Computer Systems Science & Engineering
DOI:10.32604/csse.2021.017224
Article

Tech Science Press

NVM Storage in IoT Devices: Opportunities and Challenges

Yang Liu[1], Shan Zhao[1,*], Wenhan Chen[1], Xuran Ge[1], Fang Liu[2], Shuo Li[3] and Nong Xiao[1]

[1]College of Computer, National University of Defense Technology, Changsha, 410000, China
[2]School of Design, HuNan University, Changsha, 410000, China
[3]School of Informatics, University of Edinburgh, Edinburgh, EH8 9JU, UK
*Corresponding Author: Shan Zhao. Email: zhaoshan18@nudt.edu.cn
Received: 24 January 2021; Accepted: 03 March 2021

Abstract: Edge storage stores the data directly at the data collection point, and does not need to transmit the collected data to the storage central server through the network. It is a critical technology that supports applications such as edge computing and 5G network applications, with lower network communication overhead, lower interaction delay and lower bandwidth cost. However, with the explosion of data and higher real-time requirements, the traditional Internet of Things (IoT) storage architecture cannot meet the requirements of low latency and large capacity. Non-volatile memory (NVM) presents new possibilities regarding this aspect. This paper classifies the different storage architectures based on NVM and compares the system goals, architectures, features, and limitations to explore new research opportunities. Moreover, the existing solutions to reduce the write latency and energy consumption and increase the lifetime of NVM IoT storage devices are analyzed. Furthermore, we discuss the security and privacy issues of IoT devices and compare the mainstream solutions. Finally, we present the opportunities and challenges of building IoT storage systems based on NVM.

Keywords: IoT; NVM; storage system; energy efficiency; security and privacy

1 Introduction

With the rapid development of IoT technologies and 5G networks, the number of network edge devices has rapidly increased, and the volume of generated data has grown exponentially [1,2]. The IoT closely connects the physical and digital worlds in the context of urban security, smart city development, target identification, tracking, positioning services, and other fields [3,4]. From the perspective of data processing, IoT can be divided into different layers, including the perception layer, network layer, data layer, and application layer from the top to the bottom, as shown in Fig. 1. The data layer supports the entire IoT system [5]. A core function of the data layer is to store the data collected by the terminals and place these data in a storage medium in a specific organizational form [6].

Data storage systems can ensure the continuous accumulation of perception data and provide a large amount of historical data, from which the IoT can extract information. However, the rapid growth of the amount of edge data poses severe challenges to the capacity, performance, and power consumption of

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

edge storage systems [7]. Traditional data processing and deep learning model training techniques usually adopt cloud computing models and centralized management schemes [8]. Uploading data to the cloud with long distance transmission can cause time delays, thereby rendering it challenging to meet the requirements of real time applications such as augmented reality (AR) and vehicle internet. Therefore, researchers have proposed a distributed edge storage architecture that can store data in edge devices or edge data centers. The use of such frameworks can dramatically shorten the physical distance pertaining to the data generation, storage, and calculation, thereby ensuring high speed and low latency data access for edge computing [9].

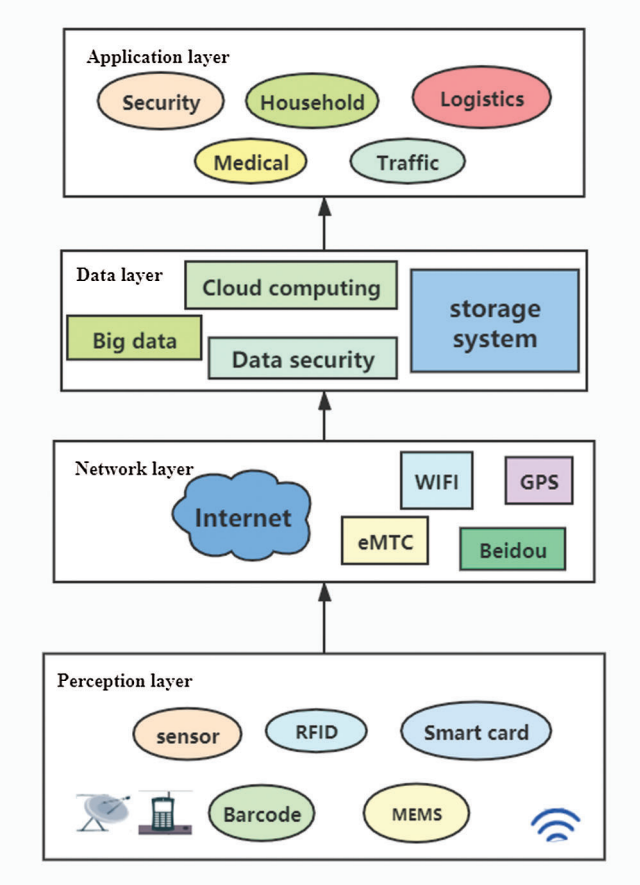

Figure 1: IoT architecture

With the development of various new nonvolatile storage media, large capacity storage in IoT devices can be realized. Compared with the process of transferring data to the cloud, data processing in embedded devices is more rapid and effective [10]. The recent research on NVM has been mainly focused on media such as spin transfer torque RAM (STT-RAM), phase change memory (PCM), domain wall memory (DWM), resistive random access memory (ReRAM), NAND Flash, and 3D Xpoint [11–14]. The STT-RAM uses a magnetic tunnel junction to store data. The resistance value of the MTJ is changed by controlling the relative magnetic direction of the free layer and reference layer, corresponding to the representation of different logic values. The PCM uses different values of chalcogenide glass crystals in different states to store the information. By applying voltages of different magnitudes and directions to change the resistance value, the ReRAM represents different logical values. Tab. 1 presents the

comparison of the performance parameters pertaining to nonvolatile storage media and traditional volatile media such as DRAM and SRAM.

Table 1: Comparison of different storage media [11–14]

Feature	SRAM	DRAM	PCM	ReRAM	STT-RAM	NAND Flash	3DXpoint
Cell Size/F2	120–200	6–10	4–12	4–10	6–50	4–5	—
Capacity/MB	≤32	$\leq 10^6$	$\leq 8 \times 10^3$	$\leq 10^6$	≤64	$\leqq 10^6$	$\leq 10^6$
Read Latency/ns	1–100	30	5–20	10–50	2–10	50	10
Write Latency/ns	1–100	50	60–120	10–60	2–20	10^6–10^8	30
Write Endurance	10^{16}	10^{16}	10^9	10^6	10^{15}	10^3	10^6
Write Energy	low	low	High	high	high	med	low
Retention Period	long	long	long	long	long	long	long
Nonvolatile	no	no	Yes	yes	yes	yes	yes

The emergence of a new type of NVM has disrupted the use of the original storage architecture of the IoT. Higher density storage devices allow the IoT to store more data in the terminal instead of selectively storing the data. As shown in Tab. 1, NVM media exhibit advantages of high storage density, low latency, and low power consumption. Such media represent an excellent solution to enhance the performance of the IoT. The current research has helped optimize the performance of NVM based IoT devices from different perspectives, such as write performance, energy consumption, security, and garbage collection. However, NVM based IoT devices are more vulnerable to security attacks than traditional DRAM. Therefore, several studies have proposed the use of blockchain, erasure codes, and other technologies for data protection.

The data processed through edge computing are present closer to the location in which the IoT device generates the data, and the data are not sent to the cloud or data center [15]. This approach can prevent data from being lost or tampered with during the transmission [16,17]. The blockchain technology can be used to effectively prevent the edge node data from being tampered with, and thus, this approach is widely used in the IoT domain. Moreover, blockchain techniques can improve the circulation efficiency in asset digitization, supply chain, traceability, and industrial inspection and promote the adjustment and development of the industrial structure [18]. Sensing technology, edge computing technology, and blockchain technology have high data storage requirements [19]. Consequently, a suitable approach must satisfy the large scale data storage requirements, specifically, high data read and write speeds, and high data storage reliability.

The main contributions of this paper are as follows:

- We analyze the basic characteristics of the existing IoT systems and the challenges encountered in storage systems. Next, we classify IoT devices according to different NVM based storage architectures and compare the characteristics, advantages and disadvantages of the different architectures.
- We summarize the existing solutions for IoT devices based on the NVM read and write asymmetry problem and analyze the approaches from three perspectives: write latency, write energy and lifetime.
- This paper is aimed at providing a more secure and reliable foundation for large scale applications of IoT devices. Therefore, we analyze the storage reliability and security strategies of IoT devices. Finally, we summarize the challenges encountered by NVM based IoT edge devices, such as those related to the device heterogeneity, security, device life, and garbage collection.

This work is expected to stimulate further research on IoT devices. The remaining paper is organized as follows. Section 2 introduces the characteristics and problems of storage systems pertaining to IoT systems. Section 3 describes the different virtual machine based storage architectures for IoT devices. Section 4 describes the different performance optimization techniques for IoT devices based on NVM. In particular, we index the different optimized classic solutions. Furthermore, in Section 5, we introduce and compare the representative works aimed at enhancing the reliability and security of IoT storage systems. The open challenges and current research trends are presented in Section 6. Section 7 presents the concluding remarks.

2 Storage Requirements in IoT Systems

2.1 IoT System Characteristics

IoT data are generated by large scale heterogeneous sensing devices and describe the states of a large number of physical worlds. These data exhibit the following characteristics:

1. *Multisource isomerism*. The IoT data are generated by different sensing devices, for example, temperature sensors, video devices, and mobile terminals. Different sources have different semantics and data structures, owing to which, the data storage is challenging.
2. *Large scale*. Many sensing devices have been deployed in our daily lives. These devices continuously generate data, which leads to a rapid increase in the scale of data.
3. *Temporal and spatial correlations*. Each sampled data point in the IoT system has time and space attributes, which can be used to describe the dynamic changes in the object state in time and space, respectively.
4. *Multidimensional scalar*. IoT applications usually integrate many types of sensing devices. Because such devices can sense multiple indicators simultaneously, the IoT sampling data are usually multidimensional and may be high dimensional.
5. *High redundancy*. In IoT applications, overlapped sampling may occur, and different sensing devices may sense the same object at the same time, thereby generating considerable redundant data.

These five features render data storage highly challenging, and the performance requirements of IoT systems have become increasingly demanding. The following section provides a clear understanding of the intensity of storage requirements for IoT devices.

2.2 Requirements of IoT Data Storage

In IoT systems, data are generated in real time. The generated data must be promptly and persistently saved in many application scenarios. In particular, in the context of urban public safety, field aware data may be presented as evidence. These data provide first line data support to enable the enhanced construction of smart cities. Rapid storage involves prompt writing of the data using mass aware devices. For example, in massive video surveillance, the data stream generated per second may be as high as 1 GB/s.

In particular, IoT devices generate large amounts of data every second, and users must query these data to access useful information. Therefore, efficient retrieval is a primary function of the IoT storage system. Many experts and scholars have attempt to increase the retrieval speed from the algorithm level; however, reasonable hardware equipment matching must be ensured. Application scenarios pertaining to industrial safety, public safety, and emergency handling involve high real time performance requirements. In general, the response speed must reach the minute level. In such cases, the storage media and architecture must be optimized.

Moreover, IoT storage systems must exhibit high compatibility. Specifically, such systems must be compatible with the access of the sensor devices in various physical networks and shield the complexity

of various data interfaces. In addition, such systems must be able to be dynamically expanded. The IoT has become an essential part of smart cities. However, the cost of the necessary equipment limits the further development of IoT applications. In this regard, the energy cost of the infrastructure in the data storage process must be reduced.

This section summarizes the data characteristics and storage requirements of the IoT. In general, certain storage strategies involve several limitations in satisfying the data storage requirements of the IoT. The development of new storage media has revitalized the optimization of the IoT storage systems. Considering the aforementioned needs, many scholars have conducted related research. In the subsequent section, we summarize and analyze the storage architectures, technical details, and system security.

3 Storage Architecture for IoT Devices

NVM has been widely adopted in the field of IoT devices due to its excellent performance. Many researchers adopted NVM to enhance the performance of mobile devices. Tab. 2 summarizes the classification under different storage architectures.

Table 2: Classification of different storage architectures

Criterion	Storage architecture	Approaches	Advantages	Disadvantages
Direct use as memory	PCM	i-NVMM [20]	Maintains 78% memory data encryption	Encryption protection is incomplete
	PCM	Reference [21]	Hardware encryption (counter mode encryption)	Incurs additional overhead
	PCM	Reference [22]	Encryption does not produce additional writes	Low encryption complexity
	PCM	MobiLock [23]	Enhanced encryption performance	Loss equalization is not considered
	MRAM +PCM	AIM [24]	Speed up the encryption process	
Hybrid Architectures	DRAM +PCM	FSLRU [25]	Can provide durability and atomicity functionalities in the page cache layer	PCM lifetime is not considered
	DRAM +PCM	SQLite/PPL [26]	More granular log writes	Increased storage overhead
	DRAM +DRAM simulation NVM	IMWAL [27]	Written to the NVRAM as a write ahead data log	Uses simulated NVM
	DRAM +PCM	Reference [28]	Uses sub-dirty-block management to reduce the write overhead	Increased monitoring overhead
	DRAM +PCM	LRA [29]	Uses sub-block management and background refresh to reduce the write overhead	Increased monitoring overhead

(Continued)

Table 2 (continued).

Criterion	Storage architecture	Approaches	Advantages	Disadvantages
NVM used as storage	STT-RAM/ PCM	NAMES [30]	Increased metadata access flexibility	NVM lifetime is not considered
	STT-RAM	i-FTL [31]	NVM assisted FTL mapping table to reduce flash write magnification	Log mapping table occupies additional storage space
	STT-RAM/ PCM	NVM Compression [32]	Increased storage efficiency	Decompression costs are not considered

However, the NVM presents disadvantages in terms of a limited lifetime, large write latency, and read/ write imbalance. Therefore, many researchers have proposed various methods to optimize NVM based storage architecture. In general, researchers have proposed many practical NVM technologies for IoT devices, which can be divided into three categories. 1) The NVM is directly used as the main memory to replace the DRAM. Under this architecture, the IoT devices can promptly recover when starting from sleep due to the nonvolatility of the NVM. 2) A hybrid memory architecture that uses NVM and DRAM as memory; this architecture can support the different needs of different workloads and allow data to be exchanged between the NVM and DRAM. 3) The NVM is used as an external storage device, usually, as a storage cache device to reduce the frontend delay.

3.1 Direct Use as Memory

Using the NVM as the main memory in IoT devices ensures that the memory data are not lost in unexpected events. However, these devices are not entirely reliable. Compared with traditional SRAM and DRAM, NVM is more susceptible to external environmental factors such as the temperature and magnetic fields. After the traditional memory is powered off for a certain period, the data disappear automatically. The data not written to the memory are usually detailed text data, which may be easily stolen by adversary IoT devices, and such data are usually private data, such as industrial data or personal information. However, due to the nonvolatility of the NVM, the data of the NVM that remain after a power failure are exceptionally vulnerable to attacks. The standard approach to solve this problem is to encrypt the data. Therefore, it is essential to ensure the accuracy and protect the integrity of the data before malicious intrusions.

The I-NVMM [20] uses the AES algorithm to realize selective encryption. During operation, the memory encrypts the cold data but not the hot data to reduce the performance overhead caused by the encryption and decryption. However, the problem of this technology is that the hot data, which may be more sensitive than cold data, are not protected and directly exposed to the attacker. Kong et al. [21] proposed an approach to ensure complete data protection. An encryption technology based on antimode XOR was developed to replace the direct encryption technology of the AES. This approach uses an encryption counter as a deadline counter and dynamically adjusts the strength of the error protection and correction codes to extend the life of the NVM. Zhang et al. [22] proposed an anti-encryption scheme based on PAD-XOR. The design complexity, energy cost, and lifetime of the NVM main memory were considered. The PAD generator was used to protect the runtime data for all NVM memory data with inferior timing and low power consumption without adding other write functions.

However, the anti-encryption method requires additional storage space and incurs a computational overhead, although resources are limited in IoT devices. Therefore, Luo et al. [23] recommended the MobiLock energy sensitive encryption mechanism. MobiLock uses caching and concurrency mechanisms to enhance the encryption and decryption performance, respectively. The caching mechanism is used to cache the frequently updated encrypted intermediate data, such as hot data, to reduce the energy consumption in the decryption process. Next, using the concurrency mechanism, the PAD calculation is performed while obtaining the ciphertext in the NVM to reduce the decryption delay. MobiLock enhances the security of mobile systems with a low latency and low energy consumption. Xie et al. [24] proposed a rapid and e□cient AES in memory (AIM) implementation to encrypt whole/part of the memory only when necessary. This method did not involve additional processing applications and employed the inherent logic operation function of the NVM to implement the AES algorithm.

The existing encryption methods for the NVM memory can be divided into software and hardware level encryption strategies. Moreover, these methods can be divided into direct and counter encryption mechanisms. We analyze the corresponding solutions in different situations. Certain IoT terminal devices are mobile devices, and thus, the corresponding energy consumption and area must be considered. Moreover, the service life of the NVM must be attempted to be extended.

3.2 Hybrid Memory Architecture

A cache layer exists in the IoT storage devices to reduce the write requests for mobile storage to enhance the system performance. However, many write requests remain. For example, mobile terminal applications often use the fsync ( ) system call to trigger synchronous writes to prevent the data loss caused by power outages or system crashes. This system call affects the performance of the entire device. Many researchers have integrated the NVM into contemporary IoT devices to solve this problem.

The FSLRU [25] adopts a hybrid storage architecture composed of the DRAM and a new NVM. This FSLRU algorithm is a novel page caching algorithm that eliminates the synchronous write requests by combining the page caching and mobile storage functions, as shown in Fig. 2. The FSLRU reduces the elapsed time of the workloads on a real board by up to 3.2 and 3.7 times compared to that pertaining to the DRAM and NVM based LRU algorithms, respectively. Moreover, the FSLRU significantly saves the limited battery power by up to 99% compared the DRAM based LRU algorithm.

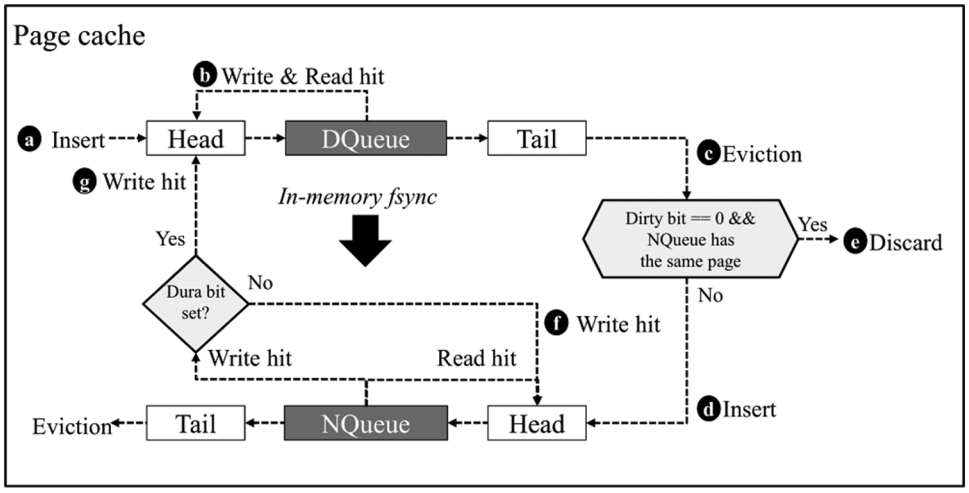

Figure 2: Overall process flow of the FSLRU [25]

Oh et al. [26] proposed a new optimization strategy called Per Page Record (PPL) for mobile data management, and Key functions have been implemented in SQLite/PPL based on the unified memory system (UMS). PCM use the same method through DIMM interface. They are interested in the potential of PCM to make updates persist in the database while avoiding the overhead of the I/O stack as much as possible. Ryu et al. [27] proposed an efficient in-memory write-ahead logging (IMWAL) technique for the embedded databases of mobile devices adopting nonvolatile random access memory (NVRAM). IMWAL performed 14% faster than the original WAL technique for embedded databases in real mobile devices on average.

Lin et al. [28] proposed a buffer cache architecture with hybrid DRAM/PCM memory, which improved the I/O performance for smartphones. They used a DRAM first-level buffer cache to provide high buffer cache performance and a PCM last-level buffer cache to reduce the impact of frequent synchronous writes. The hierarchical buffer cache improved the I/O response time by 20% compared to the conventional buffer cache. Lin et al. [29] also proposed a sub-block management and background flush to reduce the impact of the PCM write limitation and the dirty block write-back overhead, respectively. They used a DRAM first-level buffer cache to provide high buffer cache performance and a PCM last-level buffer cache to reduce the impact of frequent synchronous writes.The experimental results showed that the hierarchical buffer cache improved the I/O response time by 20% compared to the conventional buffer cache. The LRA improved the foreground application performance by 1.74x compared to the conventional CLOCK policy.

3.3 NVM as Storage

Solid state disks (SSDs) can manage the file system metadata that are persistently stored on mobile devices. Xue et al. [30] proposed a buffer cache technology based on NVM. The flash translation layer (FTL) of the SSD uses the NVM for storage. The NVM is specifically designed to manage the metadata of the SSD file system. Reference [31] proposes an NVM assisted nonredundant logging scheme for a byte addressing Android system known as I-FTL. The I-FTL consists of two main technical components: 1) file system metadata aware application level transaction, and 2) NVM assisted FTL mapping table.

Lindstrom et al. [32] ensured the optimal performance and storage effciency by introducing NVM compression methods that combine the application level compression and flash awareness. Using the new interface primitive derived from the FTL, the hybrid method for the NVM compression can enhance the compression performance by 2–7 times.

4 NVM Performance Optimization on IoT Devices

Edge storage is different from traditional cloud storage. The edge storage system is close to the edge devices in the network topology, with less communication overhead and higher service quality. In recent years, due to the rapid development of the IoT, the number of IoT devices has grown exponentially, which has led to more stringent requirements for massive IoT data storage. Compared with traditional storage media, NVM exhibits the advantages of nonvolatility, high reading speed, high integration, and low static power consumption. However, the NVM exhibits notable shortcomings in terms of the write latency, write lifetime, and write energy. The performance optimization approaches of the NVM in IoT devices are summarized in Tab. 3.

4.1 Extension of the NVM Lifetime

To address the short writing lifetime of NVM, two mainstream solutions exist, namely wear leveling and wear limiting.

Table 3: NVM optimization method classification

Criterion	Basic idea	Approaches	Storage architecture	Advantages	Disadvantages
Extend the write lifetime	Wear limit	Line Level Write Back [33]	DRAM Cache + PCM main memory	Increases the write speed, and reduces the page faults	Needs additional dirty bits per page
		Mellow Writes [34]	ReRAM as the main memory	Reduces the wear out of individual writes	Write speed is extremely low
		Region Retention Monitor [35]	MLC PCM	Enhances the balance between the system performance and memory lifetime	Incurs a higher hardware overhead for the RRM
	Wear level	Start Gap [36]	DRAM buffer +PCM as the main memory	Obviate the latency of accessing large tables	Difficult to achieve ideal performance
		Security Refresh [37]	PCM memory system	Small hardware overhead without any table	Causes performance degradation for normal program operations.
Reduce the write latency	Minimize the bit programming	Flip-N-Write [38]	PRAM	Reduces the write time and extends the write endurance	Incurs additional flip bit and memory overhead
	Encode the compressed data	DFPC [39]	NVM based main Memory	Reduces the latency and energy consumption	Adds a pair of encoder and decoder
	Enhance the SET operations	DyPhase [40]	PCM memory system	Increases the write performance and throughput	Periodically refreshes the stored data
		QnD [41]	MLC PCM	Enhances the system performance	Additional hardware overhead reduces the write lifetime
Reduce the write energy	Choose different writing modes	CDDW [42,43]	MLC PCM	Reduces the write energy consumption	Write speed is low
	Fine-grained write power budgeting	FPB [44]	MLC PCM	Enhances the write throughput and system performance	Incurs additional hardware overhead

4.1.1 Wear Limit

The wear limit is applied to reduce the number of writes. Qureshi et al. [33] discussed the balance of the main storage system composed of PCM storage and small DRAM buffers. This architecture exploits the latency advantage of the DRAM, and the capacity advantage of the PCM reduces the write traffic of

the PCM and extends its lifetime. Lunkai Zhang et al. [34] proposed the mellow write method to reduce the impact of certain write steps on the durability by performing slower writes. This approach can reduce the wear and tear associated with a single write instead of reducing the number of writes. Mingzhe Zhang et al. [35] proposed a region reservation monitor (RRM), which could record and predict the write frequency of a storage region. For each incoming memory write operation, the RRM selected an appropriate write waiting time, thereby enhancing the write lifetime.

4.1.2 Wear Level

Due to the different access frequencies of different applications, the lifespan of the hotspot storage unit is considerably smaller than that of the other elements. Wear leveling remaps the frequently written rows to less written rows to balance the writing of each memory cell. The limit life of the wear balance is the average life of the storage unit. Qureshi et al. [36] proposed a novel and effective wear leveling technology named start gap. The authors combined the start gap technology with a simple address space randomization technology. The service life of the 16 GB PCM system based on the baseline was reduced from the theoretical maximum, from 5% to 97%. Simultaneously, the total storage overhead incurred was less than 13 bytes, thereby eliminating the delay of accessing large tables. Nak Hee Seong et al. [37] proposed a novel low cost hardware mechanism named "security refresh," which used a dynamic random address mapping scheme to exchange data with a random key during each refresh to achieve wear balance.

4.2 Reduction in the NVM Write Latency

The read–write asymmetry of NVM is a key concern. The standard method to reduce the write latency is to increase the parallelism of the access to hide the write latency. Sangyeun Cho and Hyunjin Lee [38] proposed a simple microarchitecture technology named Flip-N-Write, which replaced the PRAM write operations with more e□ective read–modify–write operations. Experiments demonstrated that Flip-N-Write can reduce the write time of the PRAM by half and double the write durability. Yuncheng Guo et al. [39] proposed a highly adaptive NVM writing scheme named DFPC, which adopted a compressed writing scheme with latency optimization and energy saving to use low energy and latency encode compressed data, thereby reducing the waiting time and energy consumption.

Moreover, research has indicated that the latency of the SET operation in the PCM is considerably higher than that of the RESET operation. Certain authors attempted to reduce the set iterations in a single write operation to overcome the set operation limitation on the average writing delay of the PCM. However, in this approach, the period for data retention decreased. Thakkar et al. [40] proposed an architecture named Dynaphase, which used partial SET operations instead of SET operations and adopted distributed refresh operations to reduce the write latency by 16.2%. Mingzhe Zhang et al. [41] proposed the "quick and dirty" (QnD) technique, which could enhance the performance of the MLC PCM by choosing different write modes according to the frequency of the system write operations. QnD can increase the average performance by 30.9%.

4.3 Reduction in the NVM Write Energy

In embedded systems, energy is one of the most critical performance indicators. The write operation of the NVM consumes considerably energy. Therefore, reducing the write energy is a research hotspot in the field of embedded storage. Qingan Li et al. [42] adopted a compiler oriented two way writing (CDDW) scheme to select the most optimal writing mode for writing operations. Compared with the slow writing method, CDDW reduces the dynamic energy by 33.8% and enhances the performance by 35.9%. Moreover, the loop is the most computationally intensive part of the embedded program. To optimize the write performance and energy of the loop on the MLC PCM, Keni Qiu et al. [43] adopted a loop slicing method based on the write mode perception to maximize the effectiveness of the loop. Compared with

the CDDW method, the performance of this method on a set of benchmarks is enhanced by 50.8%, and the dynamic energy is reduced by 32.0%. Lei Jiang et al. [44] proposed a fine grained write power budget (FPB) for the MLC PCM, which exhibited significant advantages in terms of the write throughput and system performance.

5 Security of IoT Devices

With the rapid development of technologies such as vehicle internet, smart cities, and drones, IoT has been widely applied in recent years. Compared with cloud storage, edge storage exhibits advantages in terms of the transmission bandwidth and network latency and is more suitable for storing IoT devices. However, edge storage involves two notable security issues: privacy protection and reliability of data sharing. Tab. 4 presents the comparison of the different security mechanisms.

Table 4: Comparison of security assurance schemes

Security	Approaches	Type	Features
Privacy protection of data sharing	SEM-ACSI [45]	Attribute based encryption access control	Less computational overhead and lower storage costs
	CPHABE-AKDA [46]	Attribute based encryption access control	Achieves low communication and computation costs
	RBE [47]	Role based encryption access control	Operations are efficient regardless of the complexity of the role hierarchy and user membership
	RoSES [48]	Trust oriented access control	Saves the storage cost and reduces the read latency
	Blockchain technology [49–56]	Blockchain	Decentralization and trustlessness can establish point-to-point trustworthy value transfer between unfamiliar subsystems without relying on third-party trusted institutions
Fault tolerance	SPANStore [57]	Multicopy technology	Key value storage, reduces storage costs
	Beekup [58]	Multicopy technology	P2P storage framework based on Tahoe-LAFS enables cloudlike storage on edge devices

5.1 Privacy Protection of Data Sharing

With the widespread application of the IoT, the users' data are being collected and shared. IoT application data are stored in multiple edge devices, and it cannot be ensured that none of the edge server owners would leak data. Moreover, data sharing among users in the IoT environment is an essential requirement of IoT applications. With the development of technologies such as artificial intelligence and data mining, data that does not directly contain private information may also pose the risk of the privacy invasion of the users. Therefore, it is essential to provide an adaptive access control mechanism for data sharing. The current mainstream access control mechanism involves four aspects: attribute encryption based access control, role based encryption access control, trust evaluation based access control, and blockchain integrated solutions.

5.1.1 Adaptive Access Control Scheme

Access control based on attribute encryption uses ciphertext strategies to enhance the effciency and security of edge storage systems. Xiong et al. [45] built a new storage model based on CP-ABE and introduced the attribute authorization management (AAM) module. The authors proposed a novel, safe and efficient multiprivileged access control scheme for the SEM-ACSI cloud storage system of the IoT. This solution provides adaptive access control and reduces the storage overhead of public keys. Moffat et al. [46] investigated the data security of mobile devices adopting the CP-ABE method and its application in the IoT.

In role based encryption (RBAC) access control, only the requester in a specific role can decrypt the ciphertext. Zhou et al. [47] integrated the encryption technology with RBC and proposed the RBE scheme. Moreover, the authors proved that the users need to only maintain a single key for the decryption. Regardless of the complexity of the role hierarchy and user membership in the system, the system operation is effcient. Xia et al. [48] proposed a trust oriented data access strategy, which uses several agents for the trust assessment. Each agent independently manages the data access control of an edge server. In the process of data storage and sharing, the probability of data leakage is significantly reduced.

5.1.2 Privacy Protection Combined with Blockchain

The IoT is one of the main applications of blockchain [49–51]. Blockchain exerts a key influence on the IoT because of its point to point, open, transparent, and secure communication, relatively tamper proof nature, and multiparty consensus, especially in terms of the privacy protection. Li et al. [52] designed a blockchain based IoT device location chain storage system, which could provide users with location information services under the premise of location privacy. Liu et al. [53] proposed an elliptic curve encryption (ECC) asymmetric algorithm combined with the blockchain to encrypt the information. The experimental results show that the algorithm exhibits notable advantages in terms of the security and storage performance. Li et al. [54] proposed a secure transmission and storage solution for blockchain sensor images in the IoT, which exploits the advantages of blockchain decentralization, high reliability, and low cost to safely transmit and store the user image information. Huh et al. [55] used the blockchain to construct the IoT system and an RSA public key cryptographic system to manage the keys. The public and private keys are stored in Ethereum and a single device, respectively. Wang et al. [56] proposed a framework that combined the decentralized storage system IPFS, Ethereum blockchain, and attribute based encryption (ABE) technology. This approach could achieve fine-grained access control to data and solve the problem of incorrect keyword search results.

5.2 Reliability of the Edge Storage System

The edge storage system consists of many edge servers, and server failures occur common in edge storage systems. Therefore, edge storage systems must adopt effective and safe fault tolerant mechanisms to ensure data reliability. The reliability of existing edge storage systems is ensured through two methods: multicopy and erasure coding technology.

In the multicopy technology, multiple data copies of the same file are stored on the edge storage devices. When a storage node fails, a copy of the data can be obtained from other nodes to ensure data reliability. However, the storage cost for the multiple replication method is high, and the amount of data redundancy is large. [57] could effectively balance the geographic distribution and higher storage and data distribution costs to satisfy the latency requirements and achieve fault tolerance and consistency. In many cases, this approach can reduce costs by more than ten times. Rizzo et al. [58] proposed Beek up, a P2P storage framework based on Tahoe-LAFS, to ensure data reliability. Beek up supports storage on the edge devices of various applications. Aral et al. [59] proposed a dynamic replica placement method, which

could dynamically create/replace/delete replicas by continuously monitoring data requests from the edge nodes of the underlying network and combining the associated geographic locations. The SPAN storage system proposed by Wu et al.

The erasure coding technology mainly uses erasure coding algorithms to encode original data to obtain redundant data and later store the original and redundant data to ensure fault tolerance. Compared with the use of multiple copies, edge storage systems based on erasure codes can save the storage space and prevent data leakage [60,61]. Lin et al. [62] combined a threshold public key encryption scheme and variants of decentralized erasure codes to build a secure, reliable, and low cost distributed network storage system. Liang et al. [63] proposed an erasure code storage system for edge computing by using OpenMP on a multicore CPU to accelerate the erasure code and achieved satisfactory results.

6 Opportunities and Challenges

IoT data are stored in different sensing devices, local storage devices, and the application layer. The existing approaches cannot satisfy the needs of various applications in terms of storing data based on I/O characteristics or the frequency of data access. Compared with traditional storage media, NVM can more effectively meet the needs of rapid read and write. NVM has a low read and write latency, high density, low energy consumption, and data retention when power is switched off. In IoT storage systems, it is essential to save data during power outages. For example, in the case of accidents, a power outage usually occurs a few seconds before the accident, and the data pertaining to these few seconds is crucial. The emergence of NVM can help overcome the shortcomings of the current systems and save important information in time.

Due to their higher density, new storage devices allow IoT devices to store more data. Such devices support data storage for edge computing and reduce the risk of long distance data transmission. Moreover, the excellent read and write performance can help enhance the data query efficiency of the IoT application layer.

6.1 Collaboration of Heterogeneous Storage Systems

The addition of storage may change the original storage architecture. From an economic viewpoint, replacing the existing storage devices incurs workforce and material resources. Therefore, in the IoT storage system, new and old storage devices may co-exist. Nevertheless, the data distribution layer of the original storage system cannot adapt to the differences between the old and new devices that distribute different hotspot data through different devices. The optimization of the system performance under heterogeneous storage systems must be further examined.

6.2 Service Lifetime Issues

In addition to a high cost, NVM involves lifetime issues. Traditional storage media can be erased countless times. In the IoT, a large amount of data is written every day, and a long term safe and reliable storage system must be used. Researchers can consider the aspects of optimal placement of data and cooperation with the original storage device to reduce the erasure rate of the new storage device.

6.3 Flexibility and Cost

The devices in Internet of Things systems are highly different; thus, using different devices (storage oriented and computing oriented devices) can increase the stability and flexibility of the system. The IoT has a high requirement for data storage capacity. With the increase in the data volume, the hardware cost and storage energy consumption increase sharply. In future work, we can adopt and optimize the edge distributed storage architecture and integrate the storage space of all the devices to increase the total

resource pool and reduce the energy consumption of the whole system. By managing and optimizing the distributed storage systems, we can reduce the infrastructure costs, increase the total utilization of the equipment, and reduce maintenance costs.

7 Conclusion

With the development of smart cities and industrial information, the IoT has become increasingly important in daily production and life. This article summarizes the current status and problems of existing IoT storage systems. From the perspective of storage devices, we study the devices' status in the current IoT storage system, discuss new storage devices, and theoretically analyze the levels of different storage devices suitable for IoT storage systems. Finally, we summarize the opportunities and challenges of new storage device applications in IoT storage systems.

The use of new storage devices can enhance the data processing efficiency, prevent power failure, and facilitate the realization of IoT applications. The use of new storage devices provides new opportunities for storage systems, although such devices also pose novel challenges in terms of the software and hardware design of storage systems. Due to the unique characteristics of the new storage media, such as asymmetric read and write, limited life span, and garbage collection, new problems have been introduced in the software and hardware design of the computer systems. Therefore, constructing a heterogeneous storage system based on the characteristics of new storage devices is of significance to enhance the performance of IoT storage systems.

Acknowledgement: We wish to thank Dr. Guo Yeting for his assistance in this paper.

Funding Statement: This work is supported by National Key Research and Development Program of China NO.2018YFB0203904 and National Natural Science Foundation of China (61832020, 61872392, U1611261, U1811461, 61702569) the Pearl River S & T Nova Program of Guangzhou Province (201906010008), Natural Science Foundation of Guangdong Province (2018B030312002), and Key Area Research and Development Program of Guang Dong Province (2019B010107001).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Huang and G. Li, "Descriptive models for internet of things," in *Intelligent Control and Information Processing (ICICIP), 2010 Int. Conf. on Dalian, China*, pp. 483–486, 2010.

[2] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2012.

[3] A. R. Biswas and R. Giaffreda, "Iot and cloud convergence: Opportunities and challenges," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Seoul, South Korea, pp. 375–376, 2014.

[4] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan and A. V. Vasilakos, "The role of big data analytics in internet of things," *Computer Networks*, vol. 129, no. 2, pp. 459–471, 2017.

[5] M. Furini, F. Mandreoli, R. Martoglia and M. Montangero, "Iot: Science fiction or real revolution?," in *Proc. of Smart Objects and Technologies for Social Good (GoodTechs)*, Pisa, Italy: Springer International Publishing, pp. 96–105, 2016.

[6] H. Cai, B. Xu, L. Jiang and A. V. Vasilakos, "Iot-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 75–87, 2017.

[7] L. Jiang, L. D. Xu, H. Cai, Z. Jiang, F. Bu *et al.,* "An IoT-oriented data storage framework in cloud computing platform," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1443–1451, 2014.

[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, M. Zaharia *et al.,* "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[9] F. Liu, G. Tang, Y. Li, Z. Cai, X. Zhang *et al.,* "A survey on edge computing systems and tools," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1537–1562, 2019.

[10] R. Jackson and R. Lawrence, "Faster sorting for flash memory embedded devices," in *2019 IEEE Canadian Conf. of Electrical and Computer Engineering (CCECE)*, Edmonton, Canada, pp. 1–5, 2019.

[11] F. Hameed, A. A. Khan and J. Castrillon, "Performance and energy-efficient design of STT-RAM last-level cache," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 6, pp. 1059–1072, 2018.

[12] S. Rashidi, M. Jalili and H. Sarbazi-Azad, "Improving MLC PCM performance through relaxed write and read for intermediate resistance levels," *ACM Transactions on Architecture and Code Optimization*, vol. 15, no. 1, pp. 1–31, 2018.

[13] Y. Zhang, D. Feng, W. Tong, Y. Hua, J. Liu *et al.,* "CACF: A novel circuit architecture co-optimization framework for improving performance, reliability and energy of reram-based main memory system," *ACM Transactions on Architecture and Code Optimization*, vol. 15, no. 2, pp. 22:1–22:26, 2018.

[14] Y. Jia and F. Chen, "From flash to 3d xpoint: Performance bottlenecks and potentials in rocksdb with storage evolution," in *IEEE Int. Sym. on Performance Analysis of Systems and Software, ISPASS 2020*, Boston, MA, USA, pp. 192–201, 2020.

[15] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing, " in *Global Internet of Things Summit*. Geneva, Switzerland, pp. 1–6, 2017.

[16] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu *et al.,* "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[17] G. Wang, Y. Guan, Y. Wang and Z. Shao, "Energy-aware assignment and scheduling for hybrid main memory in embedded systems," *Computing*, vol. 98, no. 3, pp. 279–301, 2016.

[18] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Computing Communications Workshops (PerCom Workshops)*, Germany, Kassel, pp. 618–623, 2017.

[19] A. Thusoo, S. Zheng, S. Anthony, D. Borthakur, N. Jain *et al.,* "Data warehousing and analytics infrastructure at facebook," in *Proc. of the 2010 ACM SIGMOD Int. Conf. on Management of data*, Indianapolis, Indiana, USA, pp. 1013–1020, 2010.

[20] S. Chhabra and S. Yan, "I-nvmm: A secure non-volatile main memory system with incremental encryption," in *Proc. 38th Annual Int. Symp. Computer Architecture (ISCA)*, CA, USA, pp. 177–188, 2011.

[21] J. Kong and H. Zhou, "Improving privacy and lifetime of pcm-based main memory," in *Dependable Systems and Networks (DSN)*, Chicago, IL, pp. 333–342, 2010.

[22] X. Zhang, C. Zhang, G. Sun, J. Di, T. Zhang *et al.,* "An efficient run-time encryption scheme for non-volatile main memory," in *Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013 Int. Conf. on*, Montreal, QC, pp. 1–10, 2013.

[23] X. Luo, D. Liu, L. Liang, Y. Li, K. Zhong *et al.,* "Mobilock: An energy-aware encryption mechanism for nvram-based mobile devices," in *2015 IEEE Non-Volatile Memory System and Applications Sym. (NVMSA)*, Hong Kong, China, pp. 19–21, 2015.

[24] M. Xie, S. Li, A. O. Glova, J. Hu, Y. Wang *et al.,* "Aim: Fast and energy-efficient AES in-memory implementation for emerging non-volatile main memory," in *2018 Design, Automation Test in Europe Conf. Exhibition (DATE)*, Dresden, Germany, pp. 625–628, 2018.

[25] D. H. Kang and Y. I. Eom, "FSLRU: A page cache algorithm for mobile devices with hybrid memory architecture," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 2, pp. 136–143, 2016.

[26] G. Oh, S. Kim, S. W. Lee and B. Moon, "SQLite optimization with phase change memory for mobile applications," *Proceedings of the VLDB Endowment*, vol. 8, no. 12, pp. 1454–1465, 2015.

[27] S. Ryu, K. Lee and H. Han, "In-memory write-ahead logging for mobile smart devices with NVRAM," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 1, pp. 39–46, 2015.

[28] Y. J. Lin, C. L. Yang, H. P. Li and C. Y. M. Wang, "A buffer cache architecture for smartphones with hybrid dram/pcm memory," in *Proc. IEEE Non-Volatile Memory System and Applications Sym.*, Hong Kong, China, pp. 1–6, 2015.

[29] Y. J. Lin, C. L. Yang, H. P. Li and C. Y. M. Wang, "A hybrid DRAM/PCM buffer cache architecture for smartphones with Qos consideration," *ACM Transactions on Design Automation of Electronic Systems*, vol. 22, no. 2, pp. 27, 2017.

[30] M. Xue, C. Wang, Q. Wei, J. Yang, C. Chen *et al.,* "Nvm-accelerated metadata management for flash-based ssds," in *2016 Int. Conf. on Cloud Computing Research and Innovations (ICCCRI)*, Singapore, pp. 134–139, 2016.

[31] Y. Xu and Z. Hou, "NVM-Assisted Non-redundant Logging for Android Systems," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, pp. 1427–1433, 2016.

[32] J. Lindstrom, D. Das, T. Mathiasen, D. Arteaga, N. Talagala *et al.,* "Nvm aware mariadb database system," in *2015 IEEE Non-Volatile Memory System and Applications Sym. (NVMSA)*, Hong Kong, pp. 1–6, 2015.

[33] M. K. Qureshi, V. Srinivasan and J. A. Rivers, "Scalable high performance main memory system using phase-change memory technology," in *36th International Symposium on Computer Architecture (ISCA 2009)*, Texas, USA, pp. 24–33, 2009.

[34] L. Zhang, B. Neely, D. Franklin, D. B. Strukov, Y. Xie *et al.,* "Mellow writes: Extending lifetime in resistive memories through selective slow write backs," in *43rd ACM/IEEE Annual Int. Sym. on Computer Architecture*, Seoul, South Korea, pp. 519–531, 2016.

[35] M. Zhang, L. Zhang, L. Jiang, Z. Liu and F. T. Chong, "Balancing performance and lifetime of MLC PCM by using a region retention monitor," in *2017 IEEE Int. Sym. on High Performance Computer Architecture*, Austin, TX, USA, pp. 385–396, 2017.

[36] M. K. Qureshi, J. P. Karidis, M. Franceschini, V. Srinivasan, L. A. Lastras *et al.,* "Enhancing lifetime and security of PCM-based main memory with start-gap wear leveling," in *42st Annual IEEE/ACM Int. Sym. on Microarchitecture (MICRO-42 2009)*, New York, New York, USA, pp. 14–23, 2009.

[37] N. H. Seong, D. H. Woo and H. S. Lee, "Security refresh: Prevent malicious wear-out and increase durability for phase-change memory with dynamically randomized address mapping," in *37th Int. Sym. on Computer Architecture (ISCA 2010)*, Saint-Malo, France, pp. 383–394, 2010.

[38] S. Cho and H. Lee, "Flip-n-write: A simple deterministic technique to improve PRAM write performance, energy and endurance," in *42st Annual IEEE/ACM Int. Sym. on Microarchitecture (MICRO-422009)*, New York, New York, USA, pp. 347–357, 2009.

[39] Y. Guo, Y. Hua and P. Zuo, "A latency-optimized and energy-efficient write scheme in NVM-based main memory," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 1, pp. 62–74, 2020.

[40] I. G. Thakkar and S. Pasricha, "Dyphase: A dynamic phase change memory architecture with symmetric write latency," in *30th Int. Conf. on VLSI Design and 16th Int. Conf. on Embedded Systems*, Hyderabad, India, pp. 41–46, 2017.

[41] M. Zhang, L. Zhang, L. Jiang, F. T. Chong, Z. Liu *et al.,* "Quick-and-dirty: An architecture for high-performance temporary short writes in MLC PCM," *IEEE Transactions on Computers*, vol. 68, no. 9, pp. 1365–1375, 2019.

[42] Q. Li, L. Jiang, Y. Zhang, Y. He, C. J. Xue *et al.,* "Compiler directed write-mode selection for high performance low power volatile PCM," in *SIGPLAN/SIGBED Conf. on Languages, Compilers and Tools for Embedded Systems 2013*, Seattle, WA, USA, pp. 101–110, 2013.

[43] K. Qiu, Q. Li, J. Hu, W. Zhang and C. J. Xue, "Write mode aware loop tiling for high performance low power volatile PCM in embedded systems," *IEEE Transactions on Computers*, vol. 65, no. 7, pp. 2313–2324, 2016.

[44] L. Jiang, Y. Zhang, B. R. Childers and J. Yang, "FPB: Fine-grained power budgeting to improve write throughput of multi-level cell phase change memory," in *45th Annual IEEE/ACM Int. Sym. on Microarchitecture*, Vancouver, BC, Canada, pp. 1–12, 2012.

[45] S. Xiong, Q. Ni, L. Wang and Q. Wang, "SEM-ACSIT: Secure and efficient multiauthority access control for iot cloud storage," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2914–2927, 2020.

[46] S. Moffat, M. Hammoudeh and R. Hegarty, "A survey on ciphertext policy attribute-based encryption (CP-ABE) approaches to data security on mobile devices and its application to IoT," in *Proc. of the Int. Conf. on Future Networks and Distributed Systems*, Cambridge, United Kingdom, pp. 34, 2017.

[47] L. Zhou, V. Varadharajan and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947–1960, 2013.

[48] J. Xia, G. Cheng, S. Gu and D. Guo, "Secure and trust-oriented edge storage for internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4049–4060, 2020.

[49] D. Li, Y. Hu and M. Lan, "IoT device location information storage system based on blockchain," *Future Generation Computing Systems*, vol. 109, no. 1, pp. 95–102, 2020.

[50] H. Chen, W. Wan, J. Xia, S. Zhang, J. Zhang *et al.,* "Task-attribute-based access control scheme for IoT via blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2441–2453, 2020.

[51] B. Bordel, R. Alcarria, D. Martín and A. Sánchez-Picot, "Trust provision in the IoT using transversal blockchain networks," *Intelligent Automation & Soft Computing*, vol. 25, no. 1, pp. 155–170, 2019.

[52] D. Li, Y. Hu and M. Lan, "IoT device location information storage system based on blockchain," *Future Generation Computing Systems*, vol. 109, pp. 95–102, 2020.

[53] Y. Liu and S. Zhang, "Information security and storage of internet of things based on block chains," *Future Generation Computer Systems*, vol. 106, no. 5, pp. 296–303, 2020.

[54] Y. Li, Y. Tu, J. Lu and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the internet of things," *Sensors*, vol. 20, no. 3, pp. 916–929, 2020.

[55] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th Int. Conf. on Advanced Communication Technology (ICACT)*, pp. 464–467, 2017.

[56] S. Wang, Y. Zhang and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[57] Z. Wu, M. Butkiewicz, D. Perkins, E. Katz-Bassett, H. V. Madhyastha *et al.,* "SPANStore: Cost-effective geo-replicated storage spanning multiple cloud services," in *ACM SIGOPS 24th Sym. on Operating Systems Principles*, Farmington, PA, USA, pp. 292–308, 2013.

[58] F. Rizzo, G. L. Spoto, P. Brizzi, D. Bonino, G. Di Bella *et al.,* "Beekup: A distributed and safe P2P storage framework for IoE applications," in *2017 20th Conf. on Innovations in Clouds, Internet and Networks (ICIN)*, Paris, pp. 44–51, 2017.

[59] A. Aral and T. Ovatman, "A decentralized replica placement algorithm for edge computing," *IEEE Transactions on Network and Service Management*, vol. 15, no. 2, pp. 516–529, 2018.

[60] L. Xu, C. Xu, Z. Liu, Y. Wang, J. Wang *et al.,* "Enabling comparable search over encrypted data for iot with privacy-preserving," *Computers, Materials & Continua*, vol. 60, no. 2, pp. 675–690, 2019.

[61] M. Deng, F. Liu, M. Zhao, Z. Chen and N. Xiao, "Gfcache: A greedy failure cache considering failure recency and failure frequency for an erasure-coded storage system," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 153–167, 2019.

[62] H. Lin and W. Tzeng, "A secure decentralized erasure code for distributed networked storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 11, pp. 1586–1594, 2010.

[63] L. Liang, H. He, J. Zhao, C. Liu, Q. Luo *et al.,* "An erasure-coded storage system for edge computing," *IEEE Access*, vol. 8, pp. 96271–96283, 2020.