Ensuring Trust and Confidentiality for Adaptive Video Streaming in ICN

Fawad Khan and Hui Li

Abstract: **With the dissemination of huge amount of video content over the internet, information centric networking (ICN) has emerged as a potential candidate to effectively exploit it and improve the QoS. ICN decouples content from its location by caching, which can later be retrieved by consumers from their nearest locations. Various experimental studies have depicted the performance merits of dynamic adaptive streaming via HTTP (DASH) over ICN for improving QoS. However, there are two challenges that need to be addressed in the context of DASH over an ICN environment. The first one from content consumer domain is that the relevance, integrity, and provenance (RIP) of content should be guaranteed. RIP ensures trust establishment between publisher and consumer of content. The second one that concerns the content publisher is the confidentiality of DASH media, so that any consumer can view the particular quality or resolution of video based on his designated privileged rights. We address these two mentioned issues with the context of DASH over ICN. The performance and security analysis of our scheme depict its effectiveness for enforcing access control of adaptive streaming media in an ICN environment.**

Index Terms: **Confidentiality, information centric, name based trust, provenance, scalable media.**

I. INTRODUCTION

INFORMATION centric networking (ICN) such as named data networking (NDN) [1] and content-centric networking [2] consider named-content as the primary entity for requesting, retrieving, caching and routing of content; decoupling the location from it. Due to the large dissemination of multimedia video content over the Internet in last decades, ICN evolves as a potential candidate for future Internet (FI) to improve quality of service (QoS) [3], because of its intrinsic ability to cache and disseminate content upon request. Moreover, as content requests are furnished by potential content sources locally within the network; hence ICN reduces the upstream bandwidth and downstream latency.

For improving the quality of service of video provision, dynamic adaptive streaming over HTTP (DASH) has emerged as a hot topic in both academia and industry. Using DASH, content consumers can get the quality scalable media based on the device constraints and network resources, or the access privilege rights assigned to them. Deployment of DASH over ICN [4]–[6], is to utilize it for referencing and delivery. Moreover, for adjusting the scalability component of streaming video services [7], the scalable video coding (SVC) extension of H.264 video compression standard (H.264/SVC) [8] is utilized to encode a video content into a base layer and several enhancement layers for supporting progressive transmission.

Several recent research works [9]–[11] have depicted the applicability and advantages of adaptive video streaming in ICN environment; thereby improving the QoS due to content caching. Lederer *et al.* [9] evaluated the protocol overhead for CCN in-comparison to HTTP. Wang *et al.* [10] implemented a gateway for transforming the HTTP request and reply messages, correspondingly to the CCN interest and data messages respectively. Petrangeli *et al.* [11] exhibited the effectiveness of SVC based adaptive media streaming in ICN with effective caching.

Despite of the several advantages of SVC in ICN environment, an issue worth addressing is the confidentiality of SVC video streams based on privileged access rights of consumers. For elaboration we present a scenario in which a content provider (publisher P) wishes to publish a video with various resolutions for its clients in an ICN environment. Publisher P wants to restrict that any subscribed user with attribute $Free_{\text{User}}$ can view only a low resolution (basic quality) of video, while with attribute $Paid_{\text{User}}$ can enjoy the video of full fidelity. Enforcing the confidentiality of content in the above scenario based on consumers privileges is a challenging issue for the content provider. Some existing works [12]–[14] have focused to provide confidentiality to layers of SVC media, but all of these are formulated from a single authority CP-ABE scheme [15]. This limits the data owners/publishers to encrypt content over attributes belonging to a single specific attribute authority or a specific organization. In the real world the attributes universe is diverse, and to allow content owner to enjoy the expressiveness of his defined policy, he should be able to encrypt content over disjoint set of attributes belonging to multiple authorities. Moreover, for increasing the benefits provided by ICN, the content should be encrypted one time by publisher and shared under an expressive policy comprising of attributes from different organizations depending on a particular application scenario.

Another issue from the domain of content consumer is the relevance, integrity and provenance (RIP) of the retrieved content. We briefly explain these parameters as: (1) Relevance to make sure that the name of requested and retrieved content is

Manuscript received January 8, 2018; approved for publication by Heejo Lee, Division III Editor, March 5, 2018.

This work was supported by the National Natural Science Foundation of China (Grant No. 1401251), China 111 Project (Grant No. B16037), Shaanxi Key Basic Research Project (Grant No. 2016ZDJC-04) and National Key Research and Development Program of China (Grant Nos. 2017YFB0802201, 2017YFB0802203 and 2017YFB0802702).

F. Khan is with the State Key Laboratory of Integrated Service Networks, School of Cyber Engineering, Xidian University, Xi'an, Shaanxi 710071, P.R. China, and National University of Sciences and Technology, Islamabad 44000, Pakistan, email: fawad.khan.xdu@gmail.com.

H. Li is with the State Key Laboratory of Integrated Service Networks, School of Cyber Engineering, Xidian University, Xi'an, Shaanxi 710071, P.R. China, email: lihui@mail.xidian.edu.cn.

H. Li is the corresponding author.

Digital Object Identifier: 10.1109/JCN.2019.000026

1229-2370/19/$10.00 © 2019 KICS

Creative Commons Attribution-NonCommercial (CC BY-NC).
This is an Open Access article distributed under the terms of Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0)
which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided that the original work is properly cited.

same and bound to content; (2) integrity to check any accidental or intentional change of content; (3) provenance to make assurance regarding the originality of content, i.e., who is the provider (publisher) of content. RIP ensures the content consumer that the retrieved content by him is from an authentic trustable publisher, as in ICN there is no direct communication between publisher and consumer due to content caching and delivery. This phenomenon is in contrast to traditional TCP/IP host centric internet architecture where both the parties directly communicate with each other for content delivery. Hence, in ICN a publisher needs to make others believe about the authenticity of his content. Smetter's *et al.* [16] stated that the primary requirement for ensuring provenance is by generating a mapping triple of content-name N, content itself C signed with the publisher key P as $M_{(N,P,C)} = (N, C, Sign_P(N, C))$. Zhang *et al.* [17] employed an identity based signature (IBS) for ensuring RIP. However, an IBS signature is computationally expensive to evaluate and verify because of pairing operations. Moreover, the content name should be a human readable name so that a consumer can directly request content without involving a trusted third party (TTP) in contrast to [18].

As by principle, both ICN and attribute based encryption (ABE) [19] follow the one-to-many paradigm, i.e., same content / data message for many intended receivers. Hence this property can be exploited for providing data confidentiality in ICN. Moreover, for the assurance of RIP, i.e., relevance, integrity and provenance of content; a signature of content and content-Name needs to be signed by the publisher using his private key. Verification of the signature by consumer helps him in building trust on the publisher and its published content.

The main contributions of this work are as follows:

- We formalize the notion of a scalable media with trust and confidentiality in ICN (SMTC-ICN) for a human readable content name.
- We address the issues of relevance, integrity and provenance collectively termed as RIP. To resolve it, we employ a public key signature for binding the content to its name, which is signed by the publisher private key. This signature is part of the meta-data to be sent along with content, and helps consumer in building trust on the publisher and its published content. The employed signature is computationally effective and provides the assurance of RIP.
- We put forward an access control mechanism for ensuring confidentiality of H.264/SVC video streams. For providing confidentiality of content based on consumer's access privilege rights, we employ a multi message-multi authority-ciphertext policy ABE (MM-MA-CP-ABE), which restricts them to view the specified spatial and quality scalable H.264/SVC video content based on their assigned access rights. The employed MM-MA-CP-ABE have decentralized multiple authorities, where all authorities work independently without any coordination between them to enforce access control based on expressive monotone access policies.
- We present the comprehensive performance and security analysis to depict the effectiveness of our proposed SMTC-ICN scheme.

Rest of the paper is arranged as follows. Related work is described in Section II. Preliminary background is detailed in Section III, followed by Section IV giving an insight about adaptive SVC media and access hierarchy. Section V elaborates our proposed SMTC-ICN construction, while Section VI exhibits its analysis. Section VII concludes the paper.

II. RELATED WORK

In this section, we will review the trust establishment, i.e., relevance, integrity and provenance between content publisher and consumer and attribute based encryption with the context of ICN for enforcing content confidentiality.

Wong *et al.* [20] proposed a scheme to develop a trust relationship between content publisher and its consumer by the introduction of three identifiers namely: An authority identifier (ID), generated by the publisher public key; content identifier, evaluated by taking the cryptographic hash of content; and algorithmic identifier for binding the authority identifier to chunks of content identifier. The signature is based on public key digest employing RSA. Dannewitz *et al.* [21] proposed that a tuple containing content-ID (which is a self-certifying flat name), content itself, and meta-data combined to form an information object. Zhang *et al.* [17] proposed a name based mechanism for CCN employing identity based signature (IBS). In their scheme, content name prefix or publisher identity is set as the public key for building provenance between publisher and consumer. Although, the constructions [17], [20], [21] can partly ensure trust establishment between content publisher and consumer, they lack to provide content confidentiality.

Khoury *et al.* [22] proposed an access control mechanism in MANET setting for CCN by using the CP-ABE scheme [19]. In [22], the content identifier (CI) (self-certifying name) is generated by cryptographic-hash of ciphertext used for encrypting data with policy. Moreover, CI is made a part of meta-data ciphertext, but as there is no signature binding between the two entities, hence provenance cannot be guaranteed. Li *et al.* [18] proposed an attribute based access control mechanism for providing confidentiality in ICN environment. The scheme consists of a TTP for managing subject / object attributes. Due to content caching following the basic principle of ICN and lack of publisher control over its published data, a naming scheme for preserving the privacy of access policy is proposed. Also, the policy is used for encrypting the symmetric key used to encrypt content. The encrypted symmetric key acts as content name (content label), and content is retrieved by consumer with the help of domain name service. However, as stated in [23] the proposed naming scheme needs to be re-investigated because exposure of symmetric key would necessitate publisher with issues of re-keying and changing content name. Wu *et al.* [12] proposed an access control scheme for SVC (scalable media) in cloud aided content-sharing networks. Following their work Ma and Chen [13] proposed access control for two dimensional SVC, and Ma *et al.* [14] for multi-dimensional SVC. In all the schemes [12]–[14], the authors extended the single authority CP-ABE scheme [15] to multi-message CP-ABE by exploiting the structure of access tree. However, single authority CP-ABE constructions suffer from performance bottleneck issues and during the period of its failure / unavailability, users cannot request their attribute keys from the authority [24]. Khan *et al.* [25] proposed a multi-message multi-authority CP-ABE based on the linear secret sharing scheme (LSSS) access structure in which several authorities work in a de-centralized fashion, and users cannot collude their keys to gain access to data for which they are not entitled. In [26], a near-duplicate checking for encrypted content over CCN is studied. However, there is no proposed scheme which simultaneously addresses trust establishment, i.e., RIP and SVC content confidentiality in ICN.

III. Preliminaries

A. Hierarchal Key Derivation

Key derivation plays a significant role in providing access to users based on their roles or hierarchies [12], [27]. In this approach, nodes are arranged in hierarchal order and structured in the form of tree, and symmetric keys are assigned to them. Moreover, keys are derivable in the top-down manner, i.e., a parent node can derive the key of its child node by using its key. So, the parent nodes have access to more data while child nodes are limited to only the data encrypted by their key. We detail the hash based key derivation [12]. For a standard one-way hash function H, from key k_n the key k_i corresponding to the ith level of hierarchy is generated as:

$$k_i = H(k_{i+1}||i) \quad for \quad i = n-1, \cdots, 3, 2, 1.$$

B. Syntax of MM-MA-CP-ABE

We utilize a MM-MA-CP-ABE scheme [25] for providing confidentiality to the content, so that only legitimate users are allowed to access the data. It consists of the following algorithms.

Global setup$(\lambda) \rightarrow GP$: This algorithm outputs the global parameters GP for the system by taking the security parameter λ as input.

Authority setup$(GP) \rightarrow SK, PK$: Each attribute authority AA takes GP as input to generate secret / public (SK/PK) for itself.

Encrypt$(S_i, (A, \rho), GP, PK) \rightarrow CT$: Content owner (publisher) utilizes this algorithm for encrypting content by taking as input the messages S_i (symmetric keys corresponding to SVC media streams), access matrix $(\boldsymbol{A}, \rho)$, GP and PK of AA to output ciphertext CT under a policy.

KeyGen $(GID, GP, i, SK) \rightarrow K_{i,GID}$: Taking SK, GP as input, the algorithm generates decryption key $K_{i,GID}$ corresponding to attribute i and user (consumer) identity GID.

Decrypt $(CT, GP, K_{i,GID}) \rightarrow S_i$: For decrypting CT, GP and user (consumer) attribute keys $K_{i,GID}$ are taken as input to output any of symmetric key S_i corresponding to the set of user attributes.

IV. Scalable Media Sharing in ICN

In this section, we discuss about the structure of scalable media and the idea of granting access privileges to it, followed by the format of content meta-data for "Data" message in ICN.

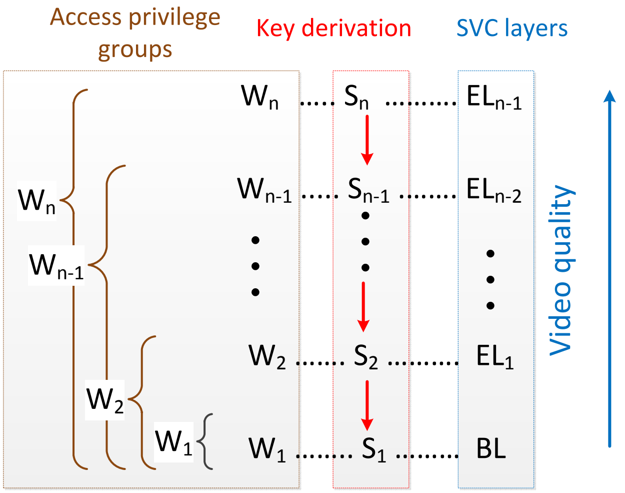
Access privilege groups
Key derivation
SVC layers
W_n
W_{n-1}
W_2
W_1
W_n ..... S_n .... EL_{n-1}
W_{n-1} ..... S_{n-1} .... EL_{n-2}
W_2 .... S_2 .... EL_1
W_1 .... S_1 .... BL
Video quality

Fig. 1. Privilege rights & key derivation.

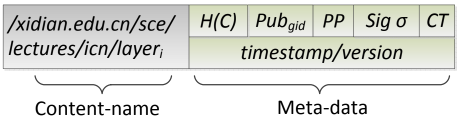

Fig. 2. Format of content meta-data.

A. Structure of Media & Access Hierarchy

We choose to explain the H.264/SVC video compression standard to elaborate how the transmission in ICN works. H.264/SVC standard supports scalability in video coding and its transmission [28]. Every video content can be coded with SVC into a BL content with necessary information regarding it, and several EL with information for improvement in video quality [12], [29]. For playing the nth quality level of video, decoding is performed for all nth layers including the base layer.

Each of the media content layer, i.e., $BL, EL_1, \cdots, EL_n$ can be considered as a logical unit [12], and can be retrieved by different groups of consumers based on their privileged rights. Consider an SVC video with BL unit and three EL units, i.e., BL, EL_1, EL_2, EL_3; we can have four access privilege groups or sets. The consumers in a group with access to BL media unit can view only the basic quality of video, but those provisioned with EL_3 unit can enjoy the full fidelity video. For SVC, in-order to view a video of high quality at a particular layer (EL_3), consumer should be having access to all lower enhancement layers (EL_2, EL_1) and base layer (BL) as well, due to the dependency of higher layers over lower layers [29], [30]. To allow a consumer with higher privilege rights for having access to lower enhancement layers (EL_i) and base layer (BL); each layer is encrypted with a hierarchal top-down derivable symmetric key as shown in Subsection III.A. Hence, the consumer will derive the hierarchal keys for lower enhancement layers and base layer from the key assigned to him based on his privileged rights. Fig. 1 shows privileges for groups / attribute sets W_i. Without loss of any generality, we can assume an SVC video to have n layers, where the base layer is encrypted with key S_1 and each $(i\text{th} - 1)$ enhancement layer EL_{i-1} with key S_i for $\{i = 2, \cdots, n\}$. Also, each of the symmetric key S_i is associated to an attribute set W_i. Attribute set W_n has the highest privilege, so consumers belonging to it can derive the keys S_i from their key S_n for $\{i = n-1, \cdots, 1\}$ to view the full quality video. The direction of red arrows in Fig. 1 indicates the key derivation. Consumers belonging to group or attribute set W_1 have access to key S_1, and can correspondingly view only the basic quality (lower resolution) video.

B. Content meta-data

The format of content meta-data is shown in Fig. 2. Content-name is human readable name. $H(C)$ is the hash of encrypted (base layer of SVC video) content with its symmetric key, i.e., $H(enc\{BL, S_1\})$, where enc is a standard symmetric key cipher like AES. Pub_{gid} is the identity of content publisher used for signature σ verification. Moreover, it can be a certificate $C_{gid,TA}$ signed by the secret key of trusted authority indicating publisher identity. PP are the public parameters corresponding to authority TA generating the signing key for publisher. Signature σ, is for ensuring the trust via its verification, and CT is for ciphertext associated to MM-MA-CP-ABE provisioning confidentiality.

V. SCALABLE MEDIA ACCESS CONTROL IN ICN

Here we will elaborate the system model, threat model, and our proposed SMTC-ICN scheme for ensuring trust, i.e., RIP and confidentiality of content in ICN.

A. System Model

The system model consists of content publishers, consumers, intermediate caching nodes, and authorities as shown in Fig. 3.

Publisher: Any node who wants to publish content. Prior to publishing the content, it first defines a human readable content-name [2] for the content (SVC video). The naming for different layers of encoded SVC video are $/BL/EL_1/EL_2$. For the assurance of trust, publisher signs the content to content-name with his signing key sk_{gid} to form a signature σ. For restricting the content access only to legitimate consumers, it defines a policy over their attributes and encrypts content employing MM-MA-CP-ABE. Moreover, publisher node on receiving an "Interest" message will forward the corresponding "Data" message to consumer along with meta-data of content, following the principles of ICN. This node can also be tagged as a server with potential content sources.

Consumer: This node can issue an "Interest" message containing the content-name of content (SVC video) along with specified layer of video to which it is entitled to view. Based on the ICN principle of named-based routing, it can get the corresponding "Data" message. The message will contain meta-data and encrypted layers of SVC content from base layer to specified level of enhancement layer requested. Consumer can then verify the signature with information available in meta-data to have assurance regarding relevance, provenance of the content, and for building trust on publisher and its published content. After that, it can decrypt the content based on the attributes possessed by him.

Intermediate / caching node: Any node lying in between consumer and potential sources of content, i.e., content router or any other caching node. It caches content according to its cache policy to be later retrieved by other content consumers by sending out an "Interest" message; there by improving the QoS in network.

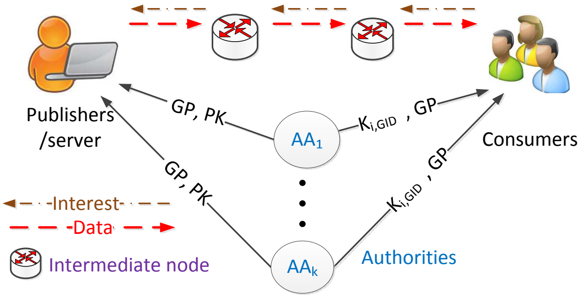

Fig. 3. System model.

Attribute authorities (AA): AA's generate the public / private key-pairs for themselves and work in a de-centralized fashion. Attributes management is performed by these authorities, and these are also responsible for assigning attribute decryption keys $K_{i,GID}$ to consumer's. Moreover, any authority can also grant a signing key sk_{gid} to publisher node corresponding to his identity gid, signed by authority's secret key. We denote gid to indicate publisher global identity used for signing the content, and represent GID to indicate a consumer global identity based on which he is assigned collusion resistant decryption keys from authorities.

B. Threat Model

In the work, we assume that the intermediate caching nodes are semi honest, which means that they follow the protocol by sending out the requested content but at the same time curious about the requested content. Moreover, they can be compromised by adversaries who try to manipulate signed content, or send out a different content instead of requested content to consumer. Publisher is honest node, who signs the content with his own key for ensuring RIP. Users have a colluding nature to gain access to content they are not entitled to get individually or beyond their privileged access. Attribute authorities are considered honest. For more details regarding the threat model we refer readers to [24], [26].

C. SMTC-ICN Scheme

In this work, we employ the public key signature [31] for binding the name to its content ensuring provenance, and laying grounds for providing relevance and integrity of content. For ensuring confidentiality, i.e., access control based on consumer's privileged rights we employ MM-MA-CP-ABE scheme proposed in [25]. Moreover, we employ the key derivation [12] as mentioned in Subsection III.A for hierarchically encrypting H.264/SVC layers.

Global setup: In global setup, a multiplicative cyclic group G of prime order p is chosen. Global parameters are set as: $GP = \{g, e(g,g), p, H'\}$; where g is a generator of group G and hash function H' maps global identities GID to elements in G.

Authority setup: Each authority selects a random value $t \in Z_p$ for itself. Moreover, for every attribute i belonging to authority, it chooses a random value $\alpha_i \in Z_p$. It keeps values $\{t, \alpha_i \forall i\}$ as secret key, SK and publishes $\{g^t, e(g,g)^{\alpha_i} \forall i\}$ as public key, PK.

KeyGen: For creating a key for consumer GID corresponding to an attribute i of authority, it computes:

$$K_{i,GID} = g^{\alpha_i/t} \cdot H'(GID)^{1/t}$$

Sign and encrypt: Publisher who wishes to publish an H.264/SVC video content will first define its human-readable content-name as shown in Fig. 2. After then it will encrypt its base layer (BL) with key S_1 and enhancements layers (EL_{i-1}) with symmetric keys S_i for $\{i = 2, \cdots, n\}$ as shown in Fig. 1. We remark that keys can be hierarchically derived downwards from S_i to S_1, for $\{i = 2, \cdots, n\}$. Thereafter, hash of encrypted base layer of SVC video is computed, i.e., $H(C) = H(enc(S_1, BL))$. Hash of only BL layer has also been employed in [29] for data de-duplication in cloud setting because higher layers of SVC depend on base layer. Following that, publisher will take m = {content-name, $H(enc(S_1, BL))$} as input for evaluating signature σ.

For providing confidentiality to content (encrypted SVC layers with hierarchal symmetric keys S_i), publisher defines an expressive monotone access control policy based on consumers attributes. In the policy, there are various attribute sets (consumers group) W_i; where every W_i is mapped to symmetric key S_i used for encrypting the SVC layers as seen from Fig. 1. Moreover, each W_i contains consumers attributes with an AND operation between them. We denote AND with $\wedge$ operation for the rest of this paper. As an example for a particular attribute set W_1 containing attributes $Subscriber, Gold$ is expressed as $W_1 = Subscriber \wedge Gold$.

The resulting $AND - OR$ based expressive access control policy appears as $W = [W_1 \; OR \; W_2 \; OR \cdots OR \; W_n]$. Then, he transforms the policy W into an LSSS matrix $\boldsymbol{A}$ of size a x b with ρ containing a map of matrix rows to its attributes. Thereafter, it gives the S_i, $(\boldsymbol{A}, \rho)$ values as input to encrypt algorithm.

To proceed, algorithm will first choose random values $q_i, v_{i,2}, \cdots, v_{i,b} \in Z_p$ to form a sharing vector $\boldsymbol{v_i} = \{q_i, v_{i,2}, \cdots, v_{i,b}\}$ for each attribute set W_i; where q_i is shared secret for each attribute set W_i. Further, it computes $\lambda_x = \boldsymbol{A_x} \cdot \boldsymbol{v_i}$ for $\rho(x) \in W_i$, where $\boldsymbol{A_x}$ is the xth row of $\boldsymbol{A}$ and corresponds to mapping $\rho(x)$. Moreover, it will choose a random vector $\boldsymbol{\omega} \in Z_p$ of length b with 0 as its first entry. Compute $w_x = \boldsymbol{A_x} \cdot \boldsymbol{\omega}$. After then, the ciphertext components CT_i are computed as:

$$CT_i = \{C_i = S_i \cdot e(g,g)^{q_i}, C_{1,x} = e(g,g)^{\lambda_x} \cdot e(g,g)^{\alpha_{\rho(x)} w_x},$$

$$C_{2,x} = g^{t w_x}\}.$$

$C_{1,x}$ and $C_{2,x}$ values correspond to attributes in attribute set W_i. The entire ciphertext $CT = \{CT_i$ for $i = 1, 2, \cdots, n, W, (\boldsymbol{A}, \rho)\}$ is made a part of content meta-data along with signature σ as shown in Fig. 2. The "Data" message will comprise of encrypted (SVC layers) content, and meta-data.

Verify and decrypt: On receiving a "Data" message in-response to a sent out "Interest" message, consumer can first check about the authenticity of publisher and its published content by verification of signature σ. To comply, it extracts content-name and $H(C)$ from meta-data to form m. Then it takes m, signature σ, PP, and Pub_{gid} from meta-data to verify the signature σ. If the signature is satisfied, then there exists a binding between name, content and its publisher; hence provisioning trust establishment between consumer and publisher. To decrypt the data, consumer will input CT, his attribute keys $K_{i,GID}$ and GP to decrypt algorithm.

For decryption, the primary assumption is that the ciphertext is encrypted under access matrix $(\boldsymbol{A}, \rho)$. If the decrypting consumer attribute keys $\{K_{\rho(x),GID}\}$ can form a span $(1, 0, \cdots, 0)$ over the subset of access matrix rows $\boldsymbol{A_x} \in W_i$, then the consumer will choose constants $u_x \in Z_p$, so that $\sum_x u_x \; \boldsymbol{A_x} = (1, 0, \cdots, 0)$ where $\rho(x) \in W_i$, and then will decrypt as follows:

$$\prod_x \left(C_{1,x}/e(C_{2,x}, K_{\rho(x),GID})\right)^{u_x} = e(g,g)^{q_i}.$$

After correctly finding $e(g,g)^{q_i}$, he will divide this by value of C_i (corresponding to an attribute set W_i for which his attributes's formed a span) to obtain S_i which is symmetric key for an encrypted SVC layer. Due to the dependency of higher layers of SVC over its lower layers specifically base layer; consumer can derive the lower hierarchy keys from his own key to view a particular resolution of video based on his access rights. As the consumer cannot derive keys up in the hierarchy; hence he would not be able to access full fidelity video content to which he is not entitled.

Correctness: The proposed access control scheme is correct. To decrypt, the consumer will first choose constants $u_x \in Z_p$, so that $\sum_x u_x \; \boldsymbol{A_x} = (1, 0, \cdots, 0)$; then will decrypt as follows:

$$\begin{aligned}
&\prod_x \left(\frac{C_{1,x}}{e(C_{2,x}, K_{\rho(x),GID})}\right)^{u_x} \\
&= \prod_x \left(\frac{e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} w_x}}{e(g^{t w_x}, g^{\alpha_{\rho(x)}/t} \cdot H'(GID)^{1/t})}\right)^{u_x} \\
&= \prod_x \left(\frac{e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} w_x}}{e(g,g)^{\alpha_{\rho(x)} w_x} \cdot e(g, H'(GID))^{w_x}}\right)^{u_x} \\
&= \prod_x \left(\frac{e(g,g)^{\lambda_x}}{e(g, H'(GID))^{w_x}}\right)^{u_x} = e(g,g)^{q_i}.
\end{aligned}$$

VI. ANALYSIS

In this section, we will exhibit the performance evaluation and security analysis of SMTC-ICN.

A. Security Analysis

Trust establishment: Content consumer on receiving the data message, can gain trust regarding the public key PK_{gid} of publisher with the certificate obtained from meta-data. Certificate is signed by the trusted authority with its private key for publisher identity *gid*. For ensuring trust, consumer will first take content-name, $H(C) = H(enc(S_1, BL))$, PP, σ from meta-data in the data message, and will verify the signature σ to build its trust on publisher, and provenance of content. For integrity the consumer can take the cryptographic hash of $(enc(S_1, BL))$, and

Table 1. Comparison with existing relevant schemes.

Scheme	C	RIP	Authority	H.264/SVC	Security assumption
[22]	✓	X	Single	X	d-parallel BDHE
[18]	✓	X	Multiple	X	Generic group
[12]	✓	X	Single	✓	Generic group
Our's	✓	✓	Multiple	✓	Generic group

Table 2. Computational comparison with existing relevant constructions.

Scheme	Encryption	Decryption
[22]	$(3N_T + 2)E$	$(2N_I + 1)P + (N_I)E$
[18]	$(3N_T + 4)E$	$(2N_I + 1)P + (2N_I)E$
[12]	$(2N_T + 2p)E$	$(2N_I + 1)P + (N_I)E$
$Our's$	$(3N_T + p)E + 3E$	$(N_I)P + (N_I)E + 3E$

compare it to its result placed in meta-data. For relevance the content-name in requested interest message and retrieved data message can be compared, as the content corresponding to name is bound by signature.

A potential attack in an ICN environment launched by an adversary can be by replacing the requested content in data message with any arbitrary content of his choice and making the consumer believe that he retrieved the requested content accordingly to its name in interest message. However, if the content-name is bound to content and signed by a publisher, than the attack is mitigated. Hence, the relevance of content in interest and data message can be ensured if the publisher signed the content with content-name placed in the data message.

As our trust mechanism relies on proven secure cryptographic functions like SHA-256, and digital signature [31]; hence it is statistically infeasible for an intruder tempering data without any modification in the signature σ, because of the pre-image attack resistance of hash function, and forgery attack resistance of digital signature. Hence, any un-authorized modification in content, or its meta-data can be detected by signature verification. Signature σ can also be checked by any intermediate content caching router node even without having any privileged access rights. So, a data message can be discarded by it, if σ is not verified to avoid malware. It ensures that the content should not be propagated in network, if it does not ensure the trust, and exhausts only the network resources.

Confidentiality and collusion resistance: For providing confidentiality to the content based on consumer's access privilege rights, we have employed MM-MA-CP-ABE [25] which is proven secure in generic group model. Moreover, the scheme provides collusion resistance against consumers key combination. Hence, consumer's will not be able to combine their keys, and attain the content they are not entitled to get individually. We refer reader for the security model and proof of MM-MA-CP-ABE scheme in Subsections IV.A and V.B of [25].

Privileged access: Our proposed scheme encrypts layers of SVC content with hash based hierarchal symmetric keys [12]. As key derivation is from a parent node to its descendant child node; hence any consumer cannot view a quality of SVC content beyond its privileged access.

B. Performance Evaluation

At first, we give the comparison of theoretical computations with existing relevant schemes and then we will demonstrate some practical results based on layered structure of H.264/SVC media.

Table 3. Average encryption and decryption time of segment 0, 1 of Blue Sky 1080p video.

Segment	Layer	Size (KB)	Enc (ms)	Dec (ms)
0	BL	139	28	12
	EL_1	385.5	85	50
	EL_2	709.9	95	108
	EL_3	1331.2	133	114
1	BL	197.9	47	34
	EL_1	448.1	76	60
	EL_2	761	85	89
	EL_3	1443.6	121	127

Table 1 shows a comparison of our scheme with existing relevant schemes [12], [18], [22] employed for providing data confidentiality. The notations used in Table 1 are: RIP indicates the provision of content relevance, integrity and provenance and C represents confidentiality/access control. Our scheme ensures trust (RIP) and confidentiality (access control) simultaneously for H.264/SVC media as seen from Table 1. In Table 2, we give a comparison of our scheme with existing constructions Khoury *et al.* [22], Li *et al.* [18], and Wu *et al.* [12] theoretically, in terms of computations involved for attribute based access control in encryption and decryption operations and signature signing and verification costs. Notations used in Table 2 are: N_T for total attributes in policy, N_I for consumer's attributes involved in decrypting ciphertext to obtain content, E for exponential operation, P for pairing operation, and p to denote the number of privileged consumer groups / attribute sets. Our proposed scheme is much efficient in comparison to other schemes in decryption operation. For the assurance of RIP, our construction incurs a cost of 3 exponential operations for signature generation and its verification as seen from Table 2 in encryption and decryption operations.

All the simulation results presented in this section are carried on a Ubuntu 14.04 virtual machine with 1.5 GB allocated Ram on a HP core-i5 CPU@3.30 GHz desktop PC with 4 GB Ram. Before moving on, we briefly state here the purpose of involvement of some simulators / libraries in our experiments. We have utilized CCNx Distillery [1] for creating a linear topology between content consumer and publisher to transfer the encrypted H.264/SVC segments (content) by sending out the interest message. To encrypt the H.264/SVC segments we employed the linux library mcrypt [2] in the cipher block chaining (CBC) mode. For decoding the media segments and playing video content accordingly for base layer and enhancements layers at the consumer side; DASH-SVC-Toolchain [32] is utilized. For enforcing trust and access control of H.264/SVC media, we implemented our proposed scheme in Charm [33]. Charm [3] is a tool for constructing and evaluating cryptographic constructions. We use "SS512" symmetric curve with "512" bit base field for carrying out CP-ABE operations in Charm simulator.

We utilized the encoded H.264/SVC video [32] for carrying out our experiments. The demo video "Blue Sky" consists of 217 frames encoded into 5 segments. Each segment is comprised of a base layer and three enhancement layers. We have

[1] CCNx. [Online]. Available: https://github.com/PARC/CCNx_Distillery

[2] Mcrypt. [Online]. Available: https://packages.ubuntu.com/trusty/mcrypt

[3] Charm. [Online]. Available: http://www.charm-crypto.com/category/charm/

Table 4. Average running time of encryption, σ generation / verification and CT, σ size.

Encryption (ms)	78.72
Ciphertext Size (KB)	6.5
σ-Generation (ms)	6.45
σ-Verification (ms)	3.51
σ Size (KB)	1.1

Table 5. Average key generation time by authority.

Consumer	Attributes	Time (ms)
U_1	Subscriber, Basic	28.38
U_2	Subscriber, Silver	25.72
U_3	Subscriber, Gold, X	35.09
U_4	Subscriber, Platinum, Y	32.25
U_5	Subscriber, X, Y, Z	43.06

Table 6. Consumer's access privilege and CT decryption time.

Consumer	Access	Key derive (KD)	KD + CT (ms)
U_1	BL	S_1	0+13.78 = 13.78
U_2	EL_1	$S_2 \rightarrow S_1$	1+14.06 = 15.06
U_3	EL_2	$S_3 \rightarrow S_2 \rightarrow S_1$	2+13.98 = 15.98
U_4	EL_3	$S_4 \rightarrow S_3 \rightarrow S_2 \rightarrow S_1$	3+13.93 = 16.93
U_5	No	—	—

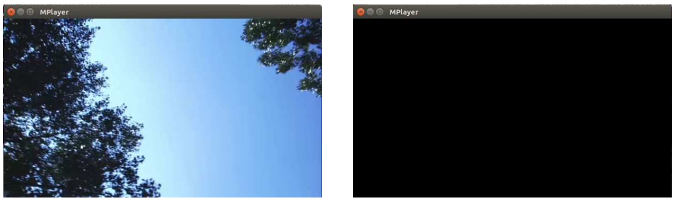

Fig. 4. Base layer content shown to U_1 on the left, while black screen shown to U_5 on the right.

encrypted segments of Blue Sky video using mcrypt in CBC mode employing hierarchal symmetric keys S_i. Table 3 lists the average encryption (Enc) and decryption (Dec) time in milliseconds for all the layers of segments 0 and 1 along with their sizes. We remark that consumer's having privileged access to base layer content will retrieve and decrypt only the base layer content. This will help improve the network overall QoS, and less metering costs for consumer's.

For providing confidentiality to H.264/SVC layers based on consumer's rights, we have defined a privileged access policy for a content producer as: $(Subscriber \wedge Basic)$ OR $(Subscriber \wedge Silver)$ OR $(Subscriber \wedge Gold)$ OR $(Subscriber \wedge Platinum)$. The goal of content producer is to limit the consumer's to view the specific spatial and quality scalability of video based on their subscribed package, i.e., Basic, Silver, Gold, and Platinum membership. We take the help of a simple policy to better explain the scenario; although, our underlying expressive access policy CP-ABE scheme can encrypt multiple attributes sets with a single ciphertext over policy efficiently. For the above defined policy, we have four attribute sets, namely $W_1 = (Subscriber \wedge Basic)$, $W_2 = (Subscriber \wedge Silver)$, $W_3 = (Subscriber \wedge Gold)$ and $W_4 = (Subscriber \wedge Platinum)$. Here, different attribute sets W_i correspond to different derivable keys S_i used for encrypting the segments of H.264/SVC video as stated in previous paragraph. The attribute sets / groups in policy are privileged as: $W_4 > W_3 > W_2 > W_1$. Hence, the consumers having attributes $Subscriber$, $Platinum$ or belonging to attribute group W_4 can enjoy the video of full fidelity, but those belonging to attribute group W_1 can view only the base layer of video. The average encryption time and ciphertext size for our defined privileged policy is evaluated in Charm simulator and is shown in Table 4. The size of ciphertext for the entire policy as seen from Table 4 depicts much smaller overhead in comparison to segments size of H.264/SVC. Moreover, the average time for signature σ generation and its verification along with its size employed for ensuring RIP is presented in Table 4. We observe that the signature generation / verification time and its size is comparatively less and constant in contrast to attribute based access control.

For demonstration purpose, we defined five content consumers with identities U_i for $\{i = 1, 2, \cdots, 5\}$ and assigned them with attributes as shown in Table 5. Moreover, the average key generation time for all five consumers corresponding to their attributes evaluated in Charm is presented in Table 5. Generally, key generation time for a user linearly increases with the number of attributes, and it is a one-time process.

For the assigned attributes to consumers in Table 5, each consumer will have access to a specific layer of H.264/SVC correspondingly to his attributes. Although, consumer U_1, U_2, U_3 and U_4 all satisfy the policy, but due to underlying multi-message CP-ABE, they will have access to a different layer of H.264/SVC video based on their attributes. Table 6 show the access privilege rights of consumer's correspondingly to their satisfaction of policy. Moreover, consumer having access to an enhancement layer based on his privileged rights will have to derive the lower hierarchy keys in-order to view a high quality video because of the dependency of higher enhancement layers of SVC over lower enhancement layers and base layer. We observed an average time of 1 ms for deriving a key from parent to child node for one hierarchal level. Table 6 lists the ciphertext decryption and key derivation time in milliseconds for consumers. In case of U_4, the key derivation KD time is 3 ms because of three hierarchy levels, i.e., $S_4 \rightarrow S_3 \rightarrow S_2 \rightarrow S_1$. The ciphertext CT decryption time is almost similar for consumers U_1, U_2, U_3, and U_4, because two attributes of every consumer are utilized for decryption. Generally, the decryption time linearly increases with the number of consumer attributes which combine to satisfy policy.

We remark that the acquired keys S_i by consumer's are used to decrypt the encrypted segments of H.264/SVC. The decryption time of corresponding layers segments of H.264/SVC can be seen from Table 3. Thereafter, the consumers can play the corresponding layer of video by decoding the video segments employing python script of DASH-SVC-Toolchain [32]. On the left in Fig. 4 shows the base layer content shown to consumer U_1 based on his attributes. As consumer U_5 does not satisfy the policy, hence he cannot decrypt the encrypted segment, and on directly decoding he will see a blank screen as shown in Fig. 4 on the right.

For a consumer U_4 having privileged access to EL_3, as seen from Table 3, the overall cumulative segment decryption time for all the layers of *segment 0* is approximately below 300 ms, which is acceptable. Moreover, the ciphertext decryption and key derivation time for U_4 is around 16.9 ms which is much less then 300 ms as seen from Table 6. It signifies that the employed access control is cost efficient in comparison to SVC video segments decryption. Content consumer U_4 while viewing the first segment of SVC can download and decrypt the next segments of video in order to experience no real time delay. Generally for real time multimedia traffic, the segments decryption time should be fairly less to display the next received segments on time.

VII. CONCLUSION

In this paper, we have proposed a suitable access control mechanism for sharing scalable media content in ICN environment. We have exploited the common characteristic of both ABE and ICN, i.e., one-to-many access paradigm, for providing confidentiality to content. For ensuring privileged access control based on consumers attributes for scalable H.264/SVC media content, we employed multi-message multi-authority CP-ABE. To establish a trust between content publisher and consumer, we have utilized a public key signature; hence provisioning relevance, provenance, and integrity of content. Analysis shows the effectiveness of our approach by having less overhead and computational time. Moreover, the consumer is restricted to play/view the specific spatial and quality scalability of video based on his attributes. By utilizing our scheme, the content can be cached and routed accordingly with the principles of ICN, but only legitimate consumers are allowed to decrypt and view the content.

REFERENCES

[1] L. Zhang, *et al.*, "Named Data Networking (NDN) project," PARC TR-2010-3, Oct. 2010.

[2] V. Jacobson *et al.*, "Networking named content," in *Proc. ACM CoNEXT*, Dec. 2009.

[3] G. Xylomenos *et al.*, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, Second Quarter 2014.

[4] S. Lederer, C. Mueller, B. Rainer, C. Timmerer, and H. Hellwagner, "Adaptive streaming over content centric networks in mobile networks using multiple links," in *Proc. IEEE ICC Workshops*, June 2013. pp. 677–681.

[5] Y. Liu *et al.*, "Dynamic adaptive streaming over CCN: A caching and overhead analysis," in *Proc. IEEE ICC*, June 2013. pp. 3629–3633.

[6] X. Yin, A. Jindal, V. Sekar, and B. Sinopoli, "A control-theoretic approach for dynamic adaptive video streaming over HTTP," in *Proc. ACM SIGCOMM*, Aug. 2015, pp. 325–338.

[7] X. Wang, T. Kwon, Y. Choi, , H. Wang, and J. Liu, "Cloud-assisted adaptive video streaming and social-aware video prefetching for mobile users," *IEEE Wireless commun.*, vol. 20, no. 3, pp. 72–79, July 2013.

[8] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H. 264/AVC standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17 no. 9, pp. 1103–1120, Sept. 2007.

[9] S. Lederer, C. Mueller, B. Rainer, C. Timmerer, and H. Hellwagner, "An experimental analysis of dynamic adaptive streaming over http in content centric networks," in *Proc. IEEE ICME*, July 2013, pp. 1–6.

[10] S. Wang, J. Bi, J. Wu, X. Yang, and L. Fan, "On adapting HTTP protocol to content centric networking," in *Proc. ACM CFI*, Sept. 2012, pp. 1–6.

[11] S. Petrangeli, N. Bouten, M. Claeys, and F. De Turck, "Towards SVC-based adaptive streaming in information centric networks," in *Proc. IEEE ICME Workshops*, June 2015, pp. 1–6.

[12] Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," *IEEE Trans. Multimedia*, vol. 15, no. 4, pp. 778–788, June 2013.

[13] C. Ma and C. W. Chen, "Secure media sharing in the cloud: Two-dimensional-scalable access control and comprehensive key management," in *Proc. IEEE ICME*, July 2014, pp. 1–6.

[14] Z. Ma, Z. Yan, and C. W. Chen, "Attribute-based multi-dimension scalable access control for social media sharing," in *Proc. IEEE ICME*, July 2016, pp. 1–6.

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE SP*, May 2007, pp. 321–334.

[16] D. Smetters and V. Jacobson, "Securing network content" PARC TR, 2009.

[17] X. Zhang *et al.*, "Towards name-based trust and security for content-centric network," in *Proc. IEEE ICNP*, Oct. 2011, pp. 1–6.

[18] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," *IEEE Tran. Dependable Secure Comput.*, vol. 15, no. 2, pp. 194–206, Apr. 2016.

[19] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. IACR PKC*, Mar. 2011, pp. 53–70.

[20] W. Wong and P. Nikander, "Secure naming in information-centric networks," in *Proc. ACM ReARCH*, Nov. 2010.

[21] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in *Proc. IEEE INFOCOM Workshops*, Mar. 2010, pp. 1–6.

[22] J. Khoury *et al.*, "An efficient and expressive access control architecture for content-based networks," in *Proc. IEEE MOLCOM*, Oct. 2014, pp. 1034–1039.

[23] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp.566–600, Sept. 2017.

[24] K. Xue *et al.*, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 953–967, Jan. 2017.

[25] F. Khan, H. Li, and L. Zhang, "Owner specified excessive access control for attribute based encryption," *IEEE Access*, vol. 4, pp. 8967–8976, Nov. 2016.

[26] H. Cui, X. Yuan, Y. Zheng, and C. Wang, "Enabling secure and effective near-duplicate detection over encrypted in-network storage," in *Proc. IEEE INFOCOM*, Apr. 2016, pp. 1–9.

[27] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Krikken, "Dynamic and efficient key management for access hierarchies," *ACM Trans. Inform. Syst. Security*, vol. 12, no. 3, Jan. 2009.

[28] Z. Liu and Y. Wei, "Hop-by-hop adaptive video streaming in content centric network," in *Proc. IEEE ICC*, May 2016, pp. 1–7.

[29] Y. Zheng *et al.*, "Toward encrypted cloud media center with secure deduplication," *IEEE Trans. Multimedia*, vol. 19, no. 2, pp. 251–265, Feb. 2017.

[30] Y. G. Won, T. M. Bae, and Y. M. Ro, "Scalable protection and access control in full scalable video coding," in *Proc. IWDW* Nov. 2006, pp. 407–421.

[31] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Proc. SCN,* Sept. 2002, pp. 268–289.

[32] C. Kreuzberger, D. Posch, and H. Hellwagner, "A scalable video coding dataset and toolchain for dynamic adaptive streaming over HTTP," in *Proc. ACM MMSys*, Mar. 2015, pp. 213–218.

[33] J. A. Akinyele, M. Green, and A. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptographic Eng.*, vol. 3, no. 2, pp. 111–128, June 2013.

Fawad Khan received his Ph.D. degree in Cryptography from School of Cyber Engineering, Xidian University in 2018. Priorly, he received the B.S. degree in Electrical Engineering from UET Peshawar in 2010 and the M.S. degree in Electrical Engineering from CECOS University in 2014. Currently, he is working as a Faculty Member at National University of Science & Technology, Islamabad, Pakistan. His research interests include cryptography and information security. Particularly, he works on attribute based encryption, homomorphic encryption and cloud security. He is the Reviewer of several journals including IET Security, FGCS, IEEE Access, and IEEE Transactions on Industrial Informatics.

Hui Li received his B.S. (1990) from Fudan University, and M.S. (1993) and Ph.D. (1998) from Xidian University, respectively. Currently, he is a Professor at the School of Cyber Engineering, Xidian University. In 2009, he was with Department of Electrical and Computer Engineering (ECE), University of Waterloo, as a Visiting Scholar. His research interests include the areas of cryptography, security of cloud computing, wireless network security, and information theory. He served as TPC Co-hair of ISPEC 2009 and IAS 2009, general Co-chair of E-Forensic 2010, ProvSec 2011 and ISC 2011. He is a Member of the IEEE.