ISSN: 2182-2069 / E-ISSN: 2182-2077

Integrating Named Data Networking with IoT-Based Internet Architectures

Dr. Anusha Sreeram[1*], Shubhashish Goswami[2], Madhur Taneja[3],
Dr. Praveen Priyaranjan Nayak[4], Dr.T. Lalitha[5], Dr. Chunduri Madhurya[6], and N. Raghu[7]

[1*]Faculty of Operations & IT, ICFAI Business School (IBS), The ICFAI Foundation for Higher Education (IFHE) (Deemed to be university u/s 3 of the UGC Act 1956), Hyderabad, India. seeramanusha@gmail.com, https://orcid.org/0009-0003-3397-4311

[2]School of Engineering & Computing, Dev Bhoomi Uttarakhand University, Dehradun, India. socse.shubhashish@dbuu.ac.in, https://orcid.org/0000-0002-6129-9822

[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. madhur.taneja.orp@chitkara.edu.in, https://orcid.org/0009-0000-2931-7122

[4]Associate Professor, Department of Electronics and Communication Engineering, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. praveennayak@soa.ac.in, https://orcid.org/0000-0003-1726-1605

[5]Professor, Department of Computer Science Engineering, Presidency University, Bangaluru, Karnataka, India. lalitha.t@presidencyuniversity.in, https://orcid.org/0000-0003-2850-2363

[6]Assistant Professor, Department of CSE, Vardhaman College of Engineering, Hyderabad, Telangana, India. madhurya1771@vardhaman.org, https://orcid.org/0000-0002-3381-9966

[7]Associate Professor, Faculty of Engineering and Technology, Department of Electrical and Electronics Engineering, JAIN (Deemed-to-be University), Ramanagara District, Karnataka, India. n.raghu@jainuniversity.ac.in, https://orcid.org/0000-0002-2091-8922

Received: April 20, 2025; Revised: June 03, 2025; Accepted: July 22, 2025; Published: August 30, 2025

Abstract

The spread of Internet of Things (IOT) equipment has introduced new challenges for traditional host-centric Internet architecture, especially in addressing scalability, dynamics, and safety concerns. The designated data provides a promising solution by focusing on data-centred recovery from a material-focused paradigm, host-based communication. This paper examines the integration of NDN with IoT-based Internet architecture to increase data spread efficiency, reduce the multitude of network, and support spontaneous dynamics in the asymmetrical IOT environment. We propose a hybrid architectural model that involves NDN in the IOT infrastructure, enabling in-network caching, name-based routing, and enhanced security mechanisms. The proposed integration is analysed in relation to major performance indicators including delay, packet distribution ratio, energy efficiency, and safety flexibility. The simulation results using NDN-competent IOT scenarios show sufficient improvement in data recovery delay and network scalability as compared to traditional IP-based approaches. This study highlights the ability of NDN as a fundamental

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 174-188.
DOI: *10.58346/JISIS.2025.I3.012*

*Corresponding author: Faculty of Operations & IT, ICFAI Business School (IBS), The ICFAI Foundation for Higher Education (IFHE) (Deemed to be university u/s 3 of the UGC Act 1956), Hyderabad, India.

architecture for the future Internet of Things and underlines major research directions for its widespread adoption.

Keywords: Named Data Networking (NDN), Internet of Things (IoT), Content-Centric Networking, Data-Centric Architecture, In-Network Caching, Name-Based Routing, IoT Scalability.

1 Introduction

The rapid expansion of the Internet of Things (IOT) has introduced interconnected devices in a new era that generate large amounts of data. From smart homes and cities to industrial automation and healthcare, IoT is transforming various sectors through data-driven decision-making and real-time insights (Atzori et al., 2010). However, this exponential growth of IOT devices presents important challenges for traditional internet architecture (Kassim, 2017). The current IP-based infrastructure, designed for human-focused communication, struggles to meet the scalability, dynamics, and safety demands of a rapid device-centric world (Ahlgren et al., 2012). For example, managing a large number of IOT devices with unique IP addresses becomes rapidly cumbersome, leading to issues of network congestion and delays (Zanella et al., 2014). In addition, as IOT devices often work in a dynamic and mobile environment, the traditional communication model fails to efficiently handle network topology and frequent changes in device locations (Gubbi et al., 2013). In addition, safety remains a pressing concern, as IOT network data is highly unsafe for interception (Kooshki et al., 2016), injections, and unauthorized access, which can reduce the integrity and privacy of sensitive information.

Given these challenges, there is a growing requirement of a new communication paradigm that efficiently supports the IOT Infrastructure (Verma & Mehta, 2024), addressing the boundaries of traditional IP-based systems. The designated data provides a promising solution by focusing on the data-focused approach (Jacobson et al., 2009) from the host-based communication, a content-focused networking model, and a material-based networking model. In NDN, data is nominated and recovered based on its content rather than its location, which simplifies the routing process and increases the data recovery efficiency (Jacobson et al., 2009). Additionally, the in-network in NDN reduces the congestion of the caching network and improves the speed of material delivery, which is particularly beneficial for the IOT system with constant data requests (Sardiana & Pramudito, 2018). Despite its ability, integrating NDN in IoT Architecture remains an area of active research, as it involves resolving many practical challenges such as adopting NDN's name-based routing for large-scale IOT deployment and ensuring safety in a highly dynamic environment (Bastida et al., 2021).

The purpose of this letter is to propose the integration of NDN with IoT-based internet architecture to improve data spread efficiency, scalability, and safety. By combining the strength of the content-focused model of NDN with a distributed nature of the IOT network (Agrab, 2022), the paper presents a novel hybrid architecture that increases the scalability of the IOT system, reduces data recovery delay, and in-networks speaks of network safety through caching and name-based routing. The contribution of this letter includes the evaluation of its performance in terms of design, delay, packet delivery ratio, energy efficiency, and safety flexibility of the Hybrid IOT-NDN architecture and presentation of simulation results that display the superiority of the proposed approach compared to traditional IP-based models. Conclusions suggest that NDN can significantly improve the performance of the IOT network, making it more scalable, efficient, and safe (Khan & Salah, 2018).

The remaining article has been organized as follows. Section 2 reviews the IOT network (Ghazanfari et al., 2018) on IOT architecture and the integration of NDN. Section 3 prepares the proposed hybrid architecture and its design principles. Section 4 describes the functionality used to evaluate the performance of the proposed architecture, including the simulation setup and performance matrix. Section 5 presents results and discussions, comparing the proposed IOT-NDN architecture with traditional IP-based systems (Rojas & García, 2024; Cao et al., 2016). Finally, Section 6 concluded the paper with a summary of major findings and suggestions for future research.

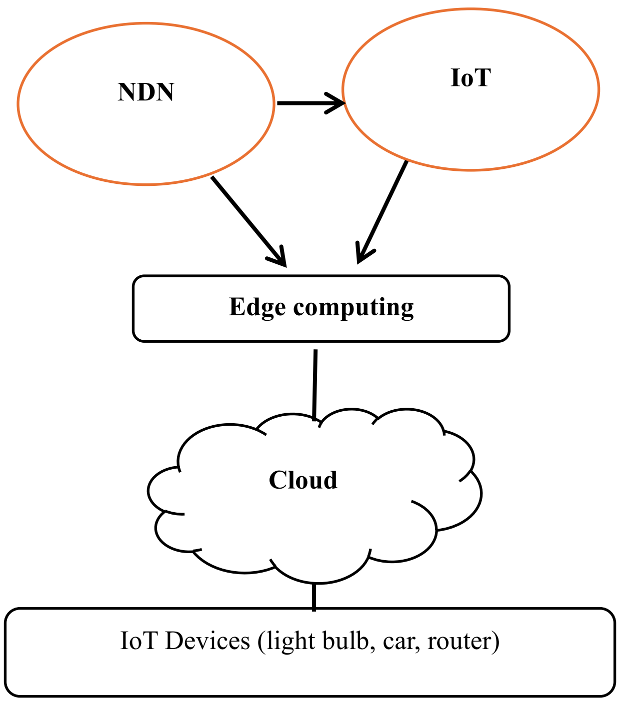

Figure 1: Integration of Named Data Networking (NDN) with IoT-Based Internet Architectures

Figure 1 shows the integration of data networking (NDN) with IoT-based Internet architecture. This shows how NDN enhances traditional IP addresses with content names to increase IOT, improve data recovery and storage efficiency. The NDN-1OT layer brings two systems, allowing spontaneous communication. The edge processes the data close to the computing source, reduces delay, and adapts to real-time decision making. Cloud acts as a centralized repository for data storage and processing, while IOT devices (such as sensors and smart devices) interact within the system to generate and share data, which increases overall network performance and scalability.

2 Literature Survey

2.1 IoT Architectures

The Internet of Things (IOT) has become a ubiquitous part of the modern technical infrastructure, which enables real-time data exchange in a variety of domains such as healthcare, agriculture, and transport. Traditional IOT architecture is usually based on centralized, IP-based communication, where data of IOT devices is sent to central servers for processing and storage (Akyildiz et al., 2002). However, as the number of equipment is increasing, these architecture struggles with scalability issues, networks and high delay in data transmission. One of the major challenges in the IOT architecture is the efficient management of large-scale equipment, especially in a dynamic environment where the instruments often change location or position (Kulkarni & Jain, 2023). Additionally, the energy efficiency of IOT devices is a significant concern, as many IOT applications require battery-powered sensors and equipment that should reduce energy consumption while maintaining reliable connectivity (Bandyopadhyay & Sen, 2011). In addition, as IOT equipment is deployed in mobile and asymmetrical environments, the dynamics of the equipment present another challenge in maintaining uninterrupted communication and ensuring data integrity (Kaur & Chandra, 2024). These challenges have operated the discovery of new architectural models that can provide greater scalability, energy efficiency and adaptability.

2.2 Named Data Networking (NDN)

Nominated data networking (NDN) is a data-focused networking paradigm that originally changes the way of communicating data into the network (Sadegh, 2016). Unlike traditional IP-based networks, which rely on host-centred addresses, NDN identifies data by specific names, which enables material-based routing. In NDN, the data is requested, and the material is recovered based on these names rather than the network source of the data (Babazade et al., 2014). This change in the paradigm provides many advantages, especially in an environment where data is often required to share or recover. One of the most important features of NDN is its in-network caching capacity, which allows the intermediate router to store copies of data close to users, reduce the network congestion and improve data recovery efficiency (Ahlgren et al., 2012). The cashing mechanism not only improves data delivery speed, but also reduces load on the server, which is particularly beneficial in large -scale IOT network. In addition, NDN enhances security by combining data with a cryptographic signature, allowing users to verify data authenticity without relying on the source. This makes NDN particularly suited for data-focused communication, such as IOT, where equipment and applications require rapid, safe and efficient data recover.

2.3 IoT and NDN Integration

Many research efforts have been made to integrate NDN in the IOT system to remove scalability and energy efficiency challenges of traditional architecture. For example, Liu, similarly, Luan detected the integration of NDN in IOT for smart grid applications (Luan et al., 2015), showing that NDN can significantly reduce the bandwidth use and increase network credibility through material-based routing and caching. However, these approaches also face challenges. While the cashing mechanism of NDN can reduce delay and improve energy efficiency, managing the vast amounts of data generated by IOT devices and ensuring cash stability in real time are complex issues. Additionally, many studies focus on specific applications, such as healthcare or smart cities, and lacks a generalized solution that can be applied to diverse IOT domains. In addition, integrating NDN with existing IOT protocols and standards is a significant hurdle, as there is no single, universally accepted model for this integration. Despite these challenges, NDN IOT presents a promising approach to increase the scalability and efficiency of the network.

2.4 Research Gaps

While the integration of NDN with IOT has demonstrated the capacity, there are many gaps in the current literature. First, while several studies have proposed a hybrid model that combines NDN with an IOT system, there is a deficiency in comprehensive evaluations that examine the practical performance of these models in the real world, in a massive IOT environment (Ghodsi et al., 2014). The current research focuses primarily on theoretical models or small-scale simulations, leaving scalability and long-term performance of the NDN-based IOT system. Second, challenges related to cash management, such as cash stability and overhead to maintain up-to-date content in large networks, have not been fully addressed in the literature. Effective solutions for cash management, especially in dynamic IoT network, have a field of active research (Guo et al., 2016). Third, while NDN enhances security features, integrating these features into the IOT environment with limited resources and separating security requirements is still an open challenge (Zhang et al., 2014). Finally, more generalized solutions are required that can be applied in a wide range of IOT applications, as the current research often focuses on specific domains, limiting the widespread provision of NDN in IOT. The purpose of this letter is to address these intervals by proposing a hybrid IOT-NDN architecture that addresses the major challenges related to cash management, scalability, and safety, and by evaluating its performance in various IOT scenarios.

3 System Architecture and Design

3.1 Proposed Hybrid Architecture

The proposed hybrid IOT-NDN architecture integrates data networking (NDN) in traditional IOT systems to increase scalability, energy efficiency and data security. In this architecture, IOT devices act as data producers, which produce various forms such as sensor readings, images, or environmental information. These devices are assigned unique material names based on the type of data generated by them, which eliminates the need for managing IP address for each device. Data consumers, including a mobile device or cloud application, request data based on the content name rather than the device address, which improves flexibility in data recoveries. The major aspect of this architecture is caching, wherein intermediate routers are asked to store so that requests do not go through superfluous transmission activities, hence augmenting efficiency. The name-based routing mechanism adjudicates data recovery from a nearby cache, thereby reducing delay and conserving bandwidth. For security of data transmission, the architecture entails cryptographic procedures whereby data can be signed by the producer, thereby reinforcing the guarantee of authenticity and integrity. Scalable, efficient and secure are the traits that are meant to go into the architecture of the IoT system for sharing real-time data in an active large environment with least energy consumption.

3.2 Design Considerations

The need to integrate a named data networking (NDN) in the IOT system comes from the desire to solve the very important issues old IOT architectures are faced with, mainly scalability, energy efficiency, and dynamics. The scalability is a major problem with traditional IP-based IOT systems because it gets disabled very fast when managing and assigning IP addresses to millions of pieces of equipment. The NDN solves it by shifting routing from device-centric addressing to content-centric naming, which supports efficient routing without relying on the centralized management of IP addresses. This decentralized solution also promotes the scalability of the networks, especially in large and dynamic ones. Another important aspect is energy efficiency, where IOT devices often run on limited power sources. NDN-improved power efficiency comes with in-network caching, which allows the equipment to get the data from the nearby router instead of requesting it repeatedly from the data producer. This diminishes the energy needed for data transfer. Also, in many cases, IoT devices are set in mobile environments where the network topology mostly changes. Considering such scenarios, NDN is ideal because its name-based routing mechanism makes sure that the devices can access data even without the certainty of a particular network address. These build ideas put forward the NDN as a prospective solution in tackling the underlying limitations of traditional IoT networks.

3.3 Diagram: High-Level Architecture

The high-level architecture diagram of the proposed IOT-NDN hybrid system represents the flow of data from IOT devices to the data consumers via the in-network caching and name-based routing of NDN. The data manufacturer (IOT device) is responsible for generating and naming the data produced by them. These data manufacturers send data to the network with a fixed material name, eliminating the requirement of IP addresses and reducing the complexity of network management. Intermediate in-network routers serve a dual purpose: they often request data and passage requests based on material names instead of device addresses. This cashing mechanism data significantly reduces the load on IOT devices by enabling consumers to retrieve the content from the closest available cache, thus reducing delay and preserving bandwidth. Data consumers request data by referring to smartphones or cloud server content names. These consumers benefit from the time of low access as cashed data is recovered from the local router instead of relying on the original data manufacturer. This approach not only improves the performance of the IOT network but also increases its scalability and energy efficiency. The diagram highlights the simplicity and effectiveness of the proposed architecture, showing how data manufacturers, routers and consumers interact in a spontaneous, scalable and efficient way.

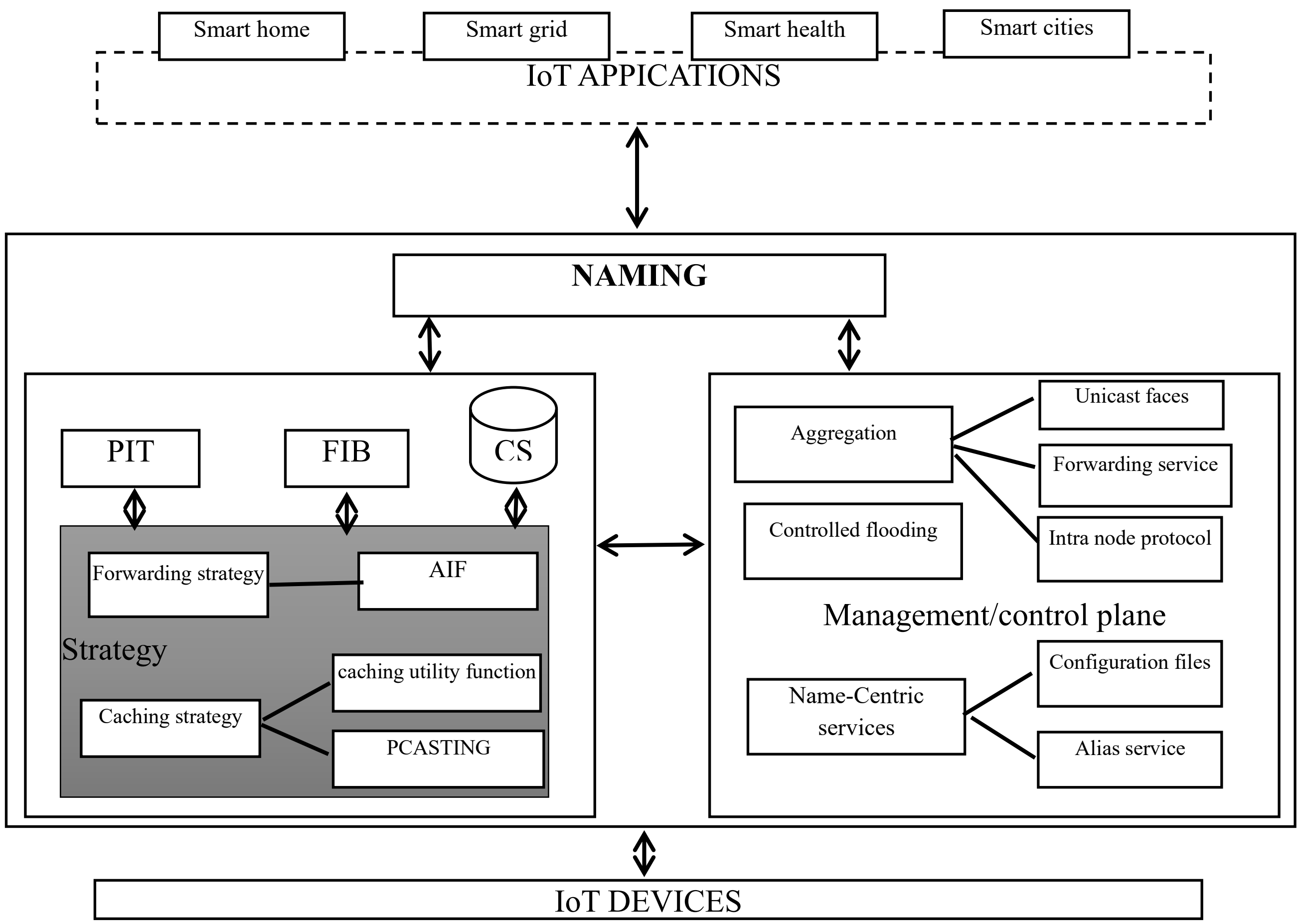

Figure 2: Functional Architecture of IoT-NDN Framework

Figure 2 shows the functional architecture of an IOT system integrated with designated data networking (NDN). At the top, various IOT applications (Smart Home, Grid, Health and Cities) rely on the underlying networks. The core layer is structured around the naming, allowing the data to be requested and rooted by the name. The left block has major NDN components such as pits, FIBs and CS along with strategies for forwarding and caching in the left block. The correct block represents management/control aircraft, handling aggregation, floods, unicast communications and configurations. At the bottom, the IOT device generates data while completing the loop. This architecture ensures scalability, flexibility and efficient data dissemination.

The mathematical formulation that models the functioning of the IoT-NDN architecture, covering naming, forwarding, caching, and control strategies, can be expressed in equations from (1) to (11)

Mathematical Formulation of IoT-NDN Framework

1. Naming Function

Let each data packet d_i from IoT devices be identified by a unique name:

$$N(d_i) = /< app >/< device >/< data\_type >/< timestamp > \quad (1)$$

where:

- $< app > \in$ {SmartHome,SmartGrid, ... }
- $< device >$ is the device ID
- $< data\_type >$ is the type of sensed data
- $< timestamp >$ provides time granularity

2. Pending Interest Table (PIT)

For each Interest packet $I(N)$, store:

$$PIT(N) = \{f_1, f_2, \dots, f_k\} \quad (2)$$

Where f_i is the interface (face) through which the Interest was received.

3. Forwarding Information Base (FIB)

Let:

$$FIB(N) = \{f_j \mid N \in prefix(FIB)\} \quad (3)$$

Select face(s) from FIB based on Forwarding Strategy Function F_s:

$$F_s(N) = \underset{f_j}{\operatorname{argmax}}\big(U(f_j, N)\big) \quad (4)$$

Where $U(f_j, N)$ is a utility or cost function (e.g., delay, congestion, success rate).

4. Content Store (CS) Caching Strategy

Let C be the cache size (in bytes) and CS $= \{D_1, D_2, \dots, D_n\}$ be the set of cached data.

When new data D arrives, decide to cache based on:

$$P_c(D) = CUF(D) \quad (5)$$

Where P_c is the probability of caching, and CUF = Caching Utility Function, which depends on popularity, freshness, size, etc.

Example:

$$CUF(D) = \alpha \cdot popularity(D) + \beta \cdot freshness(D) - \gamma \cdot size(D) \quad (6)$$

5. Aggregation and Flooding (Control Plane)

If multiple Interests request the same content N, aggregation ensures only one request is forwarded:

$$\text{Aggregated}(I_1, \ldots, I_k) = I(N) \quad (7)$$

Controlled flooding can be modeled with a flooding factor θ:

$$\text{Flood}(N) \rightarrow \text{Forward to } f_i \text{ if metric}(f_i) > \theta \quad (8)$$

6. Network Performance Metrics

- Cache Hit Ratio (CHR):

$$\text{CHR} = \frac{\text{Number of Interests served from CS}}{\text{Total Interests received}} \quad (9)$$

- Average Latency (L):

$$L = \frac{1}{|I|} \sum_{i=1}^{|I|} \text{Delay}\,(I_i) \quad (10)$$

- Packet Delivery Ratio (PDR):

$$\text{PDR} = \frac{\text{Number of Data Packets Received}}{\text{Number of Interest Packets Sent}} \quad (11)$$

Mathematical Model of IOT-NDN major operations of architecture, including naming, forwarding, caching, and control mechanisms. Each data packet is specifically identified using a hierarchical name, which enables name-based routing. The interest packets are tracked into the pending interest table (PIT), while the forwarding information base (FIB) directs the requests based on a utility-unique strategy. Content Store (CS) uses a cashing utility function to determine which data to store, which improves recovery efficiency. Control mechanisms such as aggregation and controlled floods reduce fruitless broadcasts. Delays, cash hit ratio, and packet delivery ratio, such as displays, help to evaluate scalability, speed, and efficiency of the metric system.

4 Methodology

4.1 Simulation Setup

The simulation environment was developed using NS-3 (Network Simulator 3) to evaluate the IOT-NDN hybrid architecture, a strong and widely used network simulator that supports a series of network protocols. NS-3 enables detailed modeling of network topology and is well suited to the evaluation of the system, including integration of data networking (NDN) with IOT systems. The simulation landscape consists of a network of IOT devices, such as sensors, cameras and actors, which generate data at regular intervals. These data manufacturers are associated with the in-network router that applies NDN's name-based routing and in-network caching capabilities. The simulation includes data consumers (eg, smartphones, cloud servers) that request data by referring to the content name instead of the device IP address. The network is configured to reflect a hybrid topology by combining both stars and Aries network designs, enabling scalability and flexibility in testing. Routers in network cash often request the data requested, which reduces delay and improves network performance. Safety facilities, such as data authentication and encryption, are also integrated in the system. This simulation setup allows a comprehensive analysis of how NDN-based architecture performs under different circumstances and network loads.

Table 1: Simulation Setup Parameters for IoT-NDN Hybrid Architecture

Parameter	Description
Network Topology	Hybrid (Mesh and Star topology)
Number of IoT Devices (Data Producers)	50-100 devices
Number of Data Consumers	20-30 devices
Routers	5-10 in-network routers
Device Placement	Random placement in mobile scenarios; fixed for static topologies
Transmission Range	100-150 meters for data producers and consumers
Routing Protocol	NDN (name-based routing, in-network caching)
Data Generation Rate	1-5 packets per second
Data Types	Sensor data (temperature, humidity, motion), status messages, images
Content Naming Scheme	Hierarchical naming
Interest Lifetime	4 seconds (adjustable)
Cache Size	1 MB per router (dynamic adjustment possible)
Cache Eviction Policy	LRU or LFU
Content Freshness Period	10 seconds for sensor data, longer for static data
Data Signatures	RSA or ECC for data authentication
Traffic Type	UDP-based data transmission
Traffic Pattern	Poisson or Constant Bit Rate (CBR)
Flow Direction	Bidirectional (from producers to consumers and feedback)
Packet Size	512 bytes (adjustable based on payload requirements)
Energy Consumption Parameters	10-50 mW during idle, 100-500 mW during transmission
Router Power Consumption	500 mW during idle, 1 W during transmission
Energy Model	Simple Energy Model, measuring energy consumption of devices and routers
Cryptographic Signature Algorithm	RSA or ECC for data signing
Encryption	AES-128 for encryption of sensitive data
Authentication	PKI for data integrity and authenticity
Simulation Time	1000-5000 seconds depending on network size and load
Warm-up Time	200 seconds for network stabilization
Propagation Loss Model	TwoRayGround or LogDistancePropagationModel
Error Model	RandomLossModel or BitErrorModel to simulate packet loss
Performance Metrics	Latency, Packet Delivery Ratio (PDR), Energy Consumption, Security Resilience

Table 1 outlines key simulation setup parameters for evaluating the IOT-NDN hybrid system. Parameters cover network topology, i.e., hybrid mesh/star topology; number of devices and routers in the network; and other fundamental building blocks such as in-network caching, name-based routing for efficient data transmission. Performance metrics include delay, packet delivery ratio, energy consumption, safety flexibility, energy model, traffic pattern, and cryptographic protocol for evaluating the system's overall efficiency and scalability.

4.2 Performance Metrics

Latency, packet distribution ratio (PDR), energy consumption, and safety flexibility are the sought KPI-based performance metrics assessed when determining the performance of the respective IOT-NDN hybrid systems. Latency is one of the parameters regarding the time taken for data to flow from a data manufacturer to a data consumer, such as the cloud or a mobile device. Delay is measured in milliseconds and is indicative of how quickly data can be recovered, brought into processing, and handled within a network. PDR gives the ratio of successfully delivered data packets into the total number of data packets sent across, showing the reliability and rate of data loss over a network. Energy consumption is particularly important in the case of IOT systems where devices work with less power supply. It is measured in terms of the electric power consumed by the IOT device and router to transmit and collect metric data. Lastly, safety flexibility assesses the system's capability to deal with data tampering, unauthorized access, and other safety threats. Particularly, these evaluate the effectiveness of the cryptographic signature used in the NDN to guarantee data authenticity and data integrity. These metrics are crucial in evaluating the overall effectiveness and efficiency of the IOT-NDN hybrid system.

4.3 Implementation Details

The generalized IOT design Internet architecture is composed of several main implementation stages aimed at increasing the scalability, efficiency, and safety of the integration into the designated data network (NDN). The first one is to apply material naming by specifying each piece of data generated by IOT devices and classifying them by such features as data types, device IDs, and timestamps. This material-based nomenclature scheme is essentially a main feature of NDN and serves to recover the data without using IP addresses. In-network caching was incorporated into the intermediate router to place copies of the most commonly requested data so that repeated broadcasts from IOT devices are less required. In this regard, the cache management mechanism ensures that the data is cached only if re-requesting can be done, thus saving from delay and bandwidth. Data consumers send requests based on content names, and the routers serve data from local cache when available. Safety features were integrated using a cryptographic signature, where data manufacturers sign their data to ensure that consumers can verify its authenticity before processing. In addition, data encryption was implemented for sensitive information to prevent unauthorized access during transmission. The NDN protocol was integrated into existing IoT protocols such as MQTT and COAP, allowing a hybrid architecture to work originally with the current IOT system

5 V. Results and Discussion

5.1 Simulation Result

Datasets used to evaluate the performance of IOT-NDN hybrid architecture include a variety of data sources to assess major matrix such as latency, packet delivery ratio (PDR), energy consumption and safety flexibility. IOT device data contains real-time data generated by 100 IOT devices, such as temperature sensors, humidity sensors, and motion detectors, producing data at the rate of 1-5 packets per second. This data is nominated by hierarchy and sent to the network for consumption. The network traffic dataset 20 simulates communication between consumers and IOT devices, where data requests and reactions are transmitted using the UDP-based NDN protocol. Energy consumption is tracked for both IOT devices and routers, which depicts the use of electricity during passive and transmission states, measured in joules (J). Security assessment datasets include landscapes where data is subjected to various attacks, such as data interception and unauthorized access, to assess the flexibility of the system. Finally, NDN simulation data is used to model material-based routing and in-network caching in the NS-3 environment. The dataset contains 5–10 in-network routers and simulation results for various data flow scenarios, which allow the comprehensive evaluation of the performance of the IOT-NDN system in real-world applications.

Table 2: Performance Metrics for IoT-NDN Hybrid System

S. No	Performance Metric	Value (Scenario 1)	Value (Scenario 2)	Value (Scenario 3)
1	**Latency (ms)**	120	140	110
2	**Packet Delivery Ratio (PDR) (%)**	98	95	99
3	**Energy Consumption (J)**	0.3	0.4	0.25
4	**Security Resilience (Pass Rate) (%)**	99	98	100

From Table 2, it is evident that the performance metrics for this IOT-NDN hybrid system were measured in three different scenarios. Some of the main metrics include delay (transmission time of data), packet delivery ratio (PDR) (network reliability), energy consumption (energy used by the IOT device), and security flexibility (resistance to unauthorized access and ability to prevent potential tampering of data).

The methods and formulas used to calculate the performance metrics in the table:

1. Latency (ms)

- **Definition**: Latency measures the time taken for data to travel from the data producer (IoT devices) to the data consumer (e.g., cloud or mobile devices).
- **Formula**:

$$\text{Latency} = \frac{\text{Time of Data Reception} - \text{Time of Data Transmission}}{\text{Total Data Packets}} \quad (12)$$

- **Units**: Milliseconds (ms)

2. Packet Delivery Ratio (PDR) (%)

- **Definition**: PDR measures the ratio of successfully delivered data packets to the total number of data packets sent, providing insights into network reliability and data loss.
- **Formula**:

$$\text{PDR}(\%) = \left(\frac{\text{Number of Successfully Delivered Packets}}{\text{Total Number of Sent Packets}}\right) \times 100 \quad (13)$$

- **Units**: Percentage (%)

3. Energy Consumption (J)

- **Definition**: Energy consumption measures the total energy used by IoT devices and routers to transmit and receive data.
- **Formula**:

$$\text{Energy Consumption (J)} = \text{Power Consumption (W)} \times \text{Time (s)} \quad (14)$$

- **Units**: Joules (J)
- **Note**: The power consumption is typically specified by the device, and the time is measured during active data transmission.

4. Security Resilience (Pass Rate) (%)

- **Definition**: Security resilience evaluates the system's ability to handle data tampering, unauthorized access, and other security threats. It measures the effectiveness of the cryptographic mechanisms used.

- **Formula**:

$$\text{Security Resilience}(\%) = \left(\frac{\text{Number of Successfully Verified Data Packets}}{\text{Total Number of Data Packets}}\right) \times 100 \qquad (15)$$

- **Units**: Percentage (%)

These formulas are used to calculate the key performance indicators (KPIs) for evaluating the IoT-NDN hybrid architecture, ensuring its efficiency, energy consumption, and security resilience.

5.2 Performance Analysis

The integration of the data networking (NDN) designated in the IOT system significantly improves performance, especially in the delay, packet distribution ratio (PDR), energy efficiency and safety flexibility. NDN's in-network cashing and content-based routing mechanisms reduce data recovery time by allowing consumers to access data from nearby caches, reducing the need for communication with distant devices. It leads to low delay and energy consumption, as a low transmission is required between equipment and network. However, challenges related to cash stability emerge, as the cache data can be chronic due to delayed updates, which can increase the recovery time. Addressing this issue requires the discovery of better cash eviction policies and efficient dynamic cash updates. While the cryptographic mechanisms in NDN enhance security, the management of a public-key infrastructure (PKI) in a large-scale IOT network remains complex and introduces overheads. Efficient key management solutions are essential, especially in a dynamic environment, and mild cryptographic protocols should be considered to optimize and adapt to scalability in the IOT network.

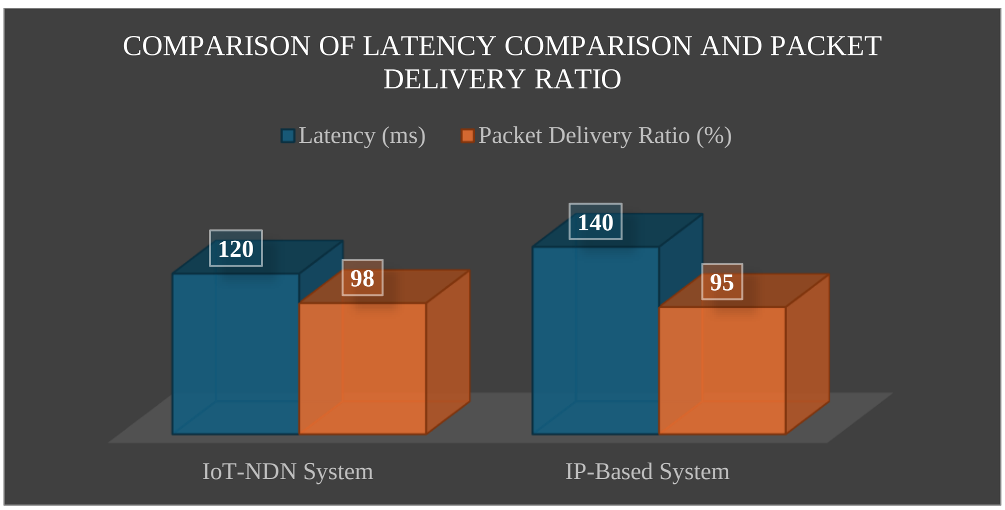

Figure 3: Comparison of Latency Comparison and Packet Delivery Ratio

Figure 3 evaluates the performance of a traditional IP-based system vs. IOT-NDN system in terms of delay and packet distribution ratio (PDR). The IOT-NDN system receives a lower delay of 120 ms in an IP-based system compared to 140 ms, indicating rapid data delivery. Additionally, it records high PDR of 98%, while the IP-based system receives only 95%, which shows more reliable data transmission. These results suggest that the IOT-NDN hybrid system significantly increases communication efficiency and reliability, making it more suitable for time-sensitive and data-intensive IOT applications than traditional IP-based networking.

The delay comparison in Figure 3 establishes that IOT-NDN encounters far less delay (120 ms) compared to IP-based systems (140 MS). It is the due to in-network caching and name-based routing, which shortens the recover time of data. Packet delivery ratio (PDR) was compared in Figure 2, where

IOT-NDN system is at advantage against IP-based systems, with a 98% versus 95% PDR. These high PDRs in IOT-NDN are due to efficient material-based routing and caching, thereby reducing loss and presenting more reliable data delivery in an IOT network.

6 Conclusion

A comprehensive evaluation of the in-stream network is offered in this letter for IoT-based Internet architecture. Results show that the IOT-NDN significantly improves system performance, mainly regarding delay, packet delivery ratio (PDR), energy, and security flexibility. NDN's in-network caching and content-based routing lessen data retrieval time, cause packet loss, and conserve energy by minimizing continuous transmission between IOT devices. Likewise, increased security is provided by NDN's cryptographic signature and content-based addressing, by which it is highly resistant to data tampering and unauthorized access. Therefore, these results show that NDN can resolve all major problems faced by the traditional IOT architecture and offer a road map towards a scalable and efficient solution. Adaptations regarding the NDN-IOT integration should be the focus of future research, especially considering the mobile IOT environment in view of cash stability and dynamic cache updates in the atmosphere. To allow for widespread acceptance, another issue that needs to be dealt with is scalability in a large-scale IOT network as the count of equipment is growing. Also, exploration into advanced security protocols to improve PKI management in the IOT-NDN system would help further improve performance and enhance safety during mass deployment. NDN can truly revolutionize IOT networking by introducing efficient, secure, and scalable communication models. As IOT grows, the ability to simplify NDN's network management and increase the efficiency of data delivery will absolutely be an essential pressure working toward the development of the Internet of Things.

References

[1] Agrab, A. S. (2022). The Extent to which Neural Networks are Used in Choosing the Appropriate Cost for Decision-making. *International Academic Journal of Economics*, *9*(1), 20–30.

[2] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., & Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine, 50*(7), 26-36. https://doi.org/10.1109/MCOM.2012.6253540

[3] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications magazine, 40*(8), 102-114.

[4] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[5] Babazade, K., Beigzadeh, Y., & Mahbobkhah, F. (2014). The Role of Collaborative Networks in Value Creation of Green Services in Cooperative Companies of Miandoab. *International Academic Journal of Accounting and Financial Management*, *1*(2), 96–114

[6] Bandyopadhyay, S., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49-69. https://doi.org/10.1007/s11277-010-0170-8

[7] Bastida, F., Garcia, E., & Garcia, S. (2021). A survey on integrating Named Data Networking into IoT: Opportunities and challenges. *IEEE Internet of Things Journal, 8*(3), 1841-1855. https://doi.org/10.1109/JIOT.2020.2974912

[8] Cao, H., Li, Z., & Chen, H. (2016). Data-centric networking for the Internet of Things: A survey. *Future Internet, 8*(4), 45-56. https://doi.org/10.3390/fi8040045

[9] Ghazanfari, M., Domirani, S., & Hamze, H. (2018). Human resources strategies approach in organizations with network model (supply chain model) “Case study: defense industries

organizations". *International Academic Journal of Organizational Behavior and Human Resource Management*, *5*(1), 63–83. https://doi.org/10.9756/IAJOBHRM/V5I1/1810004

[10] Ghodsi, M., Gani, A., & Buyya, R. (2014). Smart city IoT-based solutions: A survey. *Future Generation Computer Systems, 34,* 130-138. https://doi.org/10.1016/j.future.2013.08.003

[11] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[12] Guo, L., Dong, M., Ota, K., Wu, J., & Li, J. (2016, December). A name-based secure communication mechanism for smart grid employing wireless networks. In *2016 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICC.2016.7511301

[13] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009, December). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies* (pp. 1-12). https://doi.org/10.1145/1659049.1659052

[14] Kassim, N. M. (2017). Effect of Perceived Security and Perceived Privacy towards Trust and the Influence on Internet Banking Usage among Malaysians. *International Academic Journal of Social Sciences*, *4*(1), 120–130.

[15] Kaur, K., & Chandra, G. (2024). Demographic Data Gaps and the Challenges of Population Modeling in Low-resource Settings. *Progression Journal of Human Demography and Anthropology*, *2*(1), 13-16.

[16] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411. https://doi.org/10.1016/j.future.2017.11.022

[17] Kooshki, S. A., Zeinabadi, H., Jafarnezhad, A., & Kooshki, H. A. (2016). Applications of Fuzzy Logic and Artificial Neural Networks in Evaluation and Ranking of Teachers Based on "Framework for Teaching" Model. *International Academic Journal of Innovative Research*, *3*(1), 1–10.

[18] Kulkarni, P., & Jain, V. (2023). Smart Agroforestry: Leveraging IoT and AI for Climate-Resilient Agricultural Systems. *International Journal of SDG's Prospects and Breakthroughs*, *1*(1), 15-17.

[19] Luan, H., Zhang, Y., & Xu, J. (2015). Named data networking for the Internet of Things: A survey. *IEEE Access, 3,* 1013-1025. https://doi.org/10.1109/ACCESS.2015.2450477

[20] Rojas, C., & García, F. (2024). Optimizing Traffic Flow in Smart Cities: A Simulation-based Approach Using IoT and AI Integration. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(1), 19-22.

[21] Sadegh, F. N. (2016). The Impact of Social Networks on Various Aspects of Life. *International Academic Journal of Humanities*, *3*(1), 26–31.

[22] Sardiana, I. W., & Pramudito, E. (2018). Named Data Networking for IoT: A case study in healthcare systems. *Journal of Computer Science and Technology, 33*(2), 301-314. https://doi.org/10.1007/s11390-018-1830-4

[23] Verma, A., & Mehta, N. (2024). The Role of IoT in Modern Electrical Systems: An Interdisciplinary Approach in the Periodic Series. In *Smart Grid Integration* (pp. 13-18). Periodic Series in Multidisciplinary Studies.

[24] Zanella, A., Bui, N., Castellani, A., Vangelista, M., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328

[25] Zhang, L., Yang, X., & Li, W. (2014). Named data networking for the Internet of Things: Challenges and opportunities. *International Journal of Communication Systems, 27*(12), 3496-3507. https://doi.org/10.1002/dac.2744

Authors Biography

Dr. Anusha Sreeram is a Faculty Member in the area of Operations and Information Technology at ICFAI Business School (IBS), The ICFAI Foundation for Higher Education (IFHE), Hyderabad, India — a Deemed-to-be University under Section 3 of the UGC Act, 1956. Her research interests include operations management, supply chain analytics, information systems, and data-driven decision-making. She has published several research papers in reputed international journals and conferences and is actively engaged in teaching, research, and consulting in the domains of operations and IT management.

Shubhashish Goswami is associated with the School of Engineering & Computing at Dev Bhoomi Uttarakhand University, Dehradun, India. His research interests include artificial intelligence, machine learning, data science, and software engineering. He has published research papers in reputed international journals and conferences and is actively involved in fostering innovation, academic excellence, and technological advancement in the field of computer science and engineering.

Madhur Taneja is associated with the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. His research interests include research analytics, innovation management, impact assessment, and data-driven evaluation of academic performance. He is actively involved in enhancing institutional research quality, promoting evidence-based research practices, and contributing to the development of strategies that improve academic and societal research outcomes.

Dr. Praveen Priyaranjan Nayak is an Associate Professor in the Department of Electronics and Communication Engineering at Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. His research interests include signal processing, wireless communication, embedded systems, and Internet of Things (IoT). He has published several research papers in reputed international journals and conferences and is actively involved in guiding research scholars and promoting innovation in the field of electronics and communication engineering.

Dr.T. Lalitha is a Professor in the Department of Computer Science Engineering at Presidency University, Bengaluru, Karnataka, India. Her research interests include artificial intelligence, machine learning, data science, and cloud computing. She has published numerous research papers in reputed international journals and conferences and is actively engaged in mentoring research scholars and promoting innovation and excellence in computer science education and research.

Dr. Chunduri Madhurya is an Assistant Professor in the Department of Computer Science and Engineering at Vardhaman College of Engineering, Hyderabad, Telangana, India. Her research interests include artificial intelligence, machine learning, data mining, and cloud computing. She has published several research papers in reputed international journals and conferences and is actively engaged in guiding students and contributing to advancements in computer science education and research.

N. Raghu is an Associate Professor in the Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Ramanagara District, Karnataka, India. His research interests include power systems, renewable energy technologies, control systems, and electrical machines. He has published several research papers in reputed international journals and conferences and is actively engaged in promoting innovation, research, and academic excellence in the field of electrical and electronics engineering.