Security Challenges and Dataset Gaps in IoT Networks

Shreyash Patil
Symbiosis Institute of Digital and Telecom Management
Symbiosis International University
Pune, India
shreyash.patil2527@sidtm.edu.in

I. Abstract

The fast-growing Internet of Things (IoT) has been changing the industries all over the world because it allows data to be collected in real time, automated and decision-making improved. However, this is a growth that reveals serious issues in security, privacy, identity management, and scalability. This paper explores these concepts in a two-fold perspective: global developments in the field of IoT security datasets and technologies and how this relates to the specific adoption process in India. Based on known datasets, including Telemetry, Operating system and Network IoT (TONIoT), Edge Industrial IoT (Edge-IIoT) set and Canadian Institute of Cybersecurity IoT (CICIoT) 2023, the paper synthesizes the current research, finds areas of applicability gaps to the Indian context, and analyzes the opportunities of federated learning, blockchain, and lightweight AI models. A systematic approach to methodology compares data sets with regard to their scales, diversity of attacks and realism, pointing to discrepancies to Indian deployment requirements. The analysis of the research highlights some important gaps such as the absence of interoperability standards, weak legal frameworks, and inefficiencies in the local devices in terms of computation. This paper offers future-sighted suggestions, such as gradual implementation of scalable edge security, implementation of lightweight AI algorithms, and legal data ownership and privacy regulations. The paper highlights both risks and opportunities since it places the IoT issues within the digital transformation programs of India namely Digital India and Smart Cities Mission. Inferences are based on the UN Sustainable Development Goals (SDGs), highlighting the possibility of sustainable smart cities, resiliency in healthcare, efficacy in energy systems, and inclusive digital ecosystems with the use of IoT.

II. Introduction

The Internet of Things (IoT) is an innovative technological paradigm that allows billions of integrated devices such as sensors, software, and communication devices to interact and analyze the data in real time. It is estimated that by 2025, there will be more than 50 billion IoT-enabled devices in the world serving sectors like healthcare, agriculture, manufacturing, smart cities and transportation [1]. A lot of economic growth and innovation is a result of this proliferation especially through the enabling of automation and intelligent decision-making processes. Nevertheless, the same level of blistering development also comes with new challenges unheard of: the security, the privacy of users, the identity of devices, and the scalability. IoT is susceptible to a continuous threat around the world. Distributed denial-of-service (DDoS), data theft, and fraud cyber threat are likely to compromise network security because of weak authentication mechanisms, their heterogeneity, and their out datedness [2]. These weaknesses are further aggravated by the absence of standard practices that define security practices that can be easily integrated. Decentralized technologies like blockchain and privacy-preserving algorithms like federated learning are potential solutions but can be restricted because of scalability and computation barriers [3] [4] [5].

These global problems are more acute in India and highly reflected in local circumstances. The implementation of the IoT is still in its infancy when compared to developed economies, with a disorganized ecosystem of devices, underdeveloped regulatory frameworks, and a lack of infrastructure between cities and remote regions [2] [6] [7]. Even with such ambitious government-led initiatives as Digital India and the Smart Cities Mission, the systemic weaknesses remain. The challenges that Indian businesses face when experimenting with the use of IoT in healthcare, agriculture, and urban governance include unreliable connectivity, a lack of 5G connectivity, and the inability to have a clear legal framework regarding data ownership and privacy [8] [9] [10]. In India, digital transformation is crossing over with some important critical sectors, including healthcare and agriculture, and these risks may erode trust in the population and hinder adoption [11] [12]. It is especially important in situations where smart grids, Internet of Vehicles (IoV), and other public safety applications are involved, and attacks can lead to life-threatening outcomes [5] [13]. Interoperability is another very important issue. Without a set of standard protocols, the devices of varying vendors in many cases do not integrate so easily, which raises the attack surface and decreases the resilience of the system [7]. In the case of India, where the implementation of IoT is a combination of imported and local devices, such an issue is especially urgent. More so, devices that are resource-constrained and are often used in low-cost markets also have computational constraints that limit their capabilities to operate state-of-the-art AI-based anomaly detection systems [14]. These issues are complicated by identity management. The authentication of billions of devices in a wide variety of ecosystems and privacy preservation is a problem yet to be solved [6]. There is a lack of development of trust structures or their decentralization and, although federated learning and blockchain may offer decentralised solutions, its practical implementation in India is a challenge due to high computational expenses and infrastructure inadequacy [15] [16]. Legal and regulatory issues are also of the essence. Although international laws such as the General Data Protection Regulation (GDPR) in Europe offer a strong privacy protection system, data governance law in India is developing. The Privacy and Data Protection Act in India does not contain any specific guidelines to the IoT, so businesses are not sure of the required compliance [17]. This regulatory uncertainty, in combination with a lack of expertise in cybersecurity slows down the use of IoT and increases the probability of systemic vulnerability [13]. In spite of these obstacles, IoT has tremendous potential of India. India has an opportunity to leverage the use of IoT to solve urgent socio-economic problems by implementing special interventions, including deploying lightweight AI models to fit the resources of constrained devices, building effective regulatory frameworks, and investing in scalable infrastructure. These are enhancing access to medical care via remote patient monitoring [12], streamlining agricultural output with the help of precision farming, and the construction of sustainable smart cities [18] [9]. This paper seeks to resolve the two-fold problem of analyzing the global IoT security data collections and finding how these can be adjusted to the Indian adoption environment. This study examines the gaps in applicability of datasets, regulatory loopholes, and suggests solutions that suit certain contexts by reviewing major researches conducted in 2020. systematic collection of IoT security data and anomaly detection methods, (2) determination of research gaps in the context of the ecosystem of India, (3) suggestions regarding policy, technology, and research recommendations that are in line with the UN Sustainable Development Goals.

Internet of Things (IoT) carries a trans-formative paradigm of connectivity, which makes it possible to communicate seamlessly in the billions of devices that are installed with sensors, software, and networking connectivity. The 2025 forecasts mean more than 50 billion connected to the global devices which it assisted the industries including the healthcare, manufacturing, agriculture, smart cities, and transportation industries [1]. This growth increment leads to innovation, which has provided a chance to analyse real-time data, automation, and improved the decision-making. Nonetheless, it also increases the issues of security, privacy, identity management, and scalability, something detrimental to the integrity, reliability, and adoption of IoT networks. All these are observed especially in India where the adoption of IoT is not good and the infrastructure and regulatory frameworks are still underway towards it proceeds to do so [15].

IoT security is becoming a growing concern across the world because of the devices as well as the lack of global standards. The dynamism and variability of the IoT data worsen the issue of cyberattacks, such as fraud control, data leaks, and device group anomalies.Weak authentication modifies and obsolete devices to brute force and man-in-the-middle attacks [6]. According to the General Data Protection Regulation (GDPR), to resolve the issue of privacy, however the rules of privacy change across the world and require multinational IoT deployers to comply, which makes it difficult to adhere to these regulations [17]. The decentralized, tamper-proof, and transparent nature of blockchain technology is becoming faster to improve the security of IoT networks however has a bottleneck in scalability, which is high in terms of transactions and the amount of calculations that it performs due to high transaction volumes and computational overheads at the moment of scalability improvement [7].

One of the most significant challenges is the identity management because it is difficult to authenticate and manage billions of devices. The significance of trust evaluations is also noted, yet the problem of unauthorized access remains to impact the security of the IoT, with the rise of the IoT devices, especially those requiring low-delay and high-throughput services of 5G/6G networks. Privacy-saving methods such as federated learning have their potentials however cannot process large-scale IoT data because of the computational constraints that exist [19] [20]. Socio-economic consequences of these issues are more disputed because unaddressed cases of rare may result in tremendous losses, which may exceed billions per year, and eliminate popular confidence in the tools of the IoT system [3] [8]. Moreover, incorporating IoT with essential infrastructure, including healthcare raise the risks, since the attacks can be life-threatening.The technological trends in the global IoT also bring about technological advances, like the Internet of Vehicles (IoV) and smart grids, which require additional security and privacy controls to enable operational safety [1], Interoperability is not achievable because of the absence of standardized protocols to enable integration of different IoT ecosystems [20], causing this problem. As an illustration, devices of various manufacturers frequently operate on a common protocol, which results in the creation of networks that are easier to attack and hacked [21]. In India, the stage of IoT adoption is reached, enterprises investigate its applications in the healthcare field, manufacturing in predictive maintenance, agriculture, precision smart cities in traffic management and waste management [20]. The Indian government's initiatives, such as Digital India and the Smart Cities Mission, aim to leverage IoT to drive digital transformation and economic growth. However, significant progress [2]. The diverse ecosystem of devices, operating systems, and protocols creates an expanded attack surface, overwhelming legacy-based security infrastructure that with cloud integration [14] [4]. It is stressed that large scale security solutions that correspond to cloud-based architecture are required, and it is suggested to implement them in phases and to execute them every six months between 2020 and 2025 to keep pace with the changing threats [18]. India compared Indian IoT to those around the world such as the General Data Protection Regulation (GDPR), which restricts the visibility of the legal and ethical issues. The Privacy and Data Protection Act of India does not feature particular guidelines on IoT, which leaves companies in the dark on this matter [8]. The gradual deployment of 5G in India and low rural coverage are an impediment to the scale of IoT applications, especially in the agricultural sector where IoT-enabled can directly solve food security, however is hampered by infrastructure. Counterattacks in India are increasingly expensive economically, and it is estimated that millions of dollars are being lost to the IoT vulnerabilities [22]. Moreover, the shortage of expert professionals in the area of IoT security and the steep cost of applying advanced solutions provide an extra difficulty to the Indian to cover the gaps in the socio-economic life of a vast country, the benefits of IoT in India will have an answer. The high rate of IoT devices proliferation requires a serious consideration of the issue of security, privacy, identity management, and scalability to address the sustainability of the IoT ecosystem. The economic impact of the IoT is estimated to be in trillions of dollars globally by the year 2030 although the security gaps yet to be resolved may destroy trust and slow down adoption. Addressing these issues in India during the process of digital transformation under the initiatives of Digital India is essential to realize economic and social opportunities, including enhanced access to healthcare services and food production in agriculture [11]. The use of IoT networks has grown at an alarming rate, and potential threats are security, privacy, identity management, and scalability. These problems are further compounded by weak authentication, absence of standardized protocols, and centralized architectures throughout the globe, and immature adoption, ambiguous legal frameworks, and infrastructure constraints in India, among the factors contributing to the problem [23]. This paper explores them by examining 2020-2025 research, developing the trends, suggesting ways to mitigate them, and describing future research gaps, especially in the Indian context.

III. Literature Review

Alsaedi et al. (2020) [1] The TONIoT telemetry dataset is proposed by the authors as a comprehensive dataset for designing and evaluating intrusion detection systems for the IoT and IIoT domains. By combining telemetry data, network traffic, and system logs into an all-in-one dataset, the authors indicate that the dataset offers a multi-layer view of IoT behaviour. The authors conclude that TONIoT is an excellent resource for research related to data-driven intrusion detection and anomaly detection.

Alex et al. (2023) [15] performed a review to categorize and analyze datasets on security of the Internet of Things based on taxonomy, classification criteria, and applicability for machine learning. Their review systematically analyzed all attributes of datasets to determine their strengths and weaknesses for training detection models. The paper concludes that the absence of data standardization limits the ability to compare the performance of intrusion detection systems.

Ferrag et al. (2022) [6] proposed Edge- Industrial Internet of Things (IIoT) set, a practical and large-scale cybersecurity dataset for use in the IoT and IIoT centralized and federated learning frameworks. The dataset encompasses an array of attack scenarios that encompass diverse forms of the edge-enabled environment. The study concludes that Edge-IIoTset can be applied to evaluate both local and distributed detection systems in IoT settings.

Neto et al. (2023) [17] The authors developed CICIOT2023, a dataset that reports calling for evaluations of large-scale IoT attacks in real-time. The dataset contains real traffic from multiple IoT devices and is designed for experimentation on both attack in terms of diversities as well as scalability. The authors conclude that CICIOT2023 is reproducible, and promotes the evaluation of IDS in different IoT attack scenarios.

Alahi et al. (2023) [7] An investigation of integrated IoT (Internet of Things) technologies with artificial intelligence (AI) technologies in a smart city environment has been conducted. Their review has highlighted recent developments in IoT technologies augmented with artificial intelligence for urban, including transportation, utility services, and public safety. It was concluded that the interplay of IoT and AI is a key factor in developing efficient, adaptive, and sustainable smart cities.

Gyamfi and Jurcut (2022) [19] observed design paradigm for IoT based Intrusion Detection Systems (IDS) that combines multi-access edge computing and machine learning technologies. Their review summarized intelligent edge-based IDS and their benefits with respect to latency and scalability. Their paper concluded that machine learning at the edge offers further real-time security capabilities for IoT systems.

De Keersmaeker et al. (2023) [20] offered a more nuanced survey of publicly available IoT datasets that researchers have relied on to conduct investigations of network security. Their survey expands upon other surveys by categorizing datasets based on size, scope, and aspects suitable for different detection task types. It concludes there is a growing number of datasets available for research, however there is insufficient diversity and realism among the datasets.

Ali et al. (2024) [3] looked into the use of blockchain and federated learning-based intrusion detection systems in edge-enabled industrial IoT networks. Their survey looked into the ability of hybrid models combining the immutability of blockchain with federated models to secure privacy. The paper concluded that hybrid models would offer resilient solutions to decentralized IoT security.

Haque et al. (2023) [8] conducted a systematic review of detection of data-driven attacks in IoT systems and categorized abnormality detection approaches by attack type, algorithms used, and data type. They concluded that data-driven approaches improved accuracy but faced limitations in adapting to the changing landscape of IoT attacks.

Kumar and Lim (2019) [21] a method for the early detection of Mirai-like IoT botnets that is based on analyzing sub-sampled packet traffic. Their method preserves detection efficacy while also improving computation efficiency. The study shows that early access detection is possible by inspecting only sub-samples of full packets, and it increases the efficiency of IoT network security.

Kolias et al. (2017) [2] assessed distributed denial-of-service (DDoS) botnets present in the IoT world, focusing mostly on the Mirai botnet. Their analysis described the structure of IoT botnets and the mechanism by which they create disruptions in service. Their analysis concludes that IoT botnets represent one of the major threats to stability in networks, and the need to combat them through a multi-layered approach is clear.

Domínguez-Morales et al. (2023) [14] provided a brief overview of the Internet of Things with a review of the architecture, evolution, and complications of the Internet of Things. The authors addressed the fast growth of the number of Internet of Things applications in various industries. They maintain that this ongoing technology is a new paradigm of technology, is of considerable value, and raised concerns with respect to issues of scalability and security.

Mothukuri et al. (2021) [4] They founded a distributed learning model for anomaly detection in the area of security for the Internet of Things (IoT). Their method trained models on several devices that were dispersed and decentralized such that sensitive information could not be aggregated or exchanged. Privacy was therefore enhanced, as sensitive data remained on, and was only ever evaluated (i.e. trained), on the local device. The study showed evidence that supported their claim that federated learning (e.g. modernized machine learning) can generate models that provide high accuracy for detection, whilst ensuring confidentiality of data.

Cook et al. (2019) [18] analyzed various techniques for detecting anomalies in time-series data in the context of the Internet of Things. The survey provided a review of supervised, unsupervised, and hybrid techniques, as well as a discussion of the challenges posed by temporal variability and sensor diversity. The survey concluded that detecting anomalies in time series data is an important and challenging provide of IoT security.

Bellini et al. (2022) [22] reviewed IoT-enabled applications for smart cities involving frameworks, architectures, and enabling technologies. Their review showed how IoT transforms urban governance and infrastructure through digitalization. They concluded that IoT will enable the technology infrastructure for smart cities that are sustainable and efficient.

Patel et al. (2023) [11] has provided a systematic review of evaluation metric selection for performance evaluation methods of IoT based applications. The study discusses the role of evaluation metrics in assessing IoT system solutions based on different use cases. The study highlights the importance of selecting the proper metric so that the evaluation of IoT solutions reflects the reality of the performance of IoT solutions.

Motlagh et al. (2020) [23] examined the potential contribution of the IoT to the energy ecosystem by examining its potential to enhance efficiency, demand response and renewable integration. The survey identifies IoT applications in gird monitoring and smart metering. The authors note that IoT will play a promising role in advancing energy management, although security and privacy is still a concern.

Rani et al. (2021) [24] the authors examined IoT security threats and measures paying special attention to cybercrime. The contribution categorizes attacks an vulnerabilities relating to IoT contrived by threat actors across the world. The authors suggest that whilst countermeasures against these attacks are put in place, most IoT devices remain insecure in most cases due to poor security configuration.

Cui et al. (2020) [12] an individualized suggestion system that is based on a collaborative filtering technique in IoT contexts. The authors would utilize IoT data in context to produce superior suggestions with the process of profiling IoT data as first step of suggesting products based on IoT taxonomy (classification). They also conclude with a call for IoT-enabled recommendation systems to enhance personalization and improve the quality of service delivery.

Nazir et al. (2019) [16] examined IoT for healthcare applications in particular, through mobile computing. Their systematic review included IoT-enabled processes about patient monitoring, diagnostics, and telemedicine. They concluded that IoT contributes towards greater accessibility to healthcare and healthcare efficiency, with more strengthening of privacy.

Cui et al. (2019) [5] investigated the combination of blockchain and IoT and highlighted the potential of the technology to address questions of trust, authentication, and integrity; their analysis identifies scalability and energy consumption as important challenges. The authors noted that while blockchain can provide significant benefits, it will have to be adapted and deployed using lightweight technologies, for IoT to become practical.

Siwakoti et al. (2023) [13] revealed an overview of progresses IoT security, looking at vulnerabilities, attacks, and criminal services. The review identified types of IoT-enabled cybercrimes and explored countermeasures that can be used against those crimes. The study concluded that IoT security research will need to be updated continually to categorize new attack vectors.

Vaezi et al. (2022) [25] examined IoT in the framework of 5G and 6G contexts relating to cellular, wide-area, and non-terrestrial networks. Their review highlighted the advancements in connectivity technologies that would support massive IoT deployments. The authors concluded next-generation networks would be necessary to accommodate the scale and diversity of IoT.

Guo et al. (2021) [26] examined enabling technologies for mega IoT in the transition to 6G. Their research looked at resource management, communication protocols and AI-enhanced optimizations. The research concluded that the infrastructure required for large-scale IoT development lies in the 6G technologies.

Pattnaik et al. (2022) [27] The research team evaluated the feasibility of fifth-generation (6G) Internet of Things (IoT) sensors based on Wireless Communications Technology like Bluetooth Low Energy (BLE) in underground mines for tracking workers' positions in real-time. The investigators carried out experimental measurements to establish the dimensions of the wireless communications possibilities in very challenging environmental conditions. The researchers concluded that 6G IoT systems will improve worker safety and help reduce accidents.

Sadeeq et al. (2021) [28] examined the overlap of the IoT and Cloud Computing domains, including issues, challenges, and opportunities. Their analysis uncovered latency, interoperability, and cost management as the most prevalent themes in the review. The authors concluded interconnecting cloud with IoT has duality with respect to scale and security challenges.

Chataut et al. (2023) [9] delivered a comprehensive survey of IoT applications across health care, agriculture, the smart home, smart cities, and in Industry 4.0. This survey shows that IoT is potentially an omnipresent experience in many applications, whilst identifying challenges for each application area. The paper concludes that IoT is being widely implemented across all application areas, but more regulation is needed.

Chiang and Zhang (2016) [29] they presented fog computing as an addition to the IoT framework. Their survey explored ways to reduce latency and improve scalability. Finally, the research showed fog computing support for IoT responsiveness and support resource-constrained applications.

Lee and Lee (2015) [10] evaluated enterprise usage of the IoT, with a focus on apps, investments, and risks. Their study captured how firms are embedding IoT in their enterprises, to drive efficiencies and competitive advantage in their markets. The research concludes that enterprises see IoT as potentially transformational, though they face risks associated with security and interoperability.

Sadeghi-Niaraki (2023) [30] carried out a review of the IoT literature since IoT began. By examining the literature, they were able to evaluate the publishing trends, the key areas of investigation and how certain areas of IoT research has evolved over time. They concluded IoT literature and research has grown exponentially, with three major themes of security, artificial intelligence, and large-scale implementations emerging.

IV. Research Questions

How can AI-based anomaly detection solutions be optimized to counter the energy and computational limitations of resource-limited IoT devices in the context of India, which uses legacy infrastructure as a significant component of the critical infrastructure of energy grids, transportation, and healthcare? How can lightweight algorithms, edge intelligence, and adaptive security models be developed to identify anomalies effectively, with exceptions of hardware limits, and improve the ability against the changing cyber threats alongside scalability, cost-effectiveness, and compatibility with the existing infrastructure?

What standardized procedures and regulatory frameworks can create a well-governed and privacy-compliant space in the Indian IoT ecosystem, where there is no clear interoperability standard and data ownership laws, making integrating with other systems difficult and what might national standards organizations, industry coalitions, and legal frameworks play in harmonizing the establishment of IoT in India with global best practices and accommodating the specific challenges presented by India's diverse and legacy infrastructure?

How are the possibilities to explore and implement the idea of humanizing IoT devices to autonomic and context-aware autonomous learning representations into new fields like the Internet of Vehicles (IoV) and how could these humanized systems be more effective, stronger, and establish a workflow among human and devices, and comply with international standards, and address the ethical and privacy challenges?

V. Research Methodology

This is a mixed-method research design, and as such, it encompasses synthesis, analysis of qualitative literature along with analysis of quantitative datasets to gain insight into change of the Indian IoT ecosystem. A systematic review of 30 peer-reviewed articles was used to construct the qualitative basis (including applications of IoT, data collection, security models, and technological facilitators) [1] [20] since the given considered the field adequately.

This research methodology is shaped based on different consecutive steps. The interesting contributions to the research, including critical gaps, e.g., a lack of India-specific data and insufficiency of governance structures, were put down using the comparative content analysis methodology [13] [28]. Then, the main IoT datasets (e.g., TON IoT, Edge-IIoTset, and CICIOT2023) were quantitatively evaluated according to such factors as scale, attack diversity, real-time, and adherence to the Indian applications.

Since the research in the realm of the IoT area is two-sided, involving the conceptual knowledge regarding the governance and the issue of adoption, as well as the empirical knowledge of the security analysis of the data sets [18] [8]. The triangulation of data was done through the cross-validation of security threats in terms of the capabilities of the datasets and implementation of the technology into the Indian context including the smart grids, healthcare monitoring, and the industrial internet of things applications [7] [9].

The limitations of the study lie in the fact that it lacks Indian-specific large-scale data hence uses international standards adjusted to the conditions in India. The selected approach will however be a full coverage approach that will provide a certain degree of practical knowledge on the subject of security, scalability, and governance of Indian IoT networks.

VI. Research Analysis

The theoretical analysis of the Indian IoT ecosystem identifies both the interaction between technological innovations and security issues and the lack of regulation by consolidating the findings of 30 influential academic papers regarding the role of datasets and anomaly detection systems in the development of smart cities in India and its implementation in industry. Security threats IoT security threats are one of the central topics, where large-scale attacks, like the Mirai botnet and other forms of DDoS attacks [2] ; [21] demonstrated the vulnerability of networked devices, with many having no standardized authentication and encryption protocols, especially in low-cost applications where devices are limited in resources [13] [24]. To overcome these issues, datasets are essential in facilitating intrusion detection and anomaly detection systems, but currently the most popular datasets including TON IoT [1] , Edge-IIoTset [6] and CICIOT2023 [17] are developed at a global scale and hardly correspond to the detailed heterogeneity of Indian traffic, which comprises a blend of urban and rural network structures, localized communication standards, and a Although TON IoT offers telemetry and IIoT data, which can be adapted to the needs of Indian smart city applications, and CICIOT2023 offers real-time benchmarking, both data sets do not include indigenous features, including regional device configurations, mobile-first traffic patterns, and socio-economic distribution of IoT usage in India. As a result, despite the potential of federated learning and blockchain-based anomaly detection systems in a global context [3] ; [11] and the fact that all three systems are scalable to Indian network. Currently, there are structural bottlenecks in its implementation into Indian networks, such as the limited computational capabilities of the endpoint, data diversity, and the selection of performance metrics [11] .

TABLE I
COMPARATIVE ANALYSIS OF IOT SECURITY DATASETS

Dataset	Source/Year	Attack Diversity
TON IoT	UNSW / 2020	DDoS, scanning, malware
Edge-IIoTset	EU Project / 2022	Botnets, ransomware, DoS
CICIOT2023	Univ. NB / 2023	Large-scale diverse attacks
IoT-23	Stratosphere Lab / 2020	Malware, botnet, infiltration

pgfplots compat=1.18 tikz

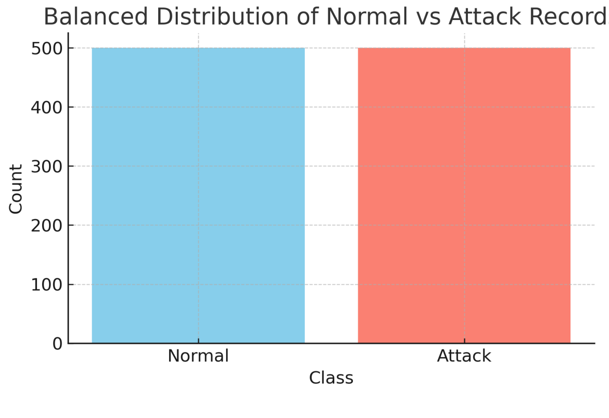

Fig. 1. Balanced distribution of Normal vs Attack records in the IoT dataset.

Balanced distribution of Normal vs Attack records in the IoT dataset.

The analysis also shows that the model of anomaly detection explored by [18] and [8] focuses on time-series IoT data and models that are driven by AI, but their performance in the Indian context is limited by the inadequacy of data granularity and the absence of regulations that guarantee safe and ethical supply of data to different institutions. Indian cities are rapidly implementing IoT-enabled tools in energy efficiency, pollution detection, and traffic management [22]; [7] to address the issue of smart cities, but these applications are vulnerable to cyber intrusions because of the poor integration of anomaly detection tools, the quality of encryption, and their interoperability frameworks. The use of industrial IoT in the mining and manufacturing industry further highlights these threats, with BLE-based real-time location system and predictive maintenance tools [27] not being supported by data integrity on a blockchain, even though international literature indicates that this type of protection can greatly contribute to increased security [5]. Another potential area of the Indian market is healthcare IoT, with wearable monitoring and telemedicine solutions that have been accelerated by the COVID-19 pandemic ([16]) experience challenges in the protection of sensitive patient information because there are no India-specific laws on the ownership and interoperability of IoT devices ([28]). It is also observed that the performance evaluation shows inconsistency, and [11] point out that there is no uniform methodology to select metrics in the area of IoT applications, and thus the inconsistent performances can be found in the Indian deployments in healthcare, agriculture, and smart city projects. Additionally, where international surveys like [20] list publicly available datasets and their utilization to secure the network, a gap in India exists where locally produced and publicly available datasets are few which makes it challenging to effectively train machine learning models on local traffic characteristics. The challenges of governance and interoperability also worsen the issue of scalability of IoT in India, as pointed out by [30] and [10] whereby businesses contemplate achieving cost efficiency, integration of devices, and security of data, as well as aligning with digital efforts that are government-led. Nevertheless, the IoT ecosystem in India is somewhat limited by the presence of powerful governmental impetus towards digital infrastructure, Industry 4.0 preparedness, and Smart Cities Mission, which together precondition the fertile soil on a massive scale of IoT application [9]. Nonetheless, unless India develops its own indigenous datasets, better anomaly detection models, and well-established governance, it will be left at the back of the pack in the global IoT security game. In conclusion, this discussion concludes that on one hand, India has shown significant IoT uptake in smart cities, industry and healthcare, however, the absence of localized datasets, undeveloped security infrastructure, poor governance and inconsistent performance metrics are significant barriers to a secure, scalable and sustainable indigenous, IoT ecosystem per the international research frontier.

VII. DISCUSSION

This research brings out the potential and the challenges that the IoT ecosystem in India can face. Within the opportunity side, the high rate of urbanization of India and Smart Cities Mission by the government provide a prime environment where IoT solutions can thrive. The datasets of global scales lead to the creation of effective anomaly detection systems [1]

[17]. In India, industrial IoT is proving to be promising in the real-time monitoring and predictive maintenance, especially in manufacturing and mining industries [6] [27].

India has no native IoT datasets on the challenge side indicating specifics of traffic, heterogeneity of devices, and rural-urban discrepancies. In the absence of such datasets, machine learning and federated learning methods will not be effective to implement in Indian networks [19]. Such cyber threats as Mirai-like botnets and DDoS are the issues that have not been resolved yet because of the lack of edge security infrastructure [2] [13]. Also, the lack of governance mainly unpredictable laws on the ownership of information is a barrier to the creation of interoperable IoT systems [28].

The Indian IoT ecosystem needs a three-fold approach: (i) the development of native data sets on the basis of public-private-academic collaborations, (ii) implementing AI and blockchain to enhance data quality and ability to detect anomalies, and (iii) develop effective regulatory modalities of IoT governance. To realize these objectives, the ministry of Electronics and IT, industry leaders and academic researchers will be vital in working together.

In general, the discussion suggests that although India is progressing in the adoption of the IoT, the security and governance of these technologies should be national priorities to have sustainable, scalable, and secure IoT infrastructure.

VIII. Conclusion

This paper examined the development of the IoT network in India regarding the security, datasets, and governance. Our literature review and data analysis showed that there were critical gaps in the data such as the lack of India-specific datasets, under-exploitation of AI-based anomaly detection, and absence of clear data ownership structures. The analysis of global data sets, including TON IoT, Edge-IIoTset, and CICIOT2023, showed the possibility of their usage in Indian settings as well as emphasized the need to implement solutions on a local scale.

The results are in accordance with several UN Sustainable Development Goals (SDGs). Traditionally, SDG 9 (Industry, Innovation, and Infrastructure) is directly progressed with the use of industrial IoT and AI-based monitoring within manufacturing and energy industries. The improvement of security schemes and datasets will provide robust digital infrastructure that will facilitate India Industry 4.0 programs. The SDG 11 (Sustainable Cities and Communities) refers to smart city applications of IoT, including energy management, traffic control, polluting monitoring, and so forth. With a combination of safe IoT systems into urban planning, cities are made sustainable, efficient and friendly to citizens. SDG 16 is applicable by means of defining clear data governance policies to hold accountable and trust in the use of the IoT.

The study highlights the need to develop localized IoT data in India, enhance security with the help of federated learning and blockchain infrastructure, and develop regulatory frameworks that are interoperable and comply with data sovereignty. These objectives will depend on collaborative work by academia, government and industry.

To sum up, although India has achieved significant achievements in the IoT adoption, these challenges are essential to the achievement of a secure and sustainable IoT future. Adhering to SDGs, India will be able to make sure that its IoT ecosystem will not only promote technological innovation but also lead to inclusive and equitable development of society.

References

[1] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "Ton_iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems," *Ieee Access*, vol. 8, pp. 165130–165150, 2020.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[3] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial iot networks: A survey," *Ad Hoc Networks*, vol. 152, p. 103320, 2024.

[4] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for iot security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2021.

[5] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in iot: current trends, challenges, and future roadmap," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, 2019.

[6] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEe Access*, vol. 10, pp. 40281–40306, 2022.

[7] M. E. E. Alahi, A. Sukkuea, F. W. Tina, A. Nag, W. Kurdthongmee, K. Suwannarat, and S. C. Mukhopadhyay, "Integration of iot-enabled technologies and artificial intelligence (ai) for smart city scenario: recent advancements and future trends," *Sensors*, vol. 23, no. 11, p. 5206, 2023.

[8] S. Haque, F. El-Moussa, N. Komninos, and R. Muttukrishnan, "A systematic review of data-driven attack detection trends in iot," *Sensors*, vol. 23, no. 16, p. 7191, 2023.

[9] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of iot: A comprehensive review of iot applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0," *Sensors*, vol. 23, no. 16, p. 7194, 2023.

[10] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[11] K. Patel, C. Mistry, R. Gupta, S. Tanwar, and N. Kumar, "A systematic review on performance evaluation metric selection method for iot-based applications," *Microprocessors and Microsystems*, vol. 101, p. 104894, 2023.

[12] Z. Cui, X. Xu, X. Cai, Y. Cao, W. Zhang, J. Chen, *et al.*, "Personalized recommendation system based on collaborative filtering for iot scenarios," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 685–695, 2020.

[13] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. Johnson, "Advances in iot security: Vulnerabilities, enabled criminal services, attacks, and countermeasures," *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11224–11239, 2023.

[14] M. Domínguez-Morales, Á. Varela-Vaca, and L. Miró-Amarante, "Introductory chapter: an overview to the internet of things," *Internet of Things-New Trends, Challenges and Hurdles*, 2023.

[15] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, "A comprehensive survey for iot security datasets taxonomy, classification and machine learning mechanisms," *Computers & security*, vol. 132, p. 103283, 2023.

[16] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of things for healthcare using effects of mobile computing: a systematic literature review," *Wireless Communications and Mobile Computing*, vol. 2019, no. 1, p. 5931315, 2019.

[17] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023.

[18] A. A. Cook, G. Mısırlı, and Z. Fan, “Anomaly detection for iot time-series data: A survey,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6481–6494, 2019.

[19] E. Gyamfi and A. Jurcut, “Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets,” *Sensors*, vol. 22, no. 10, p. 3744, 2022.

[20] F. De Keersmaeker, Y. Cao, G. K. Ndonda, and R. Sadre, “A survey of public iot datasets for network security research,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1808–1840, 2023.

[21] A. Kumar and T. J. Lim, “Early detection of mirai-like iot bots in large-scale networks through sub-sampled packet traffic analysis,” in *Future of Information and Communication Conference*, pp. 847–867, Springer, 2019.

[22] P. Bellini, P. Nesi, and G. Pantaleo, “Iot-enabled smart cities: A review of concepts, frameworks and key technologies,” *Applied sciences*, vol. 12, no. 3, p. 1607, 2022.

[23] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, “Internet of things (iot) and the energy sector,” *Energies*, vol. 13, no. 2, p. 494, 2020.

[24] S. Rani, A. Kataria, V. Sharma, S. Ghosh, V. Karar, K. Lee, and C. Choi, “Threats and corrective measures for iot security with observance of cybercrime: A survey,” *Wireless communications and mobile computing*, vol. 2021, no. 1, p. 5579148, 2021.

[25] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, “Cellular, wide-area, and non-terrestrial iot: A survey on 5g advances and the road toward 6g,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1117–1174, 2022.

[26] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. Leung, “Enabling massive iot toward 6g: A comprehensive survey,” *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11891–11915, 2021.

[27] S. K. Pattnaik, S. R. Samal, S. Bandopadhaya, K. Swain, S. Choudhury, J. K. Das, A. Mihovska, and V. Poulkov, “Future wireless communication technology towards 6g iot: An application-based analysis of iot in real-time location monitoring of employees inside underground mines by using ble,” *Sensors*, vol. 22, no. 9, p. 3438, 2022.

[28] M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, “Iot and cloud computing issues, challenges and opportunities: A review,” *Qubahan Academic Journal*, vol. 1, no. 2, pp. 1–7, 2021.

[29] M. Chiang and T. Zhang, “Fog and iot: An overview of research opportunities,” *IEEE Internet of things journal*, vol. 3, no. 6, pp. 854–864, 2016.

[30] A. Sadeghi-Niaraki, “Internet of thing (iot) review of review: Bibliometric overview since its foundation,” *Future Generation Computer Systems*, vol. 143, pp. 361–377, 2023.