy to use DL with reliable results in an industrial environment successfully. This requires individuals with a background in statistical analysis who can discover insightful information in data, and subject matter expertise with a problem-solving approach. Below we address some of the main issues of DL-assisted IIoT.

A. Complexity

One of the main problems with DL models is their complexity, which requires a lot more work to address. Due to model complexity and industrial dataset size, one of the DL performance issues is the time consumption and computational requirements of the training phase. The second problem is that overfitting reduces model accuracy and efficiency due to the lack of training examples in industrial environments. By effectively learning different characteristics from industrial data, tensor train deep compression (TTDC) models can be used to address complexity problems. By reducing the number of DL model elements, this technique speeds up the model.

B. Selection of Algorithm

There are many widely used DL algorithms available for IIoT applications. These algorithms can be used in all common scenarios, but choosing an algorithm for a specific industrial application should be based on the unique rules available. Knowing which DL algorithm works best in a given situation is important for any algorithm. Choosing the wrong DL algorithm can lead to a variety of problems, including: B. A wasteful expense resulting in loss of time, energy and resources.

C. Selection of Data

The phrase "garbage in, garbage out" perfectly sums up how training data affects the performance of deep learning algorithms. Any DL technique relies heavily on having the right type and amount of data. In industrial processes, it is important to avoid data that would lead to selective bias and to create or select data that are representative of the case.

D. Data Preprocessing

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

After selecting the data, it is important to transform the chaotic data, including missing values, outliers, and no-value entries, into a form that statistical and deep learning (DL) algorithms can understand. In this step the data is processed, cleaned and preprocessed. For example, data in other formats is converted to numbers, features are scaled (so they don't overwhelm others), and missing items are removed or replaced.

E. Data Labelling

Supervised DL algorithms are known to be the easiest and most suitable algorithms today for development, training, and deployment in many IIoT applications. On the other hand, unsupervised DL algorithms are more difficult to implement, possibly requiring a large number of failed iterations and lengthy training procedures. Although data labeling for supervised DL algorithms is difficult, it cannot be outsourced due to the complex and time-consuming task. For example, labeling medical images require medical professionals, such as doctors, to train classification models for the diagnostic process. Medical professionals see this behavior as a time-consuming process, and this is the problem.

The main organizations developing new communication and security protocols are the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF). They are essential for securing global IoT networks [79], [80]. Details of the standards and protocols are listed in Table 1.

Table 1 IOT Cybersecurity Standards and Protocols

Standards	**Security Issue**	**Application**
IEEE 802.15.4 (Perception Layer)	Replay Attacks, Integrity, Confidentiality, and Authentication	Mechanism of access control and time synchronization communication
6LowPAN (Network Layer)	Integrity, Authenticity, Nonrepudiation, Confidentiality	Transparent end-to-end security and LoWPAN device communication
RPL (Middleware Layer)	integrity, authentication and confidentiality non-repudiation, replay attacks, key management	Protect routing control messages and protect routing operations from forged routing updates
CoAP (Application Layer)	Integrity, Authentication, and Confidentiality Nonrepudiation and Replay	Protect application-level CoAP messages while maintaining transparent,

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Security	granular end-to-end security

TABLE 2 TECHNIQUES FOR DEEP LEARNING IN THE INDUSTRIAL IOT

Topic	**TECHNIQUES**	**Model**	**Function Approximation**	**Applications**
Surveillance	Siamese U-Nets and Semantic Segmentation	CNN	Regression	Network
	Two-path information propagation and stage-wise network	DNN	Classification	Software
	LSTM	CNN	Classification	Software
	Bi-directional Long Short-term Memory	DNN	Classification	Software
	Hierarchal Weighted Fusion	CNN	Classification	Software
Resource Management	Forward Central Dynamic and Available	ANN	Regression	Device
	Service Function Chain (SFC)	DRL	Regression	Network
	SFC	DRL	Regression	Network
Attacks and Threads Detection	Feature Selection and Grey Wolf Optimization.	CNN	Regression	Software
	Statistical Signal	DNN	Classification	Device

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Processing			
	Deep-Feature Extraction and Selection	DNN	Classification	Network
	Operational Code Sequence	DEL	Classification	Device
	Dual Disaggregation and Aggregation DL models	CNN	Regression	Device

The IETF Low-Power, Lossless Network Routing (ROLL) Working Group is developing routing solutions for IoT applications with its Low-Power and Lossy Networks (RPL) proposal. RPL provides a framework for a particular kind of application. The IETF's Constrained RESTful Environments (CoRE) working group is actively developing a Constrained Application Protocol (CoAP) that simplifies communication at the application layer.

TABLE 3. Comparative analysis with cutting-edge pirate detection methods.

Proposed	**Source code**	**Technique**	**Accuracy (%)**
Bandara Wijayrathna	JAVA	KNN	86%
Cosma, G And M.Joy	JAVA	LSA	99%
Son,J.-W	JAVA	Parse Tree	90%
Ullah,F	C++, JAVA, Python	LSA	80%
Ulla, F	C++, JAVA, Python	MLR	86%
Our proposed approach	C++, JAVA, Python	Deep Neural Network	**96%**

TABLE 4: Hyperparameter settings

Model	**Hidden neuron**	**Drop out**	**Batch size**	**Epochs**	**Account function**

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CNN	64	0.2	200	100	ReLu
LSTM	100	0.2	200	100	tanh
GRU	100	0.2	200	100	tanh

The Internet of Things (IoT) is a critical platform consisting of various devices, technologies, and protocols. Standardization can become, at least temporarily, a Garden of Eden where IoT systems can't afford. However, standardization could be the end result that drives the improvement and growth of IoT security. Companies or organizations that have implemented standardized concerns for both security and IoT include:

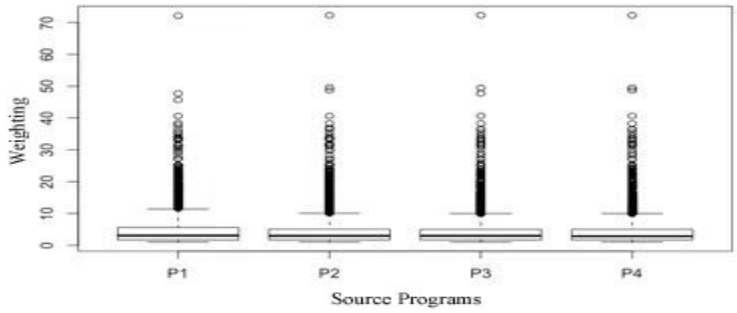

FIGURE 4. Box plot of source codes weighting values.

The contribution of each token in the document or across all documents is zoomed using the weighting algorithms. Figure 4 displays the box plot of weighting values. The programming answers to four queries are indicated on the x-axis by the letters P1, P2, P3, and P4, respectively. The y-axis displays the weighting values for each source code.

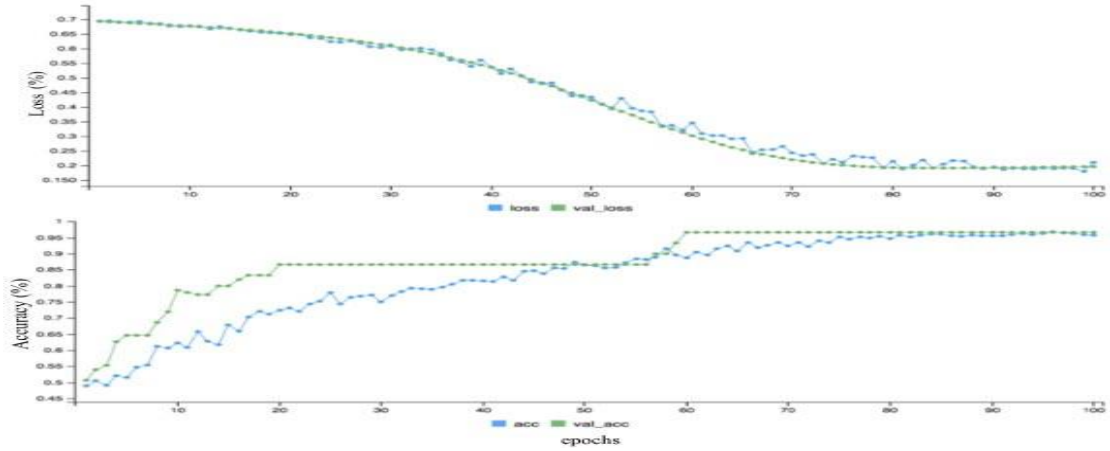

Figure 5. For source codes, a dynamic map of loss, validation loss, accuracy, and validation accuracy

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 5 shows a dynamic visualization of accuracy during validation, validation accuracy, loss, and loss rate. The top blue curve represents loss and the green curve represents validation loss. Both curves initially start at the same 0.7 point and behave identically for 35 epochs, after which the blue curve begins to oscillate above the green curve. When both curves descend, you are less likely to have overfitting problems. Overfitting occurs when these curves operate in opposite directions or uphill.

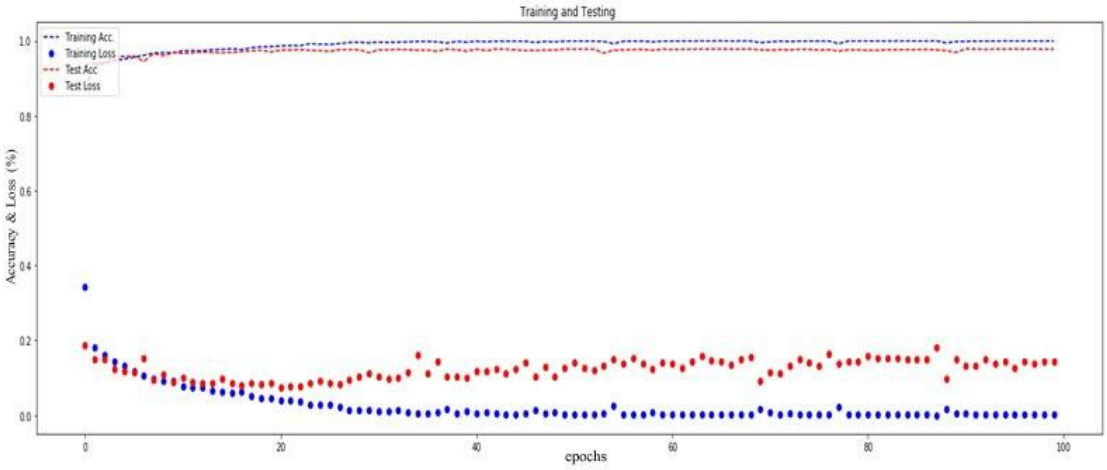

FIGURE 6. Dynamic visualization of accuracy validated accuracy, loss and validated loss (Image Ratio: 224*224).

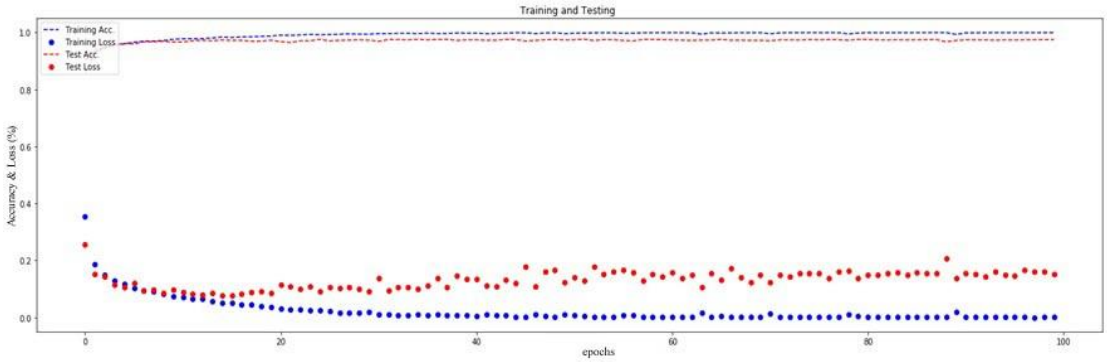

FIGURE 7. Dynamic graph of accuracy validated accuracy and loss and validated loss (Image Ratio: 229*229)

Figure 5 and **6** show the dynamic graph for Accuracy, Validated Accuracy, Loss, and Validated Loss for 224 x 224 and 229 x 229 aspect ratios. Shows the importance of ratios to demonstrate better accuracy. On the Leopard Mobile data set, a frame rate of 229 229 was achieved with a computation time of 36 seconds and a test accuracy of 97.46%. Figure 7 shows a confusion matrix with a 229 x 229 aspect ratio. We evaluated whether there were

Received: August 02 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

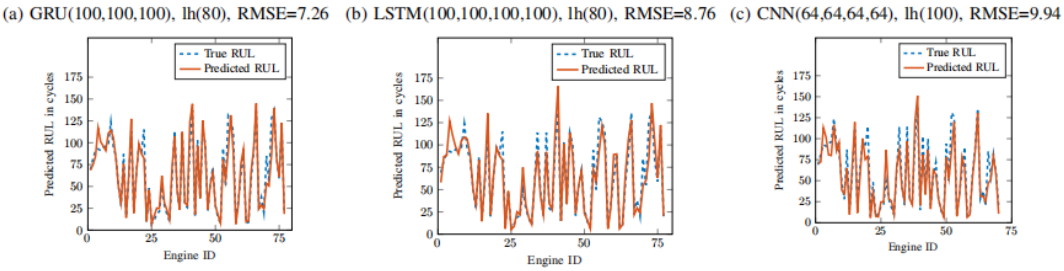

Fig. 4: Comparison of deep learning algorithms

CONCLUSION

Thanks to recent developments in the Industrial Internet of Things (IIoT) and Deep Learning (DL), industrial setups have become smarter for a wide variety of applications. However, there are still many problems that the smart industry must overcome. In this article, we've discussed how the Industrial Internet of Things (IoT) device market is growing rapidly today. The IoT technology market is vulnerable in that information is vulnerable to cybersecurity attacks due to the integration of these devices into the network infrastructure. For this reason, it is necessary to create accurate protection algorithms and effective monitoring systems. This research will help create algorithms that can reduce traffic accidents, improve traffic flow, reduce energy waste, and reduce traffic control costs. The results show that this new algorithm is 100x more curated, making it the best option for bug and threat detection. The purpose of this article is to provide key knowledge about federated deep learning strategies using state-of-the-art cybersecurity technology. For this reason, it is necessary to create accurate protection algorithms and effective monitoring systems. This research provides a new framework design for industrial manufacturing, including: B. Transport and energy based on probabilistic measurements of key parameters using state-of-the-art adaptive deep learning (ADL) methods. Unlike deterministic frameworks, the new framework is built to include a randomization component.

Reference

1. Alshboul, Y.; Bsoul, A.A.R.; Zamil, M.A.L.; Samarah, S. Cybersecurity of smart home systems: Sensor identity protection. J. Netw. Syst. Manag. **2021**, 29, 22. [CrossRef]

2. Occa, R.; Borbon-Galvez, Y.; Strozzi, F. In search of lost security. A systematic literature review on how blockchain can save the iot revolution. In Proceedings of the XXV Summer School Francesco Turco, Bergamo, Italy, 11–13 September 2020.

3. Furstenau, L.B.; Sott, M.K.; Homrich, A.J.O.; Kipper, L.M.; Al Abri, A.A.; Cardoso, T.F.; López-Robles, J.R.; Cobo, M.J. 20 years of scientific evolution of cyber security: A science mapping. In Proceedings of the

Received: August 02 ,2025

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

International Conference on Industrial Engineering and Operations Management, Dubai, United Arab Emirates, 10–12 March 2020; pp. 314–325.

4. Gorog, C.; Boult, T.E. Solving global cybersecurity problems by connecting trust using blockchain. In Proceedings of the 2018 IEEE Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1425–1432. [CrossRef]

5. Urquhart, L.; McAuley, D. Avoiding the internet of insecure industrial things. Comput. Law Secur. Rev. **2018**, 34, 450–466. [CrossRef]

6. Dhieb, N.; Ghazzai, H.; Besbes, H.; Massoud, Y. Scalable and secure architecture for distributed IoT systems. In Proceedings of the 2020 IEEE Technology and Engineering Management Conference (TEMSCON), Novi, MI, USA, 3–6 June 2020. [CrossRef]

7. Ghorbani, H.; Mohammadzadeh, M.S.; Ahmadzadegan, M.H. Modeling for malicious traffific detection in 6G next generation networks. In Proceedings of the 2020 International Conference on Technology and Entrepreneurship–Virtual (ICTE-V), San Jose, CA, USA, 20–21 April 2020. [CrossRef]

8. Raban, Y.; Hauptman, A. Foresight of cyber security threat drivers and affecting technologies. Foresight **2018**, 20, 353–363. [CrossRef]

9. Vaccari, I.; Cambiaso, E.; Aiello, M. Evaluating security of low-power internet of things networks. Int. J. Comput. Digit. Syst. **2019**, 8, 101–114. [CrossRef]

10. Laskurain-Iturbe, I.; Arana-Landín, G.; Landeta-Manzano, B.; Uriarte-Gallastegi, N. Exploring the inflfluence of industry 4.0 technologies on the circular economy. J. Clean. Prod. **2021**, 321, 128944. [CrossRef]

11. Kis, M.; Singh, B. A cybersecurity case for the adoption of blockchain in the financial industry. In Proceedings of the 2018 IEEE Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1491–1498. [CrossRef]

12. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology and Engineering Management Society Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141. [CrossRef]

13. Parasol, M. The impact of china's 2016 cyber security law on foreign technology firms, and on china's big data and smart city dreams. Comput. Law Secur. Rev. **2018**, 34, 67–98. [CrossRef]

14. Khatkar, M.; Kumar, K.; Kumar, B. An overview of distributed denial of service and internet of things in healthcare devices. In Proceedings of the International Conference on Research, Innovation,

Received: August 02 ,2025

Volume 38 No. 5 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Knowledge Management and Technology Application for Business Sustainability (INBUSH), Greater Noida, India, 19–21 February 2020; pp. 44–48. [CrossRef]

15. Frederic Thiesse and Florian Michahelles. An overview of epc technology. Sensor review, 26(2):101–105, 2006.

16. Joseph Bradley, Jeffff Loucks, James Macaulay, and Andy Noronha. Internet of everything (ioe) value index. White Paper CISCO and/or its affiliations, 2013.

17. Roberto Minerva, Abyi Biru, and Domenico Rotondi. Towards a defifinition of the internet of things (iot). IEEE Internet Initiative, 1(1):1–86, 2015.

18. Srdjan Krˇco, Boris Pokri´c, and Francois Carrez. Designing iot architecture (s): A european perspective. In 2014 IEEE World Forum on Internet of Things (WF-IoT), pages 79–84. IEEE, 2014.

19. Joseph Bradley, Jeffff Loucks, James Macaulay, and Andy Noronha. Internet of everything (ioe) value index. White Paper CISCO and/or its affiliations, 2013.

20. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems, 29(7):1645– 1660, 2013.

21. W. Lin, H. Lin, P. Wang, B. Wu and J. Tsai, “Using convolutional neural networks to network intrusion detection for cyber threats,” 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1107-1110.

22. Tapping into the potential of IoT in utilities, April 2019, Navin Joshi, Allerin, https://www.allerin.com/blog/tapping-into-the-potential-of-iotin-utilities (last accessed May2020)

23 C. M. J. M. Dourado, S. P. P. Da Silva, R. V. M. Da Nobrega, P. P. R. Filho, K. Muhammad, and V. H. C. De Albuquerque, “An open iohtbased deep learning framework for online medical image recognition,”

IEEE Journal on Selected Areas in Communications, pp. 1–1, 2020.

24 A. Ullah, K. Muhammad, J. Del Ser, S. W. Baik, and V. H. C. de Albuquerque, “Activity recognition using temporal optical flflow convolutional features and multilayer lstm,” IEEE Transactions on Industrial Electronics, vol. 66, no. 12, pp. 9692–9702, 2018.

25 M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, “Deep abstraction and weighted feature selection for wi-fifi impersonation detection,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 621–636, 2017

Received: August 02 ,2025