National Research Journal of Information Technology & Information Science
Volume No: 12, Issue No: 2, Year: 2025 (July- December)
PP: 474-488
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

PERFORMANCE ANALYSIS OF INTELLIGENT SECURITY PROVISIONS FOR INTERNET OF THINGS

Paramjit Singh Waraich

Assistant professor

PG Department of Computer Science and Applications

* GGDSD College, Sec-32, Chandigarh

ABSTRACT-.

IoT networks can be deployed in different domains. Such type of networks depend over the internet services for the transmission and data exchange thus may invite the common cyber security threats those are associated with the traditional internet services as well as these networks operate in unattended environment that is another security challenge as intruder can join the network any time to intercept the transmission. This paper explores the different types of security threats those can interrupt the communication along with their intelligent security provisions developed by different researchers and these are related to authentication, intrusion detection and prevention, trust management, data integrity and privacy etc. using various techniques based on machine and deep learning algorithms, blockchain technology and other cryptography methods etc. Study will also analysis their performance in terms of threat detection accuracy, f1-score, recall, precision etc.

Keywords- IoT networks, Network Security, Intrusion, Authentication, Machine learning, Deep learning

I. INTRODUCTION

Internet of Things (IoT) facilitates the data transmission between various devices such as mobile phones/ sensors/computers/robots/ actuators etc. Figure 1 shows the basic overview of IoT based networks that support the communication between different field devices, called sensors and end users using internet platform.

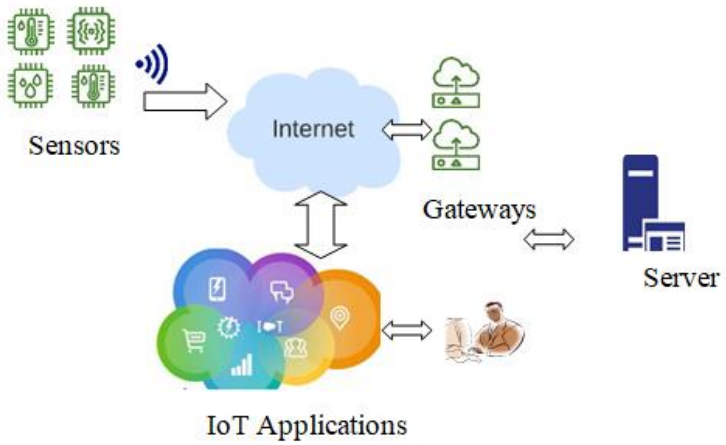

Figure 1: Overview of a IoT Network [1]

IoT network consists of different layers those are responsible for dedicated operations i.e. perception layer deals with the field sensors network layer handles the routing requests and application layer interacts with the end users and there are different security threats w.r.t. each layer as shown in Table 1.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Table 1 Security threats for IoT networks [2]

IoT network layers	Security Threats
Perception layer	Spoofing Signal Jamming Device capturing
Network Layer	Routing diversion Denial of Services Sniffing Sybil attack [3]
Application Layer	Code Injection Data Integrity Violation Unauthorized Access Session hijacking Phishing Data leakage [4] Cross scripting Malware Reply Attack Brute Force attack

Security goals for IoT networks

IoT networks should facilitate the data exchange in secure manner and a security provision must fulfill the common security goals for the end users as described in Figure 2:

Figure 2: IoT Security goals [1]

- **Data confidentiality:** IoT network must be able to retain the data confidentiality and various cryptography based methods can be used to achieve this goal. Intruders must not be able to read the data at any cost [5].
- **Authorization:** There is need to define the list of resources those may be accessible to the IoT devices. All devices must not be able to access entire network resources.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

- **Authentication:** There is need to identify the devices engaged in data transmission. IoT network must perform authentication of individual devices.
- **Data Integrity:** IoT network must ensure the data integrity during the transmission and intruder must not be able to modify the data at intermediate state.
- **Availability:** IoT network must ensure that all services are available to the end users and there should not be any interrupt during communication [6].

CHALLENGES FOR IOT NETWORKS

IoT networks perform various operations related to user data exchange and its transmission over open environment and it becomes very challenging to secure all network operation and different security holes may invite the intruders to intercept the communication. A security provision deals with the following challenges as mentioned below:

- **Access Control:** It is quite complex to manage the access control for the individual device over a large scale network. It is also a major challenge to define the roles w.r.t. each IoT device.
- **Secure routing:** IoT networks may use different routing protocols and it is quite challenging to secure the routing data over compromised network.
- **Device Identification and authentication:** IoT devices may be connected to large scale network and it is very time consuming to perform identification/ authentication of individual device [7].
- **Intrusion detection & prevention:** It is very challenging task to differentiate between legitimate and malicious devices as intruder can replicate the device signatures. IoT network must be able to analyze the abnormalities inside the network
- **Hardware compatibility:** End users may use the different devices developed by different venders. IoT network must be able to ensure the compatibility between these devices.
- **Key management:** It is quite complex to manage the key pairs for entire network, as device may join/leave the network at any time [8].

IoT networks use the low powered devices for communicaiton and there are various concerns which may act as barrier for the implementation of a security provision as given below:

- Optimal resource consumption/computational overhead etc.
- Device's hardware and software compatibilty w.r.t. universal standards defined by various vendors.

  Hetrogenious network operations [9][35]

II. LITERATURE SURVEY

These days, usage of IoT based networks is rapidly increasing along with the security threats and due to intensive dependency over the electronic devices and intruders may trigger various attacks by intercepting the end devices. Various researchers addressed the different security concerns and developed the different solutions to secure the IoT networks. Following section highlights the recently developed solutions to secure the IoT networks against various threats:

(a) Solutions for data privacy

A. Nazir et al. [10] explored the advance level security provisions for IoT networks. It includes the solutions based on blockchain, deep neural networks (DNN) and machine

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

leaning algorithms based schemes and developed a framework by integrating the logistic regression with DNN. First of all, it learns from the dataset and analyzes the traffic for abnormalities and blockchain provides data transparency. Experiments indicate that it offers robust security as compared to tradition security solutions.

D. Regvart et al. [13] presented a layered based security provision to secure the data exchange between IoT devices and cloud services. First of all, it perform authentication for intermediate IoT devices and only legitimate devices are permitted to connect over cloud platform. Experiments show that it offers multilayer security for IoT devices with optimal resource consumption.

S. Ahmed et al. [18] presented a solution to secure the communication between IoT devices and the intermediate router. IoT devices use cryptography algorithms to encrypt the packets and forward them to router that is responsible to send the packet to base station after verifying the integrity of the packets. Experiments show that it ensures the data confidentiality and integrity at optimal operational cost.

D. S. Tundalwar et al. [23] investigated the security threats (packet tracing/spoofing/intrusion etc.) for IoT networks and study found that all network can be protected using lightweight cryptography methods as well as blockchain technology can be integrated to secure the data. It also shows that machine learning support can be integrated with the existing security provision.

M. G. Spina et al. [24] integrated the cryptography method with Constrained Application Protocol (CoAP). Analysis shows that it can secure the communication over large scale heterogeneous network and it outperforms in terms of optimal energy consumption as compared to exiting solutions.

K. Kasat et al. [29] developed a solution to secure the communication over healthcare based IoT networks. It uses a cryptography method that performs encoding of data before the transmission and alter on decoding is performed at receiver end. Analysis shows that it provides robust security for IoT networks as compared to existing schemes.

(b) Authentication based solutions

D. Sharma et al. [14] developed a solution to secure the communication over IoT networks those are deployed to monitor the livestock at agriculture land. First of all, it authenticates the intermediate devices and also enforces the access control list over network resources and transmits the encrypted data over wireless channel. Experiments show that it can guard the network against eavesdropping threat efficiently as compared to existing solutions.

K. Jeysuriya [16] introduced a trust based security model that supports multiple features i.e. threat detection, access control. It builds a trust model after performing risk analysis w.r.t. IoT devices and grants the access to network resources. Malicious device is identified, if its activities are abnormal and does not match with the trust model. Experiments show that it can efficiently guard the network and it has higher anomaly detection ratio with optimal false positive ratio as compared to existing schemes.

W. Jing et al. [20] implemented a security scheme for IoT networks that authenticates the IoT devices using radio frequency based patterns. It allows the data exchange between all devices operating over same frequency and for other devices, communication is denied. Experiments show that it offers secure transmission over large scale IoT networks and can defend the network against common threats i.e. efficiently spoofing/data disclosure/ tampering etc.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

N. Chaurasia et al. [21] investigated the various security concerns related to IoT networks. Study found that it is access control to network resources is quite difficult as multiple devices can share the data over shared channel and node identification is another major issue as nodes can join the network at any time. Study also found that IoT networks are vulnerable to several security threats i.e. denial of services, man-in-middle attack etc. Analysis indicates that all these are open issues and there is need to develop robust solutions for the same.

N. Tripathi et al. [22] investigated the security issues and solutions for IoT network and it found that data privacy is the major concern over large scale network as it is quite complex to ensure the authenticity and trust level of the intermediate devices, however, data can be secured using cryptographic techniques but due to error prone transmission, it is quite difficult to maintain the data integrity. Analysis shows that all these are open issues and there is need to develop advance level solutions to secure the communication over IoT networks.

S. Tanimoto et al. [25] enforced the policy based security provision for fog computing based IoT networks. It uses different policies for different layers and allows the communication, if devices fulfill the constraints of the security policies. Analysis shows that policies can be dynamically reconfigured as per requirements and it is suitable for large scale IoT networks.

B. B. Sundaram et al. [26] presented an automated authentication scheme for the IoT devices. It uses unique signature to register the devices over network and later on, it is used for authentication purpose. Analysis shows that it is suitable for dynamic IoT network in which devices can join/leave the network at any time and there is no need to register them again.

S. Yoon et al. [27] developed an authentication scheme for IoT network. It defines the ownership of the devices using a physical unclonable function and later on it is used to authenticate the devices during transmission over cloud platform. Analysis shows that it supports the secure and open connectivity for IoT networks.

V. O. Nyangaresi [31] presented a elliptic curve based security provision that uses token based data exchange over large scale IoT network. IoT devices having valid tokens can initiate the transmission over network and analysis shows that it has less computational overhead as compared to the exiting solution (Burrows–Abadi–Needham logic) and supports the secure communication over heterogeneous environment.

F. Zhou et al. [32] explored the various security issues related to Narrow Band IoT (NB-IoT). Analysis found that unauthorized access to network resources and signal jamming are most common threats and these can be fixed using security policies i.e. device registration/certificate based identification, network traffic audit etc.

M.S. Jian et al. [33] presented hybrid security provision for IoT networks. It uses public key cryptography for communication and each IoT device uses MAC address based signature for identification over network and exchange the encrypted data using session keys. Analysis shows that it has less computational overhead as compared to traditional cryptography based solutions.

D. Liao et al. [34] proposed a blockchain based solution for data acquisition over IoT networks. It assigns different voting weights to pear devices and it uses a dynamic permission adjustment scheme for the data acquisition w.r.t. voting weights. Experiments show that it consumes fewer resources as compared to traditional data collection schemes.

(c) Machine learning & Deep learning based threat detection and prevention

R. I. Chandni et al. [11] proposed intelligent security provision for IoT networks. It uses a threat dataset to build a training model and it uses different classifiers to identify the threat

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

patterns over network traffic. Experiments indicate that it can efficiently identify the intrusion over network as compared to existing intrusion detection systems.

R. Kalaria et al. [12] developed a framework to analyze the activities of the IoT devices using Hidden Markov Model and finally, it generates the prediction for malicious device, if it is engage in any abnormal network operation i.e. continues packet drop, intensive packet forwarding etc. Analysis shows that it is more efficient and responsive as compared to the traditional intrusion detection scheme.

A. A. Dar et al. [15] developed a security audit protocol for the IoT networks. It performs risk analysis of various vulnerabilities for the IoT devices and using the risk assessment, it allows the network access to legitimate devices only. Analysis shows that it achieves different security goals i.e. data auditing, confidentiality, Integrity and availability etc.

R. Yalda et al. [17] investigated the security issues of IoT networks and integrated the open source intrusion detection and prevention scheme with the IoT platform. Analysis shows that user can customize the rules as per the security requirements and its operational cost is minimal as compared to existing security provisions.

D. Kumar et al. [19] used the support vector based intrusion detection to secure the communication over IoT networks. It uses a dataset that contains different network traffic traces. In case of intrusion, patterns are marched with the existing dataset. Simulation results indicate that it outperforms in terms of optimal threat detection rate/recall, accuracy and F-measure etc. as compared to existing solutions.

M. R. Nosouhi et al. [28] developed a learning model that enforces feature based security over advance level IoT networks. It builds a model using different features (radio frequency and data rate) and later on it is utilized to trace the abnormalities in transmission. Analysis shows that it allows only legitimate devices to access the network and it has higher threat detection rate as compared to existing solutions.

P. Kumar et al. [30] presented deep learning based advance solution to guard the IoT network against denial of service threat. It uses a predefined threat dataset to build a learning model. During the transmission, traffic patterns are verified using this dataset and malicious devices are isolated from network. Experiments show that it has higher rate for threat classification as compared existing machine learning based solutions.

There are different solutions to secure the IoT networks based communication and each solution deals with the individual security threat using different methods to handle security threat. Table 2: compares the existing security solutions developed for IoT networks:

Table 2 Comparison of different security provisions

Scheme	Outcomes	Limitations
logistic regression and DNN for data transparency [10]	robust security	performance depends over input data size
intelligent security provision using Threat classification [11]	Accurate threat detection	Predefined dataset is required
Security framework for IoT network using Hidden Markov Model [12]	Higher intrusion detection rate	Complexity
layered based security provision for Secure the data exchange between IoT	multilayer security for IoT devices	Provided a n overview of IoT

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

devices and cloud services [13]		security provisions
Data encryption & access control list for secure monitoring of livestock over agriculture land[14]	Secure data transmission	Usage of complex cryptography methods
Security audit protocol for data security [15]	Ensures the basic security goals	Complex security audit process
trust based security model for threat detection [16]	higher anomaly detection ratio with optimal false positive ratio	Control overhead
open source intrusion detection and prevention scheme [17]	Optimal operational cost	Implementation cost
Public key cryptography algorithm for secure the communication[18]	data confidentiality & integrity	Application dependency
Traffic analysis using support vector based intrusion detection [19]	optimal threat detection rate	Validation of intrusion dataset is required to optimize the outcomes
Radio frequency based pattern matching for Device authentication[20]	Secure access for legitimate devices	Radio interference may degrade the accuracy
Analysis of authentication issues[21]	Overview of identification issues & remedies	Provided an overview of common security concerns
Analysis of data security goals[22]	Overview of data privacy concerns	Operational cost
Analysis of blockchain based solutions[23]	Overview of security concerns	Excessive computational overhead
Cryptography method to secure routing[24]	optimal energy consumption	Protocol dependency
policy based security provision to exchange data over heterogeneous platform [25]	Secure transmission	Compatibility of security provision with heterogeneous network types
Signature registration for automated authentication[26]	Compatible with for dynamic IoT networks	Hardware type dependency
physical unclonable function for Authentication [27]	Secure transmission over cloud platform	Dependency over dedicated cloud platform
feature based security [28]	Efficient access control	Accuracy may vary w.r.t. extracted feature
Data encoding/decoding for secure the communication for healthcare	Lightweight security scheme	Outcomes may be affected due to

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

domain[29]		error prone encoding/decoding
Threat classification using deep learning [30]	Higher threat detection ratio	Accuracy depends over the input dataset
Secure communication using token based data exchange [31]	Data security with optimal computational overhead	Complexity
Security issues analysis for Narrow Band IoT (NB-IoT). [32]	Identification of common threats those can be fixed using security policies	Provided an overview of various security concerns
public key cryptography based node identification [33]	Secure transmission with optimal overhead	Dependency over multiple services for data security
Blockchain scheme for secure data collection [34]	Secure data acquisition	Complexity

IoT networks have various applications in healthcare, agriculture, education, military, cities and home appliances etc. and in each domain, there may be common security threats and scope of the current research work explores the various security concerns associated with IoT networks. It can be observed different researches developed various schemes but no single solution exists to achieve the IoT security goals. For different security issues, users have to deploy different solutions and study found the following research gaps as discussed below:

- IoT networks use the different platforms, devices and communication technologies thus may raise the different security threats. Only few researchers highlighted the recently developed security provisions under the constraints of advance level security threats. This is still an open issue and further investigation is required to develop a robust security solution.
- Researchers did not consider the network scalability for authentication process and it is quite critical factor for network performance and there is need to develop an authentication scheme to retain the higher degree of trust level.
- It is also challenging to secure the routing data during the transmission but only few researchers addressed this issue and there is need to integrate the security provision with IoT protocols.

III. PERFORMANCE ANALYSIS OF VARIOUS SOLUTIONS DEVELOPED BY RESEARCHERS

Table 3: Performance analysis of various security provisions

	Parameters			
Security Provisions	Accuracy	F1-Score	Recall	Precision
MISV [11]	86.4	x	x	x
OSVM [19]	97	99	96	x
SAD-IoT [30]	99.5	x	x	x

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

IoT-FP [12]	90	91	92	89
TSRN [28]	98.6	x	x	x
HMD-GCN-LSTM [36]	99	99	98	97
HCNN-LSTM [37]	97.14	x	x	82.32
HDIDS [38]	98.62	x	x	x
AGMC [39]	96.45	x	x	87
GADPL [40]	99	x	x	98.62
SFML-IoT [41]	96	96	99	94
FIDWATCH [42]	97	95.63	x	x
CART [43]	77	75	77	77
EFAP [44]	99	x	x	99
ADV-IoT-Sec [45]	98	x	99	x

Table 3: shows the performance analysis of various security provisions using different parameters used by researchers for evaluations.

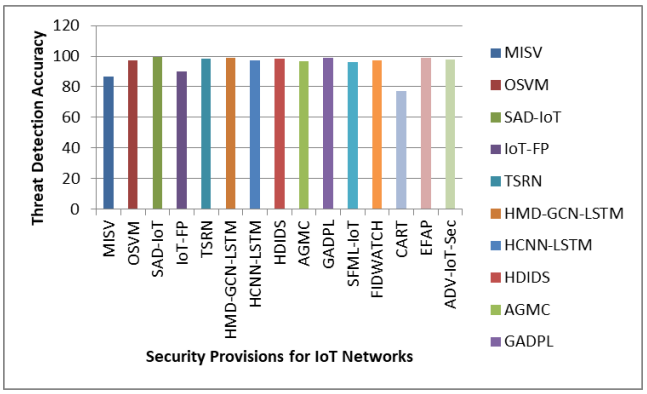

Figure : 3 Threat Detection Accuracy of Security-provisions-IoT Networks

Figure : 3 shows the threat detection accuracy of different security provisions developed for IoT Networks. It is 86.4% for MISV [11], 90% for IoT-FP [12], 97% for OSVM [19], 98.6% for TSRN [28], 99 % for HMD-GCN-LSTM [36],97.14% for HCNN-LSTM [37], 98.62% for HDIDS [38], 96.45% for AGMC [39], 99% for GADPL [40], 96% for SFML-IoT [41], 97% for FIDWATCH [42], 77% for CART [43], 99% for EFAP [44] and 98% for ADV-IoT-Sec [45] (as per the table 3).

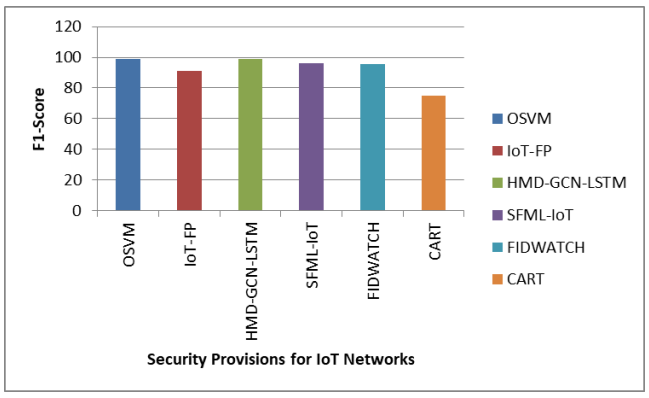

Figure: 4 F1-Score for Security-provisions-IoT Networks

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Figure: 4 shows the value of F1-Score for different security provisions developed for IoT Networks. F1-score for OSVM is 99, 91 for IoT-FP, 99 for HMD-GCN-LSTM, 96 for SFML-IoT, 95.63 for FIDWATCH and 75 for CART.

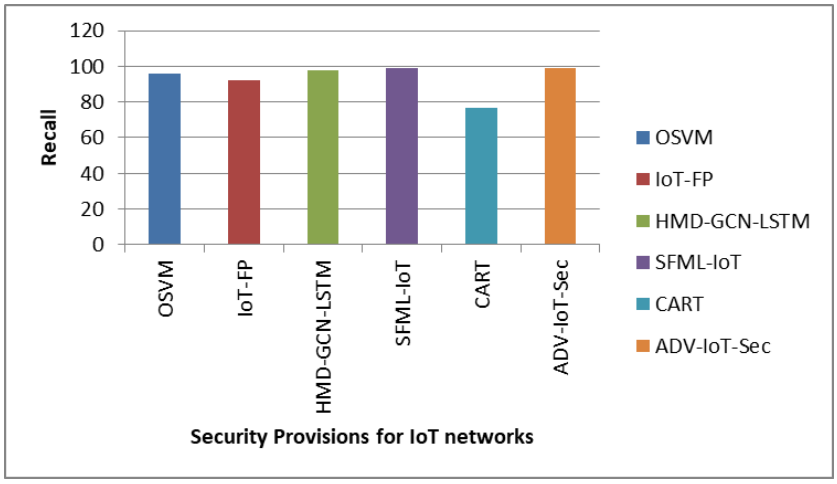

Figure: 5 Recall-for Security-provisions-IoT Networks

Figure: 5 shows the value of Recall value for different security provisions developed for IoT Networks. It is 96 for OSVM, 92 for IoT-FP, 98 for HMD-GCN-LSTM, 99 for SFML-IoT, 77 for CART, 99 for ADV-IoT-Sec.

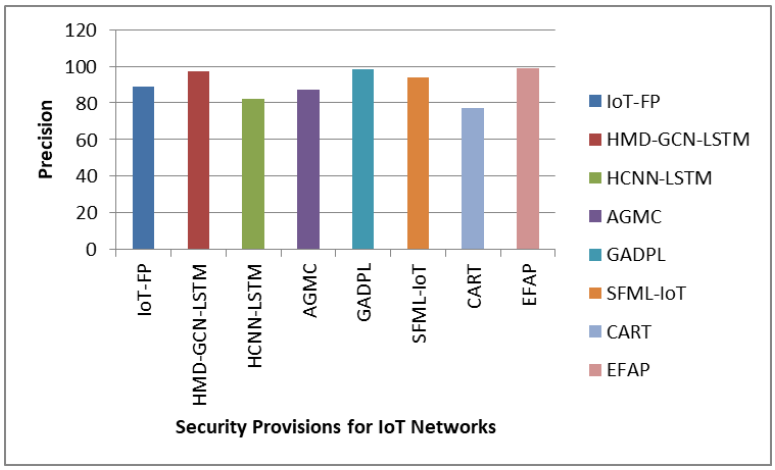

Figure: 6 Precision-for Security-provisions-IoT Networks

Figure: 6 shows the value of Precision value for different security provisions developed for IoT Networks. 89 for IoT-FP, 97 for HMD-GCN-LSTM, 82.32 for HCNN-LSTM, 87 for AGMC, 98.62 for GADPL, 94 for SFML-IoT, 77 for CART and 99 for EFAP.

IV. CONCLUSION

In this paper, different security threats along with their security provisions are explored. As per the survey, it can be observed that IoT networks have various applications and day by day, density of IoT devices is increasing and thus may raise the various security concerns. Study found that there is no single security solution that can protect the IoT network against multiple security threats and researchers developed advance level security provision using deep learning, machine learning and blockchain technology based solution to achieve the desired security goals and performance analysis of these schemes show that SAD-IoT, HMD-GCN-LSTM, GADPL and EFAP has the highest threat detection accuracy followed by

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

HDIDS, TSRN, ADV-IoT-Sec, OSVM, FIDWATCH, HCNN-LSTM, AGMC, SFML-IoT and it is average for IoT-FP and MISV. HMD-GCN-LSTM and OSVM has highest F1-score followed by SFML-IoT FIDWATCH, IoT-FP and it is lowest for CART. SFML-IoT and ADV-IoT-Sec both have highest Recall value as compared to HMD-GCN-LSTM, OSVM, IoT-FP and it is lowest for CART. Precision is highest for EFAP GADPL followed by SFML-IoT HMD-GCN-LSTM, AGMC and it is lowest for HCNN-LSTM and CART. As per analysis it can be stated that HMD-GCN-LSTM and SFML-IoT both have highest performance in terms of above mentioned parameters whereas IoT-FP is average performer and performance of CART is not up to a significant level. Study found that authentication over IoT networks is very critical and it is necessary to restrict the access to network resources, in order to prevent the security threats as well as a machine learning based solution can be developed provide the robust and secure communication over IoT networks. In future, an intelligent security framework will be introduced to enforce the authentication and security over the IoT networks using machine learning algorithms.

REFERENCES

1. M. Adam, M. Hammoudeh, R. Alrawashdeh and B. Alsulaimy, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," in *IEEE Access*, Vol. 12, IEEE-2024, pp. 57128-57149, doi: 10.1109/ACCESS.2024.3382709.
2. A. Gupta, T. Gulati and A. K. Bindal, "WSN based IoT applications: A Review",10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing, IEEE-2022, pp.1-6, doi: 10.1109/ICETET-SIP-2254415.2022.9791495.
3. C. Haar and E. Buchmann, "IoT Security With INFINITE: The 3-Dimensional Internet Of Things Maturity Model", 9th International Conference on Internet of Things: Systems, Management and Security, IEEE-2022, pp. 1-8, doi: 10.1109/IOTSMS58070.2022.10062148.
4. W. Najib, S. Sulistyo and Widyawan, "Trust Based Security Model in IoT Ecosystem", 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, IEEE-2022, pp. 195-199, doi: 10.1109/ICITISEE57756.2022.10057930.
5. M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov and M. Derawi, "A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey," in IEEE Access, Vol. 10, pp. 101362-101384, IEEE-2022, doi: 10.1109/ACCESS.2022.3207472.
6. A. Rakshe and N. Dongre, "Survey on Security Protocols for IoT," 9th International Conference for Convergence in Technology, IEEE-2024, pp. 1-5, doi: 10.1109/I2CT61223.2024.10544115.
7. A. Bhoomadevi, P. l. Soundarraj, V. Gupta, S. K. Kumaravel, S. Deivasigamani and A. Kumar, "Security and Privacy in Internet of Things (IoT) Environments", 9th International Conference on Science Technology Engineering and Mathematics IEEE-2024, pp. 1-6, doi: 10.1109/ICONSTEM60960.2024.10568633.
8. A. Raj, S.D. Shetty, "IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey", Wireless Personal Communications, Vol.122, Springer-2022, pp.1481–1517. doi:10.1007/s11277-021-08958-3.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

9. O.I Abiodun, E.O., Alawida,M.Alawida R.S. Alkhawaldeh, H. Arshad, "A Review on the Security of the Internet of Things: Challenges and Solutions. Wireless Personal Communications, Vol.119, Springer-2021, pp.2603–2637, doi:10.1007/s11277-021-08348-9.
10. A. Nazir, J. He, N. Zhu, M.S. Anwar, M. S. Pathan ,"Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain", Cluster Computing, Vol. 27, Springer-2024, pp.8367–8392, doi:10.1007/s10586-024-04436-0.
11. R. I. Chandni and M. S. Parvin, "Mitigating IoT Security Vulnerabilities Using Artificial Intelligence Approaches", 3rd International Conference on Advancement in Electrical and Electronic Engineering , IEEE-2024, pp. 1-6, doi: 10.1109/ICAEEE62219.2024.10561881.
12. R. Kalaria, A.S.M. Kayes, W. Rahayu, E. Pardede, A. Salehi S., "IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks", Computers & Security, Vol.146, Elsevier-2024, pp.1-11, doi.org/10.1016/j.cose.2024.104037.
13. D. Regvart, M. Mikuc, L. Zgrablić, Z. Morić, "Enhancing Security of Intermediate Devices in the Connection between IoT Devices and Cloud Service,"47th MIPRO ICT and Electronics Convention, IEEE-2024,pp.1537-1542, doi:10.1109/MIPRO60963.2024.10569748.
14. D. Sharma, P. Anawade, S. Gahane and Y. Patil, "Security and Privacy Considerations in IoT-Based Livestock Monitoring Systems", International Conference on Innovations and Challenges in Emerging Technologies, IEEE-2024, pp. 1-6, doi: 10.1109/ICICET59348.2024.10616284.
15. A. A. Dar, F. A. Reegu, S. Ahmed and G. Hussain, "Strategic Security Audit Protocol: Safeguarding Smart Home IoT Devices against Vulnerabilities", 11th International Conference on Computing for Sustainable Global Development, IEEE-2024, pp. 1386-1391, doi: 10.23919/INDIACom61295.2024.10498906.
16. K. Jeysuriya, "MR-TBA – An improved Trust-based Security mechanism for IoT Networks", IEEE International Students' Conference on Electrical, Electronics and Computer Science IEEE-2024, pp. 1-5, doi: 10.1109/SCEECS61402.2024.10481829.
17. R. Yalda, N. Nepal and T. El Hawari, "Enhancing IoT Security Affordably with Raspberry Pi and Open-Source IDS/IPS", IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia, IEEE-2024, pp. 1-6, doi: 10.1109/IC_ASET61847.2024.10596202.
18. S. Ahmed and M. Z. Ali, "Application-Specific Security in IoT Network", 21st Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, IEEE-2024, pp. 636-637, doi: 10.1109/CCNC51664.2024.10454649.
19. D. Kumar, P. P. Pawar, B. Ananthan, S. Rajasekaran and T. V. Prabhakaran, "Optimized Support Vector Machine Based Fused IoT Network Security Management", 3rd International Conference on Artificial Intelligence For Internet of Things, IEEE-2024, pp. 1-5, doi: 10.1109/AIIoT58432.2024.10574673.
20. W. Jing, L. Peng, H. Fu and A. Hu, "An Authentication Mechanism Based on Zero Trust With Radio Frequency Fingerprint for Internet of Things Networks," in IEEE

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Internet of Things Journal, Vol.11 (13), IEEE-2024, pp.23683-23698, doi: 10.1109/JIOT.2024.3385989.

21. N. Chaurasia, P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in IoT", e-Prime - Advances in Electrical Engineering, Electronics and Energy, Vol.4, ELsevier-2023,pp.1-7, doi.org/10.1016/j.prime.2023.100158.
22. N. Tripathi, A. K. Mishra, M. Vaqur, S. Sharma and N. K. Pandey, "Improve the Network Security During the Implementation of IoT Application Using Data Encryption and Trustworthy Network", World Conference on Communication & Computing, IEEE-2023, pp. 1-6, doi: 10.1109/WCONF58270.2023.10235075.
23. D. S. Tundalwar, R. A. Pandhare and M. A. Digalwar, "A Taxonomy of IoT Security Attacks and Emerging Solutions", 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing, IEE-2023, pp. 1-5, doi: 10.1109/PCEMS58491.2023.10136032.
24. M. G. Spina and F. De Rango, "Lightweight, Dynamic and Energy Efficient Security Mechanism for constrained IoT devices using CoAP", 20th Consumer Communications & Networking Conference, IEEE-2023, pp. 1123-1128, doi: 10.1109/CCNC51644.2023.10059854.
25. S. Tanimoto, T. Sugio, H. Sato, A. Kanai, "Security Policy Matching Model between Mobile IoT and Public Fog Computing," 14th IIAI International Congress on Advanced Applied Informatics, IEEE-2023, pp. 639-644, doi: 10.1109/IIAI-AAI59060.2023.00126.
26. B. B. Sundaram, A. Pandey, V. Janga, D. A. Wako, A. S. Genale and P. Karthika, "IoT Enhancement with Automated Device Identification for Network Security", 6th International Conference on Trends in Electronics and Informatics, IEEE- 2022, pp. 531-535, doi: 10.1109/ICOEI53556.2022.9776678.
27. S. Yoon, B. Kim, K. Kim and Y. Kang, "Enhancing IoT security with PUF-based authentication scheme", 13th International Conference on Information and Communication Technology Convergence, IEEE-2022, pp. 2319-2321
28. M. R. Nosouhi, K. Sood, M. Grobler and R. Doss, "Towards Spoofing Resistant Next Generation IoT Networks", in IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 1669-1683, 2022, doi: 10.1109/TIFS.2022.3170276.
29. K. Kasat, D. Leela Rani, B. Khan, Ashok. J, M.K. Kirubakaran, P. Malathi, A novel security framework for healthcare data through IOT sensors, Measurement: Sensors, Vol.24, Elsevier-2022, pp.1-5, doi: 10.1016/j.measen.2022.100535.
30. P. Kumar, H. Bagga, B.S. Netam, V. Uduthalapally, "SAD-IoT: Security Analysis of DDoS Attacks in IoT Networks", Wireless Personal Communications, Vol.122, Springer-2022, pp.87–108, doi:10.1007/s11277-021-08890-6.
31. V. O. Nyangaresi, "Terminal independent security token derivation scheme for ultra-dense IoT networks", Array, Vol. 15, Elsevier-2022, doi:10.1016/j.array.2022.100210.
32. F. Zhou, L. Li, "Pondering over the operation status and security issue of NB-IoT", Procedia Computer Science, Vol.183, Elsevier-2021, pp.18-22, doi:10.1016/j.procs.2021.02.025.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

33. M.S. Jian, J.MT Wu, "Hybrid Internet of Things (IoT) data transmission security corresponding to device verification" Journal of Ambient Intelligence and Humanized Computing, Springer-2021, pp.1-13, doi:10.1007/s12652-021-03122-y.

34. D. Liao,H. Li,W. Wang, "Achieving IoT data security based blockchain", Peer-to-Peer Networking and Applications, Vol. 14, Springer-2021, pp.2694–2707, doi"10.1007/s12083-020-01042-w.

35. H. Strohmier, J. R. Lowe, A. G. Rodriguez and M. M. Trammell, "Security and Privacy Threats Posed by IoT Devices Used by Students on College Campuses", 12th International Symposium on Digital Forensics and Security, IEEE-2024, pp. 1-6, doi: 10.1109/ISDFS60797.2024.10527253.

36. M. Koca, I. Avci, "A Novel Hybrid Model Detection of Security Vulnerabilities in Industrial Control Systems and IoT Using GCN+LSTM," in IEEE Access, Vol.12, IEEE-2024, pp.143343-143351, doi: 10.1109/ACCESS.2024.3466391.

37. E. M. d. Elias et al., "A Hybrid CNN-LSTM Model for IIoT Edge Privacy-Aware Intrusion Detection", IEEE Latin-American Conference on Communications, IEEE-2022, pp.1-6, doi: 10.1109/LATINCOM56090.2022.10000468.

38. A. Khacha, R. Saadouni, Y. Harbi and Z. Aliouat, "Hybrid Deep Learning-based Intrusion Detection System for Industrial Internet of Things," 2022 5th International Symposium on Informatics and its Applications (ISIA), M'sila, Algeria, 2022, pp. 1-6, doi: 10.1109/ISIA55826.2022.9993487.

39. A. Presekal, A. Ştefanov, V. S. Rajkumar and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning," in IEEE Transactions on Smart Grid, vol. 14, no. 5, pp. 4007-4020, Sept. 2023, doi: 10.1109/TSG.2023.3237011.

40. T. N. I. Alrumaih and M. J. F. Alenazi, "CGAAD: Centrality- and Graph-Aware Deep-Learning Model for Detecting Cyberattacks Targeting Industrial Control Systems in Critical Infrastructure," in IEEE Internet of Things Journal, vol. 11, no. 13, pp. 24162-24182, 1 July1, 2024, doi: 10.1109/JIOT.2024.3390691.

41. A. M. Almasabi, M. Khemakhem, F. E. Eassa, A. Ahmed Abi Sen, A. B. Alkhodre and A. Harbaoui, "A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning," in IEEE Access, vol. 12, pp. 176833-176844, 2024, doi: 10.1109/ACCESS.2024.3498603.

42. I. Alrashdi, K. M. Sallam, M. A. Alrowaily, O. Alruwaili, B. Arain, "FIDWATCH:Federated incremental distillation for continuous monitoring of IoT security threats", Ad Hoc Networks, Vol.165, Elsevier-2024,pp.1-23, doi:10.1016/j.adhoc.2024.103637.

43. A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," in IEEE Access, vol. 8, pp. 165130-165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

44. F. C. d. Santos, F. D. Figueiredo, R. E. De Grande, A. L. dos Santos, "Enhancing a fog-oriented IoT authentication and encryption platform through deep learning-based attack detection", Internet of Things, Vol.27, pp.1-19, Elsevier-2024,10.1016/j.iot.2024.101310.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

45. P.A. Mathina, K. Valarmathi, "Advancing IoT security: A novel intrusion detection system for evolving threats in industry 4.0 using optimized convolutional sparse Ficks law graph point trans-Net", Computers & Security, Vol.148, Elsevier-2025, pp.1-23,doi:10.1016/j.cose.2024.104169.