Challenges and Solutions in Integrating Narrowband IoT with Edge Computing: Resource Constraints, Security, Latency, and IDS Deployment

Waldon Hendricks and Boniface Kabaso

Abstract This study aimed to explore the integration of narrowband Internet of Things (NB-IoT) with edge computing. The study examined existing literature regarding the resource constraints of IoT devices, security challenges, latency in data transmission and addressing the need for an Intrusion Detecting System (IDS) in edge computing environments. The study further analyzed an IoT Intrusion Dataset for data analysis containing attacks captured to identify and analyze challenges on how to integrate NB-IoT with edge computing. Gaps in the literature and dataset were identified as the need for experimental studies, and interdisciplinary research was highlighted. The main aim of this study was to gather a deeper understanding of the challenges of integrating NB-IoT with edge computing.

Keywords Edge computing · Narrowband IoT · Intrusion detection systems

1 Introduction

1.1 Background

Data need to be analyzed and handled effectively as the number of IoT devices grows exponentially. Edge computing reduced bandwidth and latency and was introduced as the practical solution to process the data locally and close to the network's edge [1]. Edge computing enables faster response times for real-time applications, and resource-constrained environments require shorter response times and low latency [2].

W. Hendricks (✉) · B. Kabaso
Cape Peninsula University of Technology, Cape Town, SA, USA
e-mail: hendricskw@cput.ac.za
URL: https://www.cput.ac.za

B. Kabaso
e-mail: kabasob@cput.ac.za
URL: https://www.cput.ac.za

R. N. Shaw et al. (eds.), *Advanced Computing and Intelligent Technologies*, Lecture Notes in Networks and Systems 958, https://doi.org/10.1007/978-981-97-1961-7_8

These resource-constrained environments need robust security protocols and operate on low-latency networks, thus integrating narrowband IoT with edge computing platforms would pose a unique set of challenges [3]. IoT devices have limited processing power and limited memory against potential cyber threats and attacks; this challenge would require a lightweight algorithm and data compression techniques in order to have secure communication between IoT devices and edge computing [4].

Previous studies have shown that implementing integrated systems faces practical challenges such as scalability, security, and real-time data processing [5, 6]. Interoperability among IoT devices and platforms presents a challenge as they frequently utilize diverse communication protocols and standards. Additionally, the massive amount of data produced by IoT devices can overload traditional data storage and analysis systems, thus requiring the development of efficient big data processing techniques [7].

1.2 Objectives of the Study

The main objective of this study was to analyze the challenges in integrating narrowband IoT with edge computing platforms. The study aims to:

- Examine the resource constraints of IoT devices, such as limited storage and computing power [8].
- Investigate the security challenges, particularly in establishing end-to-end secure communication [9].
- Explore the issues related to latency in data transmission and processing [10].
- Assess the unique challenges posed by deploying Intrusion Detection Systems (IDS) in an edge computing environment [11].

The study aimed to propose practical solutions to these challenges through a multi-faceted approach.

1.3 Scope and Limitations

The scope of the study was limited to narrowband IoT devices and their integration with edge computing platforms. While the challenges discussed may have had broader implications for other IoT devices, the focus remained on narrowband IoT due to its unique constraints and growing adoption in industrial applications [12]. The study was also limited by the availability of empirical data, relying on existing literature for evidence.

2 Literature Review

2.1 Previous Work on IoT and Edge Computing

Integrating the Internet of Things (IoT) and edge computing has increased interest in academic and industrial research. Early works have focused on the benefits of edge computing in IoT applications, such as reduced latency and bandwidth efficiency [13–15]. Studies have also explored various architectures and frameworks that facilitate the integration of IoT devices with edge computing platforms [16–19] (Table 1).

Security in IoT-edge ecosystems has been another area of focus. Researchers have proposed various encryption and authentication methods tailored for resource constrained IoT devices [20–25]. However, these methods often assume stable and high-bandwidth communication links, which may not be true in narrowband IoT scenarios. Various encryption and authentication methods often assume stable and high-bandwidth communication links, which may not be true in narrowband IoT scenarios.

Traditional encryption algorithms like Advanced Encryption Standard (AES) and International Data Encryption Algorithm (DEA) do not satisfy the power and complexity criteria required for Correlation Power Analysis (CPS) or IoT networks [32]. Additionally, they exhibit poor bit error ratio (BER) performance in a noisy wireless channel [33]. To address these issues, modified security algorithms like AES-P with X-OR mapping on AES have been proposed, which reduce power consumption and complexity while maintaining the required security level [34]. Another approach uses artificial bandwidth extension (ABE) techniques to provide toll-quality recovered speech over narrowband communication links [35]. These techniques involve encoding high-band (HB) features into the bit stream of a narrowband speech coder and extracting them at the receiver to reproduce HB-recovered speech. These advancements aim to enhance security and reliability in narrowband IoT scenarios.

The literature on edge computing and IoT security has significantly expanded in recent years, reflecting the field's rapid evolution. A notable study proposed an innovative combination of machine learning and cryptography for IoT security in edge computing, focusing on early detection of abnormal behaviors and introducing a lightweight key management scheme [26]. Another pivotal work addressed the diverse security challenges of various IoT devices, discussing their vulnerabilities to remote and physical attacks and exploring mitigation strategies [27]. Further contributions included research on reducing security overhead in cloud-assisted IoT applications through a data transfer aware grouping technique [28]. A comprehensive survey was also conducted, outlining existing edge-based IoT security solutions and suggesting future research directions [29]. Additionally, the exponential growth of IoT and the consequent traffic surge in cloud services were examined, focusing on resource management and service delivery in cloud-based edge computing environments [30]. Lastly, a detailed overview of current trends, challenges, and future

Table 1 Preliminary literature summary

References	Year	Authors	Research database	Key challenges
Kaur and Batth [13]	2021	G. Kaur and R. S. Batth	IEEE	Various
Sarker et al. [14]	2019	V. K. Sarker et al.	IEEE	Integration
Röbert et al. [15]	2023	Kevin, Röbert et al.	ACM	Real-time applications
Zawish et al. [16]	2023	Muhammad, Zawish et al.	IEEE IoT Journal	Energy efficiency
Anees et al. [17]	2023	T. Anees et al.	Sustainability	Issues and challenges
Varghese et al. [18]	2022	Ashwin, Varghese Anthony et al.	IJETMS	Challenges, applications
Hoque and Harras [19]	2022	M. N. Hoque and K. A. Harras	IEEE Comm. Standards Mag	Potential and challenges
Goveas [20]	2023	Neena, Goveas	IEEE	Resource constraints
Iqbal et al. [21]	2022	Yasir, Iqbal et al.	IEEE	Constrained devices
Arthur et al. [22]	2023	Pedro, Arthur Pinheiro Rosa et al.	IEEE TNSM	Large-scale environments
Xu et al. [23]	2022	Dongdong, Xu et al.	IEEE IoT Journal	Post-quantum
Wang et al. [24]	2022	Rining, Wang et al.	SPIE	Resource-constrained devices
Noura et al. [25]	2022	Hassan, N. Noura et al.	IEEE IoT Journal	Limited devices
Shen et al. [26]	2023	T. Shen, L. Ding, et al.	IEEE	Machine learning and cryptography
Roy et al. [27]	2023	Roy, A., Kokila, J. et al.	Springer	Security of IoT devices
Hsu [28]	2023	Ching-Hsien Hsu	Wiley	Secure data transfer
Sha et al. [29]	2023	Sha, Kewei and Yang, et al.	ScienceDirect	Survey of edge-based IoT
Velmurugadass et al. [30]	2023	P. Velmurugadass, et al.	IEEE	Resource management in cloud based edge
Carvalho et al. [31]	2023	Carvalho, G., et al.	Springer	Trends and challenges in edge computing

directions in edge computing was presented, highlighting valuable research papers as key resources for detailed information on each edge computing architecture [31].

2.2 Identified Areas Requiring Improvement

While existing literature provided valuable insights into the general challenges and solutions for narrowband IoT and edge computing integration, there were notable areas identified that required improvement:

1. **Resource Constraints in Narrowband IoT**: Most studies focus on IoT devices with moderate to high computing capabilities, overlooking the unique challenges posed by narrowband IoT devices, such as limited storage and computational power. The key research challenges in developing resource efficient narrowband IoT devices include low modulation data rates, energy expensive channel coding techniques, and the fast-growing number of connected devices [36]. These challenges hinder the design and deployment of NB-IoT systems and require efficient resource management techniques to meet the quality of service requirements of 5G. While several techniques have emerged to address these challenges, further research is needed to enhance NB-IoT resource management regarding data rate performance, energy efficiency, and scalability [36].
2. **End-to-end Security**: Although security protocols for IoT devices have been extensively studied, there needs to be more research on end-to-end security solutions that are feasible for resource-constrained, narrowband IoT devices. Developing end-to-end security solutions for resource-constrained, narrowband IoT devices faces challenges and opportunities. The challenges include the need for lightweight protocols for accessing public key infrastructure (PKI) services, which results in the prevalence of pre-shared keys (PSK) that do not provide strong authentication and cannot be revoked [37]. Additionally, resource-constrained IoT devices make it difficult to adopt standard security measures, necessitating periodic penetration testing and ethical hacking simulations to identify vulnerabilities [38].
3. **Latency in Real-World Scenarios**: While theoretical models exist for latency reduction in IoT-edge systems, empirical studies that validate these models in real-world narrowband IoT scenarios are scarce. The challenges in measuring latency in real-world narrowband IoT scenarios include meeting different delay requirements for different types of IoT applications, such as life-saving applications requiring low-latency emergency message transmission [39]. Furthermore, policy obstacles may hinder the ability to make measurements and obtain complete latency data sets and security measures, and system-related challenges threaten the implementation of narrowband IoT in healthcare applications [40].
4. **IDS Deployment**: Intrusion Detection Systems (IDS) in edge computing environments have been studied, but not specifically in narrowband IoT. These low-resource devices unique challenges in an IDS setup remain largely unexplored. Implementing an IDS in a narrowband IoT environment poses several key challenges. There were not enough datasets for training and testing Intrusion Detection Systems in implementing an IDS in a narrowband IoT environment with the need for advanced detection techniques, this absence of datasets made it more challenging [41].

3 Methodology

To identify and analyze the challenges associated with integrating narrowband IoT with edge computing platforms, a quantitative approach was taken leveraging the IoT Intrusion Dataset for data analysis.

3.1 Data Collection

Unique insights into the Internet of Things and edge computing were retrieved from the IoTID20 dataset [42].

3.2 Data Analysis Resource Constraints

The IoT Intrusion Dataset [42] was analyzed to summarize the resource constraints of IoT devices, like limited storage and computing power.

Security Challenges

The IoT Intrusion Dataset [42] was used to categorize and quantify security incidents to identify significant factors contributing to security vulnerabilities.

Latency Issues

The IoT Intrusion Dataset [42] was analyzed to calculate latency metrics and assess the impact of different configurations.

IDS Deployment Challenges

The IoT Intrusion Dataset [42] was analyzed to evaluate the effectiveness of Intrusion Detection Systems (IDS) in edge computing environments.

The study findings were limited by the availability and quality of the datasets, as well as the scope and limitations inherent in the collected data.

4 Steps Used to Study the Dataset

We used a structured approach to address our research objectives. This involved several phases, starting from data acquisition to final interpretation. Each phase had specific steps aimed at building on the previous one, resulting in a comprehensive analysis. Table 2 contains details of the phases and their corresponding steps. By adopting this approach, we were able to conduct a thorough analysis of the challenges of integrating narrowband IoT with edge computing platforms. We mainly focused

Table 2 Steps used to study the datasets

Phase	Steps
1. Data acquisition	1.1 Download dataset 1.2 Initial inspection
2. Data preprocessing	2.1 Data cleaning 2.2 Data transformation 2.3 Feature selection
3. Exploratory data analysis	3.1 Descriptive statistics 3.2 Data visualization
4. Data analysis	4.1 Resource constraints analysis 4.2 Security challenges analysis 4.3 Latency issues analysis 4.4 IDS challenges analysis
5. Interpretation and conclusion	5.1 Interpret findings 5.2 Draw conclusions 5.3 Recommendations for future work

on resource constraints, security challenges, latency issues, and IDS deployment challenges.

5 Data Analysis

5.1 Phase 1: Data Acquisition

After downloading the dataset, the sub-phase was to do an initial inspection to understand the dataset structure and the type of data it contains. The dataset format was stored as comma-separated values (CSV).

- `Flow_ID`: Identifier for the network flow
- `Src_IP`: Source IP address
- `Src_Port`: Source port
- `Dst_IP`: Destination IP address
- `Dst_Port`: Destination port
- `Protocol`: Network protocol
- `Timestamp`: Time of the event
- `Flow_Duration`: Duration of the flow
- `Tot_Fwd_Pkts`: Total forward packets
- `Tot_Bwd_Pkts`: Total backward packets
- `Label`: Classification label (e.g., “Anomaly”)
- `Cat`: Category of the anomaly (e.g., “Mirai,” “DoS”)
- `Sub_Cat`: Sub-category of the anomaly (e.g., “Mirai-Ackflooding,” “DoS-Synflooding”)

5.2 Phase 2: Data Preprocessing

Feature selection was a critical step in data analysis. To help identify the most important features contributing to the objectives of this study: resource constraints, security challenges, latency issues, and Intrusion Detection System (IDS) deployment challenges. While these objectives were specific, the dataset used may or may not have contained direct indicators for each. Therefore, a good starting point was to examine the existing features to see how they relate to these objectives.

- Resource Constraints: Features related to the total number of packets (`Tot_Fwd_Pkts`, `Tot_Bwd_Pkts`) or the flow duration (`Flow_Duration`) were indicative of network resource consumption.
- Security Challenges: Features like `Label`, `Cat`, and `Sub_Cat` directly relate to the type of security incidents. Other features like the protocol used (`Protocol`) were also indicative.
- Latency Issues: Features such as `Flow_Duration` and packet counts were relevant.
- IDS Deployment Challenges: Features like `Src_IP`, `Dst_IP`, `Src_Port`, `Dst_Port`, and `Protocol` were critical for understanding the network topology and how an IDS could be effectively deployed.

Summary of Selected Features

- `Flow_Duration`: The mean duration is around 742 ms, with a high standard deviation of approximately 4390 ms, indicating a wide range of values.
- `Tot_Fwd_Pkts`: The mean number of forward packets is around 1.68, with a standard deviation of ~ 3.56.
- `Tot_Bwd_Pkts`: The mean number of backward packets is around 1.47, with a standard deviation of ~ 0.78.
- `Protocol`: The protocols mainly range between 0 and 17, with a mean of around 10.39.
- `Src_Port` **and** `Dst_Port`: These ports have a wide range, as expected, and their means are around 35,333 and 16,839, respectively.

From Fig. 1, we observed that:

- Numerical Features:
  - `Tot_Fwd_Pkts` and `Tot_Bwd_Pkts` have a moderate positive correlation.
  - Most other numerical features show low correlation with each other, suggesting they are relatively independent.
- Categorical Features:
  - `Src_P`, `Dst_IP`: These are the source and destination IP addresses.
  - `Label`, `Cat`, `Sub_Cat`: These are related to the type of network behavior (normal or anomaly) and the category and sub-category of anomalies.

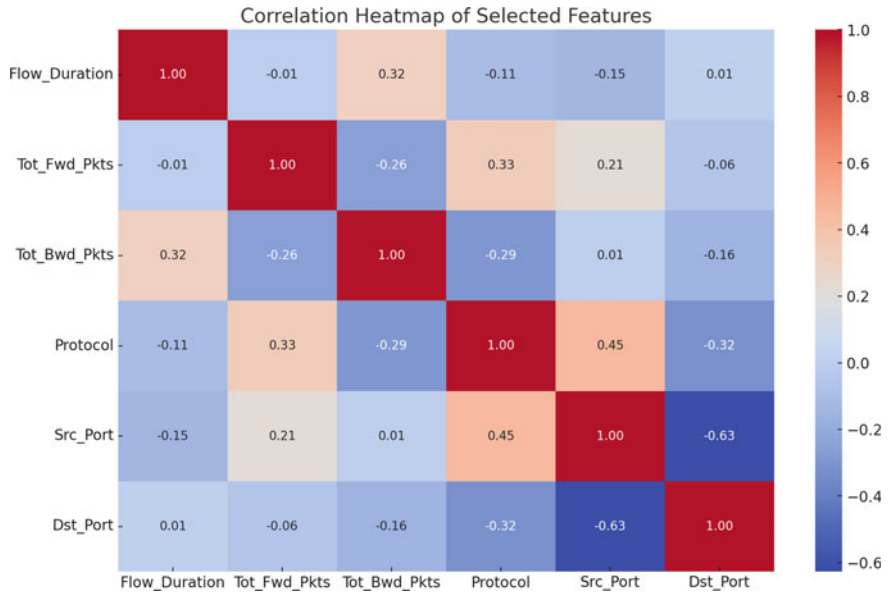

Fig. 1 Correlation heatmap of selected features

- Relevance to Objectives:

  – Resource Constraints: `Flow_Duration`, `Tot_Fwd_Pkts`, and `Tot_Bwd_Pkts` were relevant as they indicated network load and duration.
  – Security Challenges: `Label`, `Cat`, and `Sub_Cat` were directly relevant.
  – `Protocol` also indicated the type of traffic and its security implications.
  – Latency Issues: `Flow_Duration` was selected as an indicator of latency.
  – IDS Deployment Challenges: `Src_IP`, `Dst_IP`, `Src_Port`, `Dst_Port`, and `Protocol` were all critical for understanding network behavior and potential points for IDS deployment.

5.3 Phase 3: Exploratory Data Analysis (EDA)

This was crucial in understanding the dataset. EDA involved visualizing and summarizing the main characteristics of the dataset, with the help of statistical graphics, plots, and tables.

Given the large number of features in this dataset, the study focused on the subset of features that were most relevant to the objectives:

- Resource Constraints:

  – `Flow_Duration`
  – `Flow_Pkts/s`

- Security Challenges:
  - `Dst_Port`
  - `Init_Bwd_Win_Byts`
- Latency Issues:
  - `Flow_Duration`
  - `Flow_IAT_Mean`
- IDS Deployment Challenges:
  - `Dst_Port`

The study looked at the distributions of these features and the relationships between these features and the target variable `Label` (anomalies) as shown in Fig. 2.

- `Dst_Port`: The distribution appeared to be highly skewed, with some ports being much more common than others.
- `Init_Bwd_Win_Byts`: This feature showed a skewed distribution, with a cluster of values around zero.
- `Flow_Duration`: The distributions were skewed toward lower values, indicating that most flows have a shorter duration.
- `Flow_Pkts/s`: This feature had spiked at lower values but also showed a long tail, indicating a wide range of packet rates.
- `Flow_IAT_Mean`: The distributions were heavily skewed toward lower values.

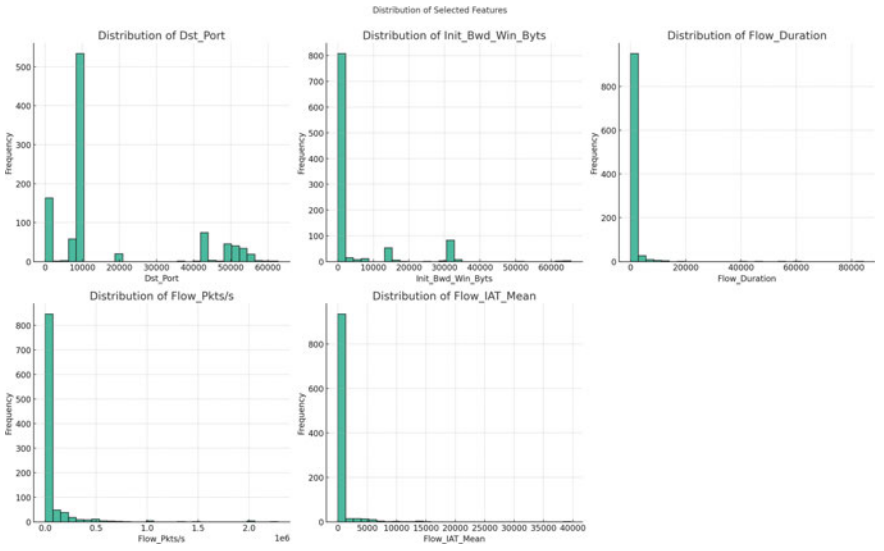

Fig. 2 Distribution of selected features

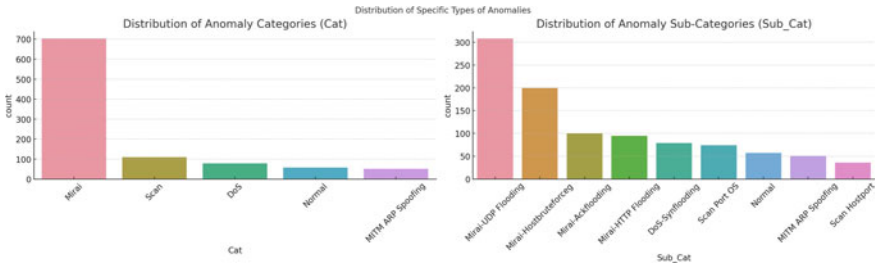

Fig. 3 Distribution of anomalies

5.4 Phase 4: Data Analysis

IDS Deployment Challenges Analysis The IoT Intrusion Dataset on IDS deployment's challenges and effectiveness was analyzed for when an IDS is deployed in edge computing environments due to resource limitations, latency issues, and the heterogeneous nature of IoT devices.

The features `Flow_Duration`, `Tot_Fwd_Pkts`, and `Tot_Bwd_Pkts` were used to gain insights into these constraints. The `Label`, `Cat`, and `Sub_Cat` features were used to categorize network behavior and identify different types of attacks or anomalies for the IDS to detect. To ensure real-time intrusion detection, attention was paid to time-sensitive data using features like `Flow_Duration` and `Flow_AT_Mean`. Lastly, network topology played an important role in effective IDS deployment, and insights were gained using features like `Src_IP`, `Dst_IP`, `Src_Port`, and `Dst_Port`.

The plots and counts shows the distribution of specific anomalies categorized in Fig. 3 under `Cat` (Category) and `Sub_Cat` (Sub-category):

- Distribution of Anomaly Categories (Cat):
  - Mirai: 703 instances
  - Scan: 110 instances
  - Denial of Service (DoS): 79 instances
  - Normal: 57 instances
  - MITM ARP Spoofing: 51 instances.
- Distribution of Anomaly Sub-categories (Sub-cat):
  - Mirai-UDP Flooding: 308 instances
  - Mirai-Hostbruteforce: 200 instances
  - Mirai-Ackflooding: 100 instances
  - Mirai-HTTP Flooding: 95 instances
  - DoS-Synflooding: 79 instances
  - Scan Port OS: 74 instances
  - Normal: 57 instances
  - MITM ARP Spoofing: 51 instances

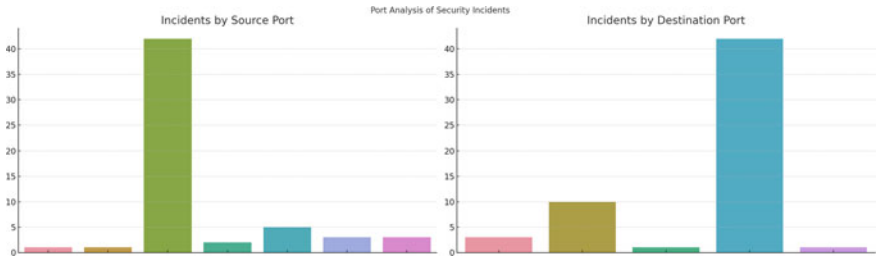

Fig. 4 Port analysis

– Scan Hostport: 36 instances.

Security Challenges Analysis Port Analysis: This determined which ports were most commonly associated with security incidents. This helped identifying vulnerable points in the network.

The bar plots in the Fig. 4 show the distribution of source and destination ports involved in security incidents:

- Incidents by source port:
  - Port 9020: 42 incidents
  - Port 49,793: 5 incidents
  - Port 49,796: 3 incidents
  - Port 50,966: 3 incidents
  - Port 49,789: 2 incidents
  - Port 80: 1 incident
  - Port 443: 1 incident.
- Incidents by destination port:
  - Port 49,784: 42 incidents
  - Port 9020: 10 incidents
  - Port 443: 3 incidents
  - Port 53,229: 1 incident
  - Port 40,278: 1 incident.

Latency Issues Analysis Latency in network systems can have critical implications, especially in real-time applications and edge computing environments. High latency can degrade the performance of an Intrusion Detection System (IDS), making it less effective at detecting and mitigating threats in real time. The density plots in Fig. 5 show the distribution of latency-related features for both normal traffic and security incidents.

- `Flow_Duration`: Both normal traffic and security incidents had a peak at lower durations. However, normal traffic appears to have a wider spread, indicating some instances of longer durations as well.

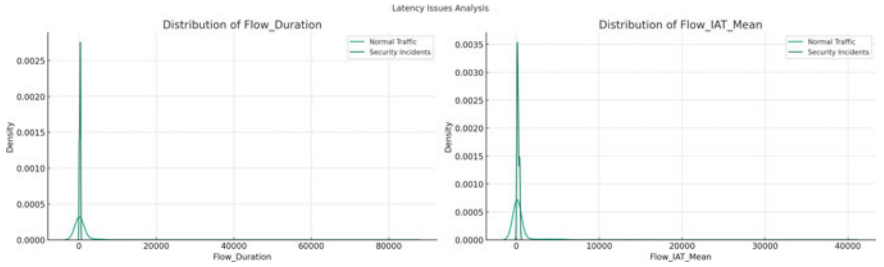

Fig. 5 Latency analysis

- `Flow_IAT_Mean` (Flow Inter-arrival Time Mean): The distributions for normal traffic and security incidents were both skewed toward lower values, indicating that most flows have lower inter-arrival times.

6 Conclusion

We identified the most relevant features for intrusion detection. The most important were the `Src_Port`, `Dst_Port`, `Flow_Duration`, `Tot_Fwd_Pkts`, and `Tot_Bwd_Pkts`.

The `Cat` and `Sub_Cat` fields did not offer meaningful segmentation due to an issue with the dataset. Therefore, we had to adapt our approach. Ports 9020 and 49,784 were identified as hotspots for security incidents, suggesting areas that require increased monitoring. Short-lived connections and low packet counts were common in security incidents, making them harder to detect based on duration and volume alone. Metrics like mean, median, and standard deviation were calculated for latency-related features (`Flow_Duration` and `Flow_IAT_Mean`). Security incidents generally involved shorter flow durations and lower inter-arrival times. Given the low flow durations and inter-arrival times, especially in security incidents, real-time or near-real-time analysis is crucial for effective detection and mitigation.

Regarding IDS deployment, the dataset showed that Mirai-related attacks were particularly prevalent in IoT settings. This underscored the necessity for IoT-specific IDS systems to be well-equipped to detect various attacks, especially those commonly found in IoT infrastructures. Less frequent but highly damaging attacks, such as DoS and MITM ARP spoofing, were also noted. The implication was that specialized algorithms or rule sets would be essential for handling these less common but potentially devastating attack types. Furthermore, understanding the distribution of real-world attack types has been instrumental in shaping the deployment strategy for IoT-focused IDS systems.

Regarding security, the dataset indicated that certain ports, like 9020 and 49,784, were more susceptible to security incidents in the IoT landscape. These ports had emerged as hotspots for potential vulnerabilities, necessitating extra vigilance and security measures. Ports 80 and 443, although generally considered secure due to

their roles in HTTP and HTTPS traffic, were also not immune to security risks, especially given their significance in IoT applications.

Intrusion Detection Systems (IDS) need to adapt to handling different latency requirements due to ports and some features of IoT devices. These ports are all most vulnerable to security incidents and need to be closely monitored and analyzed. The analysis provided a view of the challenges of deploying an IDS in edge computing environments with IoT devices.

7 Areas for Further Research

The study's results offer valuable insights and recommendations for implementing and deploying Intrusion Detection Systems (IDS) in edge computing environments, particularly in the context of narrowband IoT (NB-IoT) networks. The research highlights the significance of monitoring source and destination ports and the informative nature of flow duration and network packet counts in detecting security incidents in IoT networks. Certain ports and traffic patterns were identified as vulnerable to security incidents, guiding proactive threat mitigation.

Moreover, the study emphasizes the need to explore adaptive IDS techniques that adjust to changing network conditions and emerging threats in IoT environments. Additionally, it underscores the urgent need for IoT-specific datasets to identify vulnerabilities in NB-IoT environments empirically, improving the accuracy and efficiency of threat detection and prevention. These findings collectively enhance the security of IoT deployments in the dynamic landscape of edge computing.

References

1. Yun C, Milan P, Dario S, Nurit S, Young V (2015) Mobile edge computing: a key technology towards 5G Valerie. ETSI White Paper 11
2. Chen N, Chen Y, Blasch E, Ling H, You Y, Ye X (2017) Enabling smart Urban surveillance at the edge. In: Proceedings of the 2017 IEEE international conference on smart cloud (SmartCloud), New York, NY, pp 109–119. https://doi.org/10.1109/Smart-Cloud.2017.24
3. Ahmed E et al (2017) Bringing computation closer toward the user network: is edge computing the solution? IEEE Commun Magaz 55(11):138–144. https://doi.org/10.1109/MCOM.2017.1700120
4. Fazeldehkordi E, Grønli T-M (2022) A survey of security architectures for edge computing-based IoT. IoT 3(3):332–365. https://doi.org/10.3390/iot3030019
5. Tiberiu N, Pasika R, Nhien-An LK (2020) Security considerations for internet of things a survey
6. Alrowaily M, Lu Z (2018) Secure edge computing in IoT systems: review and case studies. In: Proceedings of the 2018 IEEE/ACM symposium on edge computing (SEC), Seattle, WA, pp 440–444. https://doi.org/10.1109/SEC.2018.00060
7. Morabito R, Cozzolino V, Ding AY, Beijar N, Ott J (2018) Consolidate IoT edge computing with lightweight virtualization. IEEE Netw 32(1):102–111. https://doi.org/10.1109/MNET.2018.1700175

8. Thakor VA, Razzaque MA, Khandaker MRA (2021) Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities. IEEE Access 9:28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867
9. Usman M, Asghar MR, Ansari IS, Qaraqe M (2018) Security in wireless body area networks: from in-body to off-body communications. IEEE Access 6:58064–58074. https://doi.org/10.1109/ACCESS.2018.2873825
10. Chen X, Shi Q, Yang L, Xu J (2018) Thrifty edge: resource-efficient edge computing for intelligent IoT applications. IEEE Netw 32(1):61–65. https://doi.org/10.1109/MNET.2018.1700145
11. Lin F, Zhou Y, An X, You I, Choo K-KR (2018) Fair resource allocation in an intrusion-detection system for edge computing: ensuring the security of internet of things devices. IEEE Consum Electr Magaz 7(6):45–50. https://doi.org/10.1109/MCE.2018.2851723
12. Kadusic E, Zivic N, Ruland C, Hadzajlic N (2022) A smart parking solution by integrating NB-IoT radio communication technology into the core IoT platform. Fut Internet 14(8):219. https://doi.org/10.3390/fi14080219
13. Kaur G, Batth RS (2021) Edge computing: classification, applications, and challenges. In: Proceedings of the 2021 2nd international conference on intelligent engineering and management (ICIEM), London, pp 254–259. https://doi.org/10.1109/ICIEM51511.2021.9445331
14. Sarker VK, Queralta JP, Gia TN, Tenhunen H, Westerlund T (2019) A survey on LoRa for IoT: integrating edge computing. In: Proceedings of the 2019 fourth international conference on fog and mobile edge computing (FMEC), Rome, pp 295–300. https://doi.org/10.1109/FMEC.2019.8795313
15. Röbert K, Bornholdt H, Fischer M, Edinger J (2023) Latency-aware scheduling for real-time application support in edge computing. https://doi.org/10.1145/3578354.3592866
16. Zawish M, Ashraf N, Ansari RI, Davy S (2023) Energy-aware AI-driven framework for edge-computing-based IoT applications. IEEE Internet Things J 10:5013–5023. https://doi.org/10.1109/JIOT.2022.3219202
17. Anees T, Habib Q, Al-Shamayleh AS, Khalil W, Obaidat MA, Akhunzada A (2023) The integration of WoT and edge computing: issues and challenges. Sustainability 15(7):5983. https://doi.org/10.3390/su15075983
18. Varghese A, Anthony S, Koshy S, Praveen P, Kuriakose S, Sreenath K (2022) Industrial edge computing: architecture, challenges, applications. Int J Eng Technol Manag Sci 14:360–364
19. Hoque MN, Harras KA (2022) Web assembly for edge computing: potential and challenges. IEEE Commun Stand Magaz 6(4):68–73. https://doi.org/10.1109/MCOMSTD.0001.2000068
20. Goveas N (2023) Use of blockchain in securing IoT systems with resource constrained devices. https://doi.org/10.1109/ICSA-C57050.2023.00055
21. Iqbal Y, Amjad MF, Khan FN, Abbas H (2022) The implementation of encryption algorithms in MQTT protocol for IoT constrained devices, pp 804–810. https://doi.org/10.1109/CICN56167.2022.10008320
22. Rosa PAP, Souto A, Cecílio J (2023) Light-SAE: a lightweight authentication protocol for large-scale IoT environments made with constrained devices. IEEE Trans Netw Serv Manag 12:1. https://doi.org/10.1109/tnsm.2023.3275011
23. Xu D, Wang X, Hao Y, Zhang Z, Hao Q, Jia H, Dong HP, Zhang L (2022) Ring-ExpLWE: a high performance and lightweight post-quantum encryption scheme for resource constrained IoT devices. IEEE Internet Things J 9:24122–24134. https://doi.org/10.1109/JIOT.2022.3189210
24. Wang R, Guo G, Wang Z, Meng Z, Li J, Wang JS (2022) Research on lightweight encryption algorithm for IoT devices. 12455:124550T-124550T. https://doi.org/10.1117/12.2655337
25. Noura HN, Salman O, Couturier R, Chehab A (2022) A single-pass and one-round message authentication encryption for limited IoT devices. IEEE Internet Things J 9:17885–17900. https://doi.org/10.1109/JIOT.2022.3161192

26. Shen T, Ding L, Sun J, Jing C, Guo F, Wu C (2023) Edge computing for IoT security: integrating machine learning with key agreement. In: Proceedings of the 2023 3rd international conference on consumer electronics and computer engineering (ICCECE), Guangzhou, pp 474–483. https://doi.org/10.1109/ICCECE58074.2023.10135211
27. Roy A, Kokila J, Ramasubramanian N et al (2023) Device-specific security challenges and solution in IoT edge computing: a review. J Supercomput 79:20790–20825. https://doi.org/10.1007/s11227-023-05450-6
28. Hsu C-H (2023) 5G, IoT, and edge computing convergence—systems, services, and security. Int J Commun Syst 36:e5373. https://doi.org/10.1002/dac.5373
29. Sha K, Yang TA, Wei W, Davari S (2020) A survey of edge computing-based designs for IoT security. Dig Commun Netw 6(2):195–202. https://doi.org/10.1016/j.dcan.2019.08.006
30. Velmurugadass P, Dhanasekaran S, Sasikala S (2021) The cloud based edge computing with IoT infrastructure and security. In: Proceedings of the 2021 international conference on computational performance evaluation (ComPE), Shillong, pp 030–034. https://doi.org/10.1109/ComPE53109.2021.9751942
31. Carvalho G, Cabral B, Pereira V et al (2021) Edge computing: current trends, research challenges and future directions. Computing 103:993–1023. https://doi.org/10.1007/s00607-020-00896-5
32. Ho WG, Pammu AA, Lwin NKZ, Chong KS, Gwee BH (2020) High throughput and secure authentication-encryption on asynchronous multicore processor for edge computing IoT applications. In: Proceedings of the 2020 international SoC design conference (ISOCC), Yeosu, pp 173–174. https://doi.org/10.1109/ISOCC50952.2020.9333008
33. Upadhyay R, Baghel SS, Singh S, Soni A, Bhatt UR (2019) Low complexity security algorithm for CPS/IoT networks. J Telecommun Electr Comput Eng
34. Bhatt N, Kosta Y (2015) A novel approach for artificial bandwidth extension of speech signals by LPC technique over proposed GSM FR NB coder using high band feature extraction and various extension of excitation methods. Int J Speech Technol 18(1):57–64. https://doi.org/10.1007/S10772-014-9249-1
35. Restuccia G, Tschofenig H, Baccelli E (2020) Low-power IoT communication security: on the performance of DTLS and TLS 1.3. 1–6. https://doi.org/10.23919/PEMWN50727.2020.9293085
36. Rajarshi R, Chowdhury P, Abas E (2022) A survey on device fingerprinting approach for resource-constraint IoT devices: comparative study and research challenges. Internet Things. https://doi.org/10.1016/j.iot.2022.100632
37. Höglund J, Furuhed M, Raza S (2023) Lightweight certificate revocation for low-power IoT with end-to-end security. J Inform Sec Appl. https://doi.org/10.1016/j.jisa.2023.103424
38. Yaacoub JPA, Noura HN, Salman O, Chehab A (2023) Ethical hacking for IoT: security issues, challenges, solutions and recommendations. Internet Things Cyber Phys Syst. https://doi.org/10.1016/j.iotcps.2023.04.002
39. Alrubei S, Ball EA, Callum RJ, Willis A (2020) Latency and performance analyses of real-world wireless IoT-blockchain application. IEEE Sens J. https://doi.org/10.1109/JSEN.2020.2979031
40. Kumar M, Kumar A, Verma S, Bhattacharya P, Hosen A (2023) Healthcare internet of things (H-IoT): current trends, future prospects, applications, challenges, and security issues. Electronics. https://doi.org/10.3390/electronics12092050
41. Alhowaide A, Alsmadi I, Tang J (2022) Balanced datasets for IoT IDS. https://doi.org/10.48550/arXiv.2301.04008
42. Ullah S, Mahmoud QH (2020) A scheme for generating a dataset for anomalous activity detection in IoT networks. In: Goutte C, Zhu X (eds) Advances in artificial intelligence. Canadian AI 2020. Lecture Notes in computer science, vol 12109. Springer, Cham