Applied Science and Innovative Research
ISSN 2474-4972 (Print) ISSN 2474-4980 (Online)
Vol. 10, No. 1, 2026
www.scholink.org/ojs/index.php/asir

Original Paper

Analysis of the Promoting Role of Computer Science and Technology in the Development of the Internet of Things

Wanduo Wang

Xihua University, Chengdu, Sichuan, 610039, China

Received: January 15, 2026 Accepted: March 12, 2026 Online Published: March 19, 2026

doi:10.22158/asir.v10n1p131 URL: http://dx.doi.org/10.22158/asir.v10n1p131

Abstract

As the cornerstone of the modern information society, computer science and technology play a crucial role in promoting the development of the Internet of Things (IoT). The essence of IoT lies in the deep integration of the physical world and the digital world, and computer science and technology serve as the bridge and engine for realizing this integration. This paper deeply analyzes the application of computer science and technology in all levels of the IoT architecture, including front-end data collection and preprocessing, core big data analysis, underlying wireless communication and 5G technology, as well as the security guarantee mechanism running through the whole system. Through detailed case analysis and theoretical discussion, this paper aims to reveal how computer science and technology enhance the efficiency of IoT by improving computing power and optimizing network communication, ensure its stability through fault detection and redundant design, and strengthen its security through advanced encryption and authentication technologies. Finally, this paper prospects the development direction of the deep integration of computer science and technology and IoT in the future, emphasizing that continuous technological innovation will be the key to unleashing the full potential of IoT.

Keywords

Computer Science and Technology, Internet of Things, Data Processing, Network Communication, Security Assurance, Edge Computing

1. Application of Computer Science and Technology in the Internet of Things

(I) Data Processing Technology

1. Data Collection and Preprocessing

At the perception layer of IoT, hundreds of millions of sensors and devices continuously generate raw data streams. However, such data are often "dirty data", containing noise, missing values, duplicate information, and inconsistent formats. Computer science and technology play a vital role in "cleaning" and "shaping" the data at this stage. Firstly, at the data collection level, operating system-level device drivers and embedded systems optimize the sampling frequency and accuracy of sensors, ensuring that data can be efficiently and accurately captured from the physical world. Subsequently, preprocessing technology becomes the core link to enhance data value. Data cleaning algorithms, using statistics and rule engines, automatically identify and eliminate outliers caused by sensor failures or environmental interference—for example, filtering out instantaneous spike noise by setting reasonable thresholds for temperature sensors. Data deduplication technology eliminates redundant data packets in the network caused by multi-path transmission or repeated reporting by devices through hash verification or time window comparison, thereby saving storage space and consumption of subsequent computing. Data normalization and format conversion are the keys to solving the heterogeneity of IoT data. Whether in JSON, XML, or binary format, whether in degrees Celsius or Fahrenheit, conversion tools and middleware provided by computer science and technology can unify these data into standard formats, ensuring that upper-layer applications can seamlessly understand and process them. This series of seemingly underlying processing tasks has greatly improved the quality and credibility of IoT data, laid a solid foundation for subsequent accurate big data analysis, effectively reduced the phenomenon of "garbage in, garbage out", and guaranteed the decision-making reliability of IoT systems.

2. Big Data Analysis

The core value of IoT does not lie in connection itself, but in analyzing the massive data generated by connections and gaining insights into the laws therein. Faced with the typical 4V characteristics of IoT data (Volume, Variety, Velocity, Value), traditional relational databases and stand-alone processing modes are powerless. The big data processing system introduced by computer science and technology provides a powerful engine for mining the deep value of IoT data. Distributed storage systems (such as HDFS and Cassandra) can store petabyte-level even exabyte-level IoT data across hundreds or thousands of nodes, achieving horizontal expansion of storage capacity and high availability. On this basis, distributed computing frameworks (such as Spark and Hadoop MapReduce) and stream processing engines (such as Flink and Kafka Streams) have emerged. For example, in the industrial IoT scenario, sensors deployed on wind turbines generate data such as vibration, temperature, and rotational speed every second. Through parallel processing technology, the system can divide these data into numerous small tasks and assign them to multiple nodes in the computing cluster for simultaneous spectrum analysis and trend prediction, shortening the analysis process that originally took hours to minutes. This makes real-time equipment fault prediction possible—when the analysis model detects abnormal characteristics in the vibration spectrum, the system can immediately issue an early warning to avoid unplanned downtime. In addition, in the smart retail field, through real-time correlation analysis of Wi-Fi probe data, surveillance video, and POS machine data in stores, big data technology can depict customers' moving heat maps, dwell time, and final purchase conversion rates, helping merchants optimize product display and precision marketing. Computer science and technology have propelled IoT from the simple stage of "connecting everything" to the intelligent stage of "inspecting everything".

(II) Network Communication Technology

1. Wireless Communication Technology

IoT devices are deployed in diverse environments, from indoor smart homes to vast farmlands, from the human surface of wearable devices to metal environments in industrial plants, making a single communication technology unable to meet all demands. The role of computer science and technology here is to continuously optimize and innovate diverse wireless communication protocol stacks to adapt to different IoT application scenarios. For example, in the field of short-distance, high-rate transmission, Wi-Fi technology, by introducing technologies such as OFDMA and MU-MIMO, not only improves network throughput when multiple devices are concurrent but also effectively reduces latency, meeting the transmission needs of 4K/8K video streams in smart homes. In personal area networks, the development of Bluetooth Low Energy technology, especially the maturity of BLE Mesh technology, enables smart lighting systems to realize self-organizing networking among devices. The failure of any bulb will not affect the communication of the entire network, while power consumption is controlled at an extremely low level, which can be maintained for several years only with button batteries. For sensor networks in smart homes and industrial automation, Zigbee technology, with its strong self-healing ability and large network capacity, constructs a stable and reliable mesh network. When a node fails, data can automatically find other paths for transmission. Computer science and technology not only optimize the radio frequency performance of the physical layer but also design sophisticated protocols at the network layer and application layer, such as congestion control algorithms, dynamic power adjustment mechanisms, and sleep-wake strategies, ensuring that IoT devices can find the optimal balance among data transmission rate, communication distance, power consumption, and cost in complex environments, thus meeting diverse business demands.

2. 5G Technology

If previous generations of mobile communication technologies mainly solved the connection between people, 5G technology is born for the interconnection of all things. The three application scenarios of 5G—enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and massive Machine-Type Communications (mMTC)—precisely target the core pain points of IoT development. Computer science and technology act as a key enabler in the integration of 5G and IoT. Firstly, at the network architecture level, Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) abstract traditional dedicated network hardware into software functions, enabling the flexible deployment of 5G core networks like building blocks and the rapid construction of customized virtual private networks according to the needs of different industry users. Secondly, for applications extremely sensitive to latency such as autonomous driving and remote surgery, computer science and technology optimize the collaboration between edge computing and 5G core networks, sinking application servers to near base stations, reducing end-to-end latency to the millisecond level and ensuring the real-time performance of control instructions. For example, in the scenario of remotely controlling port gantry cranes, operators precisely control robotic arms thousands of miles away to grab containers through multiple 4K high-definition videos transmitted in real time via 5G networks. Any slight lag or delay may lead to accidents. Thirdly, for massive sensors in smart cities (such as water meters, electricity meters, and environmental monitors), the mMTC feature of 5G supports millions of connections per square kilometer, ensuring reliable access for each node. Breakthroughs in channel coding, massive antenna technology, and non-orthogonal multiple access in computer science and technology enable 5G networks to efficiently handle massive concurrent small data packets while ensuring extremely low power consumption. It can be said that 5G endows IoT with faster response, wider connection, and more intelligent scheduling capabilities.

(III) Security Assurance Technology

1. Data Encryption Technology

IoT systems are widely deployed in various physical environments, and the data they collect and transmit often involve personal privacy, trade secrets, and even national security, such as fingerprint information of smart door locks, real-time locations of the Internet of Vehicles, and control instructions of power grids. Therefore, the confidentiality and integrity of data during transmission and storage are crucial. Computer science and technology provide a multi-level data encryption system to address this challenge. At the data transmission level, considering the limited computing power of IoT devices, lightweight encryption algorithms (such as PRESENT and SPECK) have been designed, which can encrypt sensor data with extremely low CPU and memory overhead to prevent data from being illegally eavesdropped over the air. For gateways or cloud nodes with strong computing power, higher-level asymmetric encryption algorithms (such as Elliptic Curve Cryptography, ECC) can be used to securely negotiate session keys, ensuring that the keys themselves are not intercepted during distribution. At the data storage level, the exploration of homomorphic encryption has opened up a new path for the secure utilization of IoT data. It allows direct computation on encrypted data, and the decrypted computation result is consistent with the result of direct computation on plaintext. This means that even cloud service providers cannot see users' actual data but can provide computing services, greatly protecting data privacy. In addition, hash functions (such as SHA-256) are widely used for data integrity verification. Any slight modification to the original data will lead to a huge change in the hash value, ensuring that the data has not been tampered with after storage or transmission. It is these encryption methods derived from computer science and technology that put a solid "invisible armor" on IoT data and build a full-link data security barrier from the collection end to the application end.

2. Identity Authentication Technology

In the era of interconnection of all things, identifying whether the "things" accessing the network are credible and whether the "people" operating the system are legal is the first gateway to building an IoT security defense line. The traditional username-password method faces huge challenges in IoT scenarios: countless screenless sensor devices cannot input passwords, and weak password vulnerabilities are the main entry point for botnet attacks (such as the Mirai virus). The development of computer science and technology provides a multi-dimensional identity authentication scheme to solve this problem. At the device level, digital certificate technology based on Public Key Infrastructure (PKI) is widely used. Each IoT device is implanted with a unique, tamper-proof digital certificate when leaving the factory. When it attempts to access the network, the network end verifies the validity of its certificate through a challenge-response mechanism, and only devices with legal certificates are allowed to access, thus eliminating impersonation by illegal devices from the source. At the user level, biometric technology has become a standard configuration for mobile IoT terminals (such as smartphones and smart door locks). The combination of capacitive sensing for fingerprint recognition and deep learning image algorithms has reduced the false acceptance rate to less than one in a million; facial recognition technology can accurately construct a three-dimensional model of the human face through 3D structured light or TOF cameras, effectively preventing attacks from photos or videos; iris recognition, with its high uniqueness and stability, plays a role in high-security scenarios such as financial payment. In addition, multi-factor authentication further strengthens access control. For example, when performing remote home control, the system not only requires a password but also dynamic verification codes pushed via mobile APP or fingerprint confirmation. Even if the password is leaked, attackers cannot complete the login. By integrating cryptography, biometric identification, and behavior analysis, computer science and technology build a dynamic, multi-level zero-trust identity authentication system, ensuring that only legitimate devices and users can access IoT resources.

2. Improvement of IoT Efficiency by Computer Science and Technology

(I) Improvement of Computing Power

1. Edge Computing

With the explosive growth of the number of IoT devices, the traditional cloud computing mode of transmitting all massive data to the cloud for processing is facing unprecedented challenges, mainly reflected in network bandwidth bottlenecks and increased response latency. For example, an autonomous vehicle needs to identify obstacles ahead and make braking decisions within milliseconds. If video data is transmitted back to the cloud hundreds of kilometers away for processing, the round-trip latency is enough to cause a tragedy. The edge computing model proposed by computer science and technology is the key to solving this problem. The core idea of edge computing is to sink computing power to the network edge close to data sources, such as routers, base stations, and even IoT gateways themselves. Computer science and technology provide comprehensive technical support for this architecture. Firstly, at the virtualization level, container technology (such as Docker) can quickly deploy and isolate different application services on edge devices with limited resources, realizing a lightweight computing environment. Secondly, at the task scheduling level, collaborative algorithms are designed to intelligently determine which data needs to be processed in real time at the edge (such as real-time control instructions) and which can be filtered or aggregated before being sent to the cloud for long-term storage and in-depth analysis (such as periodic statistical reports). For example, in a smart factory, vibration sensors on thousands of industrial robot arms continuously generate data. Edge servers deployed on-site run fault diagnosis models in real time. Once abnormal vibration of an arm is detected, a shutdown instruction is issued immediately, and the whole process is completed in a local closed loop, avoiding large-scale scrapping of production lines. At the same time, edge servers only upload abnormal data and hourly production statistics summaries to the enterprise cloud center. This "edge-cloud collaboration" mode greatly reduces network bandwidth pressure, reduces the response time of core applications from seconds to milliseconds, and significantly improves the real-time processing efficiency and business agility of IoT systems.

2. Cloud Computing

If edge computing is responsible for handling "local" transactions requiring rapid response, cloud computing undertakes the important tasks of "global" convergence, in-depth analysis, and long-term storage of massive data in IoT systems. By building an elastic and scalable cloud computing platform, computer science and technology provide IoT with nearly unlimited computing power resources. At the infrastructure level, virtualization technology breaks the boundaries of physical servers. One physical machine can be virtualized into multiple independent virtual machines running different IoT applications respectively, greatly improving resource utilization. Object storage technology provides a cheap and reliable storage solution for a large amount of unstructured data (such as pictures, videos, and logs) in IoT. At the platform level, cloud service providers provide a wealth of IoT PaaS services, such as device access and management, message queues, and stream data processing. Developers do not need to care about the operation and maintenance and expansion of underlying servers, and can quickly build highly available IoT applications only through API calls. For example, a smart home startup can use a cloud platform to easily support the simultaneous online and voice interaction of millions of smart speakers. The automatic elastic scaling function of the cloud platform can dynamically increase or decrease computing resources according to traffic changes during morning and evening peaks, ensuring user experience while avoiding resource waste. More importantly, cloud platforms integrate artificial intelligence and big data analysis services, and IoT data can conveniently call these services for model training and value mining. For example, new energy vehicle enterprises upload vehicle driving data across the country to the cloud platform, use the powerful GPU computing power of the cloud to train autonomous driving algorithm models, and then issue the trained models to each vehicle through OTA, forming a closed loop of data-driven evolution. Computer science and technology make cloud computing the brain center of IoT, endowing IoT systems with the core ability to handle complex services and realize intelligent evolution.

(II) Optimization of Network Communication

1. Low-Power Wide-Area Network

In many IoT application scenarios, such as smart water meters, environmental monitoring, and smart agriculture, devices are usually deployed in remote, scattered, and power-supplied difficult environments, requiring battery life of several years or even ten years, while needing wide-area coverage of several kilometers. Traditional cellular networks (such as 2G/3G/4G) have wide coverage but high power consumption; short-distance communication technologies (such as Wi-Fi/Bluetooth) have low power consumption but small coverage. The emergence of Low-Power Wide-Area Network (LPWAN) technology perfectly fills this gap, and computer science and technology is the core driving force behind it. LPWAN technologies represented by LoRa and NB-IoT achieve extremely low power consumption through in-depth optimization of communication protocols. At the physical layer, spread spectrum modulation and other technologies are adopted, exchanging higher receiving sensitivity and stronger penetration ability at a lower rate, enabling signals to penetrate multiple floors or go deep underground. At the MAC layer, an efficient sleep-wake mechanism is designed. Devices are in deep sleep (microampere-level current) most of the time, waking up quickly only when data needs to be sent, and sleeping immediately after sending, thus greatly extending battery life. Computer science and technology also optimize the network protocol stack, simplify the handshake process, and reduce unnecessary signaling overhead. For example, in NB-IoT, the introduction of PSM (Power Saving Mode) and eDRX (extended Discontinuous Reception) technologies allows devices to negotiate a sleep cycle of up to several hours with the network, during which devices are completely "invisible" and do not listen to any network paging, thus minimizing power consumption. These underlying innovations in computer science and technology enable LPWAN networks to achieve an optimal balance among coverage, node cost, and terminal power consumption, providing the possibility of large-scale deployment for massive, scattered low-rate IoT sensors.

2. Network Slicing

IoT application scenarios are extremely diverse, and different applications have vastly different requirements for network performance. For example, autonomous driving requires extremely low latency, smart grids require ultra-high reliability, while smart meter reading in smart cities has low requirements for latency and bandwidth but needs to support massive connections. The traditional "one-size-fits-all" public network cannot meet these differentiated demands at the same time. Breakthroughs in computer science and technology, especially in the field of network virtualization, have given birth to 5G network slicing technology, providing a revolutionary solution to this contradiction. The core idea of network slicing is to use Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) technologies to logically slice a physical 5G network into multiple isolated and customized virtual networks. Each network slice is an end-to-end logical private network with independent network resources, topology, and management strategies. Computer science and technology acts as a "network architect" in this process. Firstly, at the core network side, network element functions (such as mobility management and session management) are decoupled into software through NFV, which can be flexibly combined according to slice types. Secondly, at the radio access network side, SDN controllers can perform fine-grained slicing and scheduling of air interface resources. For example, for autonomous driving services, a "low-latency slice" can be created, allocating exclusive wireless resources and edge computing nodes to ensure millisecond-level transmission of control instructions; at the same time, for massive smart meter services, a "massive connection slice" is created to support millions of connections by optimizing resource allocation strategies, allowing these devices to report data at an extremely low rate and frequency to save spectrum resources. Although these slices share the same physical infrastructure, they are logically isolated from each other, and congestion or attacks on one slice will not affect the security and stability of other slices. Computer science and technology make networks programmable and orchestratable, enabling operators to provide customized network services for all walks of life just like providing cloud services of different levels, greatly improving the utilization efficiency of network resources and the support capacity for diverse IoT applications.

3. Guarantee of IoT Stability by Computer Science and Technology

(I) Fault Detection and Recovery

1. Equipment Monitoring

The stability of IoT systems depends on the continuous and healthy operation of their massive underlying devices. The failure of any key device, such as a malfunctioning temperature sensor in cold chain logistics or a crashed robotic arm controller on a smart factory assembly line, may lead to serious economic losses or even safety accidents. Computer science and technology provide a comprehensive and intelligent equipment monitoring and fault detection system for this purpose. Traditional monitoring methods rely on preset static thresholds, such as an alarm when CPU load exceeds 90%, which is difficult to cope with complex and dynamic environments. Modern computer science and technology have introduced intelligent operation and maintenance technology based on machine learning. Firstly, the system continuously collects various operating indicators of devices, such as temperature, power consumption, connection signal strength, response time, etc., to construct a dynamic baseline of equipment health. Then, using time series analysis and anomaly detection algorithms (such as the 3-sigma rule and Isolation Forest), the system can automatically identify abnormal behaviors deviating from the baseline. For example, the hard disk response time of a storage server cluster usually fluctuates between 2-5ms. When the response time of a certain hard disk suddenly and continuously rises to 20ms, even if it has not yet reached the "fault" state, the intelligent monitoring system will judge it to have a high risk of "sub-health" and imminent failure based on the prediction model, and issue an early warning in advance. Furthermore, through correlation analysis, the system can connect seemingly isolated alarm events and quickly locate the root cause of the fault. For example, in the face of dozens of network delay alarms, the system can find that they all converge on the same core switch through topology analysis, thus quickly locking the fault point. Computer science and technology transform equipment monitoring from post-incident "firefighting" to pre-incident "fire prevention", greatly improving the active defense capability and operational stability of IoT systems.

2. Redundant Design

In complex IoT systems, failures are inevitable. Random hardware failures, potential software vulnerabilities, and sudden network congestion may lead to service interruption. Therefore, the key to improving stability is not only to detect faults in a timely manner but also whether the system can maintain uninterrupted service in the face of faults, which relies on the classic redundant design concept in computer science and technology. The core of redundant design is to "eliminate single points of failure", that is, to ensure that the failure of any component in the system will not lead to the paralysis of the entire system. At the hardware level, key IoT nodes (such as industrial controllers and core gateways) often adopt 1+1 or N+1 backup. When the master device is running, the backup device is in standby or synchronous state. Once the master device crashes, the monitoring system detects the abnormality through heartbeat detection and immediately triggers failover, and the backup device takes over services within seconds or even milliseconds, with the whole process transparent to upper-layer applications. At the software level, microservice architecture and stateless design enable application instances to run in multiple replicas. When one instance crashes, the load balancer automatically switches traffic to other healthy instances. At the data level, distributed storage systems adopt a multi-replica mechanism, and the same data is automatically saved to multiple nodes in different racks or even different data centers. Even if a node or even an entire data center encounters a disaster, data can still be recovered from other replicas. At the network level, ring or mesh network topologies are widely used in industrial IoT. When a communication link is interrupted, the Spanning Tree Protocol or more advanced ERPS ring network protection protocol can automatically activate the backup link within 50 milliseconds to restore communication. Through carefully designed redundant schemes at different levels and dimensions, computer science and technology build a solid fault-tolerant mechanism for IoT systems, ensuring the high continuity and stability of core services in the face of various accidents.

(II) Data Consistency Assurance

1. Distributed Databases

IoT systems are typical distributed systems, with data generated, stored, and processed at thousands of nodes around the world. How to ensure that these scattered data can ultimately remain consistent is a huge challenge to guarantee the correctness of upper-layer application logic. For example, in a smart grid, metering data of multiple power stations and power consumption terminals need to be recorded at the same time. If these data are inconsistent, it will lead to wrong billing or grid scheduling imbalance. The theory of distributed databases in computer science and technology and its engineering practice provide a systematic solution to the problem of IoT data consistency. According to the CAP theorem, distributed systems need to make trade-offs among Consistency, Availability, and Partition tolerance. For different IoT scenarios, database systems provide different consistency models. For scenarios with extremely high requirements for data accuracy, such as inventory counting and financial payment, a strong consistency model can be adopted. Through consistency protocols such as Paxos or Raft, data is written to most nodes before returning success, and any read request can read the latest write. Although this incurs certain latency overhead, it ensures absolute data reliability. For scenarios with high real-time requirements and tolerance for temporary inconsistency, such as smart home status reporting, an eventual consistency model can be adopted. Data is first asynchronously replicated to different nodes, and the system ensures that all nodes can finally see consistent data after a period of time. Computer science and technology also optimize data synchronization mechanisms, such as using incremental log synchronization and conflict detection and resolution algorithms, to handle data merging after network partition recovery. It is these complex distributed database technologies that enable IoT systems to maintain the accuracy and consistency of core business data like a highly coordinated whole while spanning a vast geographical space.

2. Blockchain Technology

In IoT scenarios involving multi-party participation, such as supply chain traceability, sharing economy, and cross-institutional data sharing, data consistency is not only related to technical synchronization but also to mutual trust at the trust level. Traditional centralized databases rely on a single trusted party, which has the risk of data tampering or single point of failure. Blockchain technology introduced by computer science and technology provides a new paradigm of decentralized, tamper-proof, and traceable data consistency assurance for IoT. In a blockchain network, data is no longer stored on a single central server, but linked into a chain in the form of blocks through cryptographic hash pointers, and redundantly stored on each participating node in the network. Any tampering with historical data will destroy the integrity of the hash chain and be immediately discovered by other nodes in the network. Consensus mechanisms (such as Proof of Work, PoW, and Practical Byzantine Fault Tolerance, PBFT) are the core of blockchain, ensuring that all honest nodes reach an agreement on the order and content of transaction records without a central authority. This feature has great value in the IoT field. Taking food traceability as an example, data collected by IoT devices (such as thermometers, GPS, and cameras) in each link from farm breeding, processing and packaging, logistics and transportation to retail shelves are recorded on the chain in real time and cannot be tampered with. Consumers can scan a QR code to see a "product resume" endorsed by multiple parties and cannot be falsified. In the Internet of Vehicles, blockchain can be used to record vehicle driving data, insurance claims, and maintenance records, providing a credible basis for used car transactions and insurance pricing. By integrating cryptography, P2P networks, and distributed consensus, computer science and technology make blockchain the cornerstone of building a trusted IoT data space, fundamentally solving the problem of data trust in distributed IoT environments.

4. Conclusion

As an important supporting force for the development of IoT, computer science and technology run through every level of the IoT architecture. From data cleaning and intelligent collection at the perception layer, 5G optimization and low-power wide-area network innovation at the network layer, to cloud computing, edge computing and big data analysis at the platform and application layers, as well as security encryption, identity authentication and trusted data assurance throughout the whole process, every progress of computer science and technology injects new vitality into IoT. Through in-depth analysis, it can be seen that computer science and technology not only solve specific technical problems of IoT in massive connection, real-time processing, security and reliability, but more importantly, by continuously promoting the transformation of computing paradigms, network architectures and application models, it continuously improves the overall efficiency, stability and intelligence level of IoT systems. Looking forward to the future, with the further breakthrough of cutting-edge computer science and technologies such as artificial intelligence, quantum computing and 6G communication, IoT will no longer be just a network connecting everything, but will become a distributed intelligent ecosystem with autonomous perception, intelligent decision-making and trusted collaboration, profoundly changing the production and lifestyle of human society. Continuously promoting the innovation of computer science and technology will be the key to unleashing the infinite potential of IoT and building a smart future.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347-2376.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787-2805.

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.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Li Kenli, Li Zhetao, & Li Renfa. (2021). Key Technologies of Edge Computing and Internet of Things Systems. *Journal of Computer Research and Development*, *58*(05), 897-899.

Liu Yunhao. (2017). *Introduction to the Internet of Things* (3rd ed.). Beijing: Science Press, 2017.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, *3*(5), 637-646.

Sun Qibo, Liu Jie, Li Shan, et al. (2010). Internet of Things: A Survey on Concepts, Architecture and Key Technologies. *Journal of Beijing University of Posts and Telecommunications*, *33*(03), 1-9.

Zhang Sufeng. (2024). Analysis of the Promoting Role of Computer Science and Technology in the Development of the Internet of Things. *Software*, *45*(04), 169-171.