TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 2, 2025

Received: 15.11.2024
Revised: 13.03.2025
Accepted: 30.04.2025

UDC 004.056:004.738.5

DOI: 10.30857/2786-5371.2025.2.6

Analysis of the key models, methods, and means of data collection in the Internet of Things

Maksym Savka*

Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-2049-9438

Abstract. The rapid development of mobile technologies and the technological revolution are contributing to the active implementation of the Internet of Things, leading to an increase in the number of physical devices connected to the Internet. However, along with the advantages of the Internet of Things, there are also growing disadvantages, including cyber threats, privacy violations, and risks of unauthorised data collection. In this regard, research into the challenges and security measures in the field of the Internet of Things is necessary to ensure the safe implementation of these technologies. The purpose of the present study was to analyse key models, methods, and tools for data collection in the Internet of Things environment. The methodological framework of this study included a systematic approach, which allowed presenting public policy in the field of the Internet of Things as a complex, structurally organised system that requires improvement and development. The study employed general scientific and specific methods (systemic, abstraction and comparison, formalisation, institutional analysis, historical-genetic, logical-semantic, classification, generalisation, analysis, formalisation, and comparison), as well as statistical data, which was used extensively and consistently. The study found that among the existing data collection technologies, sensor networks and cloud computing are the most widely used, but they do not cover all the requirements of mobile Internet of Things systems, specifically in terms of energy efficiency, throughput, and security. It was found that modern architectural solutions (including social architectures of the Internet of Things) allow scaling the system and connecting various devices, but have limitations related to deployment complexity and bandwidth. The study also found that the major security threats arise at all levels of mobile Internet of Things networks, from devices to cloud infrastructure, confirming the need for a comprehensive approach to their protection. It was shown that most existing solutions do not simultaneously meet the requirements for low power consumption, speed of data collection and processing in networks with dynamic topology, as well as the requirements for reliability and confidentiality. The proposed developments complemented existing methods, enhancing the flexibility and resilience of the data collection process and laying the foundation for the development of new energy-efficient and secure tools in the Internet of Things

Keywords: cloud computing; IoT architecture; data security; CoAP protocol; fog computing

Introduction

Changes in network structure complicate the determination of the level of trust between devices. The primary reason for this situation is the complex structure of the network. Mobility forces devices to consume more energy, but their resources stay unchanged, and therefore data collection in dynamic Internet of Things (IoT) networks with complex structures becomes a pressing issue. Data encryption increases the overhead costs of data transmission, which contributes to increased network traffic, higher network energy consumption, and a shorter network lifetime. Therefore, fresh solutions are necessary to ensure that the basic requirements of the Internet of Things are met when collecting data from mobile device networks. The complexity of data collection tasks in the Internet of Things is increasing considerably due to the transition from the use of simple static IoT devices to the use of a wide range of smart mobile devices, such as mobile phones, smart watches, smart vehicles, and mobile devices in smart

Suggested Citation:
Savka, M. (2025). Analysis of the key models, methods, and means of data collection in the Internet of Things. *Technologies and Engineering,* 26(2), 66-78. doi: 10.30857/2786-5371.2025.2.6.

*Corresponding author

cities. Modern mobile device networks are heterogeneous networks with complex dynamic structures. Data collection in such networks poses new challenges, such as new opportunities for attacks (Mishra & Pandya, 2021).

W.E.H. Youssef *et al*. (2023) addressed the problem of secure data transmission between end devices and servers in the Internet of Things using cryptographic mechanisms. The essence of their study was to present a novel approach to solving IoT security problems by introducing a secure lightweight cryptosystem based on Chaos. The findings of the study confirmed the effectiveness of the approach in terms of computational complexity, memory requirements, and energy consumption. The researchers noted that after reviewing and comparing their findings with the existing reports, the advantage of their cryptosystem became evident. Modelling results and performance analysis revealed that the proposed secure chaos-based lightweight cryptosystem (SCBLC) can be considered an ideal choice for protecting communications in resource-constrained IoT devices, taking major steps towards improving IoT network security. However, some drawbacks included increased computational overhead on IoT devices caused by their complexity, the need for reliable key management protocols, and the probability of susceptibility to advanced cryptanalytic attacks. The problems of data collection and transmission delays and high energy consumption have been solved with the ESR (energy-efficient and secure routing protocol); the ESR protocol for the Internet of Things was developed by K. Haseeb *et al*. (2019). As the researchers noted, experimental findings using a network simulator demonstrated that the proposed routing protocol achieved a 37% improvement in network lifetime, a 24% improvement in average end-to-end delay, a 30% improvement in packet delivery rate, average communication cost by 29%, network overhead by 28%, and route reopening frequency by 38% compared to existing work in dynamic network topologies. The proposed protocol created various energy-efficient clusters based on the intrinsic qualities of nodes. Based on the (k,n) threshold scheme of Shamir's secret sharing, reliability and security of sensor information between the base station (BS) and the cluster head were achieved. The proposed security scheme provided an easy solution to combat intrusions created by malicious nodes. This protocol can reduce energy consumption and data transmission delays. Notably, this only provided data protection from nodes to the cluster head and further to the base station from malicious threats. This protocol was not extended to factor in the network communication with multiple hops. These studies did not fully address the issue of data transmission security along with energy efficiency in highly resource-constrained environments.

The basic concept of the Internet of Things envisages the ubiquity of objects (things, devices) that can interact to achieve shared goals using wireless and wired connections and unique addressing schemes. Internet of Things networks generate multiple data streams, each with its unique characteristics (Khare & Totaro, 2019). D. Honcharenko *et al*. (2023) offered a detailed analysis of modern approaches to building an information system for monitoring physical indicators based on Internet of Things technologies, with a particular focus on the selection of network solutions and IoT platforms according to performance and energy efficiency requirements. Thus, there is currently no solution that guarantees the simultaneous fulfilment of the three basic requirements of the Internet of Things: security of data collection and transmission, low network response time, and minimal energy consumption. Therefore, the purpose of the present study was to comprehensively compare models, methods, and protocols for data collection in mobile IoT systems in terms of energy efficiency, delays, and security.

Materials and Methods

The study employed a comprehensive scientific and methodological approach combining systematic analysis, comparison and classification methods, as well as the use of relevant statistical data and literary sources. To obtain objective and comprehensive findings, each stage of the study was conducted sequentially, ensuring verifiability and reproducibility. The first step was to select scientific publications, monographs, conference materials, and official documents (international standards, recommendations, patents) on the topic of the Internet of Things (IoT). The focus was on recent studies reflecting the current state of technology in the field of mobile IoT systems, the specific features of social IoT solution architectures, as well as various data collection methods.

The study analysed open statistical materials (specifically, reports of analytical agencies, data available on the websites of international organisations), covering indicators of IoT solution implementation, data transfer volumes, the dynamics of the mobile device market, and cyberattack risk assessments. The study was conducted considering the multi-level structure of IoT systems (devices, network, cloud infrastructure), as well as the factors affecting the security and efficiency of data collection at each level. The use of a systematic approach helped to identify internal and external interrelationships between components of IoT architectures.

Abstraction and comparison methods were employed to identify key parameters and characteristics of data collection models and methods, which allowed generalising and systematising the information obtained from various sources. The descriptions of existing data collection technologies were formalised to simplify further analysis and comparison of technical characteristics (throughput, response time, energy consumption, scalability, etc.). Within the framework of the classification, analysis, and generalisation methods based on the collected data, existing technical solutions were systematised and structured according to their architecture type and technological features, and their relevance for mobile IoT systems was determined.

At the stage of sampling and initial analysis, a search, selection, and analysis of scientific papers and statistical

materials on the topic was performed. The results were systematised in a database according to key parameters (year of publication, description of technologies, areas of application, security features). The study determined the criteria for evaluating the effectiveness and security of data collection (e.g., energy consumption, performance, security complexity, scalability). Based on general scientific methods of comparison and classification, several groups of technological solutions were formed (e.g., sensor networks, cloud and fog computing, social IoT architectures), and their features and possible areas for development were identified. Particular attention was paid to the study of threats at various levels of the IoT: from devices to central (cloud) infrastructure, as well as protection mechanisms that can be applied during data collection.

Data analysis was performed using publicly available software (Microsoft Excel) and specialised libraries for processing, visualising, and comparing the technical characteristics of solutions. To assess security and performance indicators, the results of experimental studies with network load modelling and review tests of security tools described in scientific literature were used. The study only considered solutions with up-to-date technical documentation and fairly widespread practical application. Highly specialised products or protocols with limited scope or at an early stage of development were not considered. It was also assumed that the conditions for integrating IoT solutions into mobile networks may vary depending on the concrete region and regulatory environment, yet the general technological approaches, data collection and processing methods were still comparable on a global scale. Overall, this approach and set of methods allowed covering a variety of data collection models and analysing their compliance with the requirements of mobile IoT systems in terms of energy consumption, throughput, security, and adaptability to dynamic environments. This allowed identifying the advantages and disadvantages of various solutions and helped to formulate proposals for their improvement.

Results and Discussion

General architecture of the Internet of Things

Based on a review of the literature on Internet of Things (IoT) system architectures, the study found that IoT system architecture consists of three layers (Fig. 1): physical, network, and applied (application or service layer). The applied layer includes services such as smart grids and smart transport services. IoT devices collect data about events occurring in the physical environment. This data is sent to the network layer; the primary task of the IoT network layer is to process the collected data. Wired or wireless networks are used to transfer data to higher levels: LAN (local area network), WAN (wide area network), Wi-Fi (wireless fidelity), LTE (long-term evolution), 3G (3rd Generation). Various network technologies can be used for data transfer, including Bluetooth and ZigBee.

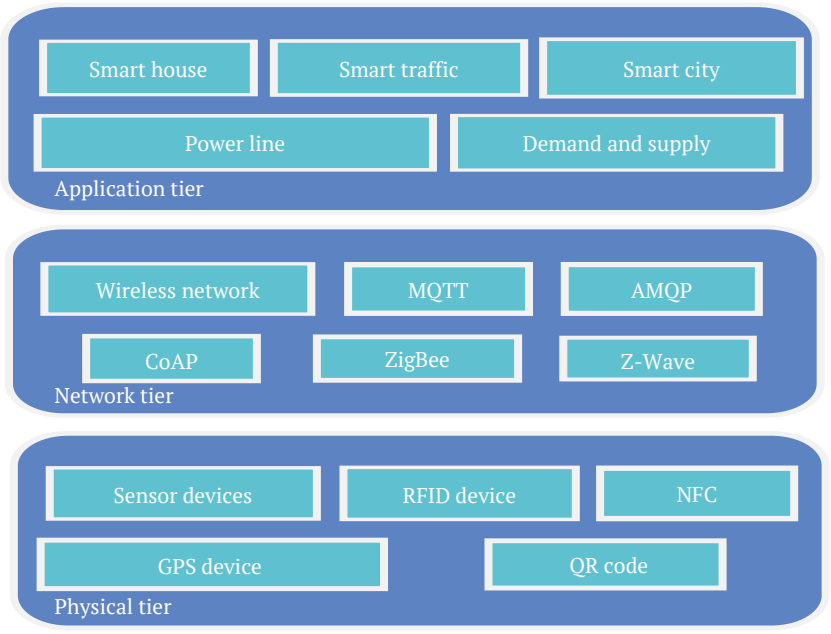

Figure 1. *Schematic representation of the three-tier architecture of the Internet of Things system*
Source: *developed by the author of this study based on the experimental research results*

The three-tier architecture ensures direct interaction between the device and the application layer. No intermediate nodes are required to convert or interpret data; building a system with a three-tier architecture allows using the existing equipment to create a unified Internet of Things infrastructure that collects and transmits data from end devices to applications. The advantage of this is that services are independent of each other and of the

physical hardware. Abstraction of the physical tier facilitates access to network resources from the application tier (Chanal & Kakkasageri, 2020).

Architecture of IoT systems with middleware platforms (Fig. 2). Middleware platform technology in IoT systems emerged in parallel with the concept of cloud computing. Middleware platforms enable the integration of many systems with different functionalities on their own basis. The platform ensures requirements such as enhanced data security and resource sharing. Middleware platforms are designed to provide access to data collected about environmental objects and their interactions anytime, anywhere, and from any device. Middleware platforms provide services to software applications hosted in the cloud. The platform can be built to create an infrastructure for running applications and use general tools for programming physical devices (Waheed *et al.*, 2024).

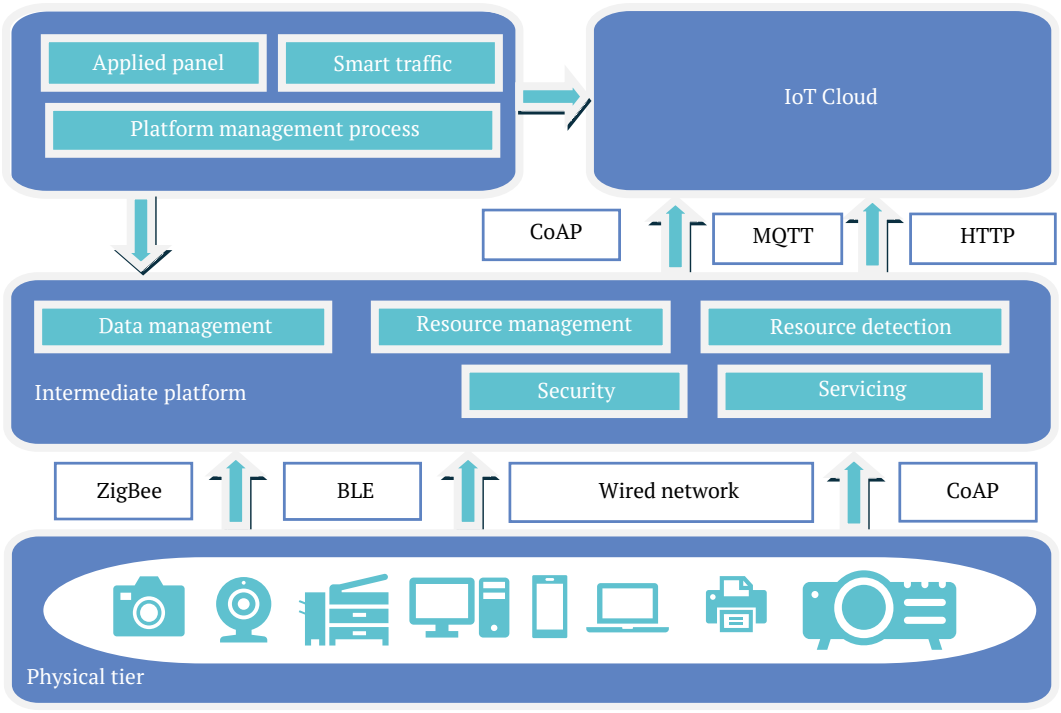

***Figure 2**. Architecture of IP systems with an intermediate software platform*
***Source:** developed by the author of this study based on the experimental research results*

In a conventional three-tier architecture, data processing and support tiers, also known as the interface tier or middleware tier, are created and used. In this architecture, the data processing tier is located between the applied and network tiers. The primary tasks of this tier are to receive user requests, collect the data necessary to fulfil them, and provide responses. Various services must be used to process requests. Therewith, the necessary level of security must be ensured when collecting and transmitting data. Cloud computing architectures focus on the distributed processing of raw data collected from a device. Various data analysis methods, including machine learning methods, can be used for processing. It may be necessary to process query history, information about previous actions of mobile devices, and connections between devices, or to process operational data in real time.

Data processing in cloud nodes extends the processing capabilities offered by cloud services. Processing is performed in close proximity to the data source. System performance is improved by reducing the amount of data transferred to the cloud for processing, analysis, and long-term storage. Cloud computing is currently the most popular option because it allows protecting and managing data in an IP environment and building systems with sufficiently high performance. The study (Ivanov *et al.*, 2023) proposed an architectural model for IP that included the use of cloud computing and described existing standards for the collection, processing, and transmission of data from mobile devices. IoT environments are based on the collection, storage, and processing of data. IoT devices such as sensors, RFID tags, and Bluetooth devices generate massive amounts of data that is transferred to cloud environments for storage and processing, which users can subsequently access. These standards form the basis for the interconnection of the Internet of Things and Big Data. The problematic of the cited study was the increasing complexity of processing and analysing the collected data. As conclusions, further research was proposed to develop new methods for collecting and processing data from IoT devices in the context of Big Data, especially in the area of developing effective algorithms for optimising the processing of large amounts of data. S. Kasiviswanathan *et al.* (2024) enabled the validation of IoT system deployments by providing dynamic deployment of distributed IP applications,

computing infrastructure management, and automation of visualisation systems.

S. Supreeth & K. Patil (2022) proposed an approach (VMS-EDMVM) to distributed virtual machine management in a cloud computing environment focused on real-time data processing. This method uses only cloud data centre resources and does not consider intermediate (edge/fog) nodes, focusing on dynamic migration and scaling of virtual machines to ensure continuity and efficient resource utilisation. Y. Huang *et al*. (2024) proposed a cloud-based model called E-norm. This model provides centralised management of applications and nodes. Proximity to the end user is factored in when distributing workloads between nodes. Furthermore, an automatic scaling mechanism is implemented to adjust resource allocation according to network delays and task execution times.

U. Khadam *et al.* (2024) proposed a cloud computing-based data aggregation model. This model performs two-dimensional data aggregation, which reduces data transmission costs and increases network throughput. V.K. Prasad *et al.* (2023) proposed using a cloud computing layer to minimise server resource consumption and determine the resources required for data collection and processing. M. Peyman *et al*. (2021) proposed an IoT solution for data collection and analysis focused on the efficient use of cloud resources and optimisation of energy consumption. The model involves step-by-step processing: initial signal processing is performed directly at the nodes, while deeper analysis and long-term storage are performed in the cloud. The researchers pointed out that this approach reduced the load on the local infrastructure and improved the scalability of the system as the number of sensors increased.

Cloud computing provides virtually unlimited scalable processing and storage resources. However, routing data to remote data-centres typically increases the round-trip time (RTT) for mobile and IoT devices. For latency-sensitive workloads ($\leqslant$ 50 ms), architects therefore employ edge- or fog-computing approaches, which shift computation closer to the data source and, in practice, lower end-to-end latency by a factor of 2-4. Such responsiveness is essential, for instance, when developing software for autonomous vehicles. Thus, the edge (fog) computing tier acts as an intermediate layer between the device tier and the centralised cloud, optimising data processing and storage while improving the quality of service delivered to end users.

Registration of new social objects, creation of new device groups, determination of "social connections" between devices, management of established connections. A socially oriented approach to defining IP networks allows extending the conventional IP model by adding social elements. Social IP architecture was developed as part of Software as a Service (SaaS), which offers heterogeneous sensor data. This service ensured data compatibility and reusability. As presented in Figure 3, the architecture of a social IS system includes a physical tier, a network tier, and an application software tier. The physical and network tier allow collecting data from devices using various data transmission networks.

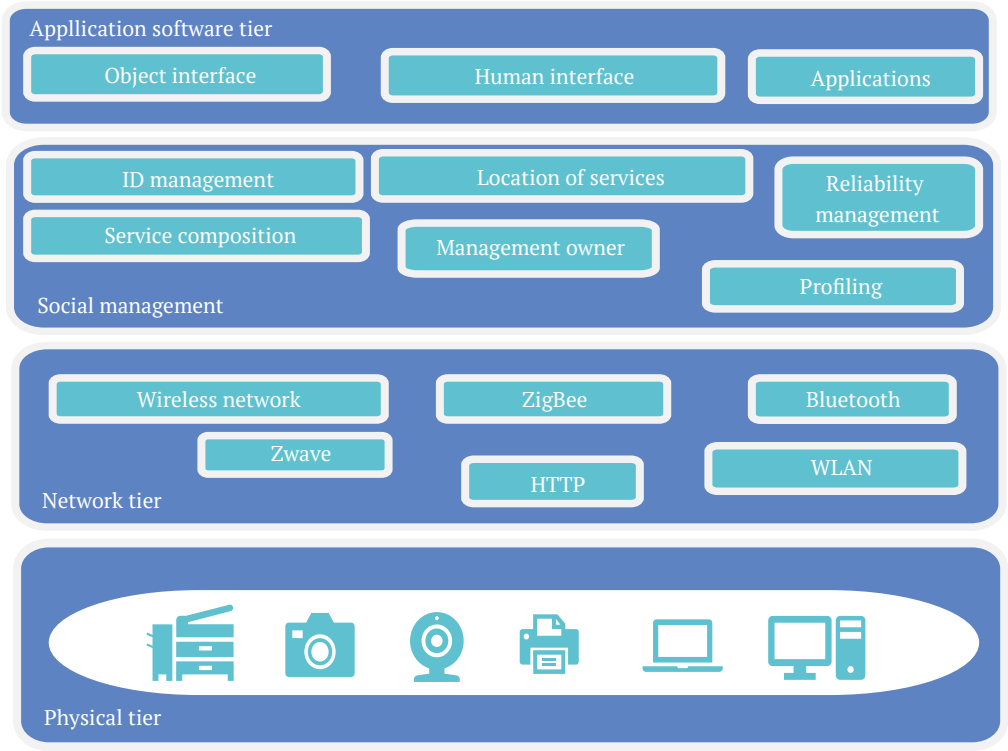

***Figure 3**. Architecture of social IP systems*

***Source:** developed by the author of this study based on the experimental research results*

At the application level, IP applications are deployed together with services, the functionality of which is enabled by social connections between objects. Such services form an independent sub-tier of the application tier. These include identity management services for identifying objects, profiling services for semi-automatic collection of data about objects, and management services for determining the actions that objects can perform. The relationship management service is one of the basic services for establishing relationships between objects. Reliability management services are used to create a database of reliable objects based on the analysis of object behaviour. The reliability management service is closely related to the relationship management service.

Communication technologies and data transfer protocols in IoT

Communication technologies for data collection in IoT define the rules for transmitting digital messages, including packet size parameters, data transfer rates, synchronisation methods, types of possible errors, address mapping methods, as well as rules for packet delivery control and data flow management. In Internet of Things systems, data is transmitted using various protocols.

Bluetooth LE (Low Energy), Wi-Fi, ZigBee, and LoRaWAN (Long Range Wide Area Network) are used for device-to-device communication at the channel level. At the application level, DDS (Data Distribution Service), MQTT (Message Queue Telemetry Transport), HTTP (Hypertext Transfer Protocol), CoAP (Constrained Application Protocol), and XMPP (Extensible Messaging and Presence Protocol) protocols are used to transfer data from devices to servers, while AMQP (Advanced Message Queuing Protocol) is used to transfer data from servers. The Data Distribution Service (DDS) architecture has two tiers of information transfer to the destination and an additional tier of data flow management. It is an open standard that defines the mechanism for transferring information in a publish-subscribe paradigm. Unlike the conventional client-server model, DDS is focused on distributed, decentralised interaction between nodes, where data is published and consumed by various applications without the need for a central broker or server for routing (Internal documentation…, n.d.). The key advantage is decentralisation, which eliminates a single point of failure, as DDS does not require a central broker. Data is published and received directly between nodes. The disadvantages of DDS include the complexity of configuration and compatibility issues between implementations from different vendors.

The MQTT (Message Queuing Telemetry Transport) protocol is designed to collect data from devices and send it to a server (MQTT version 5.0, n.d.). This protocol can collect data from different devices and works on top of the Transmission Control Protocol (TCP) to ensure reliable data transfer and prevent data loss. The key disadvantage of this protocol is that it is not suitable for devices with limited resources. The CoAP (Constrained Application Protocol) protocol is analogous to the HTTP (Hypertext Transfer Protocol) protocol. However, HTTP has greater computational complexity, lower data transfer rates, and higher energy consumption than CoAP. CoAP was developed as a special data transfer protocol for web networks. CoAP offers the possibility of use by nodes with limited resources (Shelby *et al*., 2014). Although HTTP is versatile, it has higher overhead and longer connection establishment times compared to lightweight IoT protocols such as CoAP. It provides independence and scalability of network components; HTTP is a suitable option for organising interaction between nodes in a local network. AMQP (Advanced Message Queuing Protocol). This protocol is designed to organise interaction between servers. AMQP is implemented by two key components. The data exchange component routes messages and stores them in a queue. The message queue is used to store messages until they are sent to their destination; the second component, the TCP protocol, is used by providers to interact with subscribers and provides a reliable point-to-point connection.

The study considered the most widespread applied-tier protocols. Table 1 presents a comparative overview of key characteristics and communication approaches (client-server or publisher-subscriber architecture), allowing their suitability for various data collection and processing scenarios to be assessed. DDS provides decentralised interaction without a broker, while MQTT, AMQP, and XMPP are based on the presence of a server or broker. HTTP and CoAP offer a client-server (request-response) model, but CoAP is designed for substantially limited devices and typically runs on top of UDP (User Datagram Protocol), providing lower bandwidth costs.

Table 1. *Comparative review of applied-tier protocols*

Protocol	Interaction model	Transport	Advantages	Disadvantages
DDS	Decentralised “pub-sub”	UDP/TCP (RTPS)	No single point of failure. Rich set of QoS. Real-time support.	Complexity of configuration. Different versions may be incompatible.
MQTT	Broker-oriented “pub-sub”	TCP	Ease of implementation. Widespread popularity in IoT.	Not sufficiently optimised for devices with ultra-low resources. Requires a broker.
CoAP	Lightweight client-server model (REST)	UDP (often)	Low overhead costs. Optimised for limited resources.	Fewer delivery guarantees. Some security features require additional extensions.

Table 1. Continued

Protocol	Interaction model	Transport	Advantages	Disadvantages
HTTP	"Client-server" (request-response)	TCP	Universal web standard. Easy to integrate.	Relatively high load.
AMQP	"Pub-sub", queues, advanced routing	TCP	Powerful shift model. Flexible route settings.	Complex protocol. Requires more resources. More frequently used at the server-to-server level.

Source: *developed by the author of this study based on the experimental research results*

The information in the table about DDS, MQTT, CoAP, HTTP, and AMQP protocols reflects various approaches to organising the application tier of interaction in IoT systems and distributed environments. DDS is characterised by a decentralised pub-sub model, which avoids a single point of failure and ensures real-time operation thanks to flexible QoS mechanisms. MQTT, on the other hand, relies on a broker-oriented pub-sub scheme, where all messages pass through a central broker. This greatly simplifies implementation and administration but can create a single point of failure.

CoAP represents a client-server architecture adapted for resource-constrained environments. CoAP operates primarily over UDP, using acknowledged and unacknowledged messages, which reduces network overhead. HTTP, compared to CoAP, is more versatile and understandable, but has high overhead due to TCP connections and a more complex transmission scheme, which can be critical for microcontroller devices with minimal computing resources. AMQP is mostly used in enterprise systems that require advanced routing and queuing mechanisms. It supports both the pub-sub model and queuing but requires more resources and is typically not used directly on low-power devices, but rather on servers. AMQP is often chosen for systems where finely tuned message distribution is critical.

The choice between DDS, MQTT, CoAP, HTTP, or AMQP depends on several key factors: performance requirements, reliability level, available network resources, and security and scalability needs. DDS is best suited for real-time industrial applications, MQTT is a versatile solution for most IoT scenarios, while CoAP is an option for resource-constrained sensor networks. HTTP is the basic protocol for web-oriented applications, but it is somewhat excessive in resource-constrained environments. AMQP is the best solution when detailed routing and queue management are required.

Internet of Things data exchange and collection technologies

The technology for exchanging information between machines on the Internet of Things is called 'M2M' (Machine to Machine). It allows devices such as mobile phones to send and receive data via cellular networks. Satellites are mostly used for communication in industrial environments where small amounts of data must be transmitted. The Wi-Fi protocol is used to provide Internet access to devices within the coverage area of a wireless network. Wi-Fi is widely used in Internet of Things systems. The use of Wi-Fi offers advantages such as security, integrity, flexibility, and scalability in data transmission, and this connection is based on the use of IP (Internet Protocol) protocols (Farhan *et al*., 2021).

Bluetooth technology allows transferring data between two or more devices in close proximity to each other in conditions that do not require high network bandwidth. It also provides service discovery and configuration to regulate the interaction between devices. Bluetooth provides network addresses and sets permissions for data access. Secure data transmission is guaranteed by the Bluetooth protocol. Radio frequency communication is one of the simplest forms of communication between devices; both ZigBee and ZWave use low-power radio frequency receivers embedded in electronic devices and systems. In the Internet of Things, these technologies offer considerable advantages such as low power consumption, high security, and network scalability.

RFID technology uses electromagnetic fields to identify objects. In this case, a device is installed that reads the data stored in an RFID tag, which can be used for many applications. NFC (near field communication) technology uses magnetic field induction for communication, where two frame antennas are placed in a magnetic field close to each other, effectively forming an air-core transformer. The key disadvantage of this technology is the relatively low security of data transmission and the possibility of unauthorised connections (Onumadu & Abroshan, 2024). Below is a comparative analysis of the key wireless technologies and protocols used in the Internet of Things, including Wi-Fi, Bluetooth, ZigBee, LoRaWAN, RFID, NFC, etc. (Table 2).

Table 2*. Comparison table of wireless technologies for IoT*

Technology	Operating range/radius	Throughput	Area of application	Key benefits	Key disadvantages
M2M	Variable (satellite, cellular).	Depends on the operator (2G/3G/4G/5G, etc.).	Industrial systems, remote monitoring.	Global coverage. Autonomous data exchange.	Cost depends on tariffs. Often requires licensed bands.

Table 2. Continued

Technology	Operating range/radius	Throughput	Area of application	Key benefits	Key disadvantages
Wi-Fi	~30-100 m (depending on standard and obstacles).	High (tens to hundreds of Mbps).	Home/office IoT systems, smart homes, video surveillance.	High speed. Widespread infrastructure.	Relatively high energy consumption. Shorter range compared to some LPWANs.
Bluetooth	~1-100 m (depending on class and version).	Low/medium (< 24 Mbps for Bluetooth 5).	Wearable devices, personal gadgets, audio devices.	Low power consumption (especially BLE). Easy connectivity.	Limited range. Only suitable for local applications.
ZigBee / Z-Wave	~10-100 m (mesh-network).	Low (up to ~250 Kbps for ZigBee).	Smart homes, industrial sensor networks, lighting.	Low energy consumption. Mesh topology (self-organising nodes).	Low bandwidth. Requires a gateway to connect to the Internet.
LoRaWAN	Up to 2-5 km in urban conditions; up to 15 km in rural areas.	Very low (0.3-50 Kbps).	Distributed sensor networks, smart meters, agriculture.	Very low power consumption. Wide coverage area. Operates in the free frequency band (ISM).	Low transmission speed. Not suitable for large amounts of data. Dependence on the density of base stations.
RFID	Several centimetres to several metres.	Very low (only identification data).	Logistics, access control, inventory.	Affordable tags. Passive operation (no battery required).	Very short distance. Small amount of data stored.
NFC	Up to ~10 cm	Very low (identification data).	Contactless payments, fast identification.	Easy interaction with smartphones. Quick device pairing.	Extremely short distance. Potential vulnerability (possibility of unauthorised connections).
Satellite communications	Global (orbit coverage).	Low/medium.	Remote industrial facilities, transport, sea vessels.	Large coverage area. Access to hard-to-reach regions.	High cost. Signal delays. Low speed compared to terrestrial networks.

Source: *developed by the author of this study based on the experimental research results*

The study examined Internet of Things data collection technologies, including cloud computing and middleware technologies. Cloud computing is a web technology that provides end-user applications with access to distributed computing resources. It ensures data storage and processing capabilities, enabling access to resources as a local service. As a result, computing resources, data storage, and other services are located between the user's device and the cloud server. A prominent advantage is that cloud computing nodes are closer to the end user, which substantially reduces data transfer delays. Furthermore, the spatial distribution of resources allows using these technologies effectively in mobile device networks.

Another significant technology is middleware platforms, which act as an interface between the hardware and application levels. They enable interaction with devices, manage information, and provide a unified model for working with various devices. Such platforms also help solve the problem of device distribution that arises when end users access them. Many sensors, which form an integral part of smart objects, are widely used to collect data in Internet of Things applications. They are affordable, consume minimal energy, and are characterised by battery capacity and ease of deployment. Since data collection, transmission, and storage require a strong level of security, encryption methods play a critical role. Their key purpose is to prevent unauthorised monitoring, access, misuse, and modification of information. At the same time, conventional cryptographic algorithms are not always suitable for resource-constrained devices. For this purpose, lightweight encryption methods are used, which enable data protection even on devices with low computing power (He *et al.*, 2024).

Apart from encryption, social network analysis methods are an effective tool for analysing information in the Internet of Things. They allow establishing connections between objects based on human interactions in the digital environment. These "social connections" can be used to search for and collect data on the Internet. A major challenge in the Internet of Things is the transmission of massive data flows. In this context, routing methods play a vital role, ensuring the secure and efficient transport of large amounts of information from devices to storage facilities, thereby ensuring the reliable operation of the entire system.

Security and data management issues in IP systems

Many security problems in IP systems are related to the limited computing and energy resources of the devices used. Many of these devices are mobile, which determines the dynamic nature of the network. Data transmission

delays often occur in networks with a dynamic structure. Therefore, it is necessary to ensure network security, considering the possibility of data transmission delays and energy resource limitations. Security issues can be addressed through node authentication and identification and data access restrictions. Data management issues include data routing problems during data transmission and data storage problems. The complexity of solving these problems is determined by the large amounts of data coming from devices in modern IP networks. The increase in data volume is achieved by expanding the components of the data collection system. Threats can arise at different architectural tiers of the IP system, such as threats to the security of the IS system at the physical tier, which is the base tier of the IS system. At this tier, there are physical and virtual objects. Physical objects include various sensors, including wireless ones. At the physical tier, various data transmission technologies and protocols are used, such as the ZigBee protocol, RFID tags, QR codes, and GPS systems for positioning mobile devices. The key function of this tier is to collect data about environmental objects and the environment itself. For instance, parameters such as wind speed, acidity, humidity, and vibration can be measured.

With the increase in the number of devices connected to a dynamic IP network, new data management challenges arise, such as data collection, classification, compression, and archiving. In a dynamic network, the configuration of devices is constantly changing. New elements are connected to the network, while others leave it. Devices generate large amounts of data that must be processed and stored. These tasks are handled by data management systems. The need to provide real-time access to data and high requirements for response times to user requests impose limitations on the amount of data that can be processed and stored in modern systems. To achieve network scalability, lightweight infrastructures must be created and used. When designing such an infrastructure, it is necessary to factor in the security requirements for data collection and storage, as well as current resource constraints, including energy.

The primary cause of threats is the dynamic change in the network structure caused by the changing location of mobile devices that form part of the network. Attackers exploit changes in the network structure to organise their attacks. Attacks on the network at the physical level can include denial-of-service (DDoS) attacks and network eavesdropping. Attacks may also include the capture of nodes or the addition of malicious nodes. Attacks via side channels are also possible. Attacks may be aimed at gaining unauthorised access to data, disrupting data routing, or disrupting normal customer service, which may result in data integrity violations or network overload. There are also threats to the security of IP systems at the network level. At this level, data is transmitted over wired and wireless networks, where data routing tasks are performed. IEEE 802.15 (n.d.) is used for data transmission.4, which is a technical standard that defines the operation of low-speed wireless personal area networks (LR-WPAN), 3G, 4G, LTE, Wi-Fi, ZigBee, and MQTT, but the choice of a concrete technology depends on the devices used and the type of data to be transmitted.

At the network tier, secure connection of IP devices is ensured by various communication protocols, network interfaces, and communication channels. There are various network management mechanisms. As a result, secure data transmission from the physical tier to the data processing tier must be guaranteed. This tier is crucial for data management, network intrusion detection, and network traffic coordination in IP systems. Attacks by malicious actors at the network tier that can compromise data security include denial of service (Al-Hadhrami & Hussain, 2021), man-in-the-middle attacks, attacks on gateways, attacks on data stores, as well as attacks based on traffic analysis and spoofing attacks. DDos/DoS attacks can cause destructive changes to network components and threaten the security of Wi-Fi connections. In a man-in-the-middle attack, an attacker transmits data or alters the connection between two nodes, believing that they are communicating directly.

As a result, the nodes lose access to the necessary information. Attackers often target gateways. Gateways are a crucial element of IP systems. If an attack on a gateway is successful, the attacker gains control over the part of the IP system where the gateway acts as a bridge between the device and the cloud. Therefore, network-level security consists of ensuring the authenticity, confidentiality, and integrity of data as it is transmitted over the network. Encryption algorithms based on cryptographic keys, node authentication mechanisms, and intrusion detection tools can be used to protect the network from attacks. The data processing layer is part of the network layer. This level hosts the middleware platform. Functions at this level include the implementation of cloud computing, the distribution of data processing between nodes and cloud services, and data storage using various database management systems (DBMS).

The data management tier processes and stores heterogeneous data from devices. This includes web data, documents, sensor data, and emails. This data is irrelevant, and various formats are used to represent it. Processing and analysing such data require the use of intelligent data analysis and machine learning methods (Mahdavinejad *et al.*, 2018). These methods can be employed to extract the data needed to solve an application problem from the original information flow. The resulting data can be placed in temporary storage on a node or transferred to the cloud for long-term storage. Cloud nodes can process device data in real time, and processing on nodes involves data collection. Cloud services allow processing, analysing, and providing stored data to end users on demand (Abdulkareem *et al.*, 2021). Thus, cloud nodes in combination with cloud services enable short-term and long-term data storage, processing, and analysis of stored data in real time.

Attacks on cloud services and nodes are among the most widespread types of attacks. Data transmitted and stored in the cloud is at the greatest risk (Somani *et al.*, 2017). At the

processing tier, the primary types of attacks include denial-of-service (DoS) attacks and man-in-the-middle attacks. In conclusion, attackers gain control over shared network resources and can gain unauthorised access to data through hidden paths. Most services provided in the cloud on demand are accessible via the Internet (Younis *et al*., 2024). In this case, attackers can use the Internet to penetrate IP networks. Once inside the network, they can perform actions aimed at disrupting the operation of the network or its elements. Therefore, the problem of protecting data stored in the cloud can be considered one of the key security challenges for IP systems. There are also threats to the security of IP systems at the application level. Various applications for creating an intelligent environment are located at the application level. At this level, intelligent applications are managed and accessible to end users.

Data management at the application tier must ensure that data is provided to end users. Management is based on the requirements of the application running in real time. For example, healthcare and transportation applications must have access to operational data and process it in real time. Delays in data delivery can have severe negative consequences. Applications that collect information about people's daily lives, such as travel routes, shopping habits, and daily energy consumption, do not have strict processing time requirements. However, because the data is sensitive, security requirements for its collection, transmission, and processing still apply. At the application tier, security issues are caused by the creation and use of computer viruses, worms, Trojan horses, spyware, and other malicious software. Attacks at this level can lead to data interception, incorrect data exchange, and denial of service. Successful attacks also result in the attacker being recognised by the system as a legitimate user and gaining unrestricted access to applications and data containing confidential information. Data and application security at the application level requires preventing unauthorised access and use of data, as well as restoring the functionality of applications after an attack.

To ensure security, vulnerabilities that may exist in applications should be identified and access rights to data should be restricted. Data encryption methods can also be used, but their use leads to an extensive increase in data transfer delays. Other security mechanisms include firewalls, intrusion detection systems (IDS), and antivirus software. As a rule, when choosing a method of protecting applications and data at the application tier, the risks of various threats and the probability of successful attacks by malicious actors should be assessed.

The reviews by M.F. Usmani (2021) and D. Dinculeană & X. Cheng (2019) are most relevant to the subject under study, where the researchers also analysed various application-tier protocols in IoT networks. Specifically, M.F. Usmani (2021) emphasised that MQTT is most often used to collect telemetry from many nodes due to its simplicity and low overhead. The researchers' findings confirmed these conclusions, as MQTT truly provides effective data collection in device-to-cloud scenarios. At the same time, analogously to the comments of D. Dinculeană & X. Cheng (2019), the present study also noted that MQTT is not always suitable for devices with extremely limited resources, as it still requires a persistent connection (TCP) and the presence of a broker, as well as the use of TLS protocols for data protection.

G. Sciangula *et al*. (2023) or M.-H. Ho *et al*. (2022) offered a slightly distinct perspective, where the use of DDS in real-time mode was evaluated. The researchers concluded that DDS has advantages in decentralisation and provides lower latency compared to the conventional client-server model. The present review confirmed this thesis: according to (Internal documentation…, n.d.), DDS allows publishers and subscribers to interact without a central broker, eliminating the single point of failure. However, the complexity of DDS configuration and possible differences in implementations by different vendors (RTI, OpenDDS, etc.) may be a serious obstacle to mass adoption. S.K. Routray *et al*. (2023) focused on CoAP and demonstrated that this protocol is the optimum solution for resource-constrained devices due to its simpler structure (UDP) and lower power consumption compared to HTTP. The researchers confirmed that CoAP does have lower overhead costs, which is consistent with the official specifications of Z. Shelby *et al*. (2014). The issue of scalability was also considered. The researchers found that CoAP works better in small networks, while in large-scale environments, delays may occur due to large amounts of broadcast traffic.

M. Saban *et al*. (2021) and Z. Liu *et al*. (2022) addressed low-power protocols (LoRaWAN, ZigBee). They suggested that LoRa and ZigBee were among the best options for remote sensor nodes due to their wide range and very low power consumption. The presented review confirmed this opinion: Wi-Fi is suitable where greater throughput is required and a constant power supply is available, while LoRa allows collecting small amounts of data over long distances. However, the findings revealed that LoRa is not always capable of providing low latency, which can be a problem for some mobile applications.

In terms of security, A. Alrawais (2020) highlighted the potential risks of using NFC, particularly the danger of unauthorised connections. The researcher's analysis found that NFC does have a short range, but insufficient protection against 'over-the-shoulder' attacks (especially without additional encryption measures). This position is consistent with that of P. Onumadu & H. Abroshan (2024), who, in their study of technologies for IoT, also emphasised the significance of security protocols for data transmission in the near field. Most researchers agree on the absence of a single 'universal' technology for data collection and transmission in IoT. The conclusion remains that the choice of protocol or technology (MQTT, DDS, CoAP, Wi-Fi, LoRaWAN, etc.) depends on the use case, among which the following are decisive: access to energy resources, requirements for data speed and volume, permissible delay and real-time criticality, and the level of security and safety.

Thus, the literature review and comparison with previous studies showed that the presented findings were consistent with the findings of other researchers (Usmani, 2021; Ho *et al.*, 2022; Sciangula *et al.*, 2023) regarding the effectiveness of DDS in real time and the suitability of MQTT for telemetry. They also confirmed the findings of M. Saban *et al*. (2021) and Z. Liu *et al*. (2022) on the advantages of LoRaWAN and ZigBee in energy-efficient sensor networks. The views of A. Alrawais (2020) and the position of P. Onumadu & H. Abroshan (2024) on NFC security risks coincided with the reservations presented in the current study on the low security of near-field technologies. The difference in emphasis (QoS, energy consumption, security) indicated that the subject of IoT communication requires further investigation, particularly in the context of integrated hybrid solutions. This will enable developers to tailor data collection systems to the concrete requirements of a particular industry, increasing their flexibility, scalability, and reliability.

Conclusions

The study analysed five key application-level protocols (DDS, MQTT, CoAP, HTTP, and AMQP). It found that decentralised DDS eliminates a single point of failure but is characterised by complex configuration. MQTT simplifies telemetry but requires a broker and a persistent TCP connection. CoAP is optimised for resource-constrained nodes but provides fewer delivery guarantees. HTTP continues to be versatile but creates additional overhead. AMQP provides advanced queuing mechanisms but requires more hardware resources. It was found that the choice of protocol depends on the use case and the acceptable energy consumption, data transfer volumes and delays. It was established that Wi-Fi, Bluetooth, ZigBee, LoRaWAN, RFID, and NFC wireless technologies cover different ranges, bandwidths, and energy consumption levels. None of them is universal for all applications. This was confirmed by the feasibility of developing and using hybrid approaches that combine the advantages of several protocols and technologies depending on the environmental conditions. The study also analysed the concept of M2M (machine communication via cellular and satellite networks). The comparison showed that none of the existing methods and protocols for collecting data in the Internet of Things (including DDS, MQTT, CoAP, LoRaWAN, ZigBee, etc.) would be capable of simultaneously meeting all the key requirements of mobile IoT systems by 2025: high security, minimal delays and energy efficiency. In real dynamic environments, a compromise must be found between data exchange speed, energy consumption, and security level, which complicates the development of a universal solution.

The conclusions obtained suggest the need for a comprehensive, multi-stage approach to the implementation of mobile IoT networks: protocols must be optimised depending on the physical environment, specialised tools must be used to reduce energy consumption, and mechanisms to counter unauthorised actions must be put in place. Specifically, for nodes with critically low resources and a need for energy-saving modes, it is advisable to use protocols such as CoAP or LoRaWAN, while in cases where fast response and scalability are critical, DDS-based approaches with decentralised interaction may be justified. For telemetry with many sensors and reliance on a broker-oriented "publisher-subscriber" scheme (MQTT), server performance and connection security requirements (TLS, key management, etc.) should be factored in. It is also advisable to provide additional security mechanisms (authentication, encryption, intrusion detection), as security measures have substantially influence latency and energy consumption. Further research should focus on three interrelated tasks. First, empirical verification of the effectiveness of DDS, MQTT, and CoAP protocols in mobile IoT networks with dynamic topology is required, with a particular focus on complex security mechanisms, which are currently largely unexplored. Second, the development of hybrid architectures combining publish-subscribe protocols (DDS, MQTT) with lightweight transport solutions (CoAP) and low-power LPWAN technologies (e.g., LoRaWAN) is promising; this approach will simultaneously ensure decentralisation, scalability, and energy efficiency in large sensor networks. Third, these integrated solutions must be tested in real-world dynamic environments to better understand the trade-offs between security, latency, and resource efficiency, thereby increasing the flexibility of IoT deployment in various application areas.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Abdulkareem, N.M., Zeebaree, S.R.M., Sadeeq, M.A.M., Ahmed, D.M., Sami, A.S., & Zebari, R.R. (2021). IoT and cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, 1(2), 1-7. doi: 10.48161/QAJ.V1N2A36.

[2] Al-Hadhrami, Y., & Hussain, F.K. (2021). DDoS attacks in IoT networks: A comprehensive systematic literature review. *World Wide Web*, 24, 971-1001. doi: 10.1007/s11280-020-00855-2.

[3] Alrawais, A. (2020). Security issues in near field communications (NFC). *International Journal of Advanced Computer Science and Applications*, 11(11), 621-628. doi: 10.14569/IJACSA.2020.0111176.

[4] Chanal, P.M., & Kakkasageri, M.S. (2020). Security and privacy in IoT: A survey. *Wireless Personal Communications*, 115, 1667-1693. doi: 10.1007/S11277-020-07649-9.

[5] Dinculeană, D., & Cheng, X. (2019). Vulnerabilities and limitations of MQTT protocol used between IoT devices. *Applied Sciences*, 9(5), article number 848. doi: 10.3390/APP9050848.
[6] Farhan, L., Hameed, R.S., Ahmed, A.S., Fadel, A.H., Gheth, W., Alzubaidi, L., Fadhel, M.A., & Al-Amidie, M. (2021). Energy efficiency for green Internet of Things (IoT) networks: A survey. *Network*, 1(3), 279-314. doi: 10.3390/network1030017.
[7] Haseeb, K., Almogren, A., Islam, N., Din, I.U., & Jan, Z. (2019). An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. *Energies*, 12(21), article number 4174. doi: 10.3390/EN12214174.
[8] He, P., Zhou, Y., & Qin, X. (2024). A survey on energy-aware security mechanisms for the Internet of Things. *Future Internet*, 16(4), article number 128. doi: 10.3390/FI16040128.
[9] Ho, M.-H., Lai, M.-Y., & Liu, Y.-T. (2022). Implementation of DDS cloud platform for real-time data acquisition of sensors for a legacy machine. *Electronics*, 11(13), article number 2096. doi: 10.3390/ELECTRONICS11132096.
[10] Honcharenko, D., Mokin, V., & Protsenko, D. (2023). Building an information system for monitoring physical indicators based on the internet of things technology. *Information Technologies and Computer Engineering*, 52(2), 99-108. doi: 10.31649/1999-9941-2023-57-2-99-108.
[11] Huang, Y., Liu, Y., Song, J., & Meng, W. (2024). A lightweight and efficient raw data collection scheme for IoT systems. *Journal of Information and Intelligence*, 2(3), 209-223. doi: 10.1016/J.JIIXD.2024.03.004.
[12] IEEE 802.15.4. (n.d.). Retrieved from https://docs.nordicsemi.com/bundle/ncs-latest/page/zephyr/connectivity/networking/api/ieee802154.html.
[13] Internal documentation – OpenDDS 3.28.0. (n.d.). Retrieved from https://opendds.readthedocs.io/en/dds-3.28/internal/index.html.
[14] Ivanov, D., Alekseienko, V., & Yarmolenko, T. (2023). Features of the interdependence of Big Data and Internet of Things technologies. *Bulletin of Priazovsky State Technical University*, 46, 13-27. doi: 10.31498/2225-6733.46.2023.288096.
[15] Kasiviswanathan, S., Gnanasekaran, S., Thangamuthu, M., & Rakkiyannan, J. (2024). Machine-learning- and Internet-of-Things-driven techniques for monitoring tool wear in machining process: A comprehensive review. *Journal of Sensor and Actuator Networks*,13(5), article number 53. doi: 10.3390/JSAN13050053.
[16] Khadam, U., Davidsson, P., & Spalazzese, R. (2024). Exploring the role of Artificial Intelligence in Internet of Things systems: A systematic mapping study. *Sensors*, 24(20), article number 6511. doi: 10.3390/S24206511.
[17] Khare, S., & Totaro, M. (2019). Big Data in IoT. In *2019 10th international conference on computing, communication and networking technologies, ICCCNT* (pp. 1-7). Kanpur: India. doi: 10.1109/ICCCNT45670.2019.8944495.
[18] Liu, Z., Li, Y., Zhao, L., Liang, R., & Wang, P. (2022). Comparative evaluation of the performance of ZigBee and LoRa wireless networks in building environment. *Electronics*, 11(21), article number 3560. doi: 10.3390/ELECTRONICS11213560.
[19] Mahdavinejad, M.S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., & Sheth, A.P. (2018). Machine learning for Internet of Things data analysis: A survey. *Digital Communications and Networks*, 4(3), 161-175. doi: 10.1016/J.DCAN.2017.10.002.
[20] Mishra, N., & Pandya, S. (2021). Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, 9, 59353-59377. doi: 10.1109/ACCESS.2021.3073408.
[21] MQTT version 5.0. (n.d.). Retrieved from https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html.
[22] Onumadu, P., & Abroshan, H. (2024). Near-Field Communication (NFC) cyber threats and mitigation solutions in payment transactions: A review. *Sensors*, 24(23), article number 7423. doi: 10.3390/S24237423.
[23] Peyman, M., Copado, P.J., Tordecilla, R.D., Martins, L.D.C., Xhafa, F., & Juan, A.A. (2021). Edge computing and IoT analytics for agile optimization in intelligent transportation systems. *Energies*, 14(19), article number 6309. doi: 10.3390/EN14196309.
[24] Prasad, V.K., Dansana, D., Bhavsar, M.D., Acharya, B., Gerogiannis, V.C., & Kanavos, A. (2023). Efficient resource utilization in IoT and cloud computing. *Information*, 14(11), article number 619. doi: 10.3390/INFO14110619.
[25] Routray, S.K., Pappa, M., Jha, M.K., & Sharmila, K.P. (2023). Performance of CoAP in the limited resource environment: An empirical study. In *5th international conference on inventive research in computing applications, ICIRCA* (pp. 510-515). Coimbatore: India. doi: 10.1109/ICIRCA57980.2023.10220891.
[26] Saban, M., Aghzout, O., Medus, L.D., & Rosado, A. (2021). Experimental analysis of IoT networks based on LoRa/LoRaWAN under indoor and outdoor environments: Performance and limitations. *IFAC-PapersOnLine*, 54(4), 159-164. doi: 10.1016/J.IFACOL.2021.10.027.
[27] Sciangula, G., Casini, D., Biondi, A., Scordino, C., & Di Natale, M. (2023). Bounding the data-delivery latency of DDS messages in real-time applications. In *35th Euromicro conference on real-time systems (ECRTS 2023). Leibniz international proceedings in informatics (LIPIcs)* (pp. 9:1-9:26). Vienna: Austria. doi: 10.4230/LIPICS.ECRTS.2023.9.
[28] Shelby, Z., Hartke, K., & Bormann, C. (2014). *The Constrained Application Protocol (CoAP)*. doi: 10.17487/RFC7252.
[29] Somani, G., Gaur, M.S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, 107, 30-48. doi: 10.1016/J.COMCOM.2017.03.010.

[30] Supreeth, S., & Patil, K. (2022). VM Scheduling for Efficient Dynamically Migrated Virtual Machines (VMS-EDMVM) in cloud computing environment. *KSII Transactions on Internet and Information Systems*, 16(6), 1892-1912. doi: 10.3837/TIIS.2022.06.007.

[31] Usmani, M.F. (2021). *MQTT protocol for the IoT – review paper.* Frankfurt: Frankfurt University of Applied Sciences. doi: 10.13140/RG.2.2.26065.10088.

[32] Waheed, S., Hanif, S., Hafeez, R., Sharif, M.I., Siddique, K., & Akhtar, Z. (2024). A comprehensive survey on applications, challenges, threats and solutions in IoT environment and architecture. *Journal of Computer Science*, 20(3), 310-332. doi: 10.3844/JCSSP.2024.310.332.

[33] Younis, R., Iqbal, M., Munir, K., Javed, M.A., Haris, M., & Alahmari, S. (2024). A comprehensive analysis of cloud service models: IaaS, PaaS, and SaaS in the context of emerging technologies and trend. In *5th international conference on electrical, communication and computer engineering, ICECCE* (pp. 1-6). Kuala Lumpur: Malaysia. doi: 10.1109/ICECCE63537.2024.10823401.

[34] Youssef, W.E.H., Abdelli, A., Kharroubi, F., Dridi, F., Khriji, L., Ahshan, R., Machhout, M., Nengroo, S.H., & Lee, S. (2023). A secure chaos-based lightweight cryptosystem for the Internet of Things. *IEEE Access*, 11, 123279-123294. doi: 10.1109/ACCESS.2023.3326476.

Аналіз основних моделей, методів та засобів збору даних в Інтернеті речей

Максим Савка

Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0003-2049-9438

Анотація. Швидкий розвиток мобільних технологій та технологічна революція сприяють активному впровадженню Інтернету речей, що веде до зростання кількості фізичних пристроїв, підключених до Інтернету. Однак поряд із перевагами Інтернету речей зростають і недоліки, зокрема кіберзагроза, порушення приватності та ризики несанкціонованого збору даних. У зв'язку з цим дослідження викликів та заходів захисту в сфері Інтернету речей є необхідним для забезпечення безпечного впровадження цих технологій. Метою дослідження було проаналізувати ключові моделі, методи та інструменти збору даних у середовищі Інтернету речей. Методологічною основою роботи був системний підхід, який дозволив представити державну політику у сфері Інтернету речей як складну, структурно організовану систему, що потребує вдосконалення та розвитку. В роботі застосовувались загальнонаукові та специфічні методи (системний, абстрагування та порівняння, формалізації, інституціонального аналізу, історико-генетичний, логіко-семантичний, класифікації, узагальнення, аналізу, формалізації та порівняння), а також широко і послідовно використовувалися статистичні дані. Встановлено, що серед існуючих технологій збору даних найширше застосовуються сенсорні мережі й хмарні обчислення, але вони не покривають усіх вимог мобільних систем Інтернету речей, зокрема щодо енергоефективності, пропускної здатності й безпеки. Виявлено, що сучасні архітектурні рішення (у тому числі соціальні архітектури Інтернету речей) дають змогу масштабувати систему та підключати різноманітні пристрої, однак мають обмеження, пов'язані зі складністю розгортання та пропускною здатністю. З'ясовано, що основні загрози безпеці виникають на всіх рівнях мобільних мереж Інтернету речей – від пристроїв до хмарної інфраструктури, що підтверджує необхідність комплексного підходу до їх захисту. Показано, що переважна більшість наявних рішень не задовольняє одночасно вимоги до низького енергоспоживання, швидкості збору й обробки даних у мережах із динамічною топологією, а також вимоги до надійності й конфіденційності. Запропоновані напрацювання доповнюють існуючі методи, посилюючи гнучкість і стійкість процесу збирання даних та створюючи підґрунтя для розробки нових енергоефективних і безпечних засобів в Інтернеті речей

Ключові слова: хмарні обчислення; архітектура IoT; безпека даних; протокол CoAP; fog-обчислення