Indonesian Journal of Electrical Engineering and Computer Science
Vol. 39, No. 3, September 2025, pp. 1891~1899
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v39.i3.pp1891-1899

Core machine learning methods for boosting security strength for securing IoT

Sneha Nelliyadan Pavithran[1], Jayanna Veeranna Gorabal[2]
[1]Department of Computer Science and Engineering, Acharya Institute of Technology,
Affiliated to Visvesvaraya Technological University, Belagavi, India
[2]Department of Computer Science and Engineering, ATME College of Engineering,
Affiliated to Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Dec 12, 2024
Revised Apr 9, 2025
Accepted Jul 2, 2025

Keywords:

Artificial intelligence
IoT
Machine learning
Privacy
Security

ABSTRACT

Internet-of-things (IoT) revolutionized the mechanism of larger scale of network system offering more engaged, automated, and resilient data dissemination process. However, the resource-limited IoT devices potentially suffers from security issues owing to various inherent weakness. Artificial intelligence (AI) and machine learning (ML) has evolved more recently towards boosting up the security features of IoT offering a secure environment with higher privacy. Till date, there are various review papers to discuss elaborately security aspect of an IoT; however, they miss out to present the actual gap existing between commercial available products and research-based models. Hence, this paper contributes towards discussing the core taxonomy of evolving security methods using ML along with their research trend to offer better insight to existing state of effectiveness. The study further contributes towards highlighting the potential trade-off between the real-world solution and on-going ML based approaches.

Corresponding Author:

Sneha Nelliyadan Pavithran
Department of Computer Science and Engineering, Acharya Institute of Technology
Affiliated to Visvesvaraya Technological University
Acharya College Road, Soladevanahalli, Bengaluru, Karnataka – 560107, India
Email: sneha.np23@gmail.com

1. INTRODUCTION

Internet-of-things (IoT) facilitates a highly connected network of various devices in order to facilitate a highly interactive network system with acquisition of massive data [1]. As IoT connects massive number of devices with heterogeneous protocols, security is a critical concern inducing threats to data integrity, safety, and privacy [2]. The current security schemes in IoT is meant for safeguarding personal privacy, resisting cyber attacks, securing critical infrastructure, maintaining system integrity, etc. The number of attacks in IoT are quite large e.g. data interception, device hijacking, distributed denial-of-service (DDoS), malwares, physical attacks, Firmware attack, issues in authentication, side-channel attacks, and many more [3]. At present, the security solution towards mitigating such threats are mainly classified to cryptographic based and artificial intelligence (AI) based [4]. Cryptographic approaches with their wider ranges of variants assists in mainly stopping the threats upon positive identification; however, their capability to explore the novel form of threats are highly restricted. Although, cryptographic based solution is potential for resisting defined threats, they are also quite expensive from the view point of storage of secret keys and demands of prime resources saturating the processing capabilities of resource-limited IoT devices. This problem is noticeably solved by adoption machine learning (ML) algorithms which is capable of identifying the complex behavioral pattern of threats followed by evolving intelligent strategies to stop them. ML algorithm can be used for identifying abnormalities without any dependencies on predefined signatures towards newly evolving threats. Further, IoT is characterized by increased volumes of data which can be handled effectively by ML algorithms using supervised or unsupervised or hybrid learning approaches. They render the data analysis process much efficient with filtering out noises in order to determine the potential attack vector. Apart from this, as IoT devices has lack of standardization which acts as an impediment towards deploying a generalized security solution, ML approaches can quite easily adopt to this dynamic characteristics without much need of reengineering a conventional security system. It is also noted that IoT devices are characterized by weaker authentication method that make them much susceptible to illegitimate access and such problem of authentication can be well-handled by ML algorithms. The process of authentication of devices can be enhanced by ML algorithm by identifying the behavior of device operation followed by performing monitoring of all incoming and outgoing traffic by generating an intelligent authentication scheme. Detection of threats in real-time is one of the essential demands of every IoT devices while this can be addressed using ML algorithm where interactions, device logs and network traffic can be analyzed by ML algorithm to offer analysis of its state in real time. It can be also used for alerting or generating notification in an event of abnormal behavior by prompting involuntary response system towards reducing possibilities of threats. Hence, there ae various beneficial perspective of using ML algorithms towards IoT security due to its optimized implementation of encryption, dynamic adaptativity towards various schedules and policies for boosting privacy with effective incident response and mitigation plan. However, ML algorithms are relatively new and its potential is yet to be more solidified especially when it comes to large and complex network system of an IoT. It is necessary to review the effectiveness of existing approaches using ML prior to modelling any innovative approaches towards IoT security.

Different types of related work has been studies in order to gain a better insight towards the existing approaches of ML in IoT security. The work carried out by Sun *et al.* [5] have presented discussion towards data fusion operation using ML towards variable applications of IoT while the study infers that there an open-end issue pertaining to dataset adoption towards accomplishing better model performance. Paracha *et al.* [6] have investigated existing solution towards privacy issues to find the importance of feature engineering using ML approaches. Interestingly, the study comments that some of the standard operation of ML (e.g., data cleaning) contributes to various model performance challenges. Dubey *et al.* [7] have presented discussion on deep learning methods to find that almost all the approaches have associated shortcoming. Similar line of discussion has been also presented by Bharati and Podder [8]. According to Alwahedi *et al.* [9], the usage of ML and AI has manifold application towards futuristic IoT security in perspective of language models and generative AI. At the same time, authors concluded with various unsolved challenges mainly related to dynamic form of attacks, heterogeneity of devices, and complexity of data in IoT security. The study presented by Zhiyan *et al.* [10] have identified ongoing challenges pertaining to malware detection, adversarial attacks, and dataset issues towards network intrusion while ML is adopted. El-Sofany *et al.* [11] have presented a simplified and ensembled ML model towards classifying the cyberthreats in IoT devices to find that their model offers extensively higher accuracy in contrast to other related ML schemes.

After reviewing the existing review works towards usage of ML in IoT security, various loopholes and challenges have been discovered. The identified research problems in this perspective are: i) although existing ML approaches is quite capable of identifying complex patterns of threat, yet they suffers issues of overfitting and higher dependencies of trained dataset; ii) existing ML approaches has increased involvement of sophisticated analytical operation that demands increasing resources, which are often ignored in existing ML based approaches; iii) at present, there are wide number of commercially deployed security tools towards IoT security which offers significant protection; however, this capability is quite limited and doesn’t cover up the wider ranges of technological advancement discussed in existing implementation-based research articles; and iv) there are lack of benchmarked study model to offer a full-proof solution towards IoT security in an advent of large innumerable number of security threats by different names and characteristics. Hence, there is a need of a study that can offer a snapshot of current state of ML approach for gaining better insight.

The prime aim of the proposed study is to present the state of existing ML methods used for securing the IoT environment and discover potential gaps existing in current methods. The value-added contribution of the study are as follows: i) the study presents discussion of frequently adopted research methods using ML towards IoT security with identified advantages and limitations; ii) the study has also presented identified updated research trend towards adoption of ML based and typical encryption based solutions adopted for IoT security; and iii) finally, the study presents compact and crisp discussion of research gap between the existing research-based solution with commercially available tools. The next section presents method adopted to carry out the study.

2. METHOD

At present, there are large number of research-based solution offered by using ML algorithms towards improving IoT security. However, the number and actual domain of the studies are so highly scattered that it is quite challenging to shortlist and understand the core strategies to address security issues. Hence, the core motive of the proposed study is to offer a crisp information associated with taxonomies of only core methods evolved and frequently adopted by ML algorithm. Different from existing review models, this study doesn't discuss about individual research work, but rather identifies the core ML methodologies extracted after reviewing multiple current research article to offer crisp insight to existing ML-based security solutions. Figure 1 showcases the method implemented to carry out this current study.

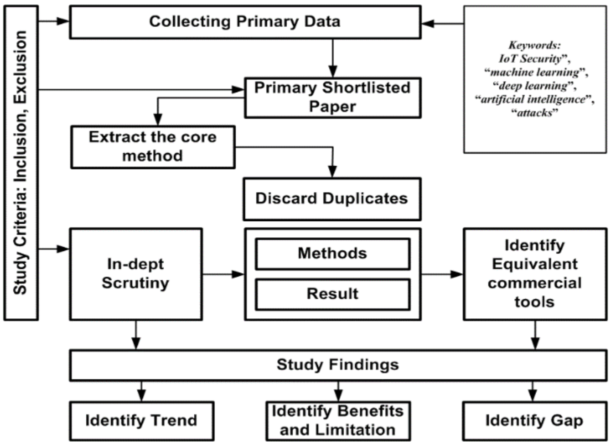


Figure 1. Adopted study method

Figure 1 highlights various steps involved in proposed study where the initial part is towards collecting primary data i.e., research articles pertaining to ML based IoT security. The keywords used for this purpose is a combination of following: "IoT Security", "machine learning", "deep learning", "artificial intelligence", "attacks". This combination generates large number of primary data. The next step is towards extracting the core method in order to build a core taxonomy of current state of ML approaches. The next step is towards discarding some of the collected primary data in case they are found to be duplicated. The filtered research articles are then scrutinized deeply with respect to their methodology which is finally found to be of multiple classes. Along with this, a deeper investigation is carried out towards existing commercial tools along with their feature specification matching with explored methods. The inclusion criteria of the study are i) only implementation-based research articles/journals from reputed journals are reviewed, and ii) papers must use ML with clear definition of attacks that they are attempting to address.

The exclusion criteria of the study are i) research papers published before 2019 have not been considered, ii) no conference papers have been reviewed, iii) research papers with no clear discussion on method and actual outcome have been filtered out, iv) finally, the study outcome offers two results viz. Performance outcome claimed in research articles with respect to shortlisted method and feature-based capabilities of existing commercial tools using ML for IoT security. It has been noted that there is a large gap in its findings. Hence, the last step of the method is towards further yield updated research trend and research gap with respect to multiple attributes. The next section presents discussion of the study outcome associated with identified methods of ML towards IoT security.

3. RESULTS

The review work has come across various types of ML approaches meant for addressing the security pitfals in large scale network system like IoT. It is essential to understand that ML method is not meant for substituting cryptographic solution, but it is meant to optimize the performance of security system in order to make it suitable when encountering dynamic and complex nature of IoT applications. Existing studies of ML has been noted to be presented towards optimizing typical security methodologies. This section will discuss about different types of frequently identified methodologies used for securing IoT followed by briefing trends of research and highlighting learning outcomes of the review.

3.1. Frequently identified methodology

The present state-of-art methods using ML is seen to evolve up with varied ranges of security methodologies that involves anomaly detection, intrusion detection and prevention, malware detection, threat classification, and predictive threat intelligence. All these approaches, in its standalone form, uses ML to optimize its performance by identifying the complex form of threat behavior. Different researchers have used manifold ML techniques; however, the core goal remains same towards offering secure IoT networks. Following are the briefing of identified methodologies frequently deployed in IoT security:

- Anomaly detection: current studies towards this methodology is noticed with training the ML model initially with various attributes of behavior associated with an IoT device (e.g., sensor readings, activity of device, and network traffic). The trained model is then considered for determining any form of deviation from regular behavior representing security threats [12]-[17].
- Intrusion detection and prevention: this methodology is another frequently adopted security approaches where device logs or network traffic is subjected to ML algorithm in order to identify and classify actions of an intruder. By observing patterns of suspicious data, multiple attempts towards vulnerability exploitation, and unauthorized access, a sophisticated pattern of an intruder is determined using ML algorithms [18]-[21].
- Malware detection: various current ML-based approaches emphasizes towards determining the malwares by learning the complex behavior associated with an IoT device. Any usual patterns as well as specific forms of signatures represents presence of malware with possible infection with ransomware [22]-[27].
- Threat classification: this type of methodology is adopted in two combination viz. i) methodology with detection and classification and ii) methodology with only classification. However, both these typical approaches doesn’t have much significant differences as ML algorithm used here is meant to either perform binary or multiple classification of threats. The idea is to offer broader insight of attack vector types for undertaking necessary security measures [28]-[32].
- Predictive threat intelligence: this is another evolving methodology where the ML approach is used to analyze various historical data related to intruder. The prime purpose is to predict the possibility of intruding activities as well as behavioral identification using supervised, unsupervised, and hybrid form of ML approaches [33]-[35].

Apart from the above frequently deployed methodologies, existing system has also identified some more additional methodologies i.e., network traffic analysis [36], behavioral analysis [37], vulnerability scanning [38], security audits [39], firmware analysis [40], device fingerprinting [41], risk assessment [42], honeypot [43], endpoint security monitoring [44], threat intelligence [45], and access control monitoring [46]. All these standard methods have a unique mechanism towards identification of direct threat behavior either in networks or in devices of an IoT. Table 1 highlights the summarize version of these methods along with exhibits of tools, advantages and limitations. The prime ideology of these methods are dual folds:

- To resists known attacks: this principle is adopted by above-mentioned approaches when they have well-known definition of threats. In such cases, the existing methods attempts to find the origination point of such adversaries, which could be either genuine attacker or a victim node followed by either stopping them or isolation them from normal networks. However, this method is less effective when the attacker is smart enough to adopt multiple complex strategies to launch the attack vector.
- To identify patterns of undefined attacks: this principle is deployed when there is no well-defined definition of vulnerabilities. The complexity of identifying and confirming the attacker is quite high in this case as they will need to carry out series of computation and analytical operation towards decision making. The resources consumption during this process is quite high compared to strategies towards capturing known attack; however, it is one of the best alternative towards catching hold information related to much intelligent and complex form of an attacker.

3.2. Identified research trend

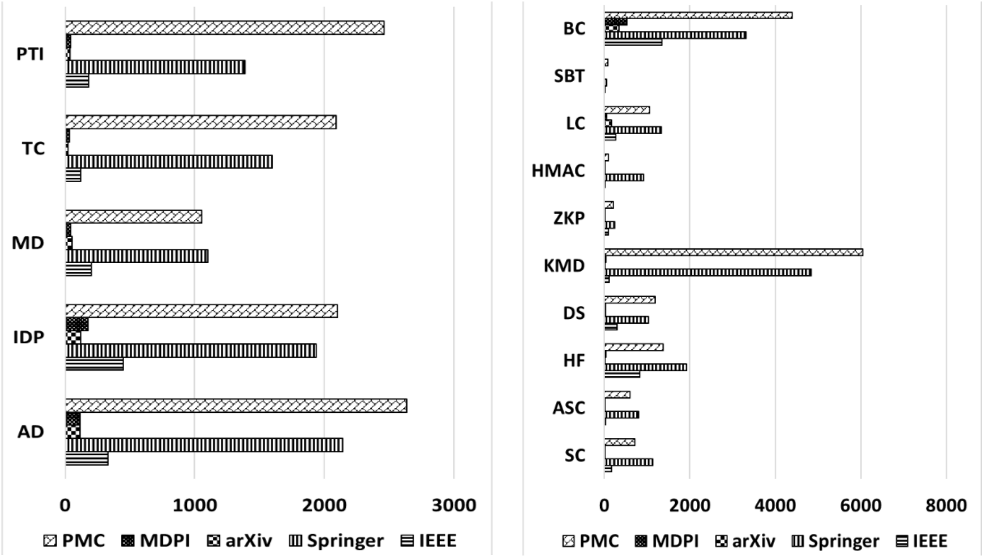
The identification of the research trend offers a significant insight to the pattern of adopted methodology towards securing IoT ecosystem. Figure 2 highlights the prime differences between two most frequently adopted approaches of ML methods and cryptographic methods (CM). The trend shows that number of ML methods (n=20541) is significantly higher than that of cryptographic methods (n=35866) noted in last 5 years of publication of research journals. The notable findings of the trends are as follows:

- Trend interpretation for ML: from the perspective of ML approaches (Figure 2(a)), it is noted that more studies are carried out towards anomaly detection (AD)(n=5,340) as well as intrusion detection and prevention (IDP)(n=4,782). There is also an evolving trend on predictive threat intelligence (PTI)(n=4,110) as well as threat classification (TC)(n=3,859). However, ML approaches towards malware detection (MD) (n=2,450).

- Trend interpretation for CM: from the perspective of CM (Figure 2(b)), it is noted that there are large number of typical methods e.g. symmetric cryptography (SC), asymmetric cryptography (ASC), hash function (HF), digital signature (DS), key management and distribution (KMD), zero knowledge proof (ZKP), hash-based message authentication (HMAC), lightweight cryptography (LC), secure boot and trusted environment (SBT), and blockchain (BC). The trend shows higher number of publication towards KMD (n=11,058) and BC (n=9,924) in contrast to the other CM approaches. Much less adoption of SBT (n=134) and ZKP (n=575) is noted in existing publication trends.

Table 1. Existing methods towards IoT security

Methods	Techniques	Tools	Advantage	Limitation
Network traffic analysis	Flow analysis, intrusion detection	Snort, Suricata, Wireshark	– Offers real-time captures of network. – Identify abnormal traffic pattern.	– Analysis affected by encrypted traffic. – Demand increased computational power.
Behavioral analysis	Anomaly detection, ML	ML, Darktrace, Splunk	– Adapts and learns over time. – Can detect zero-day attack.	– Time consuming setup. – Cannot detect novel threats.
Vulnerability scanning	Automated, penetration testing	Qualys, OpenVAS, Nessus	– Can be automated. – Offers insight for weak security.	– Not eligible for unknown attack. – Generate outliers.
Security audits	Manual, automated	Nessus	– Systematic review of security tools.	– Resource intentive. – Limited detection.
Firmware analysis	Static/dynamic code analysis	Radare2, Binwalk	– Can identify malwares. – Identify insecure setup.	– Complex in operation. – Time-consuming.
Device fingerprinting	Passive/active scanning	Fing, Nmap, Shodan	– Detects unrecognized devices. – Improves network segmentation.	– Not resistive against spoofing. – Cannot be effective for encrypted devices.
Risk assessment	Risk matrices, threat modelling	STRIDE, OCTAVE	– Can prioritize vulnerabilities. – Assists resource allocation.	– Overlooks new threats. – Demands frequent updates for operations.
Honeypot	Deception network	Conpot, Honeyd	– Assists in diverting attacks.	– Demands higher maintenance.
Endpoint security monitoring	Endpoint detection and response, local logging/alerting	Carbon Black, CrowdStrike	– Ensure device integrity. – Resists malwares.	– Increased overhead on device resources.
Threat intelligence	Threat sharing, automated intelligence updates	IBM X-Force, ThreatConnect	– Highly integrated options.	– Information overload. – Cannot be much effective for new attacks.
Access control monitoring	Identity and access management (IAM), audit logs	Custom IAM, Microsoft Azure AD, Okta	– Robust authentication. – Analyses user behavior.	– Complex management. – May generate outliers.



(a) (b)

Figure 2. Research trend: (a) ML methods and (b) cryptographic methods

The final conclusive outcome of this trend analysis is that number of ML approaches towards IoT security is evolving increasingly to higher number in contrast to conventional CM approaches. However, it should be noted that majority of the approaches adopts ML approaches in combination with CM methods. Hence, it can be stated that ML methods usage is meant for boosting up the performance of CM methods by furnishing more intellectual information of complex forms of threats. Such identification task is quite limited within CM approaches. This is one of the primary reason behind more number of adoption of various ML approaches in securing data and communication within IoT environment which is potentially exposed to innumerable number of both known and unknown threats. However, a prime pitfall observed is that ML approaches are also witnessed with various flaws (e.g., overfitting and dependencies of data) that cannot always offer real-time protection.

3.3. Gap between research and commercial tools

From the previous section, it is noted with an evidence of trends, that ML approaches are proliferating in contrast to typical CM approaches. After reviewing the implications of varied ML approaches towards IoT security, it is noted that they all have potential advantages as well as shortcomings. It is quite agreeable with shortcomings as ML approaches demands more rigorous real-time deployment whereas IoT security in ML is still in nascent stage. However, there are some potential trade-off in ML approaches from the perspective of research methods and commercial tools towards IoT security that demands serious attention as follows:

- Scalability and performance: existing ML-based research methods could offer potential enhancement in niche sector of IoT but it has a shortcoming of scalability especially when real-time deployment is demanded. Existing commercial tools can support large-scale application with reduced latency but is not meant for resisting complex threats.
- Customization and flexibility: majority of ML-approaches are knowns for their customization when adopted with research model by tuning the parameters with respect to threats. However, it is bit time consuming and complex to integrate. Commercial tools doesn't offer better customization due to its pre-configured attributes of security with less flexibility towards resisting complex attack vectors.
- Data availability and quality: this is another significant trade-off between research methods and commercial tools as real-time data availability is quite poor for former while quite good for latter. Hence, model doesn't perform well for research methods while although commercial tool can handle bigger sized data but it eventually leads to data privacy (due to lack of access to new intruders).
- Security and risk mitigation: there is no doubt that ML-based research methods is known for their discovering capability for different attacks; however, their success is not proven yet for large scale commercial deployment. On the other hand, commercial tools offers increased confidence and trust but lacks proactiveness when they are exposed to new threats.
- Cost and accessibility: at present, usage of open-source is much adopted in ML-based research approaches which saves cost while it still demands higher computational resources. One the contrary, commercial tools are quite easier for deployment with regular updates; however, they still incurs increased maintenance cost when deployed on large scale environment.

Although, there are increasing volumes of research work towards adoption of ML in IoT security, yet, there are quite a less number of well-established study model. Majority of existing studies are witnessed with this gap between research approach and commercial application, which is still quite far away from actual demands of complex form of IoT security. Next section briefs discussion of accomplished outcome.

3.4. Discussion

The results of this study highlight how ML techniques are being used more and more to secure IoT networks, providing potential answers to challenging security issues. In particular, ML is widely used in threat classification, malware detection, anomaly detection, intrusion prevention, and predictive threat intelligence. It is also clear that ML is frequently combined with traditional cryptographic techniques, including key management, to improve security and authentication procedures. Even though ML-based tools are developing, the study finds a disconnect between commercial and research applications, with the former frequently falling short of the latter's capabilities.

This study contributes to an expanding corpus of research that examines the relationship between ML and IoT security. Prior research has demonstrated that ML can be an effective tool for detecting unknown threats and speeding up reaction times. But as other evaluations have noted, there hasn't been as much focus on the integration of ML with cryptographic techniques, which is what this study emphasizes. By emphasizing how ML might enhance rather than replace conventional security solutions in IoT systems, our work expands on these findings. Furthermore, the results about the shortcomings of the available ML-based technologies in business settings are consistent with previous research, which indicates that although ML has enormous promise, practical implementation is still difficult.

In summary, although ML holds great potential for improving the security of IoT networks, its effective incorporation into commercial applications is still a work in progress. Refining ML approaches to handle real-world complexities, increasing industry-academia collaboration, and closing the gap between research and commercial technologies are all critical to the future of IoT security. In order to combat the increasingly complex and varied threats that IoT settings face, the developing synergy between ML and cryptography techniques will be essential.

4. CONCLUSION

This paper has presented a snapshot of discussion towards the current adoption of ML for promoting IoT security performance. There is no doubt that adoption of IoT incorporates the strength in modelling towards gaining fair insight to complex patterns of threats essential for preventing them. The prime contribution of this study in the form of learning outcomes are; first, the study finds that there is an increased number of ML methods wide wider scope of deployment area towards strengthening IoT security. Second, another explored fact noted that is that ML approach is increasing used in combination of CM approaches with maximized deployment on key management strategies that is essential for boosting authentication proactively. Third, there are also increasingly evolving number of ML-based security tools in IoT; however their capabilities are witnessed to be slightly limited far off from what the research papers has presented. Fourth, potential gap is witnessed in multiple perspective between research-based and commercial tool based solution.

Hence, the future work will be carried out towards addressing the identified gap and issues explored from the current study. Although the current study provides insightful information, it also creates opportunities for further investigation. In order to handle the ever-changing nature of IoT security threats, it is first necessary to investigate more reliable methods of combining ML with cryptography solutions. To ensure that ML algorithms can be used successfully in large-scale, resource-constrained IoTs scenarios, research could concentrate on enhancing their scalability and real-time deployment. Future research should also focus on the practical issues that restrict the real-world efficacy of research-based models, such as data availability, computational resources, and privacy concerns, in order to close the gap between these models and commercial tools. Additionally, research into hybrid ML models-which combine supervised and unsupervised learning-may yield more precise and proactive threats identification.

ACKNOWLEDGEMENTS

We wish to confirm that no known conflicts of interest are associated with this publication and all the authors have contributed equally.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Sneha Nelliyadan Pavithran	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Jayanna Veeranna Gorabal		✓		✓		✓		✓	✓	✓	✓	✓		

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding acquisition
Fo	: **Fo**rmal analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author.

REFERENCES

[1] S. N. Poojari Thippeswamy, A. P. Raghavan, M. Rajgopal, and A. Sujith, "Efficient network management and security in 5G enabled internet of things using deep learning algorithms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 1, p. 1058, 2024, doi: 10.11591/ijece.v14i1.pp1058-1070.

[2] N. Fathima, R. Banu, and G. F. A. Ahammed, "A signature-based data security and authentication framework for internet of things applications," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, p. 3298, 2022, doi: 10.11591/ijece.v12i3.pp3298-3308.

[3] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," *Journal of Information and Intelligence*, vol. 2, no. 6, pp. 455–513, 2024, doi: 10.1016/j.jiixd.2023.12.001.

[4] S. Sánchez-Solano, L. F. Rojas-Muñoz, M. C. Martínez-Rodríguez, and P. Brox, "Hardware-efficient configurable ring-oscillator-based physical unclonable function/true random number generator module for secure key management," *Sensors (Basel)*, vol. 24, no. 17, p. 5674, 2024, doi: 10.3390/s24175674.

[5] B. Sun, R. Geng, L. Zhang, S. Li, T. Shen, and L. Ma, "Securing 6G-enabled IoT/IoV networks by machine learning and data fusion," *EURASIP Journal on Wireless Communications, Networking*, vol. 2022, no. 1, 2022, doi: 10.1186/s13638-022-02193-5.

[6] A. Paracha, J. Arshad, M. B. Farah, and K. Ismail, "Machine learning security and privacy: a review of threats and countermeasures," *EURASIP Journal on Information Security*, vol. 2024, no. 1, 2024, doi: 10.1186/s13635-024-00158-3.

[7] K. Dubey, R. Dubey, S. Panedy, and S. Kumar, "A review of IoT security: machine learning and deep learning perspective," *Procedia Computer Science*, vol. 235, pp. 335–346, 2024, doi: 10.1016/j.procs.2024.04.034.

[8] S. Bharati and P. Podder, "Machine and deep learning for iot security and privacy: applications, challenges, and future directions," *Security and Communication Networks, Wiley*, 2022. doi:https://doi.org/10.1155/2022/8951961.

[9] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167–185, 2024, doi: 10.1016/j.iotcps.2023.12.003.

[10] C. Zhiyan *et al.*, "Machine learning-enabled IoT security: open issues and challenges under advanced persistent threats," *arXiv [cs.CR]*, 2022. [Online]. Available: http://arxiv.org/abs/2204.03433.

[11] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports*, vol. 14, no. 1, pp. 1–19, 2024, doi: 10.1038/s41598-024-62861-y.

[12] T. Lai, F. Farid, A. Bello, and F. Sabrina, "Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis," *Cybersecurity*, vol. 7, no. 1, 2024, doi: 10.1186/s42400-024-00238-4.

[13] M. Balega, W. Farag, X.-W. Wu, S. Ezekiel, and Z. Good, "Enhancing IoT security: optimizing anomaly detection through machine learning," *Electronics (Basel)*, vol. 13, no. 11, p. 2148, 2024, doi: 10.3390/electronics13112148.

[14] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," *Scientific Reports*, vol. 14, no. 1, pp. 1–16, 2024, doi: 10.1038/s41598-024-56126-x.

[15] M. Zakariah and A. S. Almazyad, "Anomaly detection for IoT systems using active learning," *Applied Sciences (Basel)*, vol. 13, no. 21, p. 12029, 2023, doi: 10.3390/app132112029.

[16] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," *Sensors (Basel)*, vol. 24, no. 2, p. 713, 2024, doi: 10.3390/s24020713.

[17] I. Mutambik, "An efficient flow-based anomaly detection system for enhanced security in IoT networks," *Sensors (Basel)*, vol. 24, no. 22, p. 7408, 2024, doi: 10.3390/s24227408.

[18] A. M. Banaamah and I. Ahmad, "Intrusion detection in IoT using deep learning," *Sensors (Basel)*, vol. 22, no. 21, p. 8417, 2022, doi: 10.3390/s22218417.

[19] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," *Computers*, vol. 12, no. 2, p. 34, 2023, doi: 10.3390/computers12020034.

[20] A. Javed, A. Ehtsham, M. Jawad, M. N. Awais, A.-U.-H. Qureshi, and H. Larijani, "Implementation of lightweight machine learning-based intrusion detection system on IoT devices of smart homes," *Future Internet*, vol. 16, no. 6, p. 200, 2024, doi: 10.3390/fi16060200.

[21] H. Alshahrani, A. Khan, M. Rizwan, M. S. A. Reshan, A. Sulaiman, and A. Shaikh, "Intrusion detection framework for industrial internet of things using software defined network," *Sustainability*, vol. 15, no. 11, p. 9001, 2023, doi: 10.3390/su15119001.

[22] S. Riaz *et al.*, "Malware detection in internet of things (IoT) devices using deep learning," *Sensors (Basel)*, vol. 22, no. 23, p. 9305, 2022, doi: 10.3390/s22239305.

[23] A. A. Almazroi and N. Ayub, "Deep learning hybridization for improved malware detection in smart internet of things," *Scientific Reports*, vol. 14, no. 1, pp. 1–18, 2024, doi: 10.1038/s41598-024-57864-8.

[24] T. Shi, R. A. McCann, Y. Huang, W. Wang, and J. Kong, "Malware detection for internet of things using one-class classification," *Sensors (Basel)*, vol. 24, no. 13, p. 4122, 2024, doi: 10.3390/s24134122.

[25] T. A. Ahanger, U. Tariq, F. Dahan, S. A. Chaudhry, and Y. Malik, "Securing IoT devices running PureOS from ransomware attacks: leveraging hybrid machine learning techniques," *Mathematics*, vol. 11, no. 11, p. 2481, 2023, doi: 10.3390/math11112481.

[26] I. Mutambik, "Enhancing IoT security using GA-HDLAD: a hybrid deep learning approach for anomaly detection," *Applied Sciences (Basel)*, vol. 14, no. 21, p. 9848, 2024, doi: 10.3390/app14219848.

[27] F. A. Demmese, A. Neupane, S. Khorsandroo, M. Wang, K. Roy, and Y. Fu, "Machine learning based fileless malware traffic classification using image visualization," *Cybersecurity*, vol. 6, no. 1, 2023, doi: 10.1186/s42400-023-00170-z.

[28] A. Alrefaei and M. Ilyas, “Using machine learning multiclass classification technique to detect IoT attacks in real time,” *Sensors (Basel)*, vol. 24, no. 14, p. 4516, 2024, doi: 10.3390/s24144516.

[29] J. Ehmer, Y. Savaria, B. Granado, J.-P. David, and J. Denoulet, “Network attack classification with a shallow neural network for internet and internet of things (IoT) traffic,” *Electronics (Basel)*, vol. 13, no. 16, p. 3318, 2024, doi: 10.3390/electronics13163318.

[30] C. Ioannou and V. Vassiliou, “Network attack classification in IoT using support vector machines,” *Journal of Sensor and Actuator Networks*, vol. 10, no. 3, p. 58, 2021, doi: 10.3390/jsan10030058.

[31] H.-C. Chu and Y.-J. Lin, “Improving the IoT attack classification mechanism with data augmentation for generative adversarial networks,” *Applied Sciences (Basel)*, vol. 13, no. 23, p. 12592, 2023, doi: 10.3390/app132312592.

[32] A. A. Alsulami, Q. Abu Al-Haija, A. Tayeb, and A. Alqahtani, “An intrusion detection and classification system for IoT traffic with improved data engineering,” *Applied Sciences (Basel)*, vol. 12, no. 23, p. 12336, 2022, doi: 10.3390/app122312336.

[33] S. Mishra, A. Albarakati, and S. K. Sharma, “Cyber threat intelligence for IoT using machine learning,” *Processes (Basel)*, vol. 10, no. 12, p. 2673, 2022, doi: 10.3390/pr10122673.

[34] L. Alevizos and M. Dekker, “Towards an AI-enhanced cyber threat intelligence processing pipeline,” *Electronics (Basel)*, vol. 13, no. 11, p. 2021, 2024, doi: 10.3390/electronics13112021.

[35] A. Nazir et al., “Collaborative threat intelligence: enhancing IoT security through blockchain and machine learning integration,” *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, p. 101939, 2024, doi: 10.1016/j.jksuci.2024.101939.

[36] I. A. Alwhbi, C. C. Zou, and R. N. Alharbi, “Encrypted network traffic analysis and classification utilizing machine learning,” *Sensors (Basel)*, vol. 24, no. 11, p. 3509, 2024, doi: 10.3390/s24113509.

[37] X. Cai, J. Zhang, Y. Zhang, X. Yang, and K. Han, “LIME-mine: explainable machine learning for user behavior analysis in IoT applications,” *Electronics (Basel)*, vol. 13, no. 16, p. 3234, 2024, doi: 10.3390/electronics13163234.

[38] S. B. Hulayyil, S. Li, and L. Xu, “Machine-learning-based vulnerability detection and classification in internet of things device security,” *Electronics (Basel)*, vol. 12, no. 18, p. 3927, 2023, doi: 10.3390/electronics12183927.

[39] M. Alsharif and D. B. Rawat, “Study of machine learning for cloud assisted IoT security as a service,” *Sensors (Basel)*, vol. 21, no. 4, p. 1034, 2021, doi: 10.3390/s21041034.

[40] T. Bakhshi, B. Ghita, and I. Kuzminykh, “A review of IoT firmware vulnerabilities and auditing techniques,” *Sensors (Basel)*, vol. 24, no. 2, p. 708, 2024, doi: 10.3390/s24020708.

[41] C. Koball, B. P. Rimal, Y. Wang, T. Salmen, and C. Ford, “IoT device identification using unsupervised machine learning,” *Information (Basel)*, vol. 14, no. 6, p. 320, 2023, doi: 10.3390/info14060320.

[42] T. AlSalem, M. Almaiah, and A. Lutfi, “Cybersecurity risk analysis in the IoT: a systematic review,” *Electronics (Basel)*, vol. 12, no. 18, p. 3958, 2023, doi: 10.3390/electronics12183958.

[43] A. H. E. Omar, H. Soubra, D. K. Moulla, and A. Abran, “An innovative honeypot architecture for detecting and mitigating hardware Trojans in IoT devices,” *IoT*, vol. 5, no. 4, pp. 730–755, 2024, doi: 10.3390/iot5040033.

[44] S. Tedeschi, C. Emmanouilidis, J. Mehnen, and R. Roy, “A design approach to IoT endpoint security for production machinery monitoring,” *Sensors (Basel)*, vol. 19, no. 10, p. 2355, 2019, doi: 10.3390/s19102355.

[45] E. Ortiz-Ruiz, J. R. Bermejo, J. A. Sicilia, and J. Bermejo, “Machine learning techniques for cyberattack prevention in IoT systems: a comparative perspective of cybersecurity and cyberdefense in Colombia,” *Electronics (Basel)*, vol. 13, no. 5, p. 824, 2024, doi: 10.3390/electronics13050824.

[46] M. Usman, M. S. Sarfraz, U. Habib, M. U. Aftab, and S. Javed, “Automatic hybrid access control in SCADA-enabled IIoT networks using machine learning,” *Sensors (Basel)*, vol. 23, no. 8, p. 3931, 2023, doi: 10.3390/s23083931.

BIOGRAPHIES OF AUTHORS

Sneha Nelliyadan Pavithran received the B.E. degree in computer science and engineering from Visvesvaraya Technological University, Karnataka, in 2010 and the M.Tech. degree in computer science and engineering from Visveswaraya Technological University, Karnataka, in 2013. Currently, she is an assistant professor at the Department of Computer Science and Engineering, Acharya Institute of Technology, Bengaluru, Karnataka, India Affiliated to Visvesvaraya Technological University, Belagavi, and Karnataka, India. Her research interests include machine learning, artificial intelligence, internet of things security, network security, and cyber security. She can be contacted at email: sneha.np23@mail.com.

Dr. Jayanna Veeranna Gorabal is currently, Professor, Department of Computer Science and Engineering ATME College of Engineering, Mysuru, Karnataka, India Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India. He obtained his Bachelor’s degree in computer science and engineering from BEC, Bagalkot, KUD Dharwad, M.Tech. in computer science and engineering, KBNCE Kalaburgi, VTU and Ph.D. from JNT University Anantapuram. His research interests include image processing biometric security, computer networks, and artificial intelligence. He can be contacted at email: jvgorabal@gmail.com.