Journal of Advanced Zoology

ISSN: 0253-7214
Volume 43 Issue 01 Year 2022 Page 584:594

LISF: A Security Framework for Internet of Things (IoT) Integrated Distributed Applications

D. Shravani[1*], Imtiyaz Khan[2], Amogh Deshmukh[3], Veeramalla Anitha[4], Masrath Saba[5], Syed Shabbeer Ahmad[6]

[1]*Associate Professor, Department Of ADCE, SCETW, OU, Hyderabad, TS, India* drdasarishravani@stanley.edu.in
[2]*Professor, Department Of CSE, Shadan College of Engineering and Technology JNTUH Hyderabad, TS India* imtiyaz.khan.7@gmail.com
[3]*Assistant Professor CSE, School of Technology, Woxsen University Hyderabad TS India* amogh.deshmukh@woxsen.edu.in
[4]*Assistant Professor, Department Of CSE, SCETW, OU, Hyderabad, TS, India* vanitha@stanley.edu.in
[5]*Assistant Professor, Dept of CSE, KMIT, JNTUH Hyderabad, TS, India* masrathsaba.be@gmail.com
[6]*Professor, Department Of CSE, MJCET, OU, Hyderabad, TS, India* shabbeer.ahmad@mjcollege.ac.in

**Corresponding author's E-mail:* drdasarishravani@stanley.edu.in

Article History

Received: 06 June 2022
Revised: 05 Sept 2022
Accepted: 21 Nov 2022

Abstract

Distributed applications where Internet of Things (IoT) technology integrated are vulnerable to different kinds of attacks. Machine learning algorithms are widely used to detect intrusions in such applications. However, there is need for an effective unsupervised learning approach which can detect known and also unknown attacks. Towards this end, in this paper, we proposed a framework to protect security of IoT integrated architectures that are distributed in nature. Our framework is named Learning based IoT Security Framework (LISF). The framework is designed to have machine learning based security to IoT integrated use cases. Since IoT networks cause network traffic that is to be monitored and protected from external attacks, the proposed system uses deep learning technique for automatic detection of cyber-attacks. Particularly, the system exploits deep autoencoder which comprises of encoder and decoder for automatic detection of different kinds of intrusions. It is based on unsupervised learning which is crucial for distributed environments where network flows cannot have sophisticated training samples. We proposed an algorithm named Deep Autoencoder based Cyber Attack Detection (DAE-CAD). Experiments are made using IoT use case dataset known as UNSW-NB15. Our empirical results revealed that DAE-CAD outperforms existing methods with highest accuracy 91.36%.

Keywords: *Internet of Things, Distributed Architectures, Machine Learning, Deep Learning, Security*

1. Introduction

Security plays an important role in different kinds of networks and applications. With the emergence of Internet of Things (IoT) technology, many distributed use cases came into existence. For instance, smart city is one of the use cases that has distributed architecture and very complex network containing number of smaller networks. In such scenarios, the applications are more vulnerable to attacks. Therefore, it is important to have security mechanisms in place for secure end to end communications. There are many existing solutions that contributed towards security of such applications using machine learning techniques. In fact, many researchers contributed towards security of IoT integrated distributed applications.

Kaur et al. [4] focused on IoT, a transformative force, unifies objects for human control and updates. Literature review assesses technologies, challenges, and applications, highlighting future directions. Gao et al. [7] identified application domains, integration methods, and suggests future research directions. BIM and IoT integration enhance construction efficiency. Darabkh et al. [11] explored global IoT implementation, enabling technologies, challenges, and future directions. Ubiquitous sensing through wireless networks forms the backbone of IoT technologies. Kaur et al. [15] focused on IoT, a pinnacle in communication, transforms real-world objects into smarter devices, notably in precision agriculture. Our contributions in this paper are as follows.

1. We proposed a framework named Learning based IoT Security Framework (LISF) to have machine learning based security to IoT integrated use cases.

2. We proposed an algorithm named Deep Autoencoder based Cyber Attack Detection (DAE- CAD).

3. We built an application to evaluated LISF and our algorithm DAE-CAD using a benchmark dataset.

The remainder of the paper is structured as follows. Section 2 reviews literature on existing security models used for distributed architectures. Section 3 presents our methodology including system model and proposed framework. Section 4 presents experimental results while section 5 concludes our work.

2. Literature Review

This section reviews literature on different existing security methodologies for distributed environments. Lu et al. [1] observed that emerging IoT technology transforms global networks with smart devices, data, and challenges. Security is crucial for accessibility, integrity, and scalability. Ammar et al. [2] reviewed and compares 8 frameworks, emphasizing security features for diverse applications. IoT's pervasive impact necessitates secure frameworks. Mishra et al. [3] analysed software architectures in smart cities, healthcare, and agriculture, proposing improvements for efficiency and performance. IoT automates processes, enhancing services. Kaur et al. [4] focused on IoT, a transformative force, unifies objects for human control and updates. Literature review assesses technologies, challenges, and applications, highlighting future directions. Kumar et al. [5] explored technical and social aspects, highlighting issues, applications, and big data analytics. IoT transforms lifestyles with smart applications, yet challenges persist. Zhang et al. [6] explored architectures, technologies, security, and applications, emphasizing integration benefits. Fog/edge computing enhances IoT, offering faster response and better service quality.

Gao et al. [7] identified application domains, integration methods, and suggests future research directions. BIM and IoT integration enhance construction efficiency. Alabazares et al. [8] proposed a Model-Driven Development (MDD) methodology for IoT software, addressing the lack of components. Architecture ensures interoperability in diverse devices. Javadi et al. [9] surveyed IoT applications through Systematic Literature Review, this paper categorizes and analyses research techniques, identifying challenges and future issues. Parizi et al. [10] enhanced the quality of life but presents security challenges. This survey categorizes threats and solutions by a three-layer architectural view. Darabkh et al. [11] explored global IoT implementation, enabling technologies, challenges, and future directions. Ubiquitous sensing through wireless networks forms the backbone of IoT technologies. Ahmadi et al. [12] systematic literature review explores IoT in healthcare, focusing on applications, architecture, technologies, and challenges. It emphasizes home healthcare and cloud-based architecture. Noura et al. [13] observed that IoT has seen substantial development, but interoperability issues persist due to diverse solutions. This survey categorizes and analyzes strategies and challenges for IoT interoperability.

Ahanger et al. [14] stated that IoT transforms global interactions, posing significant security challenges. Solutions must address privacy, trust, and security across all architectural levels. Kaur et al. [15] focused on IoT, a pinnacle in communication, transforms real-world objects into smarter devices, notably in precision agriculture. Comprehensive research reviews contributions and future directions. Elijah et al. [16] opined that the global population surge and resource challenges drive smart agriculture, employing IoT and data analytics for efficiency and productivity enhancement. Wu et al. [17] stated that IoT integrates with smart city, water, transportation, and manufacturing. Cloud-edge orchestration powered by AI optimizes data processing, but challenges persist. Xu et al. [18] found that IoT involves vast networks of physical devices; centralized security has limitations. Blockchain (BCT) offers security solutions, but challenges persist in integration and application scalability.

Liu et al. [19] tackled integrating field-level manufacturing data with cloud manufacturing, suggesting an IIoT gateway for efficient data management. The approach enhances decision-making and transforms traditional manufacturing into cloud systems. Adhikari et al. [20,23,26] explored fog computing for efficient real-time IoT applications, emphasizing reduced latency, energy consumption, and challenges with potential solutions. From the literature it is observed that there is need for a security framework that could detect known and unknown cyber-attacks. Chander et al. [22] Detection of Anomalies and Leaf Disease Prediction in Cotton Plant Data IIoT environment. [24], [25] They investigated the concept of security using machine learning and deep learning methods for malware detection, as well as android malware detection with classification based on hybrid analysis and N-gram feature extraction. Chander et al. [27] data, identification and detection of outliers/anomalies is a challenging issue and raised as the primary importance of data analysis in IoT applications. Bilahari et al. [28] computing applications in cyber security, and analyzes the scenario of enhancing the cyber security potentials by suggests that of accelerating the intelligence of the security systems.

3. Materials And Methods

We proposed a novel methodology that is based on the system model presented in Figure 1. It is an IoT integrated distributed application scenario where the application is vulnerable to different kinds of attacks unless security is implemented. To overcome this issue, we proposed separate layer in the system model which is elaborated in Figure 4 to have a learning-based security framework. Ours is an AI based solution towards intrusion detection. Our deep learning model takes care of monitoring application for different kinds of attacks and ensures that the system is able to detect such attacks.

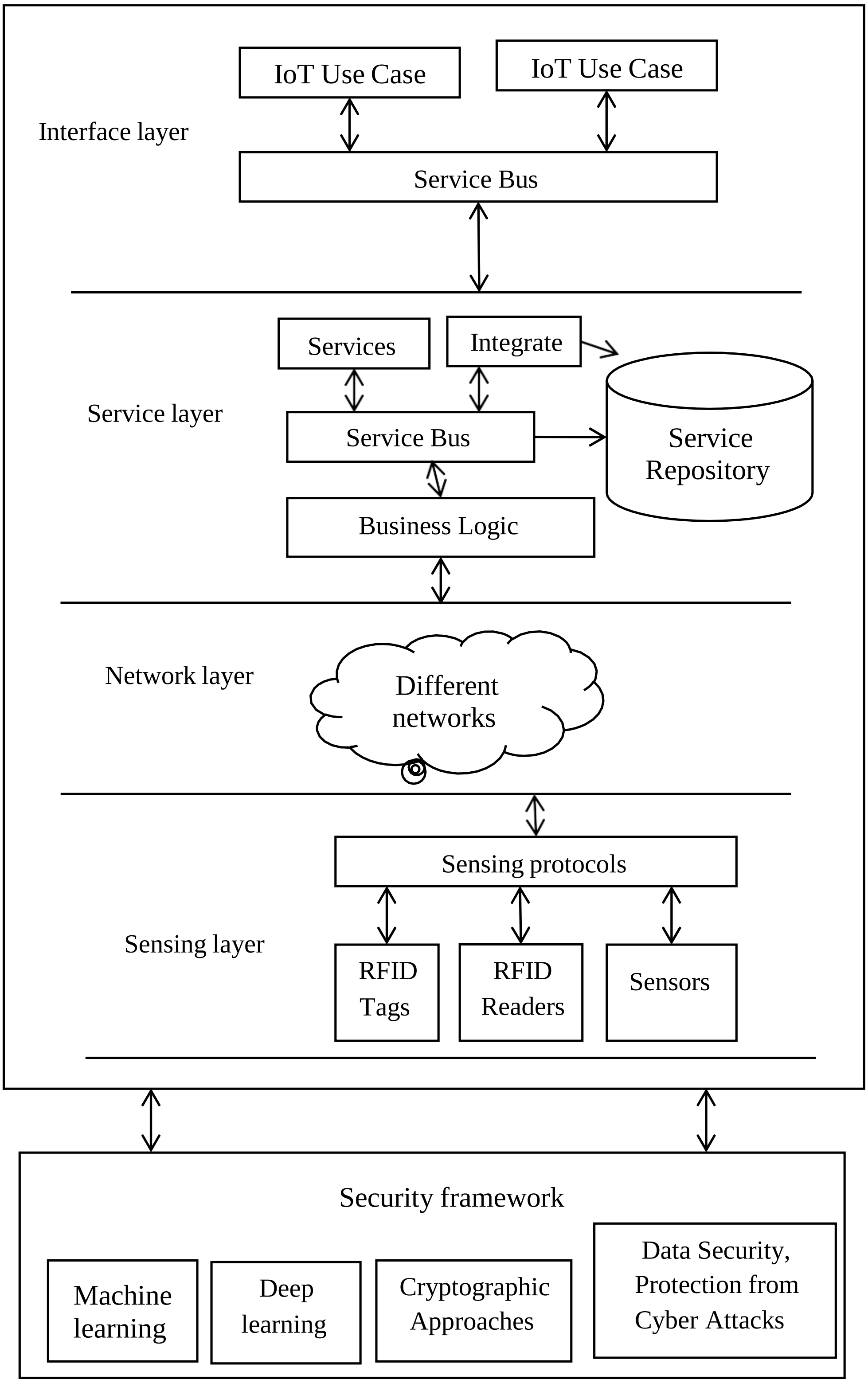

Figure 1: Overview of IoT integrated system model

As presented in Figure 1, an overview of IoT integrated system model is provided reflecting a distributed application scenario. It has provision for security framework which takes care of learning- based protection to the system. It can detect cyber-attacks by employing machine learning techniques. It is an IoT integrated system model which is distributed in nature. It has interface layer where actual IoT or distributed applications run. The service layer provides required business logic and other related services. Network layer provides desired network infrastructure. Sensing layer has sensor network for realizing different smart activities.

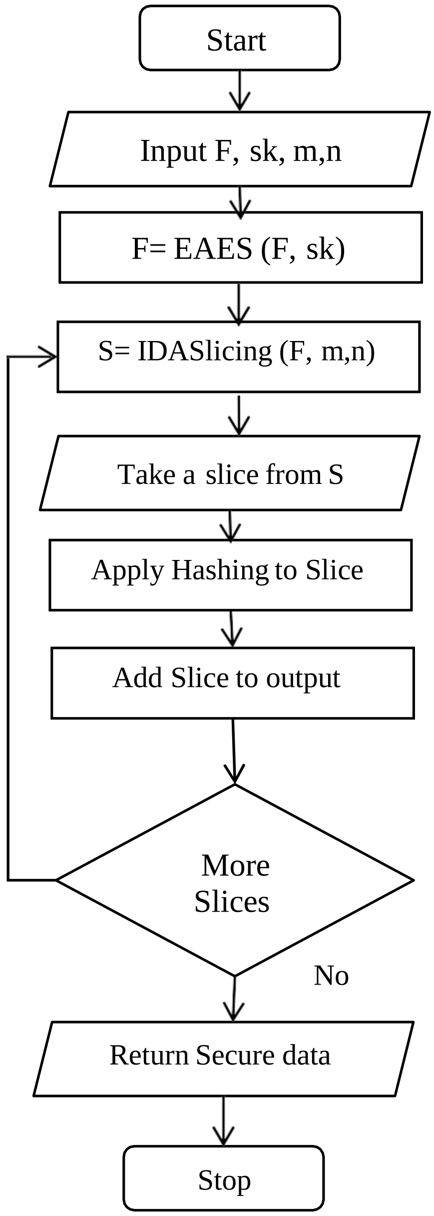

Figure 2: Overview of the proposed encoding process

As presented in Figure 2, it shows an encoding process which can protect applications from attacks that intend to steal data. It is based on many transformations to protect data from different attacks. It helps data to be protected when it is at rest and in transit. It focuses on stronger encryption model. The given file is encrypted using a modified AES algorithm. Then the resultant data is subjected slicing using IDA method. This makes the data more robust to ensure data integrity. Few slices can help in re-establishing the whole data. Finally, the data is subjected to hashing in order to achieve data integrity verification as and when needed.

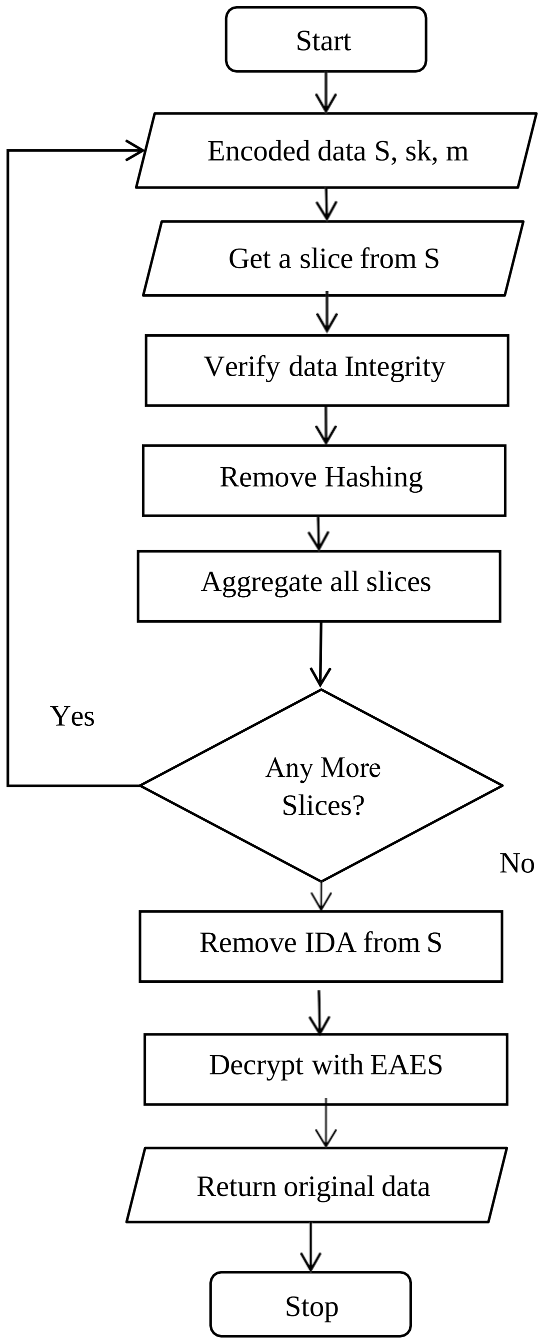

Figure 3: Overview of the proposed decoding process

As presented in Figure 3, there is decoding process which is opposite to the encoding process. It considers encoded data as input along with secret key and converts data into slices. Afterwards, there is integrity verification with the help of hashing. The IDA converts the data into encrypted file. Then the data is decrypted using the modified AES algorithm in order to obtain original content.

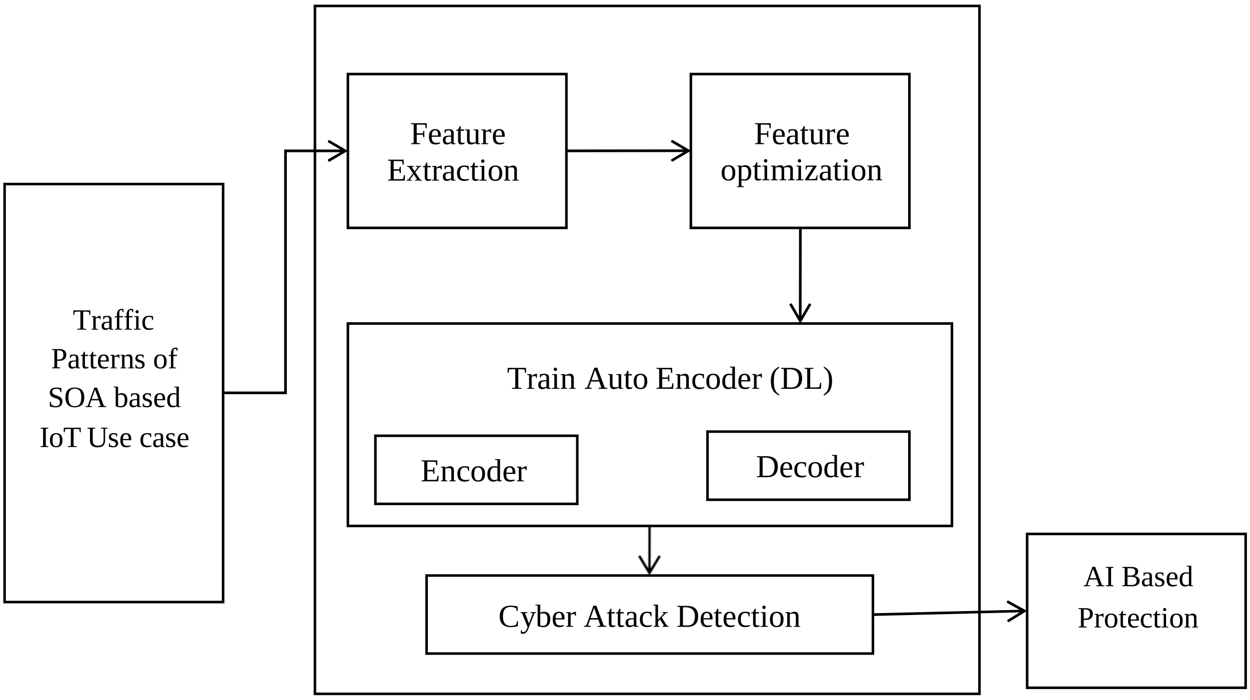

Figure 4: Learning based IoT Security Framework (LISF)

We proposed a framework known as Learning based IoT Security Framework (LISF) for protecting the system from cyber-attacks. It is based on deep autoencoder model which is based on unsupervised learning. Thus, the proposed framework can detect known and unknown attack scenarios. Encoder converts input data into some reduced representation while the decoder reconstructs it to detect different kinds of cyber-attacks. We proposed an algorithm named Deep Autoencoder based Cyber Attack Detection (DAE-CAD).

Algorithm: Deep Autoencoder based Cyber Attack Detection (DAE-CAD)

Input: UNSW-NB15 dataset D

Output: Attack detection results **R**

```
Begin
(T1, T2)←DataSplit(D)
F←EtractFeatures(T1)
F'←OptimizeFeatures(F)
Construct encoder
Construct decoder
Train encoder using F'
Train decoder using F'
R←AutoEncoder(encoder, decoder)
Return R
```

Algorithm 1: Deep Autoencoder based Cyber Attack Detection (DAE-CAD)

As presented in Algorithm 1, the given dataset is divided into training (T1) and test (T2) datasets. Features are extracted and optimized from T1. Then the optimized features are used to train encoder and decoder implicitly. The encoder and decoder perform miniature representation of data and reconstruction of data respectively. When it comes to the attack detection using test data, the autoencoder is employed to detect different kinds of attacks based on the encoding and decoding process.

3. Results and Discussion

We evaluated out framework with deep learning-based implementation to protect IoT use cases from cyber-attacks. Our algorithm named Deep Autoencoder based Cyber Attack Detection (DAE-CAD) is evaluated using an IoT use case dataset known as UNSW-NB15 [21]. This section presents results of experiments.

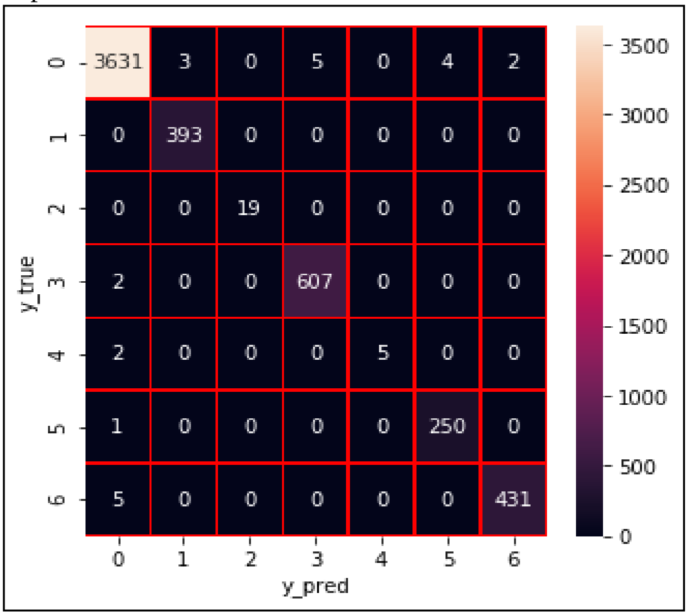

Figure 5: Confusion matrix of the proposed algorithm against different kinds of attacks

As presented in Figure 5, the proposed algorithm showed its performance reflected in the form of confusion matrix. Based on this different performance metrics shown in Table 1.

Table 1: Performance metrics used in this paper

Metric	Formula	Value range	Best Value
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$	[0; 1]	1
Precision (p)	$\frac{TP}{TP + FP}$	[0; 1]	1
Recall (r)	$\frac{TP}{TP + FN}$	[0; 1]	1
F1-Score	$2 * \frac{(p * r)}{(p + r)}$	[0; 1]	1

The proposed method is evaluated using these metrics. The experiments are made using UNSW-NB15 which has 7 kinds of attack instances. This dataset is used for training the proposed model and help in detection of attacks.

Table 2: Experimental results showing performance of different models

Attack Detection Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.78829	0.775965	0.83929	0.806395
Multilayer Perception	0.80512	0.812175	0.82246	0.81719
Decision Tree	0.806225	0.818465	0.81719	0.817785
Random Forest	0.815745	0.81855	0.831555	0.82501
Proposed Deep Autoencoder	0.913634	0.916776	0.931342	0.924011

As presented in Table 2, the proposed deep learning model is compared against different existing machine learning models.

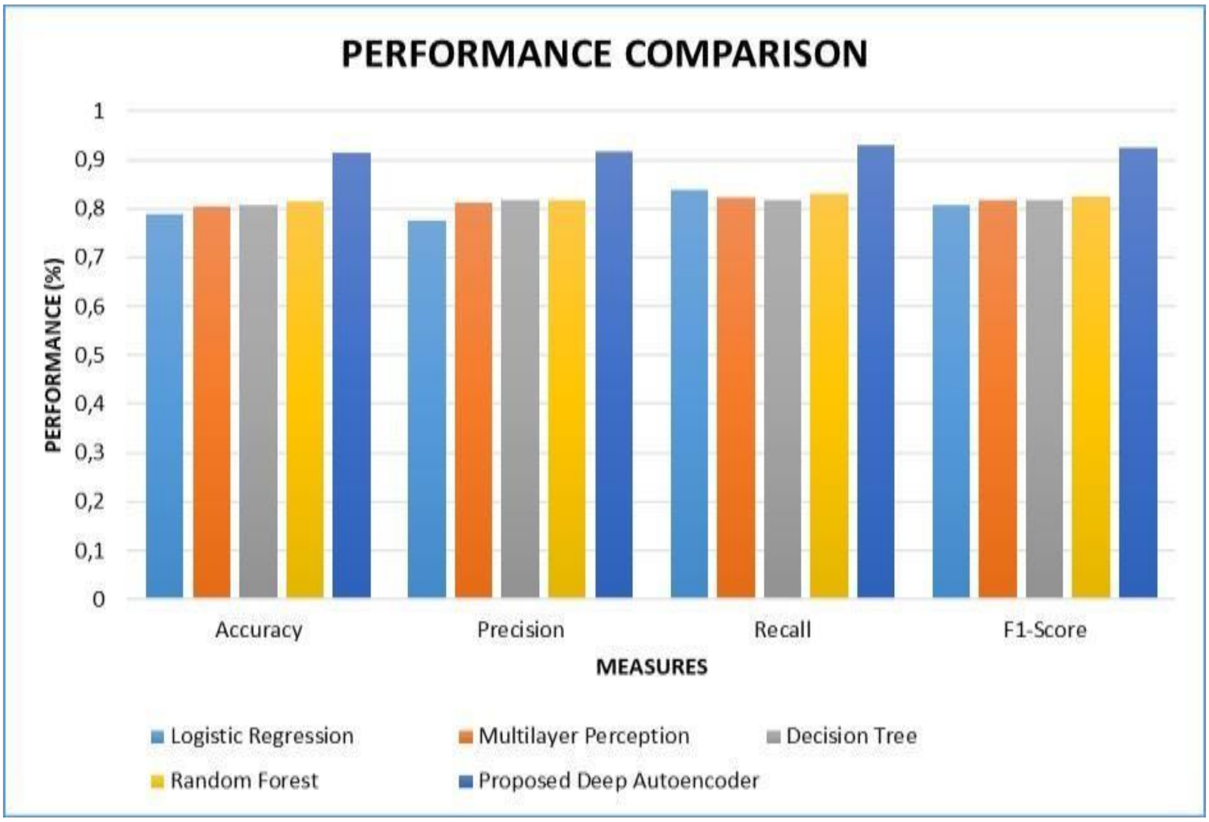

Figure 6: Performance comparison of different attack detection models

As presented in Figure 6, performance of different models in intrusion detection for given IoT use case is evaluated. Higher value for any metric used in the evaluation indicates better performance. Logistic Regression (LR) achieved 78.82% accuracy, Multilayer Perceptron (MLP) showed 80.51%, Decision Tree (DT) 80.62%, Random Forest (RF) exhibited 81.57% while the proposed deep autoencoder based model showed highest accuracy 91.36%. From the experimental results, it is found that the proposed model is capable of improving attack detection accuracy due to its modus operandi and ability to discriminate legitimate and attack traffics.

4. Conclusion

In this paper, we proposed a framework to protect security of IoT integrated architectures that are distributed in nature. Our framework is named Learning based IoT Security Framework (LISF). The framework is designed to have machine learning based security to IoT integrated use cases. Since IoT networks cause network traffic that is to be monitored and protected from external attacks, the proposed system uses deep learning technique for automatic detection of cyber-attacks. Particularly, the system exploits deep autoencoder which comprises of encoder and decoder for automatic detection of different kinds of intrusions. It is based on unsupervised learning which is crucial for distributed environments where network flows cannot have sophisticated training samples. We proposed an algorithm named Deep Autoencoder based Cyber Attack Detection (DAE-CAD). Experiments are made using IoT use case dataset known as UNSW-NB15. Our empirical results revealed that DAE-CAD outperforms existing methods with highest accuracy 91.36%. In future, we intend to improve our framework by using hybrid deep learning model for intrusion detection more efficiently.

References:

1. Lu, Yang and Da Xu, Li (2018). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2018.2869847
2. Ammar, Mahmoud; Russello, Giovanni and Crispo, Bruno (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27. http://doi:10.1016/j.jisa.2017.11.002
3. GavriloviÄ‡ , NebojÅ¡a and Mishra, Alok (2020). Software architecture of the internet of things (IoT) for smart city, healthcare and agriculture: analysis and improvement directions. Journal of Ambient Intelligence and Humanized Computing. http://doi:10.1007/s12652-020-02197-3
4. Khanna, Abhishek and Kaur, Sanmeet (2020). Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. Wireless Personal Communications. http://doi:10.1007/s11277-020- 07446-4

5. Kumar, Sachin; Tiwari, Prayag and Zymbler, Mikhail (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1), 111–. http://doi:10.1186/s40537-019-0268-2
6. Lin, Jie; Yu, Wei; Zhang, Nan; Yang, Xinyu; Zhang, Hanlin and Zhao, Wei (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2017.2683200
7. Tang, Shu; Shelden, Dennis R.; Eastman, Charles M.; Pishdad-Bozorgi, Pardis and Gao, Xinghua (2019). A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends. Automation in Construction, 101, 127–139. http://doi:10.1016/j.autcon.2019.01.020
8. Sosa-Reyna, Claudia M.; Tello-Leal, Edgar and Lara-Alabazares, David (2018). Methodology for the Model- Driven Development of Service Oriented IoT Applications. Journal of Systems Architecture, S1383762118301875–. http://doi:10.1016/j.sysarc.2018.08.008
9. Asghari, Parvaneh; Rahmani, Amir Masoud and Javadi, Hamid Haj Seyyed (2018). Internet of Things applications: A Systematic Review. Computer Networks, S1389128618305127–. http://doi:10.1016/j.comnet.2018.12.008
10. HaddadPajouh, Hamed and Parizi, Reza (2019). A Survey on Internet of Things Security: Requirements, Challenges, and Solutions. Internet of Things, 100129–. http://doi:10.1016/j.iot.2019.100129
11. Kassab, Wafa'a and Darabkh, Khalid A. (2020). Aâ€ " Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. Journal of Network and Computer Applications, 163, 102663–. http://doi:10.1016/j.jnca.2020.102663
12. Ahmadi, Hossein; Arji, Goli; Shahmoradi, Leila; Safdari, Reza; Nilashi, Mehrbakhsh and Alizadeh, Mojtaba (2018). The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society. http://doi:10.1007/s10209-018-0618-4
13. Noura, Mahda; Atiquzzaman, Mohammed and Gaedke, Martin (2018). Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Networks and Applications. http://doi:10.1007/s11036- 018-1089-9
14. Ahanger, Tariq Ahamed and Aljumah, Abdullah (2018). Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. IEEE Access, 1–1. http://doi:10.1109/ACCESS.2018.2876939
15. Khanna, Abhishek and Kaur, Sanmeet (2019). Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Computers and Electronics in Agriculture, 157, 218–231. http://doi:10.1016/j.compag.2018.12.039
16. Elijah, Olakunle; Rahman, Tharek Abdul; Orikumhi, Igbafe; Leow, Chee Yen and Hindia, MHD Nour (2018). An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2018.2844296
17. Wu, Yulei (2020). Cloud-Edge Orchestration for the Internet-of-Things: Architecture and AI-Powered Data Processing. IEEE Internet of Things Journal, 1–1. Http://doi:10.1109/JIOT.2020.3014845
18. Viriyasitavat, Wattana; Da Xu, Li; Bi, Zhuming and Hoonsopon, Danupol (2019). Blockchain Technology for Applications in Internet of Things -Mapping from System Design Perspective. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2019.2925825
19. Chao Liu, Ziwei Su, Xun Xu and Yuqian Lu. (2022). Service-oriented industrial internet of things gateway for cloud manufacturing. *Elsevier*, pp.1-14. https://doi.org/10.1016/j.rcim.2021.102217
20. Abhishek Hazra, Pradeep Rana, Mainak Adhikari and Tarachand Amgoth. (2022). Fog Computing for Next- Generation Internet of Things: Fundamental, State-of-the-Art and Research Challenges. *elsevier*, p.112–134.
21. Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.
22. Chander, Nenavath, and M. Upendra Kumar. "Comparative Analysis on Deep Learning Models for Detection of Anomalies and Leaf Disease Prediction in Cotton Plant Data." Congress on Intelligent Systems. Singapore: Springer Nature Singapore, 2022.
23. Ravi, Eslavath, and Mummadi Upendra Kumar. "A Comparative Study on Machine Learning and Deep Learning Methods for Malware Detection." Journal of Theoretical and Applied Information Technology 100.20 (2022).
24. Ravi, Eslavath, and Mummadi Upendra Kumar. "Android malware detection with classification based on hybrid analysis and N-gram feature extraction." International Conference on Advancements in Smart Computing and Information Security. Cham: Springer Nature Switzerland, 2022.
25. Chander, Nenavath, and M. Upendra Kumar. "Machine Learning Based Outlier Detection Techniques For Iot Data Analysis: A Comprehensive Survey."

26. Bilahari, Alk, And Nenavath Chander. "The Potentiality Of Artificial Intelligence In Cyber Security." (2017).