Prime Methodological Insights for Securing Devices Running within an Internet-of-Things Environment

Pushpa Rajput Narayana Singh, Neelambike Siddalingaiah

Abstract— **The usage of handheld devices in Internet-of-Things (IoT) facilitates more connectivity, portable control features, and an extensive scope of collecting and transmitting data. It will eventually mean that a handheld device characterized with constrained resources will encounter significant challenges as well as impediments towards implementing a robust security solution. Irrespective of the presence of massive archives of security solutions, it is quite cumbersome to realize the core methods. Hence, this challenge is addressed in the current manuscript by contributing a discussion towards the effectiveness of prime implementation methods arranged in a structured and compact taxonomy of security solutions towards IoT handheld devices. The study has identified prime methodologies as access control schemes, encryption schemes, secure device authentication schemes, and learning based approaches. The outcome of the study further contributes to a compact and crisp insight into the novel research gap from existing reviewed methods.**

Index Terms—**Internet-of-Things, Handheld Device, Security, Encryption, Taxonomy.**

I. Introduction

HANDHELD devices offer various ranges of applications towards increased connectivity along with their portability for facilitating interaction, control, and data collection in real-time [1]. Some of the essential applications of handheld devices in Internet-of-Things (IoT) are related to health and fitness monitoring, environmental monitoring, navigation and location tracking, security and surveillance, home automation, augmented reality, communication and connectivity, and industrial applications [2]-[5]. Different types of handheld devices in IoT are smartwatches, fitness trackers, handheld medical devices, portable sensors, mobile Point of Sale systems, handheld barcode scanners, portable Global Positioning System (GPS), handheld data loggers, etc [6]. In short, handheld IoT devices contribute towards improving operational efficiency by integrating with advanced processing capabilities, communication, and sensing. As these handheld devices are connected to the IoT ecosystem, it will eventually mean that they are exposed to a large network system with a higher degree of vulnerabilities [7]. There is a greater deal of challenges towards safeguarding such resource-constrained handheld devices in IoT. The first biggest challenge is related to implementing complex encryption or security protocols in handheld devices with limited storage, memory and very low power of processing power. The second practical constraint is related to the battery life of these handheld IoT devices, whereas any form of security approaches will demand a considerable amount of resources. The current state of handheld devices in IoT doesn't have a comprehensive user interface in order to facilitate robust methods of authentication using complex credential-based passwords or the use of biometrics. Hence, user authentication of IoT handheld devices is still an unsolved state of problem. Various forms of confidential and sensitive information, e.g., location data, health metrics, and personal information, are aggregated by IoT handheld devices. Hence, one of the critical areas of research is to focus on offering optimal privacy of such sensitive private data with equal emphasis towards data transmission as well as local storage management at the same time. The handheld devices are well-known for their usage of either Wi-Fi or Bluetooth-based communication protocols, which are very much vulnerable to public networks [8]. Such devices are exposed to unauthorised access, data interception, and eavesdropping while using conventional inbuilt communication protocols by manufacturers of devices.

Individuals wearing such handheld devices are not always exposed to consistent connectivity of their device with the core network or internet due to various practical reasons. This leads to the outage of devices, cutting them off from possible software updates and firmware patches to protect them from online threats. Apart from this, the updates encountered challenges towards being forwarded to a large number of users effectively. There is always a possibility of theft or physical loss for such handheld devices in IoT, leading to the disclosure of sensitive data to an attacker. At present, there is no foolproof solution that is capable of encrypting the data or erasing the sensitive information from the stolen handheld device by remote means. There is no concrete state of a dedicated network between the device and a certain trusted entity (could be a user or service provider). Although it is not a bigger and complex task to connect the handheld user to certain access points; however, this can be a real challenge when the device is within a range of a public network where there is a possible presence of potentially undetected attackers. Hence, access control and device pairing on public networks is a bigger security concern that has yet not be up with mitigation measures. It will eventually mean that it is quite a challenging task to identify the attacker's presence, especially if they adopt

Manuscript received June 7, 2025; revised August 29, 2025.

Pushpa Rajput Narayana Singh is a Research Scholar of Information Science and Engineering Department, GMIT, Davanagere, Karnataka-577006, India (e-mail: pushpa@jnnce.ac.in).

Neelambike Siddalingaiah is an Associate professor and Head of Information Science and Engineering Department, GMIT, Davanagere, Karnataka-577006, India (e-mail: neelambikes@gmit.ac.in).

unconventional strategies to intrude on the network system. Further, it is also noted that there is a demand for integrating this handheld device with various other parties, e.g., cloud services, or other handheld devices. Such integration demands a potentially robust and interoperable security service, which at present is missing in existing times. It is also noted that another bigger challenge is to develop a security solution by a security developer to comply with the existing standards of General Data Protection Regulation (GDPR) as well as Health Insurance Portability and Accountability Act (HIPAA), as different algorithms have different consequences and impact [9]. Finally, the security of the IoT handheld device also potentially depends upon awareness as well as user behaviour [10]. At present, there are various types of evolution of security approaches, considering both conventional techniques and advanced approaches. While going through all the existing studies, it is observed that they are massive archives of literature, while it is a very difficult task to realise the precise solution to address this challenge. Hence, it is necessary to investigate the large archives of existing solutions and then narrow them down to only prime methodologies, which makes it easier to understand the effectiveness of existing security schemes.

The *related work* of this study comprises of currently available surveyed investigations towards IoT device security. The investigation carried out by Adam *et al.* [11] and Bouzidi *et al.* [12] discusses on various architectural issues pertaining to security shortcomings in IoT, where the review concludes a higher number of open-ended issues of trust that need to be resolved. An interesting study by Mazhar *et al.* [13] has presented a discussion connecting IoT security with devices based on usage and respective identification. According to the study, there is a challenging issue in device identification using existing security frameworks in IoT. A similar line of investigation is carried out by Barua *et al.* [14] from the perspective of a wearable device connected to IoT. The study outcome suggests usage of Bluetooth in such devices renders them vulnerable to situations where it is not only challenging to identify threats but also more challenging to implement protocols to resist threats. Jmila *et al.* [15] have presented a machine learning based scheme for investigating traffic types in order to classify the IoT devices. The study outcome concluded that machine learning is a new arena quite productive in feature extraction and hence can be used in device and its usage feature identification. This also relates to the possible usage of machine learning towards device security. Muhammad *et al.* [16] have presented a discussion on various types of potentially evolving attacks that adversely influence the privacy of smartphones, where the study outcome highlighted open-ended issues in next-generation devices. Sensors are one of the common components within new brands of handheld devices, which are found to be vulnerable towards privacy-based attacks as seen in the investigation report of Santos *et al.* [17].

However, there are various *research issues* pertaining to existing review work being carried out till date, which are as follows: i) There are extensive research work discussion on all individual implementation approaches towards securing IoT, but not enough emphasis is towards realizing the actual taxonomy of some core implementation methodologies, ii) there is a prominent gap explored in existing review work; they are either inclined towards IoT security or device security with less connectivity between them, iii) existing review work has not yet explored the missing link between the existing issues in IoT that influences the shortcoming of handheld device security.

Hence, this study aims to facilitate a single-handed investigation work reporting on the effectiveness of only core implementation methods towards influencing IoT handheld device security. The objectives of the study in form of value-added contribution of this study is as follows: i) the research work extracts all current work while adopting a specific method to arrange all the individual implementation techniques in orderly and structured form for clear identification of essential taxonomy of prime security methods for IoT handheld devices, iii) an exploration of publication trends is carried out to understand the more frequently adopted implementation methodology as well as to identify the methods which has received less attention, iv) an exclusive highlights of identified research gap is contributed towards emphasizing essential operations to be undertaken for future researchers. This is how the objectives of this paper have been achieved.

II. Method

The existing literature consists of various approaches towards promoting secure features for combating potential adversaries; however, this current investigation focuses more on device security. To identify relevant articles, we searched for phrases such as "IoT device security," "IoT access control," "IoT encryption," "secure IoT devices," "device authentication in IoT," "machine learning for IoT security," "device management in IoT," "IoT security schemes" or "IoT handheld device security." We assessed the studies based on the quality of their methodology, the clarity of their study objectives, and the significance of their findings. We preferred articles with obvious experimental setups or real-world applicability. A deeper investigation towards the domain of this study shows that both device-level security and other forms of available security approaches in IoT are highly connected. The research challenge is to extract only the approaches which has potential influences on device-level security; therefore, a distinct research methodology is adopted to collect the research papers and carry out the review work. Fig.1 showcases the method adopted for this purpose.

According to Fig.1, the initial step is to *accumulate research papers* with an inclusion of manifold security schemes involved in the IoT environment towards resisting threats. The second step is towards *reviewing the abstract* for identifying if the topic of implementation is linked with device security in IoT. The next step is to perform *preliminary filtering* out certain collected articles based on inclusion and exclusion criteria. The filtered papers are subjected to *secondary review,* where a study is carried out towards the algorithm, implementation environment, and accomplished outcome contribution. Based on the accomplished outcome, the current review makes a conclusive remark on the research gap. *Inclusion criteria* involve selecting only papers where the security schemes relate either directly or indirectly to device security. Only the papers published between 2019-2024 in IEEE Xplore, PCM, arXiv, Springer, and MDPI are selected to review the

methodology and extract research trends. *Exclusion criteria* involve ruling out any papers which has no connection with Summary of review papers. To increase transparency and rigour in the review process, the table below indicates how many articles were included at each step. The numbers represent the original collection of articles, which were then device security. No conference papers are selected for reviewing in the current review study. Table I showcase the filtered for relevance to the review's focus on device-level security. Following the second round of assessment, 125 papers were identified as most related to the research objectives.

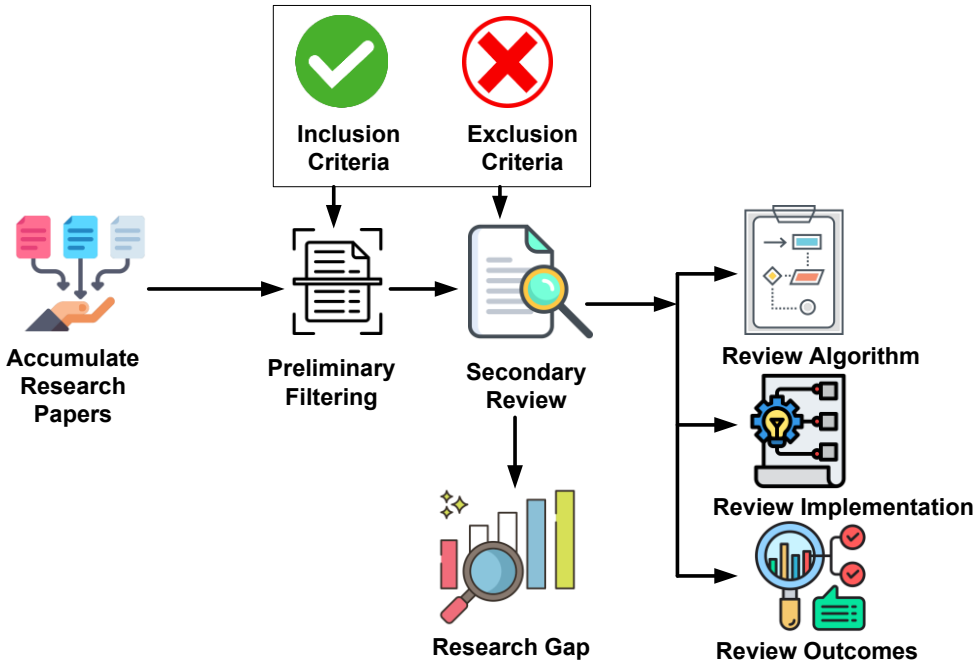

Fig. 1. Adopted Method for Proposed Review Study

TABLE 1
SUMMARY OF REVIEW PROCESS.

Stage	Number of Papers
Initial Pool (after search)	970
After Preliminary Filtering	187
After Secondary Review	70

III. RESULTS

At present, there are different variants of approaches to offer security for manifold handheld devices in IoT. It was seen that there is a stronger correlation among all these approaches, while some of them are implemented as standalone, while some are integrated with others. A crisp discussion on the effectiveness degree of these approaches is carried out considering the methodology discussed in the prior section. However, this section will highlight all the prime methodologies that have been developed in recent studies targeting securing IoT handheld devices.

A. Studies towards an Access Control Scheme

This scheme is meant to offer an interaction between the IoT devices and only authorized users. The first variant of this scheme is known as Role-based Access Control (RBAC), where a definitive role is allocated to a device and user while permission to access is granted based on these explicit roles [18]-[20]. There is a discrete permission type associated with each role. The second variant is known as Attribute-based Access Control (ABAC), where various attributes, e.g. environmental condition, device attributes, and user attributes are used for offering an access control [21]-[23]. The third variant of this scheme is known as Capability-based Access Control (CBAC), where certain capabilities or tokens are issued and deployed for granting access to a device, where a specific set of actions is defined for a specific token [24]. The fourth variant is known as Context-based Access Control (CTAC), where the decision of access control is formed based on contextual information, e.g. device status, location, time, etc [25][26]. Table II showcases the summary of the effectiveness of this scheme.

B. Studies towards Encryption Schemes

This is one of the most frequently and widely used approaches where various data associated with the operation of an IoT handheld device is encrypted to offer data integrity and confidentiality. Existing studies have reportedly used symmetric encryption (e.g. Advanced Encryption Standard) where the same secret key is used for both encryption and decryption [27][28]. Existing studies have also been witnessed to use asymmetric encryption where encryption is carried out by public key and decryption is carried out by private key using mainly Elliptical Curve Cryptography (ECC) and Rivest-Shamir Algorithm (RSA) [29][30]. It is also noted that the adoption of ECC has been emphasized in various existing literature [31][32]. ECC deploys an algebraic structure of finite field cryptography to form a unique type of asymmetric encryption. Hybrid encryption is another evolving security approach in literature that uses both symmetric and asymmetric

encryption for the exchange of keys in a highly resilient manner [33][34]. Finally, literature has witnessed the usage of homomorphic encryption, which eliminates the dependencies of decryption as the operation can be carried out on encrypted data while the outcome is the encrypted form of the result itself [35]. Table III summarizes the effectiveness of this scheme.

C. Studies towards Secure Device Management

This scheme emphasises understanding and realizing various applications, attributes, and components present within the IoT handheld device in order to carry out certain operation that securely manages the IoT device against potential threats. The term management is towards its agenda for maintaining functionality of the IoT device, security of the device and application within it, and offering data integrity. Existing literature has witnessed various studies towards device authentication that aim to connect the network with only authorized devices [36]-[39]. Usually, device credentials, pre-shared keys, and certificates are used for this purpose. It is also found that properly updating the device also assists in retaining secured devices in IoT, and one way discussed in literature is Firmware Over-the-Air Updates (FOAU) [40]-[44]. This scheme is used for permitting the device firmware to be remotely updated to improve performance and to fix any possibilities of security vulnerabilities. Another form of device management technique is to use Secure Boot, which ensures that an IoT handheld device should be able to start only when connected/hosted in a trusted secure environment [45]-[46]. This scheme also supports device lifecycle management that involves device management with decommissioning, configuration, and provisioning. However, it involves operational overhead. Network Access Control (NAC) is another secure device management scheme that constructs security postures (e.g., agreement with security standards, health of handheld device) and policies for controlling access rights of devices on a specific network [47][48]. Identity and Access Management (IAM) is another device management scheme where access rights of user as well as their identities are managed [49]-[53]. It involves managing roles defined for users, authorisation, and authentication. It is to be noted that operations related to all the above-mentioned existing schemes are further made more capable by the construction Access Control List (ACL). This scheme of ACL is responsible for configuring the permission for IoT handheld devices to specify the right to use a particular resource or adopt a particular action [54][55]. Table IV showcases the effectiveness of existing secure device management schemes.

TABLE II
SUMMARY OF ACCESS CONTROL SCHEMES

Security Method	Literatures	Strength	Limitation
RBAC	[18]-[20]	Higher consistency, better scalability, simplified management	Static nature of roles, unmanageable roles under a complex ecosystem
ABAC	[21]-[23]	Supports dynamic access, supports complex policies of access control	Induce performance overhead
CBAC	[24]	Supports decentralisation, fine-grained access control	Recovation complexity, challenging token management
CTAC	[25][26]	Granular control, adaptive security	Privacy issues induce complexities

TABLE III
SUMMARY OF ENCRYPTION SCHEME

Security Method	Literatures	Strength	Limitation
Symmetric Encryption	[27][28]	Less computational overhead, faster execution, suitable for resource-constrained IoT devices	Scalability issues, key distribution problem
Asymmetric Encryption	[29][30] [31][32]	Stronger security for signatures and key exchange simplifies key distribution.	Implementation complexity, slower, computationally intensive
Hybrid Encryption	[33][34]	Balanced security strength, suitable for IoT	Unbalanced focus on management and securing the key increases complexity
Homomorphic Encryption	[35]	Higher data confidentiality during processing, higher privacy preservation	Induce complex management not suitable for IoT handheld devices, with a highly slow response

TABLE IV
SUMMARY OF SECURE DEVICE MANAGEMENT

Security Method	Literatures	Strength	Limitation
Device Authentication	[36]-[39]	Trust building between the network and devices, and resist unauthorised devices.	Highly vulnerable to theft, with higher complexity in managing credentials.
FOAU	[40]-[44]	Simplifying device maintenance, enabling security patching in time	Higher feasibility of intrusion by malware, possibility of failed updates causing malfunction of the device
Secure Boot	[45][46]	Higher root of trust, efficient integrity protection	Potential hardware dependencies, complex verification process
NAC	[47][48]	Prevents an exploited device from connecting to the network, strict policy enforcement	Challenging management of device diversity, policy complexity
IAM	[49]-[53]	Effective auditing of access events, granular control	Cumbersome user management, complex setup
ACL	[54][55]	Customizable and flexible for different events, with precise control of resources based on a defined list	Highly dependent on maintenance and updates, with sub-optimal scalability.

D. Studies towards Learning-based Approaches

There is an increasing adoption of Machine Learning (ML) approaches towards solving issues pertaining to security problem in IoT system. Although encryption methods can effectively stop intruders but it can only happen when the system has prior information about attacker. However, ML approaches adopts proactive measure by performing predictive calculations towards generating an outcome for both detection and classification of unforeseen threats in an IoT environment. However, practical deployment of ML approach also demands it to be lightweight. There are various options for this viz. ensemble methods, Decision Tree (DT), shallow neural networks, etc. that is known for lower consumption of computational resources. Apart from this, ML approaches are also known for their adoption in feature selection methods and Principal Component Analysis (PCA) to handle large and voluminous set of high-dimensional sensory data in IoT ecosystem. There are also various hybrid models where ML is integrated with signature to offer better adaptability towards current threats. The currently undertaken proposed review work focuses on significance of tailoring the ML-based security models towards threat profiles and specific constraints of resources of an IoT devices. The notion is to accomplish a better balance between system efficiency and detection performance.

With the types of attackers becoming smarter and more complex, there is an increasing adoption of machine learning and deep learning approaches towards securing IoT devices. Such learning approaches contribute towards cumulative system resilience with anomaly detection and threat detection capabilities in predictive form. Existing studies have witnessed wider adoption of various types of supervised learning approaches which approaches including classification algorithms using Support Vector Machine (SVM), Random Forest, and DT are deployed for addressing various security threats in IoT [56][57]. Supervised algorithm using regression, e.g., Logistic Regression (LoR) and Linear Regression (LiR), has also been witnessed in existing literature towards predictive identification of threats in IoT [58][59]. Clustering algorithms like K-Means have been witnessed for unsupervised learning methods [60], while many unsupervised approaches have also used dimensional reduction algorithms for optimising the training data [61]. Extensive studies have been carried out towards anomaly detection using Autoencoders (AE) [62][63] and Isolation Forest (IF) [64]. Current implementation towards securing IoT devices is also noted by deploying Ensemble Learning methods using RF and Gradient Boosting Machine (GBM) [65][66]. It is further noted that machine learning has been deployed for scenarios with simpler tasks and smaller datasets. So, when it involves a larger dataset and a complex form of task, deep learning approaches are used, especially when dealing with high-dimensional data. However, it should be noted that machine learning approaches have lesser resource demands in contrast to deep learning approaches; while machine learning is found to be more interpretable in contrast to deep learning approaches. Apart from this, the machine learning approach is known for its wider applicability on a variety of tasks, while deep learning is restricted to a specific form of complex tasks. Current work towards the adoption of deep learning algorithms has been carried out by using Convolution Neural Network (CNN) [67], Recurrent Neural Network (RNN) / Long Short-Term Memory (LSTM) [68][69] and Miscellaneous (MSC) variants of deep neural networks [70]. Table V showcases a summary of the effectiveness of the currently reviewed learning approaches.

E. Research Trend Identification

As stated in previous sections, there are specifically 4 different variants of research implementation approaches towards ensuring device security within an IoT ecosystem. This section highlights the trends of research work being published between 2019-2024 from various reputed publishers (Table VI). The outcome shows that learning approaches using secure device management are exponentially increasing in their publication rate (n=45107), which is followed by both learning-based approaches, i.e., machine learning and deep learning approaches (n=38499).

The access control schemes (n=19787) are found with half the total publications considered to secure device management and learning approaches. Interestingly, the encryption-based approaches, which are considered to be always a preferred approach for device security, have received quite less attention in perspective of their publication (n=9511). It is also to be noted that blockchain schemes are also increasing their adoption (n=10410), and it is found to be used in joint implementation with all the other security schemes. The core findings of the research trends offers following disclosure: i) there is a higher emphasis towards secure device management especially considering network access control (n=22493) which very less emphasis is given to FOAU scheme (n=183), which is quite unbiased attention towards problems, ii) core implementation using encryption has witnessed underrated publications while joint usage of encryption with access control, secure device management, and blockchain are quite high stating less work being carried out towards evolving innovative individual encryption approach. It has been noted that the approaches pertaining to the blockchain technology is emerging in faster pace. Although, it has been mainly sought towards strengthening data integrity; however, there are increasing number of studies towards access control associated with an IoT environments. These approaches are meant towards supporting decentralization operation of blockchain as well as to improvise the tamper-resistant nature of it. However, there are significant level of operational challenges associated with it when it comes to access control mechanism. Various issues noted related to this are latency due to consensus protocol, scalability bottlenecks, challenges towards managing dynamic threat level. Reviewing various standard research articles towards such issues highlights that majority of current form of security models using blockchain technology doesn't meet the constraints associated with practical deployment with increased security robustness. This fact act as a hurdle towards real-time applications hosted in IoT ecosystem that has a demand of increased throughput and reduced latency.

There are various types of approaches as shown in Table

VI; however, not all approaches receives same attention. A closer look to the numbers will show that blockchain is just in nascent stage of security inclusion in IoT and still various conventional scheme are highly researched upon.

TABLE V
SUMMARY OF LEARNING-BASED APPROACHES

Learning Method	Literatures	Strength	Limitation
Supervised	Classification: [56][57] Regression: [58][59]	Clear decision boundaries, effective for known threats	Overfitting risk, demands labelled data, and limited flexibility
Unsupervised	Clustering: [60] Dimensional Reduction: [61]	Outlier identification doesn't need labelled data	Lacks interpretability, is sensitive to cluster initialisation, and loss of information
Anomaly Detection	AE: [62][63] IF: [64]	Can handle large datasets, suitable for complex data	Training complexity, impractical anomaly assumption, and overfitting risk
Ensemble Learning	RF / GBM: [65][66]	Robust to overfitting, higher accuracy	Computational overhead, slower training duration
Deep Learning	CNN: [67] RNN/LSTM: [68][69] MSC: [70]	Higher accuracy, Higher memory capabilities (LSTM)	Computationally intensive, vanishing gradient problem

TABLE VI
IDENTIFIED TREND OF PUBLICATIONS

Approaches	Methods	IEEE	Springer	PMC	arXiv	MDPI
Access Control	RBAC	15	6214	285	6	24
	ABAC	206	2136	548	15	37
	CBAC	0	4213	108	19	33
	CTAC	0	5686	201	18	23
Encryption	Symmetric	353	1373	907	15	30
	Asymmetric	35	907	729	7	17
	Hybrid	70	1787	1925	4	19
	Homomorphic	119	622	545	17	30
Secure device management	Device Authentication	1176	2783	3052	240	345
	FOAU	2	94	79	3	5
	Secure Boot	8	174	201	9	5
	NAC	2223	8778	11076	208	208
	IAM	158	2543	3007	10	17
	ACL	76	3944	4667	7	9
Machine Learning	RF	87	994	1278	12	40
	SVM	238	1841	2540	8	26
	DT	95	1499	2077	9	26
	LoR	22	566	1002	6	14
	LiR	20	908	2870	1	2
	K-means	16	2907	633	0	5
	IF	18	260	452	4	9
Deep Learning	AE	105	622	823	20	23
	GBM	226	645	850	8	20
	CNN	60	1102	1537	34	68
	RNN/LSTM	105	925	1257	4	16
	MSC	617	3524	5243	92	88
Blockchain		937	6335	2689	164	285

Apart from this, more information is furnished in Table VII, where a critical assessment is carried out towards existing learning approaches concerning detection accuracy, detection time, and typical applications. The numerical scores exhibited in this table are averaged after reviewing existing research papers as well as additional works, e.g. [71][72].

TABLE VII
PERFORMANCE COMPARISON OF ML AND DL MODELS FOR IOT SECURITY

Learning Approach	Model Type	Detection Accuracy (%)	Detection Time (ms)	Typical Applications
Supervised	SVM	85 – 95	50 – 150	Assists in malware detection, Binary classification
Supervised	RF	87 – 96	100 – 200	Towards packet filtering, Intrusion detection in smart city applications
Supervised	DT	80 – 90	30 – 120	Intrusion detection for smart meters, wearables
Supervised	LoR	75 – 88	25 – 80	Prediction of attacks in healthcare units
Supervised	LiR	70 – 85	20 – 60	Event prediction in sensor networks
Unsupervised	KMC	60 – 80	70 – 200	Anomaly detection in industrial IoT
Unsupervised / Anomaly Detection	IF	78 – 92	60 – 180	Outlier detection in low-power IoT
Deep Learning (Unsupervised)	AE	90 – 97	200 – 800	Anomaly detection
Ensemble Learning	GBM	88 – 96	150 – 300	Behaviour and fraud analysis
Deep Learning	CNN	91 – 98	300 – 1000	Multimedia surveillance
Deep Learning	RNN) / LSTM	89 – 96	250 – 900	Behaviour analysis in smart logistics
Deep Learning	Miscellaneous	88 – 97	300 – 1200	multivariate time-series in IoT, sensor fusion tasks, and Hybrid attacks

It shows that the applicability of different models varies from each other, while some of them are found to have a common range of applications towards a secure IoT system. The detection of threats is carried out for the considered adversary models within the cited research work discussed in these sections, towards IoT.

From the perspective of detection accuracy, it is noted that CNN and AE in deep learning models, while SVM and RF in machine learning models, are better performers with more than 95% accuracy. From the perspective of speed, the LR and DT model are known for their faster execution, which makes them more suitable for real-time IoT security applications. GBM and RF are seen to offer a better trade-off between performance and accuracy, and hence could be considered as a balanced model. However, deep learning models like CNN and other miscellaneous models are found to be dependent on GPU and TPU, as well as sometimes edge offloading, which is not found to be resource efficient.

F. Learning Outcomes of the Research Gap

The research gaps we've identified have been prioritised based on their impact and urgency, and they are as follows:

- *Less Dynamic Access Control Schemes (High Impact and Urgent)*: While there are various viable access control techniques, many are based on fixed, predetermined assumptions about the environment or devices. This is an issue, particularly in IoT networks, where the danger landscape can shift swiftly and unexpectedly.
  - *Research Questions and Directions*: i) How can we make access control models more dynamic, so they can respond to real-time changes in security requirements? and ii) Can we add machine learning to these models to make them more adaptable and responsive?
- *Hardware dependencies (Medium Impact, Urgent)*: We've made good progress in secure device management, but many of these systems still require ongoing monitoring, maintenance, and updates. Existing research does not sufficiently address these dependencies.
  - *Research Questions and Directions*: i) How can we create lightweight security solutions, hardware-independent, and that do not require regular updates or complex maintenance? and ii) Is it conceivable for low-cost, resource-constrained devices to offer secure booting and firmware updates while maintaining performance?
- *Unbalanced Evolving Schemes (Medium Impact, High Urgency)*: Learning-based approaches are becoming more widespread, although their application in resource-constrained handheld IoT devices has not been thoroughly investigated. Furthermore, prediction models often neglect the diversity of devices in IoT contexts, limiting their practical utility.
  - *Research Questions and Directions*: i) What modifications are required to make machine learning models function on resource-constrained portable IoT devices? and ii) How can we incorporate diverse IoT environments into machine learning models to increase scalability and overall effectiveness?
- *Blockchain-induced complexity (low impact, medium urgency)*: Blockchain has the potential to secure IoT devices, but it also adds additional issues, such as vulnerability to attacks (such as the 51% attack) and high computing needs, making it unsuitable for many IoT devices.
  - *Research Questions and Directions*: i) Can we improve blockchain technology to perform more effectively in resource-constrained IoT contexts while maintaining security? and ii) How can blockchain be combined with other IoT security technologies to improve performance and security?
- *Few studies on handheld device security (high impact, medium urgency)*: The majority of present IoT security research is broad in scope; however, there are few dedicated studies on handheld IoT devices. These gadgets possess distinct properties that are not well addressed in generic security models.
  - *Research Questions and Directions*: i) What specific security difficulties do portable IoT devices face, and how can we tailor existing solutions to address them? and ii) Can we create new, lightweight security models designed exclusively for handheld IoT devices that do not degrade performance or usability?

From all the above-mentioned gap highlights, the learning outcomes now reveal increasing demands for a context-sensitive, resource-aware, and highly adaptable security framework that is customized for handheld devices in IoT. Such gaps can be addressed by emphasizing scalable learning modelling with hardware-agnostic security methods and real-time access control that could function effectively on resource-constrained devices. Further, computational overhead can be minimized by fine-tuning blockchain implementation, while it is also critical to integrate various scenarios of IoT for improving both applicability and accuracy.

G. Discussion

This study examined security options for IoT handheld devices, emphasizing both device-level security and integration with larger IoT systems. It was discovered that, while classic access control models are extensively utilized, emerging models such as CTAC and CBAC provide greater flexibility but provide privacy and management difficulties. Various encryption systems, including symmetric and hybrid encryption, are widely used, with hybrid being recommended for balancing security and performance. Although secure device management solutions such as authentication and firmware updates are successful, they are limited by operational and physical constraints. The review also emphasized the importance of machine learning in threat detection; however, its implementation is constrained by resource limits in mobile devices.

Our findings back up prior research on the complexities of protecting IoT devices, particularly handhelds, due to their variety and limited resources. Like the previous study, we discovered that standard solutions such as access control and encryption frequently fail to handle the unique difficulties of these devices. Traditional access control models, such as RBAC, are inflexible in dynamic IoT

environments, whereas newer techniques, such as ABAC and CTAC, are more adaptable but raise privacy and context concerns. Although hybrid encryption provides a fair mix of security and performance, it adds administrative complexity, as previous research has shown. Furthermore, the usefulness of machine learning in detecting anomalies is generally acknowledged, but its application to resource-constrained mobile devices necessitates additional modifications.

Our findings indicated that, while IoT security has improved, major holes remain in securing resource-constrained mobile devices. We discovered that many generic IoT security solutions require modification to suit the special difficulties of portable devices, such as limited resources and fluctuating connectivity. Access control techniques such as RBAC are frequently unsuccessful in dynamic contexts, and while machine learning has potential, it confronts hurdles when applied to mobile devices. Contrary to our early assumptions, encryption is no longer the primary focus; rather, multi-layered techniques that combine encryption with additional technologies such as access control and blockchain are gaining popularity.

IV. Conclusion

The operational environment of IoT is far more complex than that of traditional wireless networks, making linked devices exposed to a variety of security attacks. IoT refers to a huge network of interconnected devices, protocols, infrastructure, software, hardware, and middleware. This intricacy makes it extremely difficult to safeguard each device from potential threats. This study provides a comprehensive review of the existing methods used to protect IoT devices, including the following significant contributions: i) a summary of essential techniques that bring together various security approaches for IoT; ii) recognition of core security methods that have been spread across different studies; iii) an examination of commonly used approaches, along with a focus on lesser-explored methods for researchers to consider; and iv) a detailed discussion of the strengths, weaknesses, and research gaps in current strategies.

The future of IoT security is dependent on closing these gaps, which are critical for increasing the protection of IoT devices. Some of the significant research gaps identified in this study include the need for dynamic access control systems, hardware-independent security solutions, the use of learning-based models in resource-constrained situations, and the operational problems associated with blockchain. These concerns are not only pressing but also crucial for designing security frameworks capable of keeping up with the constantly increasing dangers in IoT environments. By addressing these shortcomings, we may improve the security of handheld IoT devices and develop more adaptable, scalable, and efficient security mechanisms that can be used in a variety of IoT contexts.

As IoT expands and becomes more widely accepted, solving these security issues will become increasingly more critical. The research gaps discovered provide great prospects for future work, ensuring that IoT devices, particularly those with low resources, can operate securely in an increasingly complicated and hostile environment. Future research will focus on closing these gaps, beginning with the development of novel threat identification and mitigation mechanisms that use advanced machine learning techniques. Hence, the future work will be carried out towards improving the real-time deployment scenarios by emphasizing more on lightweight security methods which is capable of fine-tuning itself to a dynamic threat environment. This should be done without sacrificing any form of performance associated with a resource-constrained IoT device. Further, an extension of this study can be towards integrating adaptive access control with blockchain and machine learning for a more scalable and resilient defence system customized specifically for an IoT environment.

In a nutshell, it can be stated that there are critical research gap existing in framework of IoT security especially with respect to demand of adaptive and scalable access control to be collaborated with threat detection in real-time. This form of research challenge can be addressed by developing a novel decentralized access control by collaborative efforts of blockchain and ML models. The notion of this architecture will be towards facilitating access management with inclusion of context-aware and dynamic attributes.

References

[1] L. Falomo Bernarduzzi, E. M. Bernardi, A. Ferrari, M. C. Garbarino, and A. Vai, “Augmented Reality application for handheld devices: How to make it hAPPen at the Pavia University history museum,” Sci. & Educ., vol. 30, no. 3, pp. 755–773, 2021, doi: 10.1007/s11191-021-00197-z.

[2] E. Chatzoglou, G. Kambourakis, and C. Smiliotopoulos, “Let the cat out of the bag: Popular Android IoT apps under security scrutiny,” Sensors (Basel), vol. 22, no. 2, p. 513, 2022, doi: 10.3390/s22020513.

[3] B. D. Marah et al., “Smartphone architecture for edge-centric IoT analytics,” Sensors (Basel), vol. 20, no. 3, p. 892, 2020, doi: 10.3390/s20030892.

[4] D. Jean, B. Broll, G. Stein, and Á. Lédeczi, “Utilizing smartphones for approachable IoT education in K-12,” Sensors (Basel), vol. 22, no. 24, p. 9778, 2022, doi: 10.3390/s22249778.

[5] M. Okmi, L. Y. Por, T. F. Ang, and C. S. Ku, “Mobile phone data: A survey of techniques, features, and applications,” Sensors (Basel), vol. 23, no. 2, p. 908, 2023, doi: 10.3390/s23020908.

[6] Z. Deng, L. Guo, X. Chen, and W. Wu, “Smart wearable systems for health monitoring,” Sensors (Basel), vol. 23, no. 5, p. 2479, 2023, doi: 10.3390/s23052479.

[7] B. Al-Duwairi, W. Al-Kahla, M. A. AlRefai, Y. Abedalqader, A. Rawash, and R. Fahmawi, “SIEM-based detection and mitigation of IoT-botnet DDoS attacks,” Int. J. Electr. Comput. Eng. (IJECE), vol. 10, no. 2, p. 2182, 2020, doi: 10.11591/ijece.v10i2.pp2182-2191.

[8] E. Anthi, L. Williams, V. Ieropoulos, and T. Spyridopoulos, “Investigating Radio Frequency vulnerabilities in the Internet of Things (IoT),” IoT, vol. 5, no. 2, pp. 356–380, 2024, doi: 10.3390/iot5020018.

[9] T.-F. Lee, I.-P. Chang, and G.-J. Su, “Compliance with HIPAA and GDPR in certificateless-based authenticated key agreement using extended chaotic maps,” Electronics (Basel), vol. 12, no. 5, p. 1108, 2023, doi: 10.3390/electronics12051108.

[10] T. Jabar and M. Mahinderjit Singh, “Exploration of mobile device behavior for mitigating advanced persistent threats (APT): A Systematic Literature Review and conceptual framework,” Sensors (Basel), vol. 22, no. 13, p. 4662, 2022, doi: 10.3390/s22134662.

[11] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, “A survey on security, privacy, trust, and architectural challenges in IoT systems,” IEEE Access, vol. 12, pp. 57128–57149, 2024, doi: 10.1109/access.2024.3382709.

[12] 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,” IEEE Access, vol. 10, pp. 101362–101384, 2022, doi: 10.1109/access.2022.3207472.

[13] N. Mazhar, R. Salleh, M. Zeeshan, and M. M. Hameed, “Role of device identification and manufacturer usage description in IoT security: A survey,” IEEE Access, vol. 9, pp. 41757–41786, 2021,

doi: 10.1109/access.2021.3065123.
[14] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for Bluetooth low energy in IoT and wearable devices: A comprehensive survey," IEEE Open J. Commun. Soc., vol. 3, pp. 251–281, 2022, doi: 10.1109/ojcoms.2022.3149732.
[15] H. Jmila, G. Blanc, M. R. Shahid, and M. Lazrag, "A survey of smart home IoT device classification using machine learning-based network traffic analysis," IEEE Access, vol. 10, pp. 97117–97141, 2022, doi: 10.1109/access.2022.3205023.
[16] Z. Muhammad, Z. Anwar, A. R. Javed, B. Saleem, S. Abbas, and T. R. Gadekallu, "Smartphone security and privacy: A survey on APTs, sensor-based attacks, side-channel attacks, Google play attacks, and defenses," Technologies (Basel), vol. 11, no. 3, p. 76, 2023, doi: 10.3390/technologies11030076.
[17] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi, and R. Vera-Rodriguez, "A survey of privacy vulnerabilities of mobile device sensors," ACM Comput. Surv., vol. 54, no. 11s, pp. 1–30, 2022, doi: 10.1145/3510579.
[18] Ö. Şeker, G. Dalkılıç, and U. C. Çabuk, "MARAS: Mutual authentication and role-based authorization scheme for lightweight Internet of things applications," Sensors (Basel), vol. 23, no. 12, p. 5674, 2023, doi: 10.3390/s23125674.
[19] C. Cheng, B. Yan, and G. Wang, "The blockchain based access control scheme for the Internet of Things," Procedia Comput. Sci., vol. 202, pp. 342–347, 2022, doi: 10.1016/j.procs.2022.04.046.
[20] X. H. Le, T. Doll, M. Barbosu, A. Luque, and D. Wang, "An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow," J. Biomed. Inform., vol. 45, no. 6, pp. 1084–1107, 2012, doi: 10.1016/j.jbi.2012.06.001.
[21] Z. Yang et al., "An attribute-based access control scheme using blockchain technology for IoT data protection," High-Confidence Computing, vol. 4, no. 3, p. 100199, 2024, doi: 10.1016/j.hcc.2024.100199.
[22] S. Y. A. Zaidi et al., "An attribute-based access control for IoT using blockchain and smart contracts," Sustainability, vol. 13, no. 19, p. 10556, 2021, doi: 10.3390/su131910556
[23] H.-A. Pham, N. N. Do, and N. Huynh-Tuong, "A fine-grained access control model with enhanced flexibility and on-chain policy execution for IoT systems," Thesai.org. vol.14, Iss.6, 2023. Doi: 10.14569/IJACSA.2023.0140609
[24] Y. Liu et al., "Capability-based IoT access control using blockchain," Digit. Commun. Netw., vol. 7, no. 4, pp. 463–469, 2021, doi: 10.1016/j.dcan.2020.10.004.
[25] M. Mpyana Mwamba and I. Hoh Peter, "SC-CAAC: A smart-contract-based context-aware access control scheme for blockchain-enabled IoT systems," IEEE Internet Things J., vol. 11, no. 11, pp. 19866–19881, 2024, doi: 10.1109/jiot.2024.3371504.
[26] R. Bułat and M. R. Ogiela, "Personalized context-aware authentication protocols in IoT," Appl. Sci. (Basel), vol. 13, no. 7, p. 4216, 2023, doi: 10.3390/app13074216.
[27] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," Symmetry (Basel), vol. 11, no. 2, p. 293, 2019, doi: 10.3390/sym11020293
[28] M. Rana, Q. Mamun, and R. Islam, "Enhancing IoT security: An innovative key management system for lightweight block ciphers," Sensors (Basel), vol. 23, no. 18, p. 7678, 2023, doi: 10.3390/s23187678.
[29] B. Halak, Y. Yilmaz, and D. Shiu, "Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications," IEEE Access, vol. 10, pp. 76707–76719, 2022, doi: 10.1109/access.2022.3192970.
[30] Y. Cheng, Y. Liu, Z. Zhang, and Y. Li, "An asymmetric encryption-based key distribution method for wireless sensor networks," Sensors (Basel), vol. 23, no. 14, p. 6460, 2023, doi: 10.3390/s23146460.
[31] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," IEEE Access, vol. 8, pp. 52018–52027, 2020, doi: 10.1109/access.2020.2980739.
[32] S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das, and Y. Park, "ECC-PDGPP: ECC-based parallel dependency RFID-grouping-proof protocol using zero-knowledge property in the internet of things environment," IEEE Open J. Comput. Soc., vol. 5, pp. 329–342, 2024, doi: 10.1109/ojcs.2024.3406142.
[33] A. Munshi and B. Alshawi, "Hybrid encryption model for secured three-phase authentication protocol in IoT," J. Sens. Actuator Netw., vol. 13, no. 4, p. 41, 2024, doi: 10.3390/jsan13040041.
[34] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment," IEEE Access, vol. 8, pp. 66878–66887, 2020, doi: 10.1109/access.2020.2984317.
[35] J. L. López Delgado, J. A. Álvarez Bermejo, and J. A. López Ramos, "Homomorphic asymmetric encryption applied to the analysis of IoT communications," Sensors (Basel), vol. 22, no. 20, p. 8022, 2022, doi: 10.3390/s22208022.
[36] Y.-J. Chen, C.-L. Hsu, T.-W. Lin, and J.-S. Lee, "Design and evaluation of device authentication and secure communication system with PQC for AIoT environments," Electronics (Basel), vol. 13, no. 8, p. 1575, 2024, doi: 10.3390/electronics13081575
[37] J. H. Kang and M. Seo, "Enhanced authentication for decentralized IoT access control architecture," Cryptography, vol. 7, no. 3, p. 42, 2023, doi: 10.3390/cryptography7030042.
[38] Y. Jiang, Y. Dou, and A. Hu, "Identification of IoT devices based on hardware and software fingerprint features," Symmetry (Basel), vol. 16, no. 7, p. 846, 2024, doi: 10.3390/sym16070846.
[39] A. K. Al Hwaitat et al., "A new blockchain-based authentication framework for secure IoT networks," Electronics (Basel), vol. 12, no. 17, p. 3618, 2023, doi: 10.3390/electronics12173618.
[40] F. Mahfoudhi, A. K. Sultania, and J. Famaey, "Over-the-air firmware updates for constrained NB-IoT devices," Sensors (Basel), vol. 22, no. 19, p. 7572, 2022, doi: 10.3390/s22197572.
[41] V. Malumbres, J. Saldana, G. Berné, and J. Modrego, "Firmware updates over the Air via LoRa: Unicast and broadcast combination for boosting update speed," Sensors (Basel), vol. 24, no. 7, p. 2104, 2024, doi: 10.3390/s24072104.
[42] H.-Y. Chien and N.-Z. Wang, "A novel MQTT 5.0-based over-the-air updating architecture facilitating stronger security," Electronics (Basel), vol. 11, no. 23, p. 3899, 2022, doi: 10.3390/electronics11233899.
[43] E. N. Witanto, Y. E. Oktian, S.-G. Lee, and J.-H. Lee, "A blockchain-based OCF firmware update for IoT devices," Appl. Sci. (Basel), vol. 10, no. 19, p. 6744, 2020, doi: 10.3390/app10196744.
[44] W.-J. Tsaur, J.-C. Chang, and C.-L. Chen, "A highly secure IoT firmware update mechanism using blockchain," Sensors (Basel), vol. 22, no. 2, p. 530, 2022, doi: 10.3390/s22020530.
[45] A. S. Siddiqui, Y. Gui, and F. Saqib, "Secure boot for reconfigurable architectures," Cryptography, vol. 4, no. 4, p. 26, 2020, doi: 10.3390/cryptography4040026.
[46] K.-H. Park, S.-J. Kim, J. Yun, S.-H. Lim, and K.-W. Park, "FLEX-IoT: Secure and resource-efficient network boot system for flexible-IoT platform," Sensors (Basel), vol. 21, no. 6, p. 2060, 2021, doi: 10.3390/s21062060.
[47] M. R. Hasan et al., "Smart contract-based access control framework for Internet of Things devices," Computers, vol. 12, no. 11, p. 240, 2023, doi: 10.3390/computers12110240.
[48] S. N. Matheu et al., "Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems," Sensors (Basel), vol. 20, no. 7, p. 1882, 2020, doi: 10.3390/s20071882.
[49] K. M. Sadique, R. Rahmani, and P. Johannesson, "IMSC-EIoTD: Identity management and secure communication for edge IoT devices," Sensors (Basel), vol. 20, no. 22, p. 6546, 2020, doi: 10.3390/s20226546.
[50] K. M. Sadique, R. Rahmani, and P. Johannesson, "DIdM-EIoTD: Distributed identity management for edge Internet of Things (IoT) devices," Sensors (Basel), vol. 23, no. 8, p. 4046, 2023, doi: 10.3390/s23084046.
[51] S. Venkatraman and S. Parvin, "Developing an IoT identity management system using blockchain," Systems, vol. 10, no. 2, p. 39, 2022, doi: 10.3390/systems10020039.
[52] Z. Yang et al., "BDIDA-IoT: A blockchain-based decentralized identity architecture enhances the efficiency of IoT data flow," Appl. Sci. (Basel), vol. 14, no. 5, p. 1807, 2024, doi: 10.3390/app14051807.
[53] A. Partida, R. Criado, and M. Romance, "Identity and access management resilience against intentional risk for blockchain-based IOT platforms," Electronics (Basel), vol. 10, no. 4, p. 378, 2021, doi: 10.3390/electronics10040378.
[54] S. Namane and I. Ben Dhaou, "Blockchain-based access control techniques for IoT applications," Electronics (Basel), vol. 11, no. 14, p. 2225, 2022, doi: 10.3390/electronics11142225.
[55] H. Purnama and M. Mambo, "IHIBE: A hierarchical and delegated access control mechanism for IoT environments," Sensors (Basel), vol. 24, no. 3, p. 979, 2024, doi: 10.3390/s24030979.
[56] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," J. Sens. Actuator Netw., vol. 10, no. 3, p. 58, 2021, doi: 10.3390/jsan10030058
[57] S. Ben Atitallah, M. Driss, and I. Almomani, "A novel detection and multi-classification approach for IoT-malware using random forest voting of fine-tuning convolutional neural networks," Sensors (Basel), vol. 22, no. 11, p. 4302, 2022, doi: 10.3390/s22114302.
[58] S. Chalichalamala, N. Govindan, and R. Kasarapu, "Logistic

Regression Ensemble Classifier for Intrusion Detection System in Internet of Things," Sensors (Basel), vol. 23, no. 23, p. 9583, 2023, doi: 10.3390/s23239583.
[59] A. Guan, C.-H. Lin, and P.-W. Chi, "Secure collaborative computing for linear regression," Appl. Sci. (Basel), vol. 14, no. 1, p. 227, 2023, doi: 10.3390/app14010227.
[60] T. Mazhar et al., "Analysis of IoT security challenges and its solutions using artificial intelligence," Brain Sci., vol. 13, no. 4, p. 683, 2023, doi: 10.3390/brainsci13040683
[61] A. Andalib and V. T. Vakili, "A novel dimension reduction scheme for intrusion detection systems in IoT environments," Arxiv.org. Accessed: Sep. 06, 2024. [Online]. Available: http://arxiv.org/abs/2007.05922
[62] B. S. Sharmila and R. Nagapadma, "Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset," Cybersecurity, vol. 6, no. 1, 2023, doi: 10.1186/s42400-023-00178-5.
[63] H. Torabi, S. L. Mirtaheri, and S. Greco, "Practical autoencoder based anomaly detection by using vector reconstruction error," Cybersecurity, vol. 6, no. 1, 2023, doi: 10.1186/s42400-022-00134-9.
[64] M. E. Aminanto, T. Ban, R. Isawa, T. Takahashi, and D. Inoue, "Threat alert prioritization using isolation forest and stacked auto encoder with day-forward-chaining analysis," IEEE Access, vol. 8, pp. 217977–217986, 2020, doi: 10.1109/access.2020.3041837.
[65] O. B. J. Rabie, S. Selvarajan, T. Hasanin, A. M. Alshareef, C. K. Yogesh, and M. Uddin, "A novel IoT intrusion detection framework using Decisive Red Fox optimization and descriptive back propagated radial basis function models," Sci. Rep., vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-51154-z.
[66] J. A. Faysal et al., "XGB-RF: A hybrid machine learning approach for IoT intrusion detection," Telecom, vol. 3, no. 1, pp. 52–69, 2022, doi: 10.3390/telecom3010003.
[67] T. Lawrence and L. Zhang, "IoTNet: An efficient and accurate Convolutional Neural Network for IoT devices," Sensors (Basel), vol. 19, no. 24, p. 5541, 2019, doi: 10.3390/s19245541.
[68] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," IEEE Access, vol. 9, pp. 161546–161554, 2021, doi: 10.1109/access.2021.3128837.
[69] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," J. Big Data, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00448-4.
[70] F. Habib, S. H. Shirazi, K. Aurangzeb, A. Khan, B. Bhushan, and M. Alhussein, "Deep neural networks for enhanced security: Detecting metamorphic malware in IoT devices," IEEE Access, vol. 12, pp. 48570–48582, 2024, doi: 10.1109/access.2024.3383831.
[71] A. M. Al-Ghamdi and M. M. Alansari, "Enhancing IoT security: A comparative study of CNN and RNN-based anomaly detection using the CICIoT2023 dataset," IAENG International Journal of Computer Science, vol. 52, no.5, pp. 1424-1441, 2025.
[72] M. Selim and R. A. Sadek, "An effective fog-aware NIDS for DDoS attack detection," vol. 52, no.6, pp. 1806-1814, 2025.

Pushpa Rajput Narayana Singh is an accomplished academic and professional with a M. Tech in Computer Science & Engineering from JNNCE, Shimoga, under VTU, Belagavi and a B.E. in the same field from JNNCE, Shimoga. She has 13 years of teaching experience, she is currently working as an Assistant Professor, in the department of Computer Science and Engineering at JNNCE, Shimoga. Her expertise spans networks, Internet of Things and Machine Learning. She can be contacted at email: pushpa@jnnce.ac.in

Neelambike Siddalingaiah is an accomplished academic and professional with a Ph.D. in Computer Science & Engineering from VTU, Belagavi. She holds an M. Tech in the same field from Bapuji Institute of Engineering & Technology and a B.E. in Information Science from JNNCE, Shimoga with over 18 years of experience, she is currently working as a professor and head at GM University, Davangere. Her expertise spans networks, data analytics, cloud computing, artificial intelligence, and vehicular ad hoc networks. She has also published several papers and holds several patents, recognized for her contributions, she received the "Excellent and innovation academician" award at international convention 2021 and Excellent faculty award at GM University 2023. She can be contacted at email: neelambikes@gmit.ac.in