Identity Based Approach Under a Unified Service Model for Secure Content Distribution in ICN*

Jiangtao Luo, Guoliang Xu, Chen He,
Electronic Information and Networking Research Institute
Chongqing University of Posts and Telecommunications
Chongqing 400065, China
{Luojt, xugl}@cqupt.edu.cn; 515308454@qq.com

Edmond Jonckheere
Department of Electrical Engineering
University of Southern California
CA 90089, US
jonckhee@usc.edu

Abstract—**Various schemes have been proposed for secure content delivery and access control in Information-Centric Networks (ICN). However, it is not trivial to compare their performances due to the lack of unified service model and consistent implementation methods. In this paper, a general service model merging publish-subscribe pattern with ICN framework is proposed to enable performance evaluation of different access control schemes or various implementations. In addition, an identity based hybrid approach under this model is designed and analyzed, in which the content to be delivered is encrypted using a symmetric secret key, which is then protected by an identity-based encryption scheme together with the license to play the content, and later distributed to consumers as requested. Finally, this approach and two existing schemes are implemented on a common cryptography library, and evaluated. Test results show that the proposed approach exhibits better performance and higher energy-efficiency in mobile terminals than those existing ones.**

Index Terms—**Information-Centric Networks, access control, identity-based cryptography.**

I. Introduction

SECURE content delivery plays a vital role in modern communication networks. For personal communications or business, the content can be privacy-protected conversations or banking transaction details. For video or social media websites, the content is the digital media protected by copyright laws, which can only be accessed by authorized subscribers. To ensure confidentiality when requesting transactions, the Internet provides secure connections technologies, such as HTTPS and TLS, to create reliable channels. In addition, Media sharing providers like YouTube and Netflix put digital rights management (DRM) technologies into service to protect the massive amount of movies and video clips available on servers. However, due to the inherent nature of the Internet, the efficiency of the operations and readiness of data availability have been criticized in massive content distribution for wasting a great amount of bandwidth to transfer identical contents.

In the past decade, Information-Centric Network (ICN) and its variants such as DONA [1], CCN/NDN [2] [3] were proposed and extensively researched as clean-slate design of future Internet. ICN defines many attractive features especially optimized towards scenarios of massive content distribution, including addressable Named Data Objects (NDOs), ubiquitous in-network storage, receiver-driven communication model, content-oriented security model, etc. [4].

However, ICN is also faced with new challenges especially in the access control of content and user authorization without predefined secure channel. Specifically, by leveraging in-network caches, it allows one to get content replications from closer routers rather than remote origin servers. Therefore, in order to prohibit unauthorized content access, the system is obliged to guarantee content confidentiality as well as authorize subscribed consumers for fine-grained access, which is more complicated than just providing a secure connection as in current Internet.

Previous work on access control in ICN can be generally classified into two categories, namely the *encryption-based* approach and the *content-based* one. The former is to provide end-to-end content security while the latter is to append new security features by means of both attributes of named Data themselves and features of the underlying ICN. As typical instances of the former, Zhang [5] proposed a hybrid scheme combining traditional public-key infrastructure (PKI) and identity-based signature/encrypt (IBS/IBE) to build name-based trust and security for content-centric networks. Later, Misra [6] presented a secure framework leveraging broadcast encryption (BE) algorithm and in-network caching. Recently, Wood [7] considered a hybrid encryption approach using the identity-based proxy re-encryption (IB-PRE) scheme to protect the symmetric key. More recently, as typical examples of the content-based approach, both the name-based access control mechanism proposed by [8] [9] and the attributes-based schemes presented by [10] [11] probed the naming convention to achieve data confidentiality as well as fine-grained access control.

Previous work is not satisfactory. First, terms and service models were not unified. Different terminologies were simultaneously used without clarified definition. Second, algorithms proposed in prior literature could hardly be compared with each other as they were usually implemented based on various cryptography libraries in different programming languages. This paper is intended to address such an issue.

The contributions of this paper can be summarized in two aspects. First, it presented a well-defined reference service model. Second, it proposed an identity-based hybrid access

The work was jointly supported by the Chongqing Municipal project under GRANT cstc2015jcyjBX0009 and CSTCKJCXLJRC20.

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

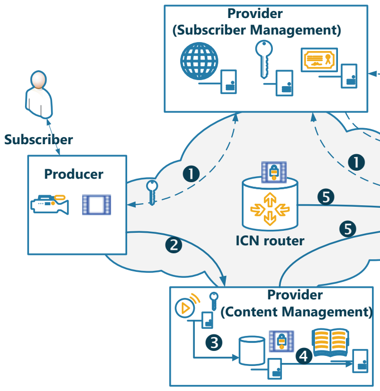

Fig. 1. The proposed service model and procedures.

control approach, and extended a common cryptography library in Python language to enable all identity-based approaches to be compared with each other.

The remainder of this paper is organized as follows: Section II presents our proposed reference service model and security approach. Section III demonstrates the analysis method, experimental setup, and results in comparison with other schemes. Finally, this paper concludes with a brief summary in Section IV.

II. Proposed Model and Approach

A. Reference Model

The proposed reference model is modified from the Microsoft PlayReady DRM Model [12] to be compatible with ICN terminologies [4], which is composed of four kinds of roles shown in Fig. 1.

- **Subscriber**. It refers to an individual who subscribes to the service by registering with a unique personal identity (e.g., email address or cell phone number) and signing a specific service agreement.
- **Producer**. It is the client program under the control of a subscriber, which produces and uploads the original content to the application platform.
- **Publisher** or **Provider**. It is the service provider that manages subscribers and contents. Its functions include managing registration, generating keys and licenses, compressing and publishing contents, etc, as shown separately in Fig. 1.
- **Requestor** or **Consumer**. It is the player program or web front-end that submits requests and retrieves content from the network. It also applies for specific license from the provider to play the content.

The steps of content publish and retrieval are numbered in Fig. 1. First, each subscriber registers to the publisher with its identity and is assigned a private key (step #1). Next, the producer creates and uploads the content with specified sharing policies (step #2). The publisher compresses and encrypts the received content by a secret key issued by a key server, which is later stored in the application storage (step #3). Then, the publisher releases the content on the web, which will be referred to by its content name (step #4). When a consumer finds the content, he can obtain it from either the original storage or in-network caches through the underlying ICN (step #5). Note that the content can be retrieved by anyone but cannot be played without the secret key and license. So, the consumer has to request for them from the publisher (step #6). The server will securely grant the consumer with the secret key and license which controls how to play the content after authenticating the identity of the consumer (step #7). Finally, with the proper key and license, the consumer can play the content (step #8).

B. Security Approach

The approach is to fulfil two objectives. One is to encrypt the content to be publicly distributed in ICN routers for anyone to get. The other is to deliver securely the corresponding key and license to specific consumers. We propose a hybrid approach, in which a symmetric cipher is used to encrypt the content, simple and fast, while a combination of IBS/IBE is used to protect the key and license, no need of keys exchange. The overall approach is called identity-based license encryption, denoted as *IBLE*.

The main algorithms in this approach are described as follows:

Setup. Given a security parameter, say sp, the publisher or provider generates a pair: $(params, msk) = Setup(sp)$, where $params$ and msk denote the public parameters and the master key, respectively. The publisher will keep the msk safely while it distributes $params$ to all subscribed consumers as they registered.

Extract. Given a pair of $(params, msk)$ and a set of identities, $ID_i \in \{0,1\}^*$, the provider, as the private key generator (PKG), generates the private keys by performing $sk_i =$ **IBE**.$extract(msk, params, ID_i)$, where $i = 0, 1, 2, \cdots N$. ID_0 and sk_0 are the identity and private key of the provider, whereas ID_i and sq_i $(i > 0)$ denote the identity and private key of Consumer i, respectively.

Content Encryption. Given a plain message, M, and a content key, k, the publisher performs a symmetric encryption and then obtain the ciphered message; that is $C = SymE(M, k)$.

Sign. Given the provider private key, sk_0, and the ciphered content to be transferred, the publisher invokes the **Sign** algorithm of *IBS* to produce the digital signature, namely $\sigma =$ **IBS**.$sign(sk_0, C)$.

License Encryption. Combining the content key, k, with the requesting subscriber's license L_i, the publisher forms a composite license, $k \oplus L_i$. Given the subscriber identity, ID_i, and the pair of $(params, msk)$, it invokes the *IBE* **Encryt** algorithm to yield the ciphered license, $CL_i =$ **IBE**.$encrypt(k \oplus L_i, ID_i, params)$.

Verification. The consumer verifies the origin of the received content by performing the **Verify** algorithm of *IBS*, denoted by **IBS**.$verify(ID_0, \sigma, C)$, using the provider's identity, ID_0.

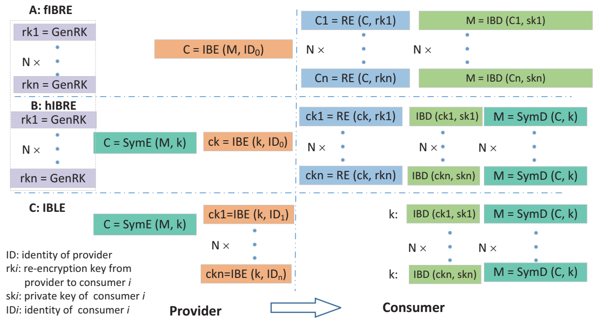

Fig. 2. Algorithms in each approach.

License Decryption. Given the private key, sk_i, and public parameters, $params$, the consumer gets out the composite license by invoking the *IBE* decryption algorithm, $k \oplus L_i =$ **IBE**$.decrypt(CL_i, params, sk_i)$ and then retrieves the content key, k, and the license, L_i.

Content Decryption. Given the content key, k, the consumer retrieves the original message by performing the symmetric decryption, $M = SymD(C, k)$.

Note that although user authentication is not the focus of this paper, it is indispensable to put this approach into practice. In some security-critical or privacy-sensitive scenarios, two-factor authentication mechanism and its improved schemes [13] [14] may be integrated with this approach, with smart cards storing the public parameters, personal information and security algorithms.

III. Evaluation

A. Different Approaches

For comparison, three different approaches of access control are analyzed and evaluated. 1) Approach A, called *full-IBRE* (abbr. *fIBRE*), is adopted from [7], in which the content is encrypted using publisher's identity; re-encrypt keys are issued for each subscriber; each consumer re-encrypts the content using the re-encrypt key, converting the encrypted content to what can be decrypted using the private key of corresponding subscriber. 2) Approach B is called *Half-IBRE*, denoted by *hIBRE*, in which the content is encrypted using a symmetric encryption algorithm with a content key protected by an *IB-PRE* method. 3) Approach C is the one proposed in this paper and described in Section II under the acronym *IBLE*, where the content is encrypted using a symmetric encryption algorithm, whereas the content key is encrypted using an IBE scheme rather than the IB-PRE one adopted in Approach B.

Consider the scenario where N subscribers request a content, M. The algorithms on both the provider and consumer sides are listed and compared in Fig. 2. The total running time of those algorithms was used as the metric.

In Approach A, the provider executes the **GenRK** algorithm N times to generate re-encryption keys for N subscribers and runs the **IBE** algorithm once on the content using its identity. Each consumer performs the **RE** algorithm, and the **IBD** algorithm on the encrypted content in sequence for getting the original one. Therefore, the total running time of this approach can be estimated by using $T_A = N \cdot \tau_{GenRK} + \tau_{IBE(M)} + N \cdot \tau_{RE(M)} + N \cdot \tau_{IBD(M)}$, where τ represents the one-shot execution time of the various algorithms, and (M) indicates that this algorithm is performed toward the message.

In Approach B, the provider runs the **SymE** algorithm once on the content using a symmetric key (k) and the **GenRK** algorithm N times, and then runs the **IBE** algorithm on the key using the identity of the provider. Each consumer executes the **RE** and **IBD** algorithms in sequence to retrieve the content key, and then finally runs the **SymD** algorithm to get the original content. Therefore, the total running time of this approach can be evaluated by using $T_B = N \cdot \tau_{GenRK} + \tau_{SymE(M)} + \tau_{IBE(k)} + N \cdot \tau_{RE(k)} + N \cdot \tau_{IBD(k)} + N \cdot \tau_{SymD(M)}$, where (k) indicates that this algorithm is performed toward the key.

In Approach C, the provider performs the **SymE** algorithm to the content using a symmetric key (k), and then runs the **IBE** algorithm N times on the key using different identities. Each consumer performs the **IBD** algorithm once to retrieve the content key, and then runs the **SymD** algorithm once to obtain the original content. Thus, the total running time of this approach can be evaluated by using $T_C = \tau_{SymE(M)} + N \cdot \tau_{IBE(k)} + N \cdot \tau_{IBD(k)} + N \cdot \tau_{SymD(M)}$.

For each approach, take the execution time per user (*ETPU*) as the metric, which is defined as the total running time divided by the number of consumers, denoted by E_x^y, where x denotes the approach index, $x \in \{A, B, C\}$; y denotes the provider or the consumer, $y \in \{P, U\}$. Based on the analysis mentioned above, E_x^P and E_x^U can be obtained as

$$E_x^P = \begin{cases} \tau_{GenRK} + \dfrac{\tau_{IBE(M)}}{N}, & \text{for } x = A \\ \tau_{GenRK} + \dfrac{\tau_{SymE(M)}}{N} + \dfrac{\tau_{IBE(k)}}{N}, & \text{for } x = B \\ \dfrac{\tau_{SymE(M)}}{N} + \tau_{IBE(k)}, & \text{for } x = C \end{cases}$$

$$E_x^U = \begin{cases} \tau_{RE(M)} + \tau_{IBD(M)}, & \text{for } x = A \\ \tau_{RE(k)} + \tau_{IBD(k)} + \tau_{SymD(M)}, & \text{for } x = B \\ \tau_{IBD(k)} + \tau_{SymD(M)}, & \text{for } x = C \end{cases}$$

Consumption of several algorithms is not taken into account while evaluating the total running time, such as the **Setup** and **Extract** algorithms of *IBE* system, the **Sign** and **Verify** algorithms of the *IB*S system, since they make no difference among all approaches. Additionally, since all consumers perform algorithms in a parallel method, the total running time here is the estimated consumption of computation resources, not exactly the real system latency.

The aforementioned approaches were all implemented based on a common cryptography library extended by us from Charm-Crypto Library [15], a well-known comprehensive framework for rapidly prototyping advanced cryptography systems using the Python language. All identity-based algorithms were derived from the *IB-PRE* scheme released in [16]. The popular CTR mode of AES with a 128-bit key was selected as the symmetric encryption algorithm. Codes were run on a

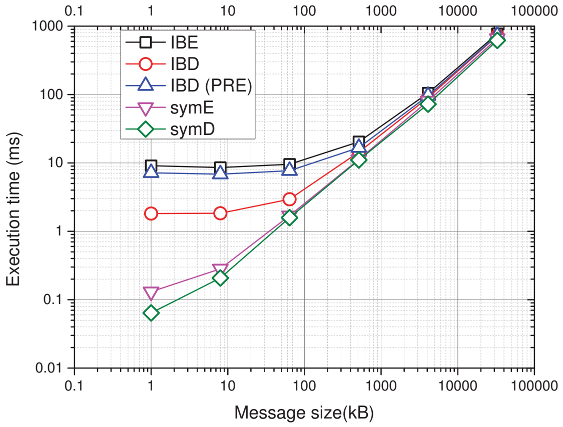

Fig. 3. Execution time of different algorithms regarding message size.

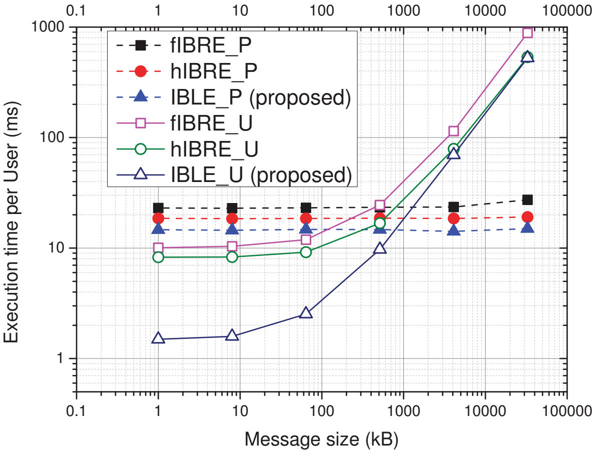

Fig. 4. Execution time per User for different schemes regarding message size with 1000 consumers.

virtual machine (VM) of Ubuntu 16.04 with 2 GB RAM and a 4-core CPU. All codes have been put on the GitHub.

B. *Efficiency of Encryption/Decryption*

The efficiency of the various encryption/decryption algorithms is investigated first. The one-short execution time of related encryption/decryption algorithms regarding the message size are illustrated in Fig. 3, where the **IBD** (**PRE**) denotes the algorithm of identity-based decryption performed after proxy re-encryption in *fIBRE*. The message size varies from 1 KB to 32 MB with a factor of 8.

As shown in Fig. 3, the running time of all algorithms grows significantly as message size increases, and tends to converge when the message size is larger than 4 MB. However, significant differences occur for smaller messages. The speed of symmetric encryption algorithms (**SymE/SymD**) is much faster than that of those identity-based ones (**IBE/IBD**), especially for short messages. To encrypt a message of 1 KB, the time consumed by **IBE** is about 100 times that of **SymE**. Without exceptions, the decryption algorithms run faster than the corresponding encryption ones, and the re-encryption will slow down the speed of decryption, making it close to that of encryption. One can observe that the curve of **IBD** (**PRE**) is very close to the one of the **IBE**.

C. *Workload per Consumer*

The computational burdens on both sides of provider and consumer are further investigated. With a fixed number of consumers, 1000, for each approach, the *ETPU*s of the algorithms running on both sides are logged and shown in Fig. 4, where _P and _U represent the side of the provider and the consumers, respectively.

According to Fig. 4, the *ETPU* on the provider side varies little as message size increases. In marked contrast, the ETPU on the consumer side goes up significantly. On both sides, the proposed *IBLE* approach exhibits the least *ETPU*. This is consistent with the analysis of E_x^P and E_x^U in Section III-A. On the provider side, all algorithms toward the message are all run for one time. When the total running time is divided by the consumer count, the increase resulting from the message size is smoothed. On the consumer side, the execution time is dominated by the decryption algorithm and therefore exhibits a rise similar to that shown in Fig. 3 as message size increases.

IV. Conclusion

In this work, a reference service model merging the publish-subscribe pattern with the ICN framework has been proposed. In addition, an identity-based license encryption (*IBLE*) approach for secure content distribution under this model was developed and presented. In this approach, the content to be delivered is symmetrically ciphered. In the meantime, the symmetric key together with the license is encrypted using an identity-based encryption (IBE) scheme where the provider or publisher plays the role of PKG. Based on a common extended cryptography library, the *IBLE* approach was implemented and executed in comparison with two other *IB-PRE* approaches. Test results show that the proposed approach (*IBLE*) exhibits better system performance and more energy-efficiency in consumer terminals, which makes it more viable for delivering content to mobile subscribers leveraging ICN technologies.

Acknowledgment

The authors would also like to thank contributors to provide the original implementation of identity-baser proxy re-encryption on GitHub (`github.com/nikosft/IB-PRE`).

References

[1] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, “A data-oriented (and beyond) network architecture,” in *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ser. SIGCOMM ’07. New York, NY, USA: ACM, 2007, pp. 181–192. [Online]. Available: http://doi.acm.org/10.1145/1282380.1282402

[2] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking named content,” in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT ’09. New York, NY, USA: ACM, Dec 2009, pp. 1–12. [Online]. Available: http://doi.acm.org/10.1145/1658939.1658941

[3] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2014. [Online]. Available: http://doi.acm.org/10.1145/2656877.2656887

[4] E. D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. Schmidt, and M. Waehlisch, "Information-centric networking (ICN) research challenges," RFC Editor, RFC 7927, 07 2016.

[5] X. Zhang, K. Chang, H. Xiong, Y. Wen, G. Shi, and G. Wang, "Towards name-based trust and security for content-centric network," in *2011 19th IEEE International Conference on Network Protocols*, Oct 2011, pp. 1–6.

[6] S. Misra, R. Tourani, and N. E. Majd, "Secure content delivery in information-centric networks: Design, implementation, and analyses," in *Proceedings of the 3rd ACM SIGCOMM Workshop on Information-centric Networking*, ser. ICN '13. New York, NY, USA: ACM, 2013, pp. 73–78. [Online]. Available: http://doi.acm.org/10.1145/2491224.2491228

[7] C. Wood and E. Uzun, "Flexible end-to-end content security in CCN," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, Jan 2014, pp. 858–865.

[8] Y. Yu, A. Afanasyev, and L. Zhang, "Name-based access control," NDN-Project, Tech. Rep., October 2015.

[9] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang, "Securing building management systems using named data networking," *IEEE Network*, vol. 28, no. 3, pp. 50–56, May 2014.

[10] M. Ion, J. Zhang, and E. M. Schooler, "Toward content-centric privacy in ICN: Attribute-based encryption and routing," in *Proceedings of the 3rd ACM SIGCOMM Workshop on Information-centric Networking*, ser. ICN '13. New York, NY, USA: ACM, 2013, pp. 39–40. [Online]. Available: http://doi.acm.org/10.1145/2491224.2491237

[11] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for icn naming scheme," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[12] Mircrosoft, "Microsoft PlayReady Content Protection Technology," Microsoft, Tech. Rep., April 2015. [Online]. Available: https://www.microsoft.com/playready/documents/

[13] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[14] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," *Information Sciences*, vol. 321, pp. 162 – 178, 2015, security and privacy information technologies and applications for wireless pervasive computing environments. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025515002431

[15] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013. [Online]. Available: http://dx.doi.org/10.1007/s13389-013-0057-3

[16] G. A. Matthew Green, "Identity-based proxy re-encryption," in *Proceedings of ACNS*, vol. 4521, 2007, pp. 288–306.