ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20240604001736
Original scientific paper

A Survey of Encryption-based Access Control Schemes in Named Data Networking

Jiaoli SHI, Xiaoping LIU, Anyuan DENG, Xiangyu LIU, Zhuolin MEI, Shunli ZHANG, Shimao YAO*, Xiancheng WANG, Liya XU, Kai HE

Abstract: Named Data Networking (NDN) completely abandons the traditional idea of IP addressing and uses the method of content matching to exchange data. This new network architecture is suitable for the emerging decentralized network. However, data access control in NDN is challenging and has been attracting a lot of researchers' attention. This paper lists the timeline of research progress in encryption-based NDN access control schemes by the cryptography primitives, discusses and analyses the schemes in the aspects of efficiency improvement and function improvement. Also, four future research directions of the construction of system model, lightweight system method, trust root deployment, permission revocation are pointed out in the field of encryption-based access control in NDN.

Keywords: encryption-based data access control; lightweight system method; named data networking; permission revocation

1 INTRODUCTION

NDN (Named Data Networking) is a new network architecture of ICN (Information-Centric Network), which will be one of the future networks. It was an NSF-funded project started around 2010 [1] and 46 institutions are participating or have participated in the past [2]. In 2015, RFC 7476 provided baseline ICN scenarios.

In 2017, ITU-T Y.3071 standardized the ICN requirements supporting 5G systems. In 2018, the ITU-T international standard approved the Decentralized Network Communication Architecture based on ICN and blockchain technology. Since the TRIAD project introduced a new level to realize ICN in the IP layer in 2021, several ICN projects have been carried out successively, such as DONA, CCN, NDN, etc. [3]. Due to its simplicity, NDN has been regarded as the most potential network architecture. Data security research around it has aroused the interest of many researchers.

The current NDN allows content to be cached on the routers, and any consumer can request access to the content. To achieve access control over sensitive content, their publisher encrypts these contents, and only consumers who get appropriate decryption keys could read them. In NDN, the data and content mean the same thing in this paper.

Although many scholars have put forward many schemes for NDN sensitive data access control, it is still difficult for these current NDN data access control schemes to consider security, efficiency, flexibility, and scalability. In terms of security, access control schemes need to support data confidentiality protection, fine-grained access control, collusion resistance, forward and backward security. In terms of efficiency, as mentioned in the literature [4], it is a challenge to achieve data access control with the most appropriate cache utilization rate, the lowest en/decryption cost and the lowest cost of consumer revocation. In terms of adaptability, it supports intermittent connections and low-latency applications. In terms of scalability, it supports the joining or quitting of large-scale consumers and the communication between various types of content data.

1.1 Related Surveys

Contrary to the work [5] or other existing surveys, there are three differences. First, our work focuses on ABE-based and IBE-based data access control schemes in NDN. Second, the time interval is different. For example, the work on [5] ended in 2020, while our work ends in 2024. Finally, our review presents different perspectives on the analyses and future directions of data access control schemes in NDN. Also, many review papers focus on data security in other scene, such as [6, 7].

1.2 Motivation

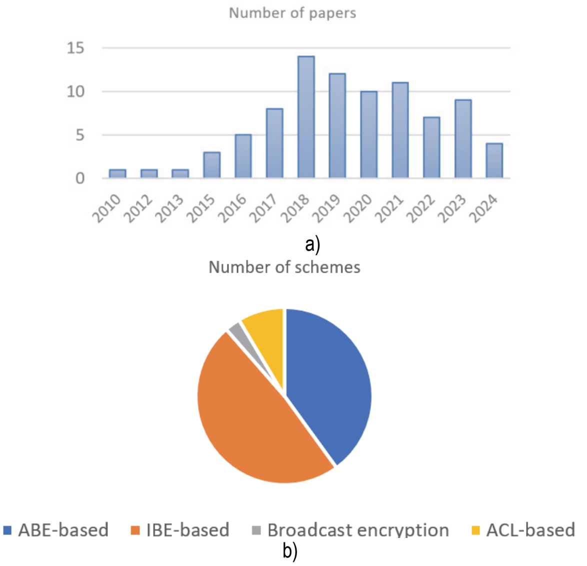
Contrary to the work [5] or other existing surveys, there are three differences. Firstly, our work compares and analyses ABE-based, IBE-based and other NDN access control schemes from two aspects of efficiency improvement and function improvement. Secondly, our work discusses NDN access control schemes and gives some future directions in the aspects of the construction of system model, lightweight system method, trust root deployment, permission revocation. Thirdly, the time span is of difference. For example, the work on [5] ended in 2019, while ours ends in 2024.

1.3 Methodology and Research Question

We have collected relevant papers available on the electronic databases and search engines, including IEEE Xplore, EI (Engineering Index), Google Scholar, as well as the NDN project website. The time span of the papers covered in this survey is from 2010 to June. 2024. There are 86 papers listed in the paper. Fig. 1a) shows the number of papers published per year and Fig. 1b) shows the distribution of papers across different types of access control schemes.

The considered Inclusion Criteria (IC) were: research papers focusing on the encryption-based access control in NDN, while the considered Exclusion Criteria (EC) were: papers where the goal is not access control or the method is not encryption-based access control as their main contribution, as well as those consisting solely of bibliography, table of contents, references and keynote talks, editorial articles, or summaries of conferences.

Our work answers two Research Questions (RQ). RQ1: What is the research progress of cryptography-based methods for data access control in NDN? RQ2: What are the possible challenge points for data access control in NDN in the future?



a)

b)

Figure 1 a) Number of papers published per year b) Different types of access control schemes

1.4 Contributions

Although the NDN access control survey paper [5] has been published, so far there is no survey paper studying encryption-based NDN access control schemes in view of its different characteristic features, like efficiency improvement, function improvement, etc. We also discuss in detail the future research directions as well as challenges relevant to deploy NDN. To the best of our knowledge, this paper is the first comprehensive effort to review the encryption-based access control in NDN, with the emphasis on the impact of selection from cryptographic primitives on access control schemes. We believe that this survey article will help researchers to stimulate works in the area of encryption-based NDN access control.

The contributions of our paper can be summarized as follows.

We survey encryption-based access control in NDN, covering cryptographic primitives, their classification, and time lines.

We comprehensively survey the recent encryption-based access control in NDN, covering state-of-the-art efficiency and function improvements, focusing on the methods, benefits and drawbacks.

We summarize the challenges faced by encryption-based NDN access control, like system model, lightweight system method, trust root deployment, permission revocation. And we also describe the future directions during deploying of access control in NDN.

1.5 Structure of the Paper

The rest of this survey is organized as illustrated in Fig. 2. Section 2 provides a description of the NDN Architecture. Section 3 reviews the progress of NDN access control schemes according to cryptography primitives. Section 4 analyses these schemes in the aspects of system model, lightweight, trust root deployment and permission revocation; at the same time, we shed light on the existing challenges. Section 5 concludes the article.

2 OVERVIEW OF NDN ARCHITECTURE

NDN keeps the same hourglass-shaped architecture [1]. This section describes briefly system model, security attacks, and design requirements of access control schemes in NDN. More detailed introduction can see the official website or the literature [1].

2.1 NDN Packet Structure

NDN is content-centered, with each content having a unique name. NDN has three roles: content providers, content consumers, and router nodes. NDN has two types of packets: *Interest* and *Data*. The former is used to carry the request of consumers for messages, and the latter is the one matching an *Interest* packet found by NDN routers.

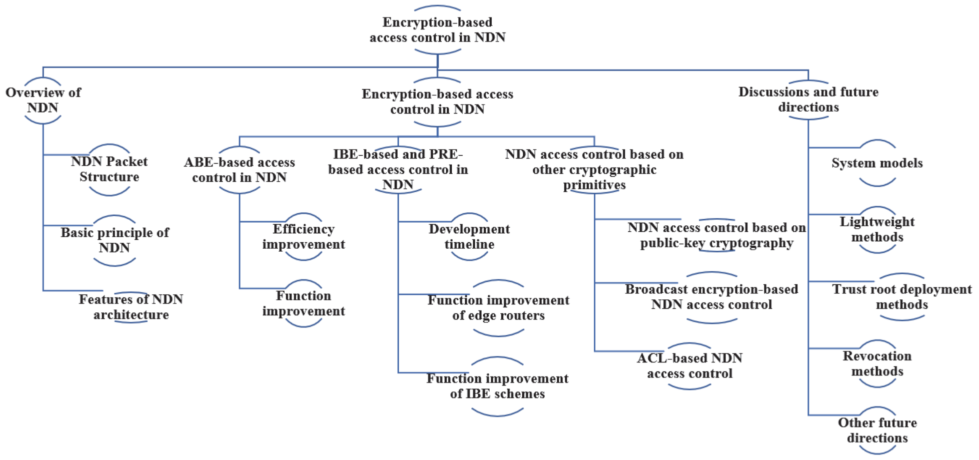

Encryption-based access control in NDN
Overview of NDN
NDN Packet Structure
Basic principle of NDN
Features of NDN architecture
Encryption-based access control in NDN
ABE-based access control in NDN
Efficiency improvement
Function improvement
IBE-based and PRE-based access control in NDN
Development timeline
Function improvement of edge routers
Function improvement of IBE schemes
NDN access control based on other cryptographic primitives
NDN access control based on public-key cryptography
Broadcast encryption-based NDN access control
ACL-based NDN access control
Discussions and future directions
System models
Lightweight methods
Trust root deployment methods
Revocation methods
Other future directions

Figure 2 Structure of the paper and taxonomy

There are three important components on each router: Content Store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB). The CS stores the passing Data packets so that they can respond directly to subsequent Interest requests. After an Interest packet arrives at a router and no matched data packet is found in

CS, it will be pended, in which PIT records the packet's name, interfaces of Interest packets incoming, interfaces of Interest packets outgoing, TTL (Time to Live) and forwarding policy label. FIB records the packet's name and interface of Interest outgoing, which are used to retrieve an outgoing interface to forward Interest packet according to the longest matching principle when the content name is not found in CS and PIT.

2.2 Basic Principle of NDN

When a router receives a packet, it determines the type of packet. 1) If the received packet is an Interest packet, it runs some incoming processes, records the name of the packet, and its entry into PIT. Then it searches the CS to find a Data matching the Interest. If there is any, it directly sends the matched Data through the entry of the Interest, sets the PIT expiry timer to now, and carries out the Interest finalization. If there is no matched packet in CS, the router searches FIB to forward the Interest packet. 2) If the received packet is a data packet from other routers, the router will perform some incoming processes and search PIT. If there is a record, it will insert the Data in CS, set PIT expiry timer to now and forward the data from all entries recorded by PIT, and then, clear PIT outrecords. If there is no request record of the Data in PIT, the Data will be identified as packets from an unknown source with unknown routes and then be dropped. At the same time, the router can also save a copy of the Data in the CS according to some cache policy.

2.3 Features of NDN Architecture

NDN is suitable for the emerging decentralized networks by exchanging data in a content-matching approach, using the name to address, and eliminating the need to mark or identify an endpoint. The new architecture has a lot of advantages: 1) It is convenient for application developments; 2) The possibility of targeted attack is decreased; 3) The information explicit naming is convenient for information managements; 4) The network cache is convenient for information distributions; 5) The information and its location are decoupled, which will adapt to the dynamic topology such as the Internet of Vehicles.

3 ENCRYPTION-BASED ACCESS CONTROL IN NDN

There are two types of methods for implementing access control in NDN: infrastructure-based methods and cryptography-based methods. The former requires the router to verify user permissions to an authorization server before providing contents, which is inefficient and has a single point of failure. The latter requires a solution that balances the efficiency of forwarding contents with the coordinating various goals of access control.

At present, the most likely cryptography methods to construct NDN data access control schemes include ABE (Attribute-based Encryption), IBE (Identity-based Encryption) and proxy re-encryption, public-key encryption, Broadcast Encryption, ACL (Access Control List) and so on.

3.1 NDN Data Access Control Based on ABE

ABE allows content providers to encrypt data using an attribute set or an access policy before publishing them. This feature allows multiple users to decrypt the authorized part of content data using his attribute private key anytime and anywhere, which supports fine-grained access control. But the computational cost on ABE is large and linear with the number of attributes. Therefore, there emerged a large number of studies focusing on the lightweight of terminal overhead. However, there are still challenges in the design of an ABE-based access control scheme that takes into account improvements in both efficiency and function. Fig. 3 shows the recent progress in improving ABE-based access control schemes. Tab. 1 summarizes the key features, advantages and disadvantages of ABE over NDN wherein C_{pair} and C_{ex} denote the pairing operation and exponentiations on a group, respectively. N_{en} denotes the number of attributes used in the encryption, N_{attr} denotes the number of attributes used in the decryption, n denotes the number of nodes in *HKT*, and $|L_G|$ denotes the order of the attribute set of a group.

3.1.1 Efficiency Improvement of ABE-Based Access Control Schemes

As for the efficiency improvement, existing studies mainly put forward the following ideas. Some works managed users in groups to reduce the user management overhead. For example, Wang et al. [8] introduced the concept of default attribute and proposed a FKP-ABE scheme for the key generation and decryption. Only multiplication or division is used in the key generation, and the pair operation in decryption is irrelated with the number of attributes. Li et al. [9] first used a symmetric encryption algorithm to encrypt content data to generate ciphertexts, generate the metadata for the ciphertexts, and then specify an access control policy to encrypt the symmetric key using ABE. The generated ciphertexts are used as content names. Silva et al. [10] introduced the concept of user group and designed an access control scheme based on ABE, whose advantage lies in the small number of encryption keys required because the number of keys is proportional to the number of members in the group. Jiang et al. [11] designed an access control scheme based on ABE for the dynamic neighbor relationship of vehicles on the Internet of Vehicles, but the simulation results showed that the scheme was not suitable for the scenario with high frequency requests of high-density vehicles. Wu et al. [12] proposed a CP-ABE access control scheme, CHTDS, which used the linear partition merging algorithm to split the content into PCS and CKS, implemented secure access control on CKS by using CP-ABE and the hash table data structure, and realized permission revocation without re-encryption of the published content. Chen et al. [13] proposed an access control system (HAC), which was based on a hierarchical naming mechanism and adopted a hierarchical key tree mechanism (HKT), which contained hierarchical authorization information and allowed users to derive keys locally according to their needs. This reduced the overhead of IoT many-to-many communication and improved the efficiency of access control. To ensure the security and efficiency of HKT, a level-oriented CP-ABE (LOCP-ABE) was proposed, which allowed users to obtain authorization levels according to the specified attribute sets alone. Then, the NDN could use a recipient-driven model and an in-network cache mechanism to improve transmission efficiency. An attribute set command verification mechanism was used to improve the efficiency of command verification on resource-constrained or isolated IoT edges.

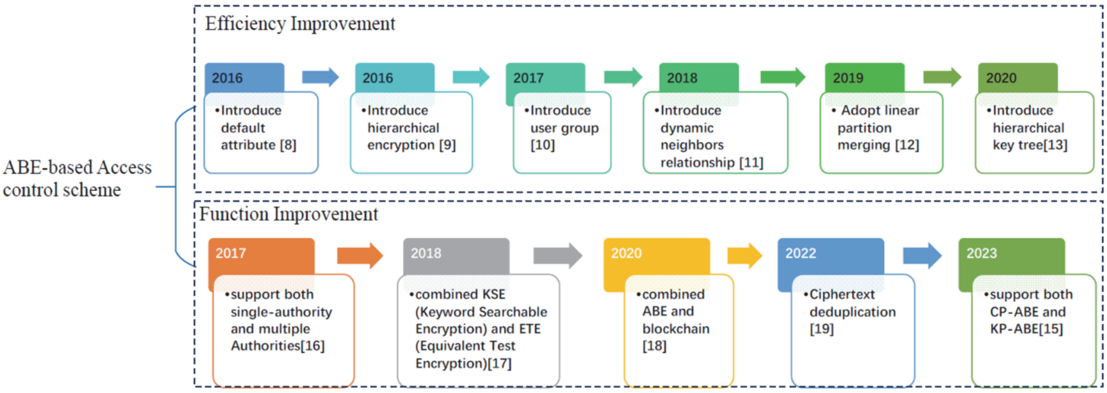

ABE-based Access control scheme
Efficiency Improvement
2016
•Introduce default attribute [8]
2016
•Introduce hierarchical encryption [9]
2017
•Introduce user group [10]
2018
•Introduce dynamic neighbors relationship [11]
2019
• Adopt linear partition merging [12]
2020
•Introduce hierarchical key tree[13]
Function Improvement
2017
•support both single-authority and multiple Authorities[16]
2018
•combined KSE (Keyword Searchable Encryption) and ETE (Equivalent Test Encryption)[17]
2020
•combined ABE and blockchain [18]
2022
•Ciphertext deduplication [19]
2023
•support both CP-ABE and KP-ABE[15]

Figure 3 The recent progress on improvement of ABE-based access control schemes

Table 1 Comparison of ABE schemes over NDN in efficiency improvement

	Year	Key features	Advantages	Disadvantages	EncryptionCost	DecryptionCost
[8]	2016	✓ Introduce default attribute	✓ Fast key generation	✓ Inefficient when attributes join in frequently	$(N_{en}+1)C_{ex}$	$C_{pair}+N_{attr}C_{ex}$
[9]	2016	✓ Use symmetric encryption algorithm to encrypt data and then encrypt the symmetric key using ABE	✓ Efficient en/decryption	✓ Users may share symmetric keys without being detected	$(3N_{en}+4)C_{ex}$	$2N_{attr}C_{pair}$
[10]	2017	✓ Introduce publisher group; ✓ Revoke permission by defining a unique attribute for each user or setting an expiration attribute.	✓ The number of keys is decreased to be linear with group members; ✓ The number of names registered on FIBs was reduced.	✓ Requires group management, especially maintain the group attribute list	Be linear with N_{en}	Be linear with $\|L_G\|$
[12]	2019	✓ Split the content into PCS and CKS; ✓ Encrypt CKS using CP-ABE; ✓ Establish a filtering mechanism to revoke permission by refreshing CKS.	✓ Fasten/decryption ✓ An attribute could be revoked without re-encryption.	✓ The publisher server must be online to provide the CKS for users.	Be linear with N_{en}	Be linear with N_{attr}
[13]	2020	✓ Hierarchical naming mechanism; ✓ Hierarchical key tree mechanism.	✓ Users was allowed to derive keys locally; ✓ The distribution efficiency was speeded up.	✓ Higher time in en/decryption ✓ Higher length in ciphertext	$(2N_{en}+2)C_{ex}$	Be linear with nN_{attr}

3.1.2 Function Improvement of ABE-Based Access Control Schemes

Some access control schemes were designed with other functions taken into account. For example, similar to [9], Zhang et al. [14] designed an NDN access control scheme (called NAC-ABE) for structured named data of military network by using a mixture of CP-ABE and symmetric cryptography, achieving the requirements of fine-grained access control and intermittent connection. However, Dulal et al. [15] observed that traditional NAC-ABE [14] is constructed based on CP-ABE, which requires knowledge of the access policy before data encryption operation. Therefore, they improved the NAC-ABE [14] by adding a component to the public parameters to support both CP-ABE and KP-ABE. Borgh et al.[16] proposed two schemes: SA-CP-ABE and MA-CP-ABE, with the former supporting a single-authority and the latter supporting multiple Authorities. Wang et al. [17] corresponded the attributes in ABE with the relevant parts of NDN, and combined KSE (Keyword Searchable Encryption) and ETE (Equivalent Test Encryption) to protect privacy. Lei et al. [18] combined ABE and blockchain to record users' registration, authorization, access, revocation and feedback to malicious publishers as transactions on the chain. A user published a register transaction carrying his own public key and a request packet ID. A publisher then released an authorization transaction including the access control policy. Then, the user published an access transaction to prove his access privilege, and a consensus mechanism was used to verify the user's privilege. If the verification succeeded, the access transaction was recorded on the blockchain and finally the publisher sent the requested resource to users. In addition, the work [18] found that the amount of calculation and storage of ABE was much smaller than that of the blockchain when dealing with the combination of ABE and the blockchain. Xue et al. [19] proposed a Secure Content Delivery and Deduplication scheme, called SCD2, in which the ciphertext uploaded onto routers can be conducted deduplication to decrease the storage cost on NDN routers.

3.2 IBE-Based and PRE-Based Access Control in NDN

The most existing NDN data access control schemes use IBE (Identity-Based Encryption) as its cryptographic primitive. IBE can be combined with PRE (Proxy Re-Encryption) to enable publishers to authorize users directly and reduce the computational overhead on the subscriber side by completing the proxy re-encryption on the border router. However, this method requires publishers to manage the permissions of each user while publishing and encrypting each content. It not only needs to maintain the user ID list, but also costs a lot of storage, computing, and communication on the publisher side. Therefore, it is only suitable for large commercial service providers such as IQiyi and Netflix. Proxy re-encryption can perform the authorization on the proxy node, reducing the terminal computation. Using the proxy re-encryption method, the content is encrypted twice with different encryption keys. The first encryption runs on the content provider to protect the confidentiality of the data. The second encryption runs on the proxy node and re-encrypts the ciphertext using an authorized re-encryption key. The user can request different re-encryption keys when accessing different contents. This approach requires the publisher to be online all the time in order to generate re-encryption keys for subscribers at all times. The development timeline of the IBE-based access control schemes is shown in Fig. 4. Tab. 2 shows the comparison of IBE and PRE-based schemes.

3.2.1 Development Timeline of IBE-Based Access Control Schemes

Fotiou et al. [20] presented a delegation-based access control. However, their work does not work in large-scale scene. Hamdane et al. [21] introduced an identity-based access control system in NDN through hierarchical tree-assisted content naming. Although the work [21] can be applied to a large-scale scene, it is not convenient to control access to specific users. Li et al. [22] proposed a lightweight integrity verification (LIVE) architecture to address seamlessly the universal content signature verification and allows a content provider to control content access in NDN nodes by selectively distributing integrity verification tokens. Fan et al. [23] adopted the re-encryption method. However, they allowed all users the right to decrypt any encrypted content in NDN. In the work [23], a user node and a forwarding node cannot switch their roles. To achieve the change of roles, Tseng et al. [24] presented an access control scheme called FGAC-NDN, which supports potential receivers and mobility. However, each router must perform a re-encryption operation for each forwarding. The FGAC-NDN allows an encrypted content to be accessed by a specific user and potential receivers simultaneously.

Consider the timeliness of data access control, He et al. [25] designed a signature algorithm to limit user access times, and edge routers were designed to filter illegitimate requests. In addition, they improved efficiency using the hash chain. This idea was also adopted in another paper, such as Xue et al. [26]. The work [26] used the hash chain to reduce the cost of continuous requests for the same file. Xue et al. [26] set an edge-based ICN access control framework named SEAF to solve the problems of high computing overhead and high delay caused by a router or a service provider when verifying user requests. The framework authenticated at the edge of the network and adopted a group signature to achieve anonymous authentication.

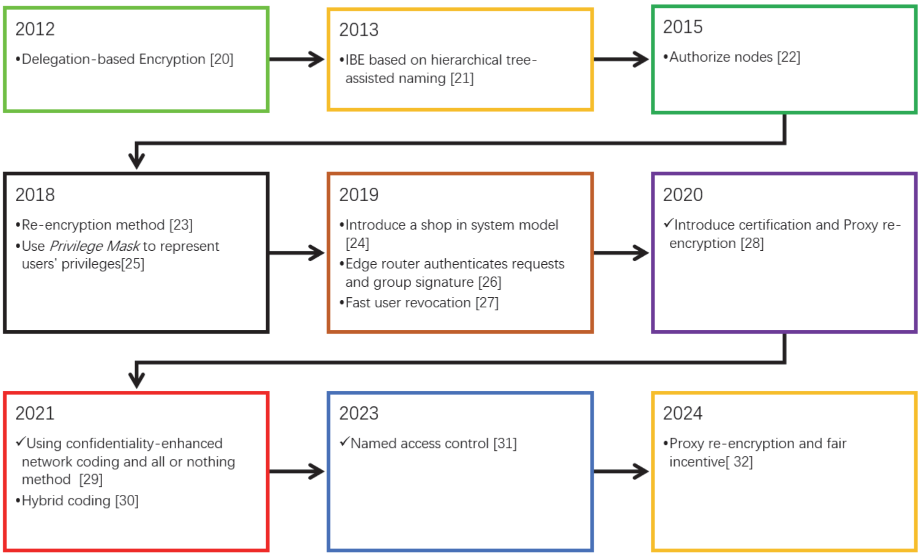

2012
•Delegation-based Encryption [20]
2013
•IBE based on hierarchical tree-assisted naming [21]
2015
•Authorize nodes [22]
2018
•Re-encryption method [23]
•Use *Privilege Mask* to represent users' privileges[25]
2019
•Introduce a shop in system model [24]
•Edge router authenticates requests and group signature [26]
•Fast user revocation [27]
2020
✓Introduce certification and Proxy re-encryption [28]
2021
✓Using confidentiality-enhanced network coding and all or nothing method [29]
•Hybrid coding [30]
2023
✓Named access control [31]
2024
•Proxy re-encryption and fair incentive[32]

Figure 4 The development timeline of IBE-based access control schemes

Misra et al. [27] proposed the AccConF scheme, which first used the symmetric encryption algorithm to encrypt the plain text, and then used the Shamir threshold secret sharing method to encrypt the symmetric key. Specifically, a secret share was allocated to each legitimate user, and the server stored one of t shares. When users needed to decrypt a content, legitimate users could use their shares and the server's t shares to decrypt it, while nonauthorized users could not decrypt due to the lack of share. When a user is revoked, the server replaces one of t shares by the revoked user's share, so that the user could scrape up t+1 shares, and thus his share became invalid. This method belonged to direct revocation. After the revocation, other users could still use the original private key to decrypt, and the ciphertext did not need to be re-encrypted under forward security and backward security. However, the latest ciphertext permission control block was required to flood every ciphertext copy as soon as possible, the server was required to be always online, and the revocation granularity was the user.

Table 2 Comparison of IBE and PRE-based schemes

	Year	Key features	Advantages	Disadvantages
[20]	2012	✓ Delegation-based Encryption	✓ Lightweight	✓ Not suitable for large-scale scene
[21]	2013	✓ Identity-based Encryption based on hierarchical tree-assisted naming	✓ Suitable for large-scale scene	✓ Not convenient to control access to specific users
[22]	2015	✓ Change tokens by cps to revoke content caching ✓ Lightweight content security policy enforcement	✓ Lightweight ✓ Efficient revocation	✓ Need to maintain a list of all identities of nodes ✓ Consider nodes are authorized or not, regardless users
[23]	2018	✓ Re-encryption	✓ Save the significant storage costs on nodes ✓ The producer does not have to always be online	✓ Allow all users the right to decrypt any encrypted content
[25]	2018	✓ Use *Privilege Mask* to represent users' privileges ✓ Edge router authenticates users' requests	✓ Only access the specific content with limited times ✓ Easy to revoke a user ✓ Lightweight	✓ Need to maintain users' information on producer ✓ The producer needs to be online ✓ Need to upgrade border routers to support authentication
[24]	2019	✓ Introduce a shop in system model	✓ suitable for digital content industry scenario ✓ Lightweight	✓ Can not resist the collusion between online shop and customers
[26]	2019	✓ Edge router authenticates requests ✓ Group signature ✓ Use hash chain to reduce cost	✓ Efficient revocation ✓ Keep users anonymous to the edge routers	✓ Need to maintain users' group information on producer ✓ Need to upgrade border routers to support authentication
[27]	2019	✓ Use symmetric encryption to encrypt data and use *shamir threshold secret sharing method* to encrypt the symmetric key	✓ Efficient user revocation or joining	✓ Control block was required to flood as soon as possible ✓ Limited number of users ✓ Server needs to be always online
[28]	2020	✓ Proxy re-encryption ✓ Introduce certification	✓ Fast direct revocation	✓ Need to maintain pseudonym certificates ✓ Server needs to be online
[29]	2021	✓ Confidentiality-enhanced network coding ✓ All or nothing method	✓ Efficient system	✓ Server needs to be always online
[30]	2023	✓ Named access control ✓ Hierarchical encryption ✓ Blockchain	✓ Naming management, access control and access policy management are considered as a whole	✓ Need to balance between granularity and consumption because temporal hierarchy is related to encryption's granularity
[31]	2024	✓ Fair incentive distribution ✓ Proxy re-encryption ✓ Group signature	✓ Achieve anonymity, access control, traceability and non-frameability simultaneously	✓ Conditional privacy ✓ Need to manage groups ✓ Edge nodes are assumed to be trusted

In order to deliver content confidentially in vehicle NDN with the features of continuous disruptions and topology changes, Jiang et al. [28] analyzed the phenomenon that content providers could not access control content because their content can be cached anywhere. They proposed an access control scheme named ESAC, which also supports a lightweight integrity verification by allowing content providers to issue integrity verification tokens selectively to authorized nodes to achieve the content access control. The content was stored in ciphertexts and the key was stored in a private token that the content provider issued to authorized users. Unauthorized users got public tokens that could not decrypt the content. The content provider generated two tokens for each content, one for the router and another for the user. The router used the token to authenticate the content. If it failed, it would not be cached. Also, the ESAC used proxy re-encryption when the provider was offline. Their ESACdealed with privacy-preserving access control and enabled periodic update and revocation operations using a proxy re-encryption method. However, the end device needs to maintain pseudonym certificates with the aid of a key distribution center. To avoid maintenance certificates, Wu et al. [29] designed ACET, an access control scheme specifically for edge networks using confidentiality-enhanced network coding. The application of the all or nothing method makes the system efficient. However, the work [29] requires that publishers be online at all times.

Similarly to the work [29], Tan et al. [32] also adopted the code method to realize the data access control. Unlike the work [29], Tan et al. [32] combined multiple encoding operations and presented a hybrid coding scheme, which perform better in terms of security and flexibility.

Li et al. [30] introduced an access control framework named NACDA, which enables dataproducer to share their data autonomously by customizing access policies. Specifically, the named-based access control model provides encryption and access control schemes.

Jiang et al. [31] presented RFIP-VEC, a revocable access control scheme with Fair Incentive for Privacy-aware content delivery in VEC (Vehicular Edge Computing), in which proxy re-encryption methods and a two-layer access control framework were designed.

Similar to Tseng et al. [24], the work [31] also requires that each edge router must be involved in each forwarding.

3.2.2 Function Improvement of Edge Routers in IBE-Based Access Control Schemes

Many studies use edge routers to do some of the extra work. Li et al. [22] decided whether to cache contents by verifying them on the edge router. Xue et al. [26] used a blacklist to revoke user permissions on the edge of the network. Agyekum et al. [33] used the edge router to undertake the computing work of proxy servers. They combined IBE and proxy re-encryption to realize the ciphertext sharing on legitimate users using edge routers as proxy servers to deal with emergency calculation. The proxy servers adopted ICN to exchange content data to improve the utilization rate of network bandwidth and quality of service, and blockchain was adopted to decentralize data storage and access control. In the research of Hlaing et al. [34], contents were only protected and authorized to authorized consumers when they were cached and forwarded on the edge router. Therefore, they can control the access duration on the edge router. Their scheme was presented by combining symmetric encryption and identity-based proxy re-encryption. Tab. 3 summarizes functions of the border router.

Table 3 Summary of functions of the border router

Publication	Year	Functions of the border router
Li [22]	2015	Decides whether to cache contents by verifying them.
Xue et al. [26]	2019	Maintains a blacklist to revoke user permissions.
Agyekum et al. [33]	2021	Undertakes the computing work of proxy servers.
Hlaing et al. [34]	2021	Controls the access duration on the edge router.

3.2.3 Function Improvement of IBE-Based Access Control Schemes

Many studies have implemented other functions as well as access control. Luo et al. [35] proposed an access control scheme that supports traceability based on IBE in view of the decoupling feature between content data, content providers and users, caused by NDN cache. Wang et al. [36] designed a proxy re-encryption scheme to reduce the computational cost on the client side and also prevent collusion attacks. Jiang et al. [11] adopted the encryption name obfuscation method to realize access control of Interest, and applied the proxy re-encryption method to realize permission revocation. However, the time spent on encryption, decryption, and signature verification increases linearly with the number of content packets. Jiang et al. [28] realized the protection of data confidentiality, access control and permission revocation of illegal vehicles in VNDN by the proxy re-encryption method, and used anonymous and IBS (Identity-Based Signature) to ensure anonymous authentication and content integrity. The specific process was that the provider used proxy re-encryption to generate an encrypted content, and then sent the encrypted content and its signature to the vehicles, and issued corresponding pseudonyms and keys to these subscriber vehicles. Then, a vehicle sent an Interest request and got the matched content from some vehicle. The vehicle then decrypted the content with an authorized key and paid an incentive for hitting the cache.

As a unique study, Tan et al. [32] divided and encoded the original content into encoded data blocks using linear and nonlinear methods, and then generated a set of decoding information for these encoded blocks. When a user sends out an Interest, the provider issues the user with decoding privilege information. The user can then decode these encoded blocks. The point is each user can obtain a unique decoding information, which can be used to trace someone efficiently.

3.3 NDN Access Control Based on Other Cryptographic Primitives

3.3.1 NDN Access Control Based on Public-Key Cryptography

Public-key encryption requires a publisher to encrypt contents using a public key of each user, which costs a lot of key management. More importantly, the same content is released to different users in different secret statuses, thus losing the advantage of NDN cache.

Hamdane et al. [37] divided access privileges into reading privilege and writing privilege, and divided the environments into the closed environment and the open environment. In the closed environment, the identity of the authorized entity was known beforehand, so managers were able to define the privilege of each entity in advance and then used the public key encryption algorithm to encrypt a content decryption key for a reader, and encrypt a content-encryption key and a content-decryption key for a writer. In the open environment, the entity privilege could not be defined in advance. They set restrictions for each privilege. Each user added specified restrictions to the search keywords and then determined whether the user had privileges based on the restrictions in the user keywords. Zhang et al. [14] employed tree-structured NDN naming rules to implement access control and implemented the prototype of the named access control scheme based on RSA. Rezende et al. [38] proposed a fast convergent certificate status query method to shorten the retrieval response time when the traditional public key infrastructure was applied to ICN. This method supports users to verify the validity of certificates before verifying data and can be widely used in various key management systems. Their work is still based on OCSP (the online certificate status protocol), which is currently used on the Internet.

Mannes et al. [4] combined public-key cryptography with proxy re-encryption to implement data security protection. A publisher encrypted a content using his public key. When the user accessed the content, an interest packet carrying search keywords was sent to request the re-encryption key. After checking the user's permissions, the publisher generated a re-encryption key, attached it to the ciphertext, constructed them as a packet, and sent back to the user. The user then could use his own private key and re-encryption key to decrypt the ciphertext. This method can ensure that the same content is published to each user in the same secret status and retains the advantage of the NDN cache to improve network performance. Fan [39] proposed a hierarchical structure naming method to specify the access control policy for Spatio-temporal data, which allowed the data owner to specify a subset of Spatio-temporal data according to the user's demand, aiming to address the privacy protection problems caused by Spatio-temporal mobile data sharing in health monitoring and driving behavior tracking scenarios. However, after the publisher uses the symmetric key CK with Spatio-temporal granularity to encrypt the data, one-to-one public-key encryption is still used for CK, that is, the manager issues the public-key KEK corresponding to the subscriber's authorized private key KDK for encryption, and only authorized users can deduce the decryption key. Compared to Mannes et al. [4], this scheme does not have the advantage of the NDN in-network cache to improve the performance of the network. Dulal et al. [40] also found the disadvantage of [39] and use ABE to overcome it.

3.3.2 NDN Access Control Based on Broadcast Encryption

Few schemes use broadcast encryption. Although it has several advantages: efficient encryption and decryption, constant ciphertext, and private key, the length of the public key is linearly related to the number of authorized users. Although the length of the public key can be reduced to be $O\left(\sqrt{n}\right)$ in some schemes, they need to increase the length of the ciphertext to be $O\left(\sqrt{n}\right)$. Sultan et al. [41] proposed an access control scheme named NDN-RBE (Role-Based Encryption for NDN) using the broadcast encryption mechanism. Their scheme supports large-scale real-world content-centric services using the role inheritance property.

3.3.3 NDN Access Control Based on Access Control List

In the researches of NDN data access control scheme, there is not much literature based on ACL (Access Control List). Marxer et al. [42] believed that the derived data also conformed to content-based security protection methods. In this paper, the ACLs was merged to realize the permission inheritance of the derived data. Marxer et al. [43] organized the content into databases by time and space dimensions, and introduced a permission table in the content's metadata to realize the data permission inheritance. Similarly to the ACL method, Li et al. [44] proposed a mandatory content access control scheme called MCAC, which can control which router nodes can cache different contents by defining security labels for these contents.

Brief summary. The ACL method maintains a list of user IDs and permissions in the metadata. Thus, it is not suitable for scenarios where the number of users is large and is changing constantly.

4 DISCUSSIONS AND FUTURE DIRECTIONS

4.1 System Models of NDN Data Access Control Schemes

The construction of system model is the first step to do research. This section gives a discussion of the system model and future directions.

4.1.1 Discussions About System Models

NDN does not specify how to design an efficient cryptographic protocol [17]. NDN does not depend on PKI nor provides trust management [45]. NDN allows publishers to embed their own security-related control information into content packets and uses names to discover, forward, and receive content data. In this system model, content packets are duplicated by routers many times, and the information and location of content packets are decoupled, which making permission management and change more difficult. There are no business relationships between routers and content owners, which is making it more difficult to protect unauthorized access to content packets. Therefore, NDN has many unexpected factors: 1) the identity of the consumer is unpredictable for the publisher; 2) the location of the cached data is unpredictable; 3) the location of the latest copy of data is unpredictable [46]. Zhang et al. [47] summarized the security mechanism under the NDN architecture. NDN not only changes the network communication model but also leads to a new framework of network security, namely, the direct implementation of data security.

The system models and security assumptions of typical NDN data access authority schemes are shown in Tab. 4.

Main Challenges. Unpredictable consumer identity, unknown data location, and irrelation between routers and producers make data access control more challenging. In addition, the function allocation of each entity in the system model varies in each application scenario.

4.1.2 Future Directions of System Models

One possibility should be considered: NDN router goes from being semi-trusted to being selfish. Semi-trusted means a router is faithful but curious about the data. Selfish means that the router may have been taken over by an attacker, not only disrupting data confidentiality, but also redesigning the router's execution path to achieve its own goals.

Unlike TCP/IP, in which the application layer caches content and realizes access control, NDN allows routers to cache and forward contents. Therefore, it is necessary to make possible extensions to the NDN network layer to achieve permission control. Many researchers assumed that the NDN router was semi-trust. That is, it is assumed that routers should always hope that the packet is not tampered with or forged, which is only reasonable for NDN network service providers who pay attention to their own reputation. Compared to the semi-trusted cloud server in the cloud scene, some NDN routers have malicious or negative assumptions. For example, routers are selfish, do not follow the cache exit rules when caching content, or provide stale content. It assumes that the cloud server is faithful but curious about data contents in a cloud environment, while routers in the NDN cannot all be assumed to be semi-trusted sometimes. Thus, the system model of the NDN access control scheme is different from that of cloud access control. In addition, access rights should be inherited when contents are aggregated or derived. Therefore, a new system model needs to be constructed.

When the hierarchical encryption system model is applied, key abuse should be avoided. Most schemes adopt the hierarchical encryption method to improve efficiency. That is, the content data is encrypted using a symmetric encryption algorithm first to ensure the confidentiality of the data, and then the symmetric encryption key is encrypted to realize the access control using ABE, IBE, proxy re-encryption, etc. This hierarchical encryption method aims to make full use of the high efficiency of the symmetric encryption algorithm and the fine granularity and flexibility of permission control. However, the security of the hierarchical encryption method is established on the assumption that an authorized user will not share the symmetric key. But in fact, the user is willing to share the symmetric key among his friends as long as it does not harm their own interests. Also, legitimate users get the symmetric keys in copy to illegal users at the same time, not leaving any information to be traced back.

Table 4 The system model and security assumptions of typical NDN data access schemes

Schemes	CryptoPrimitive	System Model		Security Assumptions
		Entities	Functions	
Misra et al. [27]	• IBE	Content Provider	• Issue users' key; • Generate and encrypt content; • Generate ciphertext privilege control block;	• CP is trusted; • An authorized user does not save the key after decryption; • Users do not hide locations;
		CDN、ISP node	• Cache and forward content	
		User	• Request and decrypt content	
Agyekum et al. [33]	• IBE • PRE	Owner	• Generate and encrypt content; • Generate re-encryption key;	• Blockchain is trusted; • The data owner is trusted; • Proxy server semi-trusted; • Cloud server semi-trusted; • Users don't share their IDs;
		Proxy server	• Cache, forward and re-encrypt content	
		Cloud server	• Store content and provide download service;	
		Blockchain	• Authorize user's ID as his private key;	
		User	• Request and decrypt content	
Xue et al. [26]	• IBE • MAC	Content Provider	• Generate and encrypt content; • Pay for ISP; • Authorize users	• CP is trusted; • ISP is a large enterprise that pays attention to reputation. It is rational, curious and greedy; • Users is untrusted;
		ISP	• Cache and forward content; • Verify users' identity;	
		User	• Request and decrypt content	
Bilal et al. [48]	• IBE • Key Derivation	Subscribe Manager	• Issue user's private key	• Subscribe Management is trusted; • Publisher is trusted; • Users don't share their IDs;
		Publisher	• Generate and encrypt content; • Issue a seed for content encryption key;	
		Subscriber	• Request content; • Derive key from a seed; • Decrypt content;	
		NDN router	• Cache and forward content;	
Chen et al. [13]	• CP-ABE • Key Derivation	IoT edge network	• Generate content;	• Server is trusted; • Gateway is semi-trusted;
		Gateway	• Maintain local edge network; • Issue content key for local device; • Construct hierarchical key tree HKT;	
		Server	• Maintain global security parameters;	
		Router node	• Cache and forward content;	
		User	• Derive key according HKT; • Request and decrypt content	
Wu et al. [12]	• CP-ABE • Hash table	Publisher	• Maintain user's register list; • Issue user's id and his private key; • Split and encrypt content;	• Publisher is trusted; • Router is faithful;

4.2 Lightweight Methods in NDN Data Access Control Schemes

4.2.1 Discussions about Lightweight Methods

NDN needs to compromise the security and efficiency of the data access control scheme. There are many parts to improving efficiency. For example, signature verification is done on routers to prevent poison content, which also causes massive computation costs. As a result, when a user retrieves data, the data content is verified on every node or only on some specified node. In scenarios where information is frequently exchanged, the choice of validation nodes also directly determines whether a data security scheme is feasible. Currently, only PURSUIT (a variant of the ICN architecture) validates packets that come into and go out of the node on all passing nodes. That is, packet-level authentication is supported.

Most researches only select some nodes for data verification. Mick et al. [49] proposed a lightweight authentication and routing scheme in hierarchical NDN over the IoT. However, three types of nodes with different functional levels were specified in this environment and their topological structure was stable and unchanged. Furthermore, batch validation of cached content also required key issuing, which remained a daunting task in distributed systems such as IoT. Yang et al. [50] encoded the result of the decision of routing and forwarding into the cache control domain of content packets, came up with a caching mechanism for the source route and a lightweight caching strategy based on the popularity ranking of the content packets. Kim et al. [51] suggested the use of selective verification to reduce the overhead of content verification. Wang et al. [52] prevented the proliferation of bad data by verifying data on the edge router. Xue et al. [26] also verify data on the edge router in their proposed data access control framework SEAF. In addition, the SEAF adopted a group signature to achieve anonymous authentication. Hashing chain was used to reduce the cost of continuous requests for the same file.

Chen et al. [53] observed that, when all nodes cached a content packet responding to an Interest packet, repeated transmission of this content packet would lead to unnecessary communication overhead. He designed a content provider selection algorithm based on one-to-many matching. Hu et al. [54] observed that, when both request aggregation and multipath forwarding were adopted to improve network performance, packet access would fail unexpectedly, thus reapplying for data and consuming network resources. Liu et al. [55] introduced the metric value of node relay pressure to assist routing decisions, which saved energy consumption and reduced forwarding delay. However, Borgh et al. [16] found that the RAM size of the sensors was the main challenge compared to execution time, RAM usage, data overhead and battery consumption when ABE was deployed in a sensor network. Nguyen et al. [56] proposed a set of methods to monitor the status of NDN nodes to perform the monitoring of IFA (Interest flooding attack) and CPA (content poisoning attack) as soon as possible.

Some works improve system efficiency by blocking. Tan et al. [57] divided the content data into *N* blocks, encrypted the content through LNC (Linear Network Coding) and determined whether the user could decrypt the content data according to whether the user obtained the decryption matrix. To improve efficiency, most of the *N* blocks were taken as PCBS (public content block), which were pushed in advance and cached in the router, while a small part of the *N* blocks was taken as CKB (content key block), which was the identification of each authorized consumer. Only authorized consumers were able to combine a PCB and a correct CKB to complete decryption. Similarly to Tan et al. [57], Wu et al. [12] also divided a content into a public content block that could be precached in the router and a content key block bound with access permission. Only CP-ABE encryption was performed on the content key block that determines data recovery. The content key block was designed to be small in order to reduce the computational overhead of access permission verification. However, Wu et al. [12] needed to maintain user IDs and their hashes on the router. Xia et al. [58] also adopted the method of content distribution in advance to improve efficiency. However, the granularity of authority control was user group, and the authority was determined according to the number of the group. Ruidong et al. [59] built a many-to-many secure sharing scheme MWBS, which adopted the data distribution and retrieval method based on grouping, constructed a bidirectional tree through group initialization and addition, and created the root of the bidirectional tree using designated forwarding and cache nodes. Compared to the existing CCN and PURSUIT, MWBS reduces the cost of control grouping and state storage.

Some works reduce computing cost on the user side. Wang et al. [36] proposed a proxy re-encryption scheme in ICN, which reduced the computation cost on the user side and prevented collusion attacks further more. Misra et al. [27] completed most of the calculation of the Lagrange coefficient on the server side, so as to reduce the calculation on the user side. Bilal et al. [48, 60] raised a content secure distribution scheme SDPC, in which the publisher generated a unique key seed for each content, so that subscribers could deduce their decryption keys according to the seed and reduced the cost of key issuing. As an example of NDN and a hot study spot, VNDN means that NDN is used as the network architecture for data exchange on the Internet of vehicles [61].

We summarize the computation cost on the decryption end in VNDN shown as Tab. 5 wherein C_{FHE} denotes the computation cost of an FHE (Fully Homomorphic Encryption) decryption algorithm. n_D denotes the number of data packets received by a node.

Main Challenges. It is challenging to design a suitable access control scheme that balances efficiency, security, scalability, flexibility, and other characteristics when ensuring the authenticity of messages and authorized access in the special scenario of decoupling publishers, routers, and consumers in NDN through signatures and encryption.

4.2.2 Future Directions of Lightweight Methods

There are three future directions for improving the efficiency of the system. On the publisher's side, blocking content and AONT (all-or-nothing) technology can reduce the computation of encryption. Inside the NDN network, nodes selecting method of data verification, content provider selecting method, request packet aggregation method can reduce computation and communication with the promise that packets are transmitted correctly. On the subscriber's side, the proxy re-encryption method can decrease the decryption computation. Besides, key derivation method can decrease the storage cost on the subscriber's side.

Table 5 Comparison of the decryption end in VNDN

Schemes	Decryption cost on user	Methods used in the schemes	Goals of the schemes
Sun et al. [62]	$(2N_{attr}+1)\cdot C_{pair}+N_{attr}\cdot C_{ex}+C_{FHE}$	• CP-ABE, • FHE, • Blockchain	Data sharing, Ciphertext computation, Correctness checking
Jiang et al. [28]	$(3n_D+3)\cdot C_{pair}+C_{ex}$	• CP-ABE, • Proxy re-encryption, • Identify-based signature, • Blockchain	Secure content delivery with lowering the overhead
Agyekum et al. [33]	$2C_{pair}$	• IBE, • Proxy re-encryption， • Blockchain	Data sharing, Lightweight decryption
Qin et al. [63]	C_{ex} (Off-chain)	• ABE， • Proxy re-encryption, • Blockchain, • Incentive mechanism	Data sharing, Lightweight decryption, Avoid endorsement whenever possible

The group-based method can be adopted to lighten a lot of work. In the group-based method, subscribers can be grouped, nodes can be grouped, and keys can be grouped. Users in the same group use the same key, so the key management overhead is related to the number of groups, not the number of users. Obviously, the number of groups is often smaller than the number of users, so introducing groups can reduce the overhead of key management. For example, Ruidong et al. [59] introduces the concept of user groups to improve key management efficiency. Then they constructed a bidirectional tree with the root as the designated forwarding and cache node, and proposed a multi-level inter-regional routing method. According to the bidirectional tree, named integrated forwarding was adopted, which supported group-based content distribution and retrieval. This grouping method requires adding group initialization, joining and leaving group members, and so on. So, it has both advantages and disadvantages. However, in any case, the grouping method can achieve a compromise between security and efficiency.

4.3 Trust Root Deployment Methods in NDN Data Access Control Schemes

4.3.1 Discussions about Trust Root Deployment Methods

NDN is a decentralized network architecture that cannot specify a trust root such as the deployment authorization center for entities with fixed addresses. It is challenging to deploy public-key infrastructure in NDN, especially maintain key management, content access control, authentication, and cache authorization in high-mobility scenarios [64].

At present, there are several representative trust root deployment methods: SDN designation [65], setting local trust anchor point [66], credit mutual evaluation [67], and suspension chain [68]. Wang et al. [17] applied ABE and SDN technologies in NDN, and the deployment of trust roots can be realized in the control layer of SDN. Li et al. [66] designed a secure login protocol SSP in the smart home environment. The protocol is based on NDN and does not use cloud services. Each home IoT system is assigned a local trust anchor with a unique name. To log securely onto the system and provide secure follow-up communication, the newly added device has two certificates: the local trust anchor's certificate and its own certificate specified by the local trust anchor. The local trust anchor authenticates other devices using passwords and its own certificate authenticates other device identities. SSP supports NDN-based resource-constrained devices. Ramani et al. [67] proposed a task-oriented fast trust establishment method based on request-response communication, enabling vehicles to make short-term trust decisions quickly to publish, use and process data safely. The fast trust model is a master trust one, in which each node calculates its trust value based on its interaction with its neighbors or service providers. This work is based on the observation of the phenomenon of short and low probability of vehicle encounters in the urban Internet of vehicle environments. Ruidong et al. [68] believed that NDN was a new method to solve the demand for big data for secure and efficient data retrieval. Big data was stored in the intermediate physical entity IPE, and users could retrieve the published data from the latest copy, so there were uncertainties among users, IPE, copy owners, and publishers. Based on the trust based on certificate authorization and trust-based on neighbors, this machine adopted the hanging chain trust model SCM to realize the arbitrary identity authentication of the user, IPE, and publisher without accessing the server. This mechanism can not only prevent malicious users from IFA, but can also prevent the cache and provision of false data.

There are also studies that use out-of-band approaches to build trust. Zhang et al. [69] proposed an NDN trust management mechanism (NDNCERT), which established trust through the out-of-band method, designed security requirements in a modular way, and supported delegation trust between certificates on a single device or across devices. Once a node obtained a valid certificate for the namespace, the node automatically became the certificate authority for the namespace and could use the same NDNCERT protocol to generate certificates for its sub-namespace. Pesavento et al. [70] extends the NDNCERT protocol by supporting proof-of-possession, which simplifies the integration of the onboarding process of a newly joined device with the various other security mechanisms.

Main Challenges. In the loosely coupled environment of NDN, it is difficult to propose a universal method for specifying or electing trust roots in the case of unknown identities, and it needs to be designed specifically according to the specific application environment.

4.3.2 Future Directions of Trust Root Deployment Methods

The current representative trust root deployment method cannot still work perfectly in NDN when designing an integrated scheme of content access control, authentication, cache authorization, and key management in high-speed mobile scenarios, such as VNDN.

SDN (Software Defined Network) may bring a new system model to NDN. With the introduction of software definition, a trust root can be deployed in the control layer of SDN and access control can also be realized by programming on a smart home router. For example, Xu et al. [71] constructed a smart home system with a new intelligent programmable family router. The router not only had the core functions of a router, such as caching, PIT, and FIB, but also had the functions of security monitoring, cooperative caching, the proxy signature for the resource-constrained IoT scenario, and so on. Data access control can be perfromed on the intelligent programmable home router.

4.4 Revocation Methods in NDN Data Access Control Schemes

4.4.1 Discussions about Revocation Methods

Permission revocation is also an important consideration in the design of an NDN data access control scheme. There are two revocation methods: indirect revocation and direct revocation. The former is to update the ciphertexts related to a revoked user's private key and the private keys of other users related to the ciphertexts. The latter is to set a user's private key to be invalid without processing ciphertexts or other users' keys. According to the time of revocation, it is divided into two types:

immediate revocation and delayed revocation. The former revokes permission immediately, and the latter does not complete the revocation until certain conditions are met. We compare various revocation methods in Tab. 6.

Silva et al. [10] proposed two revocation methods. One was to add a unique attribute representing the user in the user attribute set. The method only needed to update the ciphertext policy without re-issuing other users' keys. Another method was to revoke a user by setting the time attribute. This method was needed to maintain the registration time of all users, and users at the same registration time could be revoked at the same time. Misra et al. [27] replaced the server-side share with the user share in the ciphertext permission control block to revoke users. This method realized direct revocation on the premise of ensuring forward security and backward security without re-encrypting ciphertexts or re-issuing keys. The signature was generated using a one-way hash function, and the validation token was generated using a Merkle hash tree. The token was generated by the network node according to the policy specified by the content provider; therefore, its access was controlled by the content provider. When a token is used as a basis for permission control, revoking user permissions requires the content provider to regenerate the token for the content. The token is associated with the content, unless the content provider issues the same token to different users. However, if the token of the same content issues the same token to different users, there is a collision attack problem. From this perspective, token-based access control schemes can be classified into IBE.

In terms of control granularity, IBE, proxy re-encryption, public-key encryption, and ACL only support user revocation. Only ABE supports more fine-grained attribute revocation. In terms of difficulty, although ACL (such as Xue et al. [26]) is easy to realize. However, its scalability is poor and white or black lists are vulnerable to attacks. In terms of the time to complete the revocation, Wu et al. [12] and Misra et al. [27] need to the flood permission control block as soon as possible.

Main Challenges. In an environment like NDN where the number and location of data replicas are uncertain, if user permission revocation is used directly, it requires a flooding permission control block, which incurs a significant communication cost. If indirect revocation is used, it is necessary to promptly prohibit the revocation of user access without affecting the normal access of other users to the ciphertext. This requires calculating and flooding the ciphertext and redistributing the keys of other users, which will incur significant computational and communication costs.

4.4.2 Future Directions of Revocation Methods

Assured revocation and Consistency immediate revocation are difficult in NDN scene. The challenge of achieving assured revocation is that we have to trust NDN routers to actually revoke someone's privilege, but they may be reluctant to do it, because it still takes a certain amount of computing to do it. Consistency immediate revocation is a challenge because a content may be stored on many routers and it is difficult for these copies to immediately update their permissions, especially when using ABE for access control.

4.5 Other Future Directions

4.5.1 Proposition of the Key Management Mechanism

Whether to encrypt or authorize first will matter with key management. Encrypting first and then authorizing needs to define the key beforehand, and the key management is tedious [43]. ABE and IBE methods can realize authorization first and then encryption. However, if an ID representing user permissions is bound in a ciphertext permission control block, such as proxy re-encryption, the key management is still tedious. Chen et al. [13] and Bilal et al. [48] took advantage of the key-derivation method to reduce the cost of key management. Until now, most studies tend to adopt cryptographic methods to protect the security of NDN data, therefore the key management mechanism is very important. However, there are few studies on the key management mechanism for NDN such as decentralized network model.

Table 6 Comparison of various revocation methods

Schemes	Revocation methods	Granularity	Advantages/disadvantages
Silva et al. [10]	Define a unique attribute for each user	User	It can realize *immediate and direct revocation*; It's like adding IBE to ABE.
	Set an expiration attribute	Attribute	It is simple to realize; A user cannot be revoked until the attribute expired.
Wu et al. [12]	Revoke permission by refreshing CKS (part of content)	Attribute	It can revoke an attribute without re-encryption most of a content; The latest CKS block needs to be flood as soon as possible; Content needs to be chunked in advance.
Misra et al. [27]	Server replaces one of t shares to cause a user to fail decryption due to lack of secret share	User	It can realize *direct revocation* The latest ciphertext block needs to be flood to each copy as soon as possible; The number of revoked users must be less then t; Server was required to be always online.
Xue et al.[26]	Maintain a black list to revoke user at the edge of the network.	User	It can realize *immediate and direct revocation*; It is not be suitable for scenarios where the number of users is large and is changing constantly.

4.5.2 Privacy Protection for Both Publisher and Subscriber

Considering privacy protection, NDN networks do not require users to mark their IDs in the Interest packets. Most researches on the NDN access control focus on the security and efficiency of access control, but there are few research schemes on the privacy protection of the publisher's identity, location, and subscriber's subscription behavior. In addition, the research of blockchain to solve the trust relationship between different entities and privacy protection is still open. For example, the user must be anonymous for privacy protection, which leads to the use of transaction broadcasts that cause a large number of bandwidth consumption. There are many researches that focus on privacy protection in other scenes, such as [72-77]. However, data security and privacy protection adds additional inefficiency to the system [78, 79], especially those that share multi-dimensional data securely [80-82]. Some studies consider context or data structures, such as 3 and 4 [83, 84]. Tensor techniques can be used to reduce overhead [85, 86].

5 CONCLUSIONS

This paper reviews the latest research progress on encryption-based NDN access control schemes. We classify them into the following types according to cryptographic primitives: the ABE-based, the IBE-based and proxy re-encryption, the public-key encryption, ACL and others. We summarize these schemes in terms of security, efficiency, flexibility, and scalability. We achieve the following conclusion based on our analysis:

It is clear that most researchers consider ABE and IBE as possible approaches to realize encryption-based access control in NDN.

We observe that a suitable encryption-based NDN access control scheme requires: 1) Lightweight, fine-grained access control and large-scale applications are difficult to balance. 2) Efficient revocation often incurs overhead for list maintenance, group maintenance or certificate maintenance. 3) The function and security assumptions of border routers are the biggest differences in the design of access control schemes by various researchers.

We find the challenges, faced by encryption-based NDN access control, include system model, lightweight method, trust root deployment, permission revocation. And we also describe the future directions during deploying of access control in NDN.

Acknowledgements

This work was supported by the National Science Foundation of China [No.62062045, No.62341206, No.61962029, No.62462054].

7 REFERENCES

[1] NDN-project-team. NDN Technical Report NDN-0001. URL: https://named-data.net/publications/techreports/

[2] NDN-project-team. NDN Testbed. URL: https://named-data.net/ndn-testbed/

[3] Asaf, K., Rehman, R. A., & Kim, B. S. (2020). Blockchain technology in Named Data Networks: A detailed survey. *Journal of Network and Computer Applications, 171*, 1-15. https://doi.org/10.1016/j.jnca.2020.102840

[4] Mannes, E., Maziero, C., Lassance, L., & Borges, F. A. (2015). Optimized access control enforcement over encrypted content in information-centric networks. 2015 *IEEE 20th ISCC*, 924-929. https://doi.org/10.1109/ISCC.2015.7405632

[5] Nour, B., Khelifi, H., Hussain, R., Mastorakis, S., & Moungla, H. (2021). Access Control Mechanisms in Named Data Networks: A Comprehensive Survey. *ACM Computing Surveys (CSUR), 54*(3), 1-35. https://doi.org/10.1145/3442150

[6] Nashrul Hakiem, S. H. A. Y. S. H. S. A. M. R. S. Z. (2024). Security and Privacy Policy Assessment in Mobile Health Applications: A Literature Review. *Journal of System and Management Sciences, 14*(2). https://doi.org/10.33168/jsms.2024.0222

[7] Mirabelli, G. & Solina, V. (2021). Blockchain-based solutions for agri-food supply chains: a survey. *International Journal of Simulation Modelling, 17*(1), 1-15. https://doi.org/10.1504/IJSPM.2021.120838

[8] Wang, J. & Lang, B. (2016). An efficient KP-ABE scheme for content protection in Information-Centric Networking. 2016 *IEEE ISCC*, 830-837. https://doi.org/10.1109/ISCC.2016.7543839

[9] Bing, L., Dijiang, H., Zhijie, W., & Yan, Z. (2016). Attribute-based Access Control for ICN Naming Scheme. *IEEE Transactions on Dependable and Secure Computing, 15*(2), 194-206. https://doi.org/10.1109/TDSC.2016.2550437

[10] Silva, R. H. D., Cordeiro, W. L. D. C., & Gaspary, L. P. (2017). A scalable approach for managing access control in Information Centric Networks. 2017 *IFIP/IEEE IM*, 89-97. https://doi.org/10.23919/INM.2017.7987268

[11] Jiang, S., Liu, J., Wang, L., & Fang, Y. (2018). A Secure Data Forwarding Scheme in Vehicular Named Data Networking. 2018 *IEEE GLOBECOM* 206-212. https://doi.org/10.1109/GLOCOM.2018.8647216

[12] Wu, Z., Xu, E., Liu, L., & Yue, M. (2019). CHTDS: A CP-ABE Access Control Scheme Based on Hash Table and Data Segmentation in NDN. 2019 *18th IEEE TrustCom/BigDataSE*, 843-848. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00122

[13] Chen, B., Liu, L., & Ma, H. (2020). HAC: Enable High Efficient Access Control for Information-Centric Internet of Things. *IEEE Internet of Things Journal, 7*(10), 10347-10360. https://doi.org/10.1109/JIOT.2020.2989361

[14] Zhang, Z., Yu, Y., Ramani, S. K., Afanasyev, A., & Zhang, L. (2018). NAC: Automating Access Control via Named Data. 2018 *IEEE MILCOM*, 626-633. https://doi.org/10.1109/MILCOM.2018.8599774

[15] Dulal, S., Yu, T., Liu, S., Thieme, A. R., Zhang, L., & Wang, L. (2023). Enhancing NAC-ABE to Support Access Control for mHealth Applications and Beyond. *arXiv preprint arXiv:2311.07299*.

[16] Borgh, J., Ngai, E., Ohlman, B., & Malik, A. M. (2017). Employing attribute-based encryption in systems with resource constrained devices in an information-centric networking context. 2017 *IEEE Global Internet of Things Summit(GIoTS)*, 1-6. https://doi.org/10.1109/GIOTS.2017.8016277

[17] Wang, L., Zhang, Z., Dong, M., Wang, L., Cao, Z., & Yang, Y. (2018). Securing Named Data Networking: Attribute-Based Encryption and Beyond. *IEEE Communications Magazine, 56* (11), 76-81. https://doi.org/10.1109/MCOM.2018.1701123

[18] Lei, K., Fang, J., Zhang, Q., Lou, J., Du, M., Huang, J., Wang, J., & Xu, K. (2020). Blockchain-based cache poisoning security protection and privacy-aware access

control in NDN vehicular edge computing networks. *Journal of Grid Computing, 18*(4), 593-613. https://doi.org/10.1007/s10723-020-09531-1

[19] Xue, K., He, P., Yang, J., Xia, Q., & Wei, D. S. (2022). SCD2: Secure Content Delivery and Deduplication With Multiple Content Providers in Information Centric Networking. *IEEE/ACM Transactions on Networking, 30*(4), 1849-1864. https://doi.org/10.1109/TNET.2022.3155110

[20] Fotiou, N., Marias, G. F., & Polyzos, G. C. (2012). Access control enforcement delegation for information-centric networking architectures. 2012 *Proceedings of the second edition of the ICN workshop on Information-centric networking*, 85-90. https://doi.org/10.1145/2377677.2377773

[21] Hamdane, B., Serhrouchni, A., & El Fatmi, S. G. (2013). Access control enforcement in Named Data Networking. 2013 *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013, March 23, 2013 - March 25, 2013*, 576-581. https://doi.org/10.1109/ICITST.2013.6750268

[22] Li, Q., Zhang, X., Zheng, Q., Sandhu, R., & Fu, X. (2015). LIVE: Lightweight integrity verification and content access control for named data networking. *IEEE Transactions on Information Forensics and Security, 10*(2), 308-320. https://doi.org/10.1109/TIFS.2014.2365742

[23] Fan, C. I., Chen, I. T., Cheng, C. K., Huang, J. J., & Chen, W. T. (2018). FTP-NDN: File Transfer Protocol Based on Re-Encryption for Named Data Network Supporting Nondesignated Receivers. *IEEE Systems Journal, 12*(1), 473-484. https://doi.org/10.1109/JSYST.2016.2580299

[24] Tseng, Y. F., Fan, C. I., & Wu, C. Y. (2019). FGAC-NDN: Fine-Grained Access Control for Named Data Networks. *IEEE Transactions on Network and Service Management, 16*(1), 143-152. https://doi.org/10.1109/TNSM.2018.2864330

[25] He, P., Wan, Y., Xia, Q., Li, S., Hong, J., & Xue, K. (2018). LASA: Lightweight, Auditable and Secure Access Control in ICN with Limitation of Access Times. 2018 *2018 IEEE International Conference on Communications (ICC)*, 1-6. https://doi.org/10.1109/ICC.2018.8422829

[26] Xue, K., He, P., Zhang, X., Xia, Q., Wei, D. S. L., Yue, H., & Wu, F. (2019). A Secure, Efficient, and Accountable Edge-Based Access Control Framework for Information Centric Networks. *IEEE/ACM Transactions on Networking, 2*(3), 1220-1233. https://doi.org/10.1109/TNET.2019.2914189

[27] Misra, S., Tourani, R., Natividad, F., Mick, T., Majd, N. E., & Huang, H. (2019). AccConF: An Access Control Framework for Leveraging In-Network Cached Data in the ICN-Enabled Wireless Edge. *IEEE Transactions on Dependable and Secure Computing, 16*(1), 5-17. https://doi.org/10.1109/TDSC.2017.2672991

[28] Jiang, S., Liu, J., Wang, L., Zhou, Y., & Fang, Y. (2020). ESAC: An Efficient and Secure Access Control Scheme in Vehicular Named Data Networking. *IEEE Transactions on Vehicular Technology, 69*(9), 10252-10263. https://doi.org/10.1109/TVT.2020.3004459

[29] Wu, D., Xu, Z., Chen, B., Zhang, Y., & Han, Z. (2021). Enforcing Access Control in Information-Centric Edge Networking. *IEEE Transactions on Communications, 69*(1), 353-364. https://doi.org/10.1109/TCOMM.2020.3026380

[30] Li, M., Xue, J., Wang, Y., Ma, R., & Huo, W. (2023). NACDA: Naming-Based Access Control and Decentralized Authorization for Secure Many-to-Many Data Sharing. *Electronics, 12* (7). https://doi.org/10.3390/electronics12071651

[31] Jiang, S., Li, J., Sang, G., Wu, H., & Zhou, Y. (2024). Vehicular Edge Computing Meets Cache: An Access Control Scheme With Fair Incentives for Privacy-Aware Content Delivery. *IEEE Transactions on Intelligent Transportation Systems*, 1-15. https://doi.org/10.1109/TITS.2024.3357522

[32] Tan, X., Wang, S., Ji, L., Tong, X., Zou, C., Zheng, Q., & Yang, J. (2021). Hybrid-Coding Based Content Access Control for Information-Centric Networking. *IEEE Transactions on Wireless Communications, 14* (8), 1-14. https://doi.org/10.1109/TWC.2023.3332930

[33] Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2021). A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. *IEEE Systems Journal, 16*, 1685-1696. https://doi.org/10.1109/jsyst.2021.3076759

[34] Htet Hlaing, H., Funamoto, Y., & Mambo, M. (2021). Secure Content Distribution with Access Control Enforcement in Named Data Networking. *Sensors, 21* (13), 1-21. https://doi.org/10.3390/s21134477

[35] Luo, J., Xu, G., He, C., & Jonckheere, E. (2018). Identity Based Approach Under a Unified Service Model for Secure Content Distribution in ICN. 2018 *1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 56-60. https://doi.org/10.1109/HOTICN.2018.8605958

[36] Wang, Q., Li, W., & Qin, Z. (2019). Proxy Re-Encryption in Access Control Framework of Information-Centric Networks. *IEEE Access, 7*, 48417-48429. https://doi.org/10.1109/ACCESS.2019.2908009

[37] Hamdane, B., Boussada, R., Elhdhili, M. E., & Fatmi, S. G. E. (2017). Towards a Secure Access to Content in Named Data Networking. 2017 *IEEE 26th WETICE*, 250-255. https://doi.org/10.1109/WETICE.2017.32

[38] Rezende, D., Maziero, C., & Mannes, E. (2018). A distributed online certificate status protocol for named data networks. 2018 *33rd Annual ACM SAC*, 2102-2108. https://doi.org/10.1145/3167132.3167358

[39] Fan, L. (2021). *Secure Sharing of Spatio-Temporal Data through Name-based Access Control*. M. S. thesis, University of Memphis Digital Commons, University of Memphis.

[40] Dulal, S., Ali, N., Thieme, A. R., Yu, T., Liu, S., Regmi, S., Zhang, L., & Wang, L. (2022). Building a secure mhealth data sharing infrastructure over NDN. 2022 *9th ACM ICN*, 114-124. https://doi.org/10.1145/3517212.3558091

[41] Sultan, N. H., Varadharajan, V., Dulal, S., Camtepe, S., & Nepal, S. (2024). NDN-RBE: An Accountable Privacy Aware Access Control Framework For NDN. *The Computer Journal, 67*(4), 1572-1589. https://doi.org/10.1093/comjnl/bxad083

[42] Marxer, C., Scherb, C., & Tschudin, C. (2016). Access-controlled in-network processing of named data. 2016 *3rd ACM-ICN*, 77-82. https://doi.org/10.1145/2984356.2984366

[43] Marxer, C. & Tschudin, C. (2017). Schematized access control for data cubes and trees. 2017 *4th ACM ICN* 170-175. https://doi.org/10.1145/3125719.3125736

[44] Li, Q., Sandhu, R., Zhang, X., & Xu, M. (2017). Mandatory Content Access Control for Privacy Protection in Information Centric Networks. *IEEE Transactions on Dependable and Secure Computing, 14*(5), 494-506. https://doi.org/10.1109/TDSC.2015.2494049

[45] NDN-project-team. NDN Protocol Design Principles.URL: https://named-data.net/project/ndn-design-principles/

[46] Li, R., Asaeda, H., & Li, J. (2017). A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT. *IEEE Internet of Things Journal, 4*(3), 791-803. https://doi.org/10.1109/JIOT.2017.2666799

[47] Zhang, Z., Yu, Y., Zhang, H., Newberry, E., Mastorakis, S., Li, Y., Afanasyev, A., & Zhang, L. (2018). An Overview of Security Support in Named Data Networking. *IEEE Communications Magazine, 56*(11), 62-68. https://doi.org/10.1109/MCOM.2018.1701147

[48] Bilal, M. & Pack, S. (2020). Secure Distribution of Protected Content in Information-Centric Networking. *IEEE Systems Journal, 14*(2), 1921-1932. https://doi.org/10.1109/JSYST.2019.2931813

[49] Mick, T., Tourani, R., & Misra, S. (2018). LASeR: Lightweight Authentication and Secured Routing for NDN

IoT in Smart Cities. *IEEE Internet of Things Journal, 5*(2), 755-764. https://doi.org/10.1109/JIOT.2017.2725238

[50] Yang, Q., Deng, H., Wang, L., & Sheng, Y. (2019). An Almost-zero Latency Lightweight Mechanism for Caching Decision in ICN Content Router. *IEEE 38th IPCCC*, 1-8. https://doi.org/10.1109/IPCCC47392.2019.8958774

[51] Kim, D. & Lee, J. (2019). Efficient and Secure Device Clustering for Networked Home Domains. *IEEE Transactions on Consumer Electronics, 65*(2), 224-232. https://doi.org/10.1109/TCE.2019.2902412

[52] Wang, Y., Qi, Z., & Liu, B. (2018). Preventing "bad" content dispersal in named data networking. *China Communications, 15*(6), 109-119. https://doi.org/10.1109/CC.2018.8398508

[53] Chen, C., Wang, C., Qiu, T., Lv, N., & Pei, Q. (2020). A Secure Content Sharing Scheme Based on Blockchain in Vehicular Named Data Networks. *IEEE Transactions on Industrial Informatics, 16*(5), 3278-3289. https://doi.org/10.1109/tii.2019.2954345

[54] Hu, X., Liu, X., Zhao, L., Gong, J., & Cheng, G. (2019). Enhancing interest forwarding for fast recovery from unanticipated data access failure in NDN. *China Communications, 16*(7), 120-130.3. https://doi.org/10.23919/JCC.2019.07.010

[55] Liu, H., Zhu, R., Wang, J., Xu, W., & Cui, J. (2021). Blockchain-Based Key Management and Green Routing Scheme for Vehicular Named Data Networking. *Security and Communication Networks,* 2021, 1-13. https://doi.org/10.1155/2021/3717702

[56] Nguyen, T., Mai, H., Doyen, G., Cogranne, R., Mallouli, W., Oca, E. M. d., & Festor, O. (2018). A Security Monitoring Plane for Named Data Networking Deployment. *IEEE Communications Magazine, 56*(11), 88-94. https://doi.org/10.1109/MCOM.2018.1701135

[57] Tan, X., Ji, L., Zhou, Z., & Yan, P. (2016). Copyright protection scheme for Information-Centric Networking base on the linear network coding. 2016 *35th CCC*, 6867-6872. https://doi.org/10.1109/ChiCC.2016.7554438

[58] Xia, Q., He, P., Xue, K., Han, J., Wei, D. S. L., Yue, H., & Qin, J. (2019). TSLS: Time Sensitive, Lightweight and Secure Access Control for Information Centric Networking. *IEEE GLOBECOM*, 1-6. https://doi.org/10.1109/GLOBECOM38437.2019.9014220

[59] Li, R. & Asaeda, H. (2020). MWBS: An Efficient Many-to-Many Wireless Big Data Delivery Scheme. *IEEE Transactions on Big Data, 6*(2), 233-247. https://doi.org/10.1109/TBDATA.2018.2878584

[60] Bilal, M., Kang, S. G., & Pack, S. (2018). Effective Caching for the Secure Content Distribution in Information-Centric Networking. 2018 *IEEE 87th VTC Spring*, 1-7. https://doi.org/10.1109/VTCSpring.2018.8417854

[61] Guo, X., Wang, B., Jiang, Y., Zhang, D., & Cao, L. (2023). Homomorphic encryption based privacy-aware intelligent forwarding mechanism for NDN-VANET. *Computer Science and Information Systems, 20*(1), 1-24. https://doi.org/10.2298/CSIS220210051G

[62] Sun, S., Du, R., & Chen, S. (2021). A secure and computable blockchainbased data sharing scheme in iot system. *Information (Switzerland), 12*(2), 1-20. https://doi.org/10.3390/info12020047

[63] Qin, X., Huang, Y., Yang, Z., & Li, X. (2021). LBAC: A lightweight blockchain-based access control scheme for the internet of things. *Information Sciences, 554*, 222-235. https://doi.org/10.1016/j.ins.2020.12.035

[64] Khelifi, H., Luo, S., Nour, B., Hussain, R., Moungla, H., Faheem, Y., & Ksentini, A. (2020). Named Data Networking in Vehicular Ad Hoc Networks: State-of-the-Art and Challenges. *IEEE Communications Surveys & Tutorials, 22*(1), 320-351. https://doi.org/10.1109/COMST.2019.2894816

[65] Kalafatidis, S., Demiroglou, V., Mamatas, L., & Tsaoussidis, V. (2022). Experimenting with an SDN-Based NDN Deployment over Wireless Mesh Networks. 2022 *IEEE INFOCOM Workshop CNERT 2022*, 1-6. https://doi.org/10.1109/INFOCOMWKSHPS54753.2022.9798224

[66] Li, Y., Zhang, Z., Wang, X., Lu, E., Zhang, D., & Zhang, L. (2019). A secure sign-on protocol for smart homes over named data networking. *IEEE Communications Magazine, 57*(7), 62-68. https://doi.org/10.1109/MCOM.2019.1800789

[67] Ramani, S. K. & Afanasyev, A. (2020). Rapid Establishment of Transient Trust for NDN-Based Vehicular Networks. 2020 *IEEE ICC Workshops 2020*, 1-6. https://doi.org/10.1109/ICCWorkshops49005.2020.9145253

[68] Li, R., Asaeda, H., & Wu, J. (2020). DCAuth: Data-Centric Authentication for Secure In-Network Big-Data Retrieval. *IEEE Transactions on Network Science and Engineering, 7*(1), 15-27. https://doi.org/10.1109/TNSE.2018.2872049

[69] Zhang, Z., Afanasyev, A., & Zhang, L. (2017). NDNCERT: Universal usable trust management for NDN. *4th ACM ICN*, 178-179. https://doi.org/10.1145/3125719.3132090

[70] Pesavento, D., Shi, J., McKay, K., & Benmohamed, L. (2022). PION: Password-based IoT onboarding over named data networking. *ICC*, 1070-1075.

[71] Xu, K., Wan, Y., & Xue, G. (2019). Powering Smart Homes with Information-Centric Networking. *IEEE Communications Magazine, 57*(6), 40-46. https://doi.org/10.1109/MCOM.2019.1800732

[72] Aslam, S. & Mrissa, M. (2023). A framework for privacy-aware and secure decentralized data storage. *Computer Science and Information Systems, 20*(3), 1235-1261. https://doi.org/10.2298/CSIS220110007A

[73] Gao, G., Wan, X., Yao, S., Cui, Z., Zhou, C., & Sun, X. (2017). Reversible data hiding with contrast enhancement and tamper localization for medical images. *Information Sciences, 385*, 250-265. https://doi.org/10.33168/jliss.2023.0412

[74] Cui, Z., Lu, Z., Yang, L. T., Yu, J., Chi, L., Xiao, Y., & Zhang, S. (2023). Privacy and accuracy for cloud-fog-edge collaborative driver-vehicle-road relation graphs. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2023.3254370

[75] Guclu, M. (2022). Multi-level security model developed to provide data privacy in distributed database systems. *Tehnički vjesnik, 29*(2), 369-378. https://doi.org/10.1007/978-3-642-22709-7_56

[76] Irwan Sembiring, D. M. S. D. S. S. (2023). Strengthening the Security and Privacy of National Identity Numbers (NINs) in Smart Contract Mechanisms through AES Encryption. *Journal of Logistics, Informatics and Service Science, 10*(4). https://doi.org/10.33168/JLISS.2023.0412

[77] Gao, G. & Jiang, G. (2015). Bessel-Fourier moment-based robust image zero-watermarking. *Multimedia Tools and Applications, 74*, 841-858. https://doi.org/10.1007/s11042-013-1701-8

[78] Nathanael Terencio, W. A. S. (2023). Enhancing MySQL Database Security with MySQL Enterprise Transparent Data Encryption. *Journal of Logistics, Informatics and Service Science, 10*(4). https://doi.org/10.33168/jliss.2023.0411

[79] Cui, Z., Wu, Z., Zhou, C., Gao, G., Yu, J., Zhao, Z., & Wu, B. (2016). An efficient subscription index for publication matching in the cloud. *Knowledge-Based Systems, 110*, 110-120. https://doi.org/10.1016/j.knosys.2016.07.017

[80] Mei, Z., Zhu, H., Cui, Z., Wu, Z., Peng, G., Wu, B., & Zhang, C. (2018). Executing multi-dimensional range query efficiently and flexibly over outsourced ciphertexts in the cloud. *Information Sciences, 432*, 79-96. https://doi.org/10.1016/j.ins.2017.11.065

[81] Mei, Z., Yu, J., Huang, J., Wu, B., Zhao, Z., Zhang, C., & Wu, Z. (2023). Enabling Access Control for Encrypted Multi-Dimensional Data in Cloud Computing through Range Search. *Tehnički vjesnik, 30*(6), 1704-1716. https://doi.org/10.17559/TV-20230415000536

[82] Qafesha, W., Kilani, Y. M., & Samawi, V. W. (2024). The Impact of Big Data Dimensions on the Performance of Jordan's Medical Sector: A Case Study of Al-Bashir Hospital. *Journal of System and Management Sciences, 14*(6), 424-440. https://doi.org/10.1080/08874417.2018.1496805

[83] Milosavljevic, G., Sladic, G., Milosavljevic, B., Zaric, M., Gostojic, S., & Slivka, J. (2018). Context-sensitive constraints for access control of business processes. *Computer Science and Information Systems, 15*(1), 1-30. https://doi.org/10.2298/CSIS160628037M

[84] Zheng, G., Hu, J., & Li, G. (2019). Simulation and analysis of user-side transaction technology for energy blockchain considering multi-chain structure. *International Journal of Simulation Modelling, 14*(6), 524-534. https://doi.org/10.1504/IJSPM.2019.106169

[85] Zhang, S., Yang, L. T., Zhang, Y., Lu, Z., & Cui, Z. (2022). Tensor-based forward-backward algorithms in physics-informed coupled hidden Markov model. *IEEE Transactions on Artificial Intelligence*. https://doi.org/10.1016/j.ins.2017.01.009

[86] Zhang, S., Yang, L. T., Zhang, Y., Lu, Z., Yu, J., & Cui, Z. (2023). Tensor-Based Baum–Welch Algorithms in Coupled Hidden Markov Model for Responsible Activity Prediction. *IEEE Transactions on Computational Social Systems*. https://doi.org/10.1109/TCSS.2022.3227458

Contact information:

Jiaoli SHI, Associate Professor, PhD
School of Computer and Big Data Science,
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: shijiaoli@whu.edu.cn

Xiaoping LIU, Associate Professor
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: liuxiaoping@jju.edu.cn

Anyuan DENG, Professor
School of Computer and Big Data Science,
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: dengay@jju.edu.cn

Xiangyu LIU, Undergraduate Student
School of Computer and Big Data Science,
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: 3154662492@qq.com

Zhuolin MEI, Lecturer, PhD
Jiujiang Key Laboratory of Cyberspace and Information Security,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: meizhuolin@126.com

Shunli ZHANG, Lecturer, PhD
QingHai Institute of Technology,
No. 2 Xiuyuan Street, Chengbei District, Xining 810016, China
E-mail: shunlizh@jju.edu.cn

Shimao YAO, Lecturer, PhD
(Corresponding author)
School of Computer and Big Data Science,
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: yaoshimao@kunsan.ac.kr

Xiancheng WANG, Lecturer, PhD
School of Computer and Big Data Science,
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: 195919323@qq.com

Liya XU, Lecturer, PhD
School of Computer and Big Data Science,
Jiujiang University,
No. 551, Qianjin East Road, Jiujiang, Jiangxi 332005, China
E-mail: xuliya603@whu.edu.cn

Kai HE, Lecturer, PhD
School of Computer Science and Artificial Intelligence,
Wuhan Textile University,
Wuhan 430073, China
E-mail: khe@wtu.edu.cn