Content-Centric Privacy Model for Monitoring Services in Surveillance Systems

Kalika Suksomboon
KDDI Research, Inc.
ka-suksomboon@kddi-research.jp

Kazuaki Ueda
KDDI Research, Inc.
kz-ueda@kddi-research.jp

Atsushi Tagami
KDDI Research, Inc.
tagami@kddi-research.jp

ABSTRACT

This paper proposes a content-centric privacy (CCP) model that enables a privacy-preserving monitoring services in surveillance systems without cloud dependency. We design a simple yet powerful method that could not be obtained from a cloud-like system. The CCP model includes two key ideas: (1) the separation of the private data (i.e., target object images) from the public data (i.e., background images), and (2) the service authentication with the classification model. Deploying the CCP model over ICN enables the privacy central around the content itself rather than relying on a cloud system. Our preliminary analysis shows that the ICN-based CCP model can preserve privacy with respect to the W^3-privacy in which the private information of target object are decoupled from the queries and cameras.

CCS CONCEPTS

• **Security and privacy** → *Security protocols*; • **Networks** → *Programming interfaces*;

KEYWORDS

Information Centric Networking, Access control, Privacy, Monitoring

ACM Reference Format:
Kalika Suksomboon, Kazuaki Ueda, and Atsushi Tagami. 2018. Content-Centric Privacy Model for Monitoring Services in Surveillance Systems. In *Proceedings of ICN'18, Boston, MA, USA, September 21–23, 2018,* 2 pages. https://doi.org/https://doi.org/10.1145/3267955.3269007

1 INTRODUCTION

In a smart city, surveillance cameras are expected to be everywhere for preventing crimes and increasing public safety. Motivated by leveraging pervasive surveillance cameras, what if they can be served as a monitoring service for citizens? However, this service could not be possible since the privacy is a serious concern from citizens. This concern, hence, disrupts this advanced service.

To alleviate this concern, typical cloud-based services let a cloud server perform a trusted entity that collects surveillance video data from all cameras and serves as an authentication server. Doing so can preserve privacy on the target object against the unauthorized users by storing the data in the encrypted format. Yet, it remains an open question whether or not the centralized access control bears new worrisome issues in order to preserve W^3-privacy[1] [2]. On one hand, once an adversary compromises the cloud server, it can observe all queries. On the other hand, the cloud can learn from the queries leading to privacy leak.

This paper aims to preserve W^3-privacy for monitoring services. We proposes a content-centric privacy (CCP) model to preserve privacy access control at the content itself rather than allowing a third party to control accessing the privacy information. Since ICN offers the potential for decoupling the user/requester (*who*) from data owners or cameras (*where*), while the service authentication by the classification model can decouple cameras (*where*) from the target object (*what*), we introduce the CCP model over ICN to preserves W^3-privacy for monitoring services.

2 CONTENT-CENTRIC PRIVACY MODEL

2.1 Key ideas

First, we assume that the background images are the public data and the (target) object images are the private ones. We propose the CCP model including two key ideas as follows. (1) The separation of the private data from the public data. For the monitoring service, we can separate foreground from background images by a background subtraction technique (e.g., [1]). Moreover, the target object can be separated from bystanders in the same foreground image by means of the image recognition with respect to the classification model of that target object. (2) The classification model is used as an access key for monitoring the target object. That is, the user who has the classification model has an access right to monitor the target object. The user, hence, can see only the his/her target object. Consequently, the access control for preserving the content's privacy is central to the content itself. To the best of our knowledge, this is the first proposal makes use of the background subtraction to preserve privacy for monitoring service.

2.2 CCP model over ICN

We use a classification model as a query rather than specifying only the name of a target object as a typical ICN naming scheme to preserve privacy of *what.* Therefore, to request the monitoring service, a user sends an interest packet that encapsulates the classification model specific to the target object. The ICN/NDN forwarders forward the interest packet towards where the cameras are. The name of the interest packet is used to match with the camera's name or

ICN'18, September 21–23, 2018, Boston, MA, USA

ACM ISBN 978-1-4503-5959-7/18/09…$15.00
https://doi.org/https://doi.org/10.1145/3267955.3269007

[1] W^3-privacy consists of three dimensions. (1) **What** refers to what the query is. In the other words, it refers to what the target object is, such that the correlation between the target object and his/her name is disclose. (2) **Who** refers to who requests to monitor the target object. (3) **Where** refers to the correlation between the target object and his/her location.

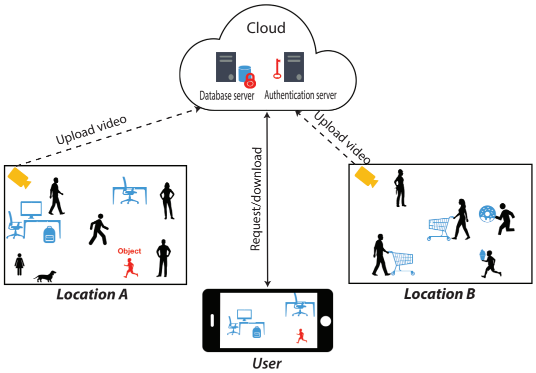

Figure 1: Cloud-based monitoring service.

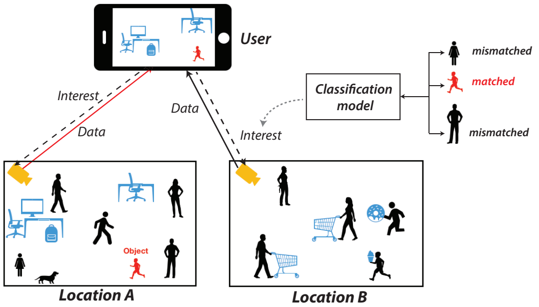

Figure 2: ICN-based CCP model for a monitoring service.

camera's location. Corresponding to ICN naming structure, each interest packet has a hierarchical name. We allow the user to request for a group of interested area (e.g., */monitoring/NY/central-park/*) or specific to a camera (e.g., */monitoring/NY/central-park/camera_id/*). After a camera receives the interest packet from the user, it verifies the classification model with its signature matching with the signature of the user. The signature does an important role in this monitoring service to prove the integrity and authority of the classification model and the user. Therefore, the signatures of classification model and users are bound to each other. We leave considering the signature mechanism for the future work. The cameras verifies the signatures of the classification model and the user. After the signatures are approved, the camera classifies the target object with the classification model. The result of the classification is encrypted with the user's public key. We assume that the camera receives the user's public key via a secure channel (e.g., SSL/TLS/SSH). There are two types of the data packet; one encapsulates the matched object and background resulted by the image recognition process from the camera, and another one encapsulates the acknowledgement message to inform no matched object. The data packet with the same name as the interest packet are sent back to the user.

2.3 Preliminary analysis

This section presents the performance and privacy analysis of the ICN-based CCP model for monitoring services comparing to the cloud-based ones as shown in Figs. 1 and 2. With the cloud-based services, all cameras have to upload their video data to the cloud in the encryption format. The cloud itself has to manage the key and the access control policy. In contrast, the ICN-based CCP model enables the access control policy central to the (target image) content itself. The cameras (or data owners) do not leak the video data to the third party.

To analyze the privacy of the ICN-based CCP model, let us define weak and strong W^3-privacy as follows. The service has *weak* W^3*-privacy* against an entity if the entity, who collects interest/data packets, learns any of three dimensions (i.e., *what*, *who* and *where*), but not all of them. In contrast, the service has *strong* W^3*-privacy* against an entity if the entity learns nothing from all of those three dimensions. Let $\mathcal{A}$ be an adversary who aims to learn the private information by eavesdropping interest/data packets from the network. We assume that $\mathcal{A}$ can compromise some of routers in the network. Nonetheless, $\mathcal{A}$ cannot compromise neither users and the cameras and also cannot break the secure channel. Table 1 summarizes the analysis of privacy preserving for the target object w.r.t. the W^3-privacy. The ICN-based CCP model satisfies the *weak* W^3-privacy against a camera (which has the target object), while it satisfies the *strong* W^3-privacy against an adversary and the other cameras. The reason is that the other cameras, which cannot matched the target object with their own data, cannot know *where* the target object is, while they also cannot know *what* the target object is (e.g., the correlation between the user and the target object). The adversary learn nothing from the interest and data packet. Unlike the cloud-based services, the cloud can learn *what*, *who* and *where* information from the query and the results of the image processing.

Table 1: Analysis of data disclosure to the entities with respect to the W^3 privacy. ("✓": disclosure; "x": oblivious).

W^3 privacy	ICN-based CCP model		Cloud-based	
	Cameras	Adversary	Cloud	Adversary
What	x	x	✓	x
Who	x	x	✓	x
Where	✓	x	✓	x

3 OPEN ISSUES AND FUTURE DIRECTIONS

There are some open issues that should be considered in the future for privacy and efficiency improvement. First, should a target be monitored with his/her consent? Second, how much does the error of image recognition impact the privacy? Finally, there might be a need of cross verification of the classification model.

ACKNOWLEDGEMENTS

This work is paper partly supported by the Horizon2020/NICT EU-JAPAN ICN2020 project, Grant Agreement No. 723014 and Contract No. 184. We would like to thank Dr. Kanokphan Lertniphonphan, KDDI Research, Inc. for the fruitful discussion.

REFERENCES

[1] Kanokphan Lertniphonphan, Supavadee Aramvith, and Thanarat Chalidabhongse. 2011. A Background Modeling for Non-Empty Scene Videos. In *The 14th International Workshop on Advanced Image Technology 2011 (IWAIT)*.
[2] Antoni Martínez-Ballesté, Pablo A. Pérez-Martínez, and Agusti Solanas. 2013. The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *IEEE Commun. Magazine* 13, 9 (2013), 136–141.