Identity-based Secret Sharing Access Control Framework for Information-Centric Networking

1st Lianglang Deng
School of Communication and Information Engineering
Chongqing University of Posts and Telecommunications
Chongqing 400065, China
13452005463@163.com

2nd Jiangtao Luo
Electronic Information and Networking Research Institute,
Chongqing University of Posts and Telecommunications
Chongqing 400065, China
Luojt@cqupt.edu.cn

3rd Jie Zhou
School of Communication and Information Engineering
Chongqing University of Posts and Telecommunications
Chongqing 400065, China
S180101160@stu.cqupt.edu.cn

4th Junxia Wang
School of Communication and Information Engineering
Chongqing University of Posts and Telecommunications
Chongqing 400065, China
D170101010@stu.cqupt.edu.cn

***Abstract*—Information-centric networking (ICN) has played an increasingly important role in the next generation network design. However, to make better use of request-response communication mode in the ICN network, revoke user privileges more efficiently and protect user privacy more safely, an effective access control mechanism is needed. In this paper, we propose IBSS (identity-based secret sharing), which achieves efficient content distribution by using improved Shamir's secret sharing method. At the same time, collusion attacks are avoided by associating polynomials' degree with the number of users. When authenticating user identity and transmitting content, IBE and IBS are introduced to achieve more efficient and secure identity encryption. From the experimental results, the scheme only introduces an acceptable delay in file retrieval, and it can request follow-up content very efficiently.**

***Index Terms*—Information-centric networking, access control, secret sharing, IBE, IBS**

I. Introduction

Since the 1970s, the Internet with TCP / IP as its core technology has faced increasingly serious technical challenges. The previous network mainly satisfied the end-to-end data transmission between hosts through the exchange of data packets and exposed many problems in the aspects of network security, reliability, flexibility, and mobility. To completely solve these problems, two technical routes for the development of the future Internet have been formed: one is "progressive", that is, continuously improving and perfecting the existing IPv4 protocol, and finally smoothly transitioning to IPv6; the other is "revolutionary", namely redesigning Information-Centric Networking (ICN) or Content-Centric Networking (CCN) as an Internet architecture to meet future Internet development needs.

With the development of society, the video transmitted on the network has become high-definition, and the network equipment is also moving rapidly. Because of the advantages of the in-network cache, information-centric networking (ICN) has played an increasingly important role in the next generation of network architecture design. Most ICN/CCN architectures use a request-response approach to achieve content acquisition. These frameworks are naming the content blocks first, and then requesting the corresponding content through the name of interest package, which realizes the transformation from "where is the content" to "what is the content". Since the idea of information-centric network was put forward, many countries in the world have laid out a series of related research projects. Various ICN architectures have been proposed, such as DONA (Data-Oriented Network Architecture) [1], NDN (Named Data Networking) [2], PSIRP (Publish-Subscribe Internet Routing Paradigm) [3], NetInf (Network of Information) [4] and so on. Although ICN brings great convenience to intranet caching, it also introduces some new challenges. Access control is one of them.

In an ICN architecture, it allows data packets to be cached anywhere in the network. Due to the feature of in-network caching, ICN intermediate routers can cache the forwarded content, and future requests can be satisfied quickly from the cached duplicates, so the Content Producers (CPs) will lose

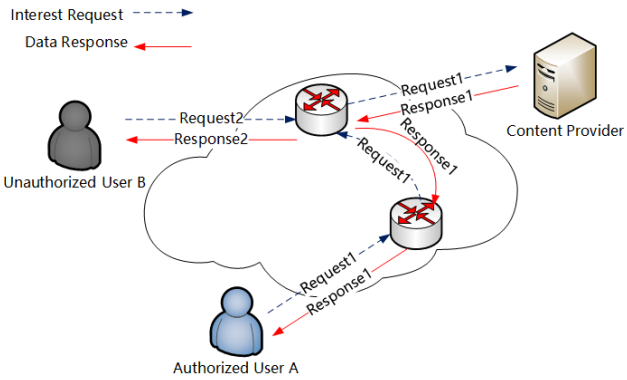

Fig. 1. The challenge of access control in ICN.

direct control over their content, which implies that access control must be built into content itself [5]. As shown in Fig 1, authorized user A sends its interest request to the content provider, and then during the response data was send back, the routers can cache these data. But the unauthorized user B can easily get the data blocks and reconstruct data if there is no access control strategy in ICN.

Therefore, new access control must be added to ICN to ensure that only legitimate users can access the content. In ICN's access control, how to verify the legitimacy of users, protect their privacy, and revoke the rights of expired users has become a problem we need to consider. In this paper, we use the characteristics of interest packages in ICN to introduce identity authentication into access control.

The remainder of this paper is organized as follows. Section II provides some related work about access control in ICN. Section III is devoted to the description of some methods exploited in our scheme. Section IV illustrates the proposed IBSS scheme. Section V provide security analysis and Section VI gives the performance evaluation. Section VII concludes this paper.

II. Related work

In recent years, more and more access control schemes have been proposed in ICN, some of which are also qualified with some other security properties. Generally speaking, however, these schemes fall into two categories.

The first is to introduce some encryption or decryption technologies into ICN access control. Based on Shamir's secret share, Misra et al. [6] proposed a definition of enabling block and introduced the secret sharing scheme to ICN, but they changed the original interest packages a lot. Zheng et al. [7] proposed a dual-phase encryption scheme, which combines one-time decryption key, proxy re-encryption and all-or-nothing transformation. [9], [10], [8] introduced ABE in network scenarios. These schemes aforementioned achieve access control by controlling users' decryption ability, but lack support for user revocation.

Another is to add control routers or control units to the network. Tao et al. [11] proposed a probability-based access control model for NDN, which is used by the intermediate routers to verify a user before forwarding the encrypted content. Li et al. [12] introduced user authentication into NDN routers. Users need to use capability and token to authenticate in NDN routers when they access CP (Content Provider). Those who fail to authenticate will not be able to enter the network. Although they resist DoS attacks, they impose a heavy burden on routers. Li et al. [13] also designed a light-weight signature and AC enforcement mechanism that uses per-content tokens, but this scheme is not very suitable for user revocation.

III. Preliminaries

A. Shamir's (t + 1, n)-threshold Secret Sharing Scheme

In this scheme, $t+1$ denotes the threshold, n denotes n users, and $t+1 \leq n$. A secret is divided into n shares, which can only be decrypted if at least $t+1$ user shares are combined. This scheme is implemented by an univariate t-degree polynomial $q_t(x)$=$a_0+a_1x+a_2x^2+\cdots+a_tx^t$, where $a_1 \cdots a_t$ is random numbers. In order to obtain secret a_0, it is necessary to take any $t+1$ shares $(x_i, q(x_i))$ on this polynomial. a_0 can be obtained by Lagrangian Interpolation Polynomial:

$$L_n(x) = f(x_0)\frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_n)}+ f(x_1)\frac{(x-x_0)(x-x_2)\cdots(x-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_n)}+\cdots+ f(x_n)\frac{(x-x_0)(x-x_1)\cdots(x-x_n)}{(x_n-x_0)(x_n-x_1)\cdots(x_n-x_{n-1})} \quad (1)$$

Note that $a_0 = L_n(0)$, and here we express the Lagrangian coefficients $\gamma_i = \prod_{0\leq j(\neq i)\leq n} \frac{x_j}{x_j-x_i}$. Hence we can get a_0:

$$a_0 = L_n(0) = f(x_0)\gamma_0 + f(x_1)\gamma_1 + \cdots + f(x_n)\gamma_n \quad (2)$$

B. DLP (Discrete Logarithm Problem) on Elliptic Curves

Obviously, q can be easily calculated through $q = g^k$ if k is known. However, it is difficult to find that k satisfies $q = g^k$ if q is known. This is the discrete logarithm problem (DLP). DLP also exists on elliptic curve: $Q = kP$ denotes the addition of k identical points P, i.e. $kP = P + P + \cdots + P$ (k times), where $Q, P \in GF_p(a, b)$, $k < P$ and $GF_p(a, b)$ is an elliptic curves group. Q can be easily calculated if k, P are known, but it's quite difficult to calculate k if we known Q and P.

C. Identity Based Cryptography

In IBC (Identity Based Cryptography), an arbitrary string, such as a user's name, address or their combinations, can be chosen as a public key and represents a unique identity unlike a traditional PKI system, which includes Identity Based Encryption (IBE) and Identity Based Signature (IBS). The corresponding secret key is generated by a private key generator (PKG) and a semi-trusted third party. Thus, neither does any pair of users need to exchange private or public keys to communicate securely, nor is a certificate authority (CA) indispensable to keep key directories.

The IBE scheme consists of the following four steps:

- **Setup**: The PKG generates a master-secret key (MSK) and system parameters (SP) when inputting a security parameter k. Only SP are made publicly available.
- **Extract**: The PKG generates a secret key SK_{ID} when inputting SP, MSK, and an identity ID.
- **Encryption**: Take as input an identity ID, a message M, and SP, and as output a ciphertext $M^{'}$.
- **Decryption**: Take as input $M^{'}$ and the corresponding SK_{ID} , and as output M.

The IBS scheme consists of the following four steps:

- **Setup & Extract**: The same as the first tow steps in IBE.
- **Encryption**: Take as input SP, M, and SK_{ID}, and as output the signature information σ that will be sent to the recipient with M together.

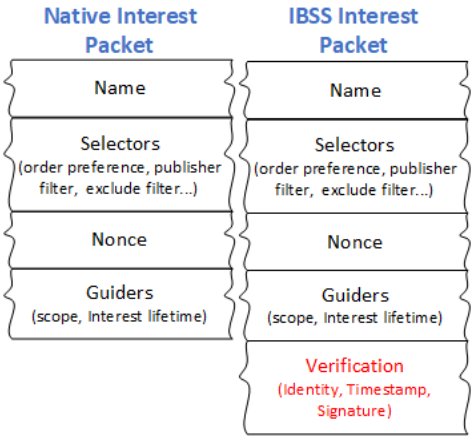

Fig. 2. New Interest Packet format in IBSS

- **Decryption**: Take as input SP, M, the corresponding ID, and σ, and as output V . Only if V is equal to 1, the signature is valid.

IV. Identity-Based Secret Sharing (IBSS)

To better solve the access control problem in ICN architecture and revoke outdated users more effectively, our scheme is presented below.

For the sake of determining the real identity of users and Content Provider (CP) in the network uniquely, user identity (UID) and CP identity (PID) are bound to their real social identities respectively. At the same time, UID and user's Secret Key (USK), PID, and CP's private secret key (PSK) constitute key pairs respectively.

A. Packet Format

To achieve the whole communication process, we extend the interest packages by adding *Verification* attributes, including the anonymous *Identity*, *Timestamp*, and *Signature*, so that they can carry the personal information of the requesting user. The new packet format is illustrated in Fig. 2, in which Timestamp that is unique for the same user in Interest Packet can prevent the malicious eavesdropper from using the legitimate requests. If an Interest packet with the duplicate Timestamp and Identity is transmitted to a CP, it can be regarded as a bogus request and dropped. Besides, Signature is generated using USK to verify the authenticity of the user further.

B. Procedure of IBSS

When encrypting identity information, consumer first encrypts CP's PID to form its *identity = IBE.encrypt (UID, PID)*. And then forms a *signature = IBS.sign((Name, Timestamp), USK)*. After receiving the interest package with users' identity, the CP first decrypts *UID = IBE.decrypt(identity, PSK)* with its own private key, and then verifies its identity through *IBS.verify(UID, signature)*, where *IBE.encrypt(·)*, *IBS.sign(·)*, *IBE.decrypt(·)*, *IBS.verify(·)* are the Identity-Based encryption, sign, decryption and verification operation respectively. Next the content encryption process is carried out.

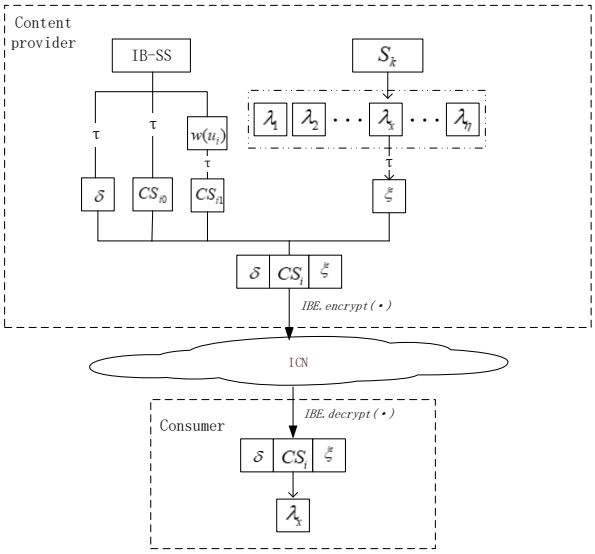

Fig. 3. How to distribute a data block S_k. CP first splits the content into small block, and then computes δ, CS_i and ξ. Through IBE encryption operation, the combination of them is transmitted to the consumer.

As shown in Fig. 3, for a large file S_k, it can be cut into smaller content blocks λ_η during transmission, i.e. $S_k = \lambda_1||\lambda_2||\cdots||\lambda_\eta$, where the symbol '||' means file connection. The encryption steps in our model are as follows:

Initialization: CP (Content Provider) first inputs the security parameters P, Q, k, where k denotes the degrees of polynomial and $P\&Q$ are large prime numbers, satisfying $P = rQ + 1$, in which r is a positive integer. Later, CP randomly generates a k-degree polynomial $q(x)$=$s + a_1x + a_2x^2 + \cdots + a_kx^k$, where $s, a_1, a_2 \cdots a_k \in Z_Q^*$, and Z_Q^* is Q-order integer multiplication group.

Generate user point: CP randomly selects k two-dimension plane points $(x_1, q(x_1)), (x_2, q(x_2)), \cdots, (x_k, q(x_k))$, in which $x_j (j = 1, 2, \cdots, k)$ are not equal to each other or zero.

Intermediate parameter: CP calculates intermediate parameter value:

$$w(u_i) = \sum_{j=1}^{k} \left[q(x_j)u_i/(u_i - x_j) \prod_{l=1, l\neq j}^{k} x_l/(x_l - x_j) \right] \quad (3)$$

and the corresponding intermediate parameter values are stored for each authorized user.

Complementary share (CS): $\tau \in Z_Q^*$, $(u_i, q(u_i))$ are random selected by CP, and then CP calculates $\xi_\eta = \lambda_\eta \cdot g^{\tau \cdot s}$, $\delta = \prod_{j=1}^{k} \frac{x_j}{x_j - u_i}$ and CS_i, in which CS_i concludes $CS_{i0} = g^{\tau \cdot q(u_i)}$ and $CS_{i1} = g^{\tau \cdot w(u_i)}$, where $\eta = (1, 2, \cdots, \mu)$, g is the generator of G_P's Q-order subgroup, and G_P is P-order cyclic group.

CS_i is constructed by CS_{i0} and CS_{i1}, and then CP encrypts the data $D_i = CS_i||\xi_\eta||\delta$ by using IBE, i.e. $CS_i^{'} = IBE.encrypt(UID, D_i)$, note that the *UID* has been verify at

the beginning. The consumer can decrypt the encrypted data through $D_i = IBE.decrypt(CS_i^{'}, USK)$. Finally, with the help of CS_{i0} and CS_{i1}, consumer can get λ_i:

$$\lambda_\eta = \frac{\xi_\eta}{CS_{i1} \cdot CS_{i0}^{\delta}} = \frac{\lambda_i \cdot g^{\tau \cdot s}}{g^{\tau \cdot w(u_i)} \cdot g^{\tau \cdot q(u_i) \cdot \delta}} = \lambda_i \quad (4)$$

The result λ_η is exactly λ_i before encryption. In which s can be precalculated like the under formula:

$$s = L_n(0) = w(u_i) + q(u_i) \cdot \delta \quad (5)$$

C. User revocation and addition

The addition and revocation of access privileges in IBSS scheme will not affect other legitimate users. When revoking a user u_x, the CP only needs to recalculate CS_i, $(i = 1, 2 \cdots m, i \neq x)$. If the user u_x requests CS_x, the CP will return a prompt message without CS_x. In addition, when adding a new user, the CP will generate new $(u, q(u))$ which must be not reused for other users, then calculate δ and $w(u)$ for it.

D. Data naming

In our scheme, a large secret share S_k cannot be distributed directly to the network, the CP will divide it into multiple smaller data blocks. To distinguish each secret share, the name of the Data package will contain the corresponding share information. At the same time, some illegal users cached copies of the dynamic shares locally before the rights were revoked. When the users were revoked and the dynamic shares were re-encrypted, such users obtained other secret shares through intermediate routers and reused them for data reconstruction with local dynamic shares. To prevent the aforementioned situation from happening, we can use a lightweight one-way hash function to generate the name of the secret share to improve its security.

When the revocation occurs, the CP generates a new CS_i, and then completes the re-encryption operation of the dynamic share to form a new $CS_i^{'}$, at the same time makes $str = CS_i^{'}$, and calculates the corresponding share name $O_{name}^{'}$:

$$O_{name}^{'} = H_0(O_{name}) = hash(O_{name} + str) \quad (6)$$

where O_{name} is the original name of data, $hash(\cdot)$ calculates the hash result of the input value.

For instance the data name "$/Alice/Movie/hello/V3/H_0(/hello/V3/B2/S12)/3.avi$ ", in which front of $H_0(\cdot)$ is the original movie information. $H_0(\cdot)$ represents the 12th secret share's alias in the 2nd block of the movie. $/3.avi$ means the sequence number of the smaller data block which the secret share is divided.

V. SECURITY ANALYSIS

A. Scalability

In the step 4 of previous IV-B, τ changes with different content objects, so when the same user accesses them, CP could calculate the corresponding CS_i quickly based on the intermediate parameter $w(u_i)$.

In the original Shamir method, $(u_i, q(u_i))$ is completely distributed to the corresponding authorized users, which is in danger of collusion to reconstruct s. But in IBSS, the users only get part of them. When adding a new user, CP is not limited by the degrees of polynomial. It can select an unused $(u_i, q(u_i))$ from the current polynomial and calculate δ. Once CP need to update secret values and polynomials, CP only needs to update $w(u_i)$ and $q(u_i)$, while δ held by existing authorized users does not need to be updated by CP. As a result, IBSS improves scalability. At the same time, once the authorized user obtains δ and requests different content objects, the CP can directly distribute the CS_i without encryption, thus completing efficient distribution of content.

B. Anonymity

This mechanism adds identity information to the Interest package and combines IBE and IBS methods to protect identity anonymously. On the one hand, it makes the identity information of the requesting user invisible to the third party, thus effectively protecting personal privacy. On the other hand, with the advantage of interest package structure, CP can verify the authenticity and reliability of the request by signature information and timestamp. IBE also can prevent D_i from being intercepted and δ from being used by malicious users.

C. Collusion resistance

In the original Shamir method, when the number of collusion users comes up to the threshold $k + 1$, the secret value can be calculated by reconstructing the interpolation theorem. But in this scheme, user only knows CS_i and δ, not holds $(u_i, q(u_i))$. When calculating τ and s, the collusion attack can be prevented because of the discrete logarithm problem (DLP).

D. Secure revocation

When a user lost the privilege to get data from content provider(CP), or the CP found a violating user, these users should be revoked efficiently. The CP only needs to calculate new CS_i, $(i = 1, 2 \cdots m, i \neq x)$. With the old δ and CS_i , the user can not calculate λ_i. Therefore, the scheme ensure revocation Security.

VI. PERFORMANCE EVALUATION

To demonstrate the feasibility of the proposed scheme for the NDN environment, we evaluate its efficiency, including the running time of generating shares and calculating CS_i, and compare the proportion of CS_i generation time in the whole process time in the testbed based on NFD testbed [14]. All simulation experiments are performed on the Ubuntu 16.04 with 4 GB RAM and a 4-core CPU. All the programs are written in the C++ language using the GNU Multiple Precision Arithmetic(GMP) library and Number Theory Library (NTL) for cryptographic operations.

In this paper, the IBSS algorithm is used to measure the overhead of computing share on the CP side and λ_i on the client-side. The degree of polynomials k increases from 100

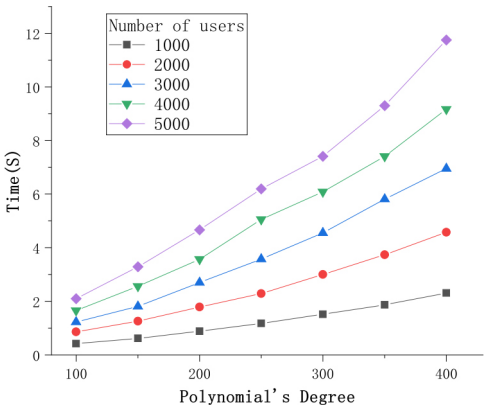

Fig. 4. The influence of user number and polynomial degree on time.

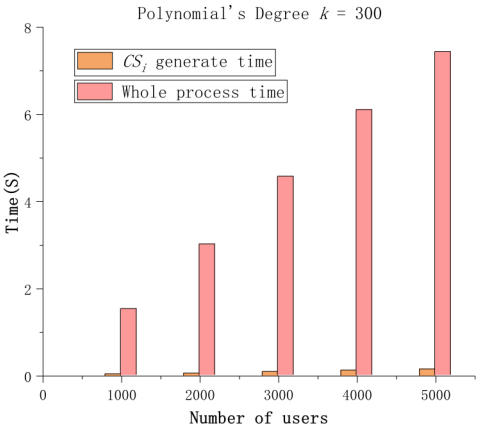

Fig. 5. The overhead comparison between CS_i generate time and whole process time

to 400, and users' quantity m increases from 1000 to 5000. All the data are the average of 100 experimental results.

Fig. 4 shows that execution time increases with k and m in computing δ and CS_i, especially when k is larger, the effect of m on execution time becomes greater. Although CP spends a lot of time calculating δ and CS_i, it can complete these processes offline. Besides, IBSS solves scalability and collusion problems. When consumers complete a content block request process, it contains a secret δ which can be used to request follow-up blocks instead of calculating δ every time. When CP needs to calculate a CS corresponding to content for authorized users, it only needs to calculate based on intermediate parameters $w(u_i)$. Therefore, without considering adding new users, CP only needs to execute step 4 of the IBSS algorithm, and then distribute CS_i directly to corresponding users.

However, for the calculation of CS, as shown in Fig. 5, it takes up a very small part of the whole time, and all other calculations have been done offline. When the authorized user requests the content from the CP again, the CP can complete the whole process with little computation. That is to say, our scheme introduces acceptable overhead, but greatly enhances the security of content transmission.

VII. Conclusion

We have proposed an efficient, lightweight, and secure enough access control scheme in ICN to solve the users' authorization, content encryption, and revocation problem. Our scheme also introduces Identity-Based Encryption into the process. When user decrypts δ with its USK, as the experimental result shows, next it can request follow-up content very efficiently because of the less time overhead in CS_i computing, which only introduces an acceptable delay in file retrieval.

References

[1] Koponen, T. , Chawla, M. , Chun, B. G. , Ermolinskiy, A. , & Stoica, I. (2007). A data-oriented (and beyond) network architecture. ACM SIGCOMM Computer Communication Review.

[2] Jacobson V, Smetters D K, Thornton J D, et al. Networking Named Content[J]. Communications of the ACM, 2012, 55(1):117-124.

[3] Vladimir Dimitrov, Ventzislav Koptchev. PSIRP project publish-subscribe Internet routing paradigm. New ideas for future Internet[C]// International Conference on Computer Systems & Technologies & Workshop for Ph.D. Students in Computing on International Conference on Computer Systems & Technologies. ACM, 2010.

[4] Christian Dannewitz, Dirk Kutscher, BRje Ohlman, Stephen Farrell, Bengt Ahlgren, and Holger Karl. 2013. Network of Information (NetInf) - An information-centric networking architecture. Comput. Commun. 36, 7 (April, 2013), 721735. DOI:https://doi.org/10.1016/j.comcom.2013.01.009

[5] X. Zhang, K. Chang, H. Xiong, Y. Wen, G. Shi and G. Wang, "Towards name-based trust and security for content-centric network," 2011 19th IEEE International Conference on Network Protocols, Vancouver, BC, 2011, pp. 1-6, doi: 10.1109/ICNP.2011.6089053.

[6] S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd and H. Huang, "AccConF: An Access Control Framework for Leveraging In-Network Cached Data in the ICN-Enabled Wireless Edge," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, pp. 5-17, 1 Jan.-Feb. 2019, doi: 10.1109/TDSC.2017.2672991.

[7] Q. Zheng, G. Wang, R. Ravindran and A. Azgin, "Achieving secure and scalable data access control in information-centric networking," 2015 IEEE International Conference on Communications (ICC), London, 2015, pp. 5367-5373, doi: 10.1109/ICC.2015.7249177.

[8] B. Li, D. Huang, Z. Wang and Y. Zhu, "Attribute-based Access Control for ICN Naming Scheme," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 2, pp. 194-206, 1 March-April 2018, doi: 10.1109/TDSC.2016.2550437.

[9] K. Xue, J. Hong, Y. Xue, D. S. L. Wei, N. Yu and P. Hong, "CABE: A New Comparable Attribute-Based Encryption Construction with 0-Encoding and 1-Encoding," in IEEE Transactions on Computers, vol. 66, no. 9, pp. 1491-1503, 1 Sept. 2017, doi: 10.1109/TC.2017.2693265.

[10] W. Li, K. Xue, Y. Xue and J. Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484-1496, 1 May 2016, doi: 10.1109/TPDS.2015.2448095.

[11] T. Chen, K. Lei and K. Xu, "An encryption and probability-based access control model for named data networking," 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC), Austin, TX, 2014, pp. 1-8, doi: 10.1109/PCCC.2014.7017100.

[12] Q. Li, P. P. C. Lee, P. Zhang, P. Su, L. He and K. Ren, "Capability-Based Security Enforcement in Named Data Networking," in IEEE/ACM Transactions on Networking, vol. 25, no. 5, pp. 2719-2730, Oct. 2017, doi: 10.1109/TNET.2017.2715822.

[13] Q. Li, X. Zhang, Q. Zheng, R. Sandhu and X. Fu, "LIVE: Lightweight Integrity Verification and Content Access Control for Named Data Networking," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 308-320, Feb. 2015, doi: 10.1109/TIFS.2014.2365742.

[14] A. Afanasyev, J. Shi, B. Zhang, L. Zhang, I. Moiseenko, Y. Yu, W. Shang, Y. Huang, J. P. Abraham, S. DiBenedetto, et al, "Nfd developers guide," Dept. Comput. Sci, Univ. California, Los Angeles, Los Angeles, CA, USA, Tech. Rep. NDN-0021, 2014.