A Selective Privacy-Preserving Approach for Multimedia Data

Huining Li and Kun Wang
Nanjing University of Posts and Telecommunications

Xiulong Liu
The Hong Kong Polytechnic University

Yanfei Sun
Nanjing University of Posts and Telecommunications

Song Guo
The Hong Kong Polytechnic University

Improved mobile devices and wireless networking technologies have created an explosion of multimedia data—and privacy leakage issues. To address such issues, a proposed method allocates encryption resources according to each packet's privacy weight and execution time.

With the significant improvements in mobile digital devices and wireless networking technologies, we are experiencing a promising multimedia era, with benefits in fields ranging from intelligent transport systems to social networking to healthcare and business forecasting.[1] Because of the volume explosion and heterogeneity of multimedia data, researchers have proposed many applications and services, including video conferencing, intelligent video monitoring, and location-based supporting systems.[2] However, these novel applications and advanced technologies entail not only an ever-growing volume of multimedia data but also considerable security issues. Multimedia data is extremely easy for attackers to eavesdrop on and access during transmission via wireless medium, especially in large-scale networks.[3,4]

Here, we focus on privacy leakage issues in multimedia systems, and we study how to maximize total privacy weights and upgrade security levels under predefined time and resource constraints. To this end, we propose a selective privacy-preserving method to adaptively allocate encryption resources according to the privacy weight and execution time of each data package, and to choose for each package the encryption method with the appropriate complexity and security level.

Our approach randomly divides data into two parts and then performs XOR operations with a generated cipher key in different cloud storage servers to prevent users' original information from being attacked by untrusted cloud operators. Here, we offer an overview of the issues and our solution, then describe our model for privacy data encryption. We also discuss our simulation results, which demonstrate our approach's advantages and improvements over previous schemes.

Problem Overview

Multimedia—including text, image, audio, and video—accounts for a large amount of Internet and mobile communication traffic. As examples, consider that Facebook generates about 500 Tbytes of social data each day, Walmart processes millions of customers' transaction information per hour, and airplanes each generate several hundred Tbytes of flight data per flight.[5]

Multimedia data is heterogeneous, vast in volume, and dynamically generated anytime and anyplace across the entire multimedia network (see Figure 1). This data includes not only simple dates, numbers, and strings but also real-time 3D, audio, video, geographic, and log data.[6,7]

Data Classification and User Privilege

We can classify multimedia data into different groups depending on privacy sensitivity levels. For instance, personal electronic medical records, license plate numbers, and facial information gathered in monitoring videos should have larger privacy weights and require higher levels of security protection than other common information.

Moreover, a user's multimedia data access privileges should change at different places and at different times. For example, staff members might be permitted to access important

1070-986X/17/$33.00 ©2017 IEEE

business data only when inside the company's internal network and not from the network when they are at home.

Traditional Solutions

Traditional encryption methods are feasible in multimedia systems, but they entail two main challenges. First, battery-powered mobile sensing equipment must handle massive amounts of multimedia with limited energy resources, which might result in high computational complexities on weak nodes during the encryption process.

Second, there is no universal privacy encryption mechanism appropriate for all applications, and thus an adaptive encryption adjustment mechanism is desirable to satisfy specific application demands.

Unlike traditional privacy-protection methods, we propose a selective model for privacy data encryption in multimedia systems. Our model can allocate encryption resources reasonably to maximize the total privacy weight values and promote the security level under limited time and resources. (For more information, see the "Related Work in Multimedia Data and Privacy" sidebar.)

Our Solution

Our objective is to carry out flexible security protection schemes for multimedia data that can be easily changed according to various access permissions. To this end, we introduce a privacy data encryption model to guarantee privacy security in multimedia systems: it first categorizes the data packages into multiple groups based on the level of privacy weight, and then decides whether a data package needs to be encrypted or not.

Our study cases are multiple data packages that require selective encryption methods to encrypt selective data packages. We introduce a parameter related to privacy weight value and the operation time of every data package to decide the encryption order. To reduce heavy load and high latency, input data packages to be encrypted are first randomly split into two separate components, and then transmitted to different cloud storage servers; this avoids having the original users' personal information directly leaked to cloud operators. When users want to retrieve data from cloud servers, we take the encrypted data from different cloud storages and execute decryption operations.

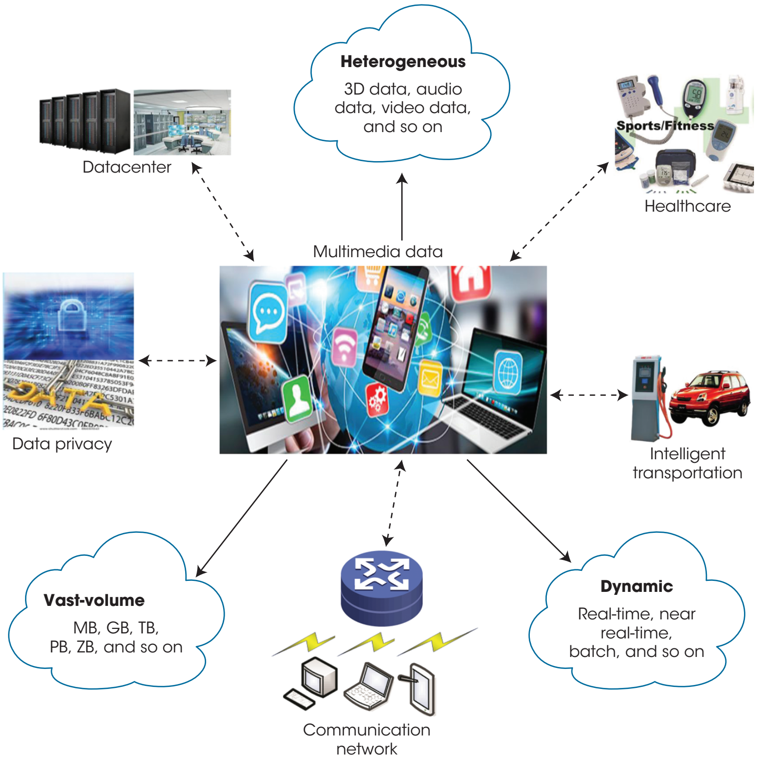
Heterogeneous
3D data, audio data, video data, and so on
Datacenter
Sports/Fitness
Healthcare
Multimedia data
Data privacy
Intelligent transportation
Vast-volume
MB, GB, TB, PB, ZB, and so on
Communication network
Dynamic
Real-time, near real-time, batch, and so on

FIGURE 1. Multimedia data system and sources. Multimedia data is generated anytime and anyplace in the multimedia network, which is heterogeneous, vast, and dynamic.

Our model's main contributions are as follows:

- We consider both resource and time-delay constraints in multimedia systems. We transform the restricted conditions of resource and time into concrete mathematical expressions, which simplifies the theoretical analysis.
- We formulate a single objective optimization problem with constraints of time delay and resources, thereby figuring out the maximum total privacy weights from a set of variables containing the amount of data package types, the privacy weight for each data package, and the operation time for the data with encryption and non-encryption.
- We propose a data-split-based encryption method to prevent malicious cloud

Related Work in Multimedia Data and Privacy

Here, we offer an overview of related work on multimedia data and privacy preservation approaches.

Multimedia Data

Janani Kalyanam and Gert Lanckriet proposed a methodology based on histogram methods—which are typically designed for unimodal data—to express unstructured multimodal data for studying heterogeneous multimedia data.[1] The authors also explore how prototypical features or code words on these histograms are explained.

One of us (Kun Wang) and his colleagues put forward a video-analysis-based hybrid-stream model in mobile Internet for multimedia data preprocessing, multimedia data classification, and multimedia data-load-reduction processing.[2] This model is designed to cut network load to a dynamic threshold by adjusting the parameter σ to control the video's input size.

Yilin Yan and his colleagues studied high-level semantic mining and retrieval in multimedia data for exploring an effective and universal cluster computing engine.[3] They investigated negative correlation in semantic concept mining via deeply analyzing large-scale repositories, which were in the Hadoop MapReduce framework.

Shangfei Wang and her colleagues set up a three-layer restricted Boltzmann machine model for multiple emotion media tagging.[4] They abstracted multimedia features from multimedia data and collected measurements of multiple emotion labels using a traditional classifier. The proposed model is built to explore higher-order relationships between emotion labels and measurements.

Grant Strong and Minglun Gong developed a self-sorting map algorithm that transforms the continuous optimization problem into a discrete labeling problem for organizing and presenting multimedia data, where the relevant items are put together and the irrelevant ones are separated.[5] This algorithm is designed to categorize data items in parallel and arrange millions of multimedia data in seconds.

Sandhya Shirale and his colleagues set up a novel system consisting of image processing and Hadoop and video processing that uses the Hadoop distributed file system and MapReduce framework for the storage and parallel processing of large-scale multimedia data.[6] The system enhances the transcoding speed and the image and video quality.

Privacy Preservation

Abid Mehmood and his colleagues offered a comprehensive survey of the privacy-protection methods in big data at different stages, including data generation, data storage, and data processing phases.[7] They compare various encryption schemes; identity-based encryption, attribute-based encryption, proxy re-encryption, and homomorphic encryption are compared in terms of features and limitations.

Jingyu Hua and his colleagues put forward a cryptographic technology-based privacy-preserving utility verification methodology that investigates data utilities according to encrypted frequencies rather than plain values of aggregated raw data.[8] Furthermore, this method detects the validity of encrypted frequencies supplied by publishers to discover dishonest publishers.

Chi Chen and colleagues proposed a hierarchical clustering methodology for fast cipher text searching on massive amounts of encrypted data, which could effectively avoid privacy-information leakage in the search phase.[9] This methodology could obtain linear computational complexity against exponential growth in encrypted data; to address this the authors also introduce a minimum hash subtree structure to check result authenticity.

Arjman Samuel and his colleagues designed a framework for composition and enforcement of context-aware disclosure rules to preserve privacy in multimedia data systems.[10] The intelligent privacy-manager prototype is also used to set up secure, private sharing of multimedia data, which could be used in multiple applications, such as Facebook.

References

1. J. Kalyanam and G. Lanckriet, "Learning from Unstructured Multimedia Data," *Proc. 23rd Int'l Conf. World Wide Web*, ACM, 2014, pp. 309–310.
2. K. Wang et al., "Real-Time Load Reduction in Multimedia Big Data for Mobile Internet," *ACM Trans. Multimedia Computing, Comm., and Applications*, vol. 12, no. 5, 2016, pp. 76:1–76:20.
3. Y. Yan, M. Shyu, and Q. Zhu, "Negative Correlation Discovery for Big Multimedia Data Semantic Concept Mining and Retrieval," *Proc. IEEE 10th Int'l Conf. Semantic Computing (ICSC)*, 2016, pp. 55–62.

4. S. Wang et al., "Multiple Emotion Tagging for Multimedia Data by Exploiting High-Order Dependencies Among Emotions," *IEEE Trans. Multimedia*, vol. 17, no. 12, 2015, pp. 2185–2197.
5. G. Strong and M. Gong, "Self-Sorting Map: An Efficient Algorithm for Presenting Multimedia Data in Structured Layouts," *IEEE Trans. Multimedia*, vol. 16, no. 4, 2014, pp. 1045–1058.
6. S. Shirale et al., "Online Multimedia Data Processing on Cloud and Hadoop Platform," *Int'l J. Computer Technology and Electronics Engineering* (IJCTEE), vol. 5, no. 2, 2015, pp. 21–24.
7. A. Mehmood et al., "Protection of Big Data Privacy," *IEEE Access*, vol. 4, 2016, pp. 1821–1834.
8. J. Hua et al., "Privacy-Preserving Utility Verification of the Data Published by Non-Interactive Differentially Private Mechanisms," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 10, 2016, pp. 2298–2311.
9. C. Chen et al., "An Efficient Privacy-Preserving Ranked Keyword Search Method," *IEEE Trans. Parallel and Distributed Systems*, vol. 27, no. 4, 2016, pp. 951–963.
10. A. Samuel et al., "A Framework for Composition and Enforcement of Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data," *IEEE Trans. Multimedia*, vol. 17, no. 9, 2015, pp. 1484–1494.

operators from violating the privacy of the user data. Specifically, this method performs the XOR operation with a generated cipher key, where the following $(i + j)$ block of data packages can be protected by the prior i block of data packages and the length of block j can be adjusted to control the encryption rate so as to satisfy different requirements in privacy protection.

We now describe our model and its performance results in more detail.

System Model and Assumptions

If we had enough computation resources for data encryption or if a long text could be encrypted without a time limitation, conventional encryption methods would be suitable. In conventional encryption methods, all symbols and bits are assumed to be of equal significance in plaintext, and average resources are allocated to encrypt them. However, large-scale multimedia sensing systems and collaborative work produce massive amounts of multimedia data, creating great challenges for protecting data privacy given the limited computation and energy resources. Therefore, it is inappropriate to use conventional encryption methods to allocate encryption resources for privacy protection for multimedia.

As Figure 2 shows, our proposed selective model for privacy data encryption can carry out reasonable allocation of encryption resources to increase the security of multimedia data because it considers both resource and time constraints. $\Psi(D,DES)$ and $\Omega(D,DES)$ represent the function of total used resources and operation time, respectively. We introduce an adjustable parameter α $(0 \le \alpha \le 1)$ to balance between resource and time constraints for maximum total privacy weight values Φ. Our selective model can be mathematically expressed as follows:

$$max\ \Phi = \alpha\, \Phi_1 + (1 - \alpha)\, \Phi_2,$$

$$such\ that\ \Psi\ (D,DES) \le M,$$

$$\Omega(D,DES) \le T_m,$$

where D and DES represent the multimedia data set and corresponding multimedia data encryption scheme, M is denoted as the extreme value of throughput of general encryption schemes on network nodes, and T_m is denoted as the limited time.

If M is a single data package, MES can be the corresponding data encryption scheme. If M contains multiple data packages, MES means a whole scheme system consisting of selective data packages to be encrypted and selective encryption methods to be used. Our model is constructed to arrange encryption order and encryption algorithm for every data

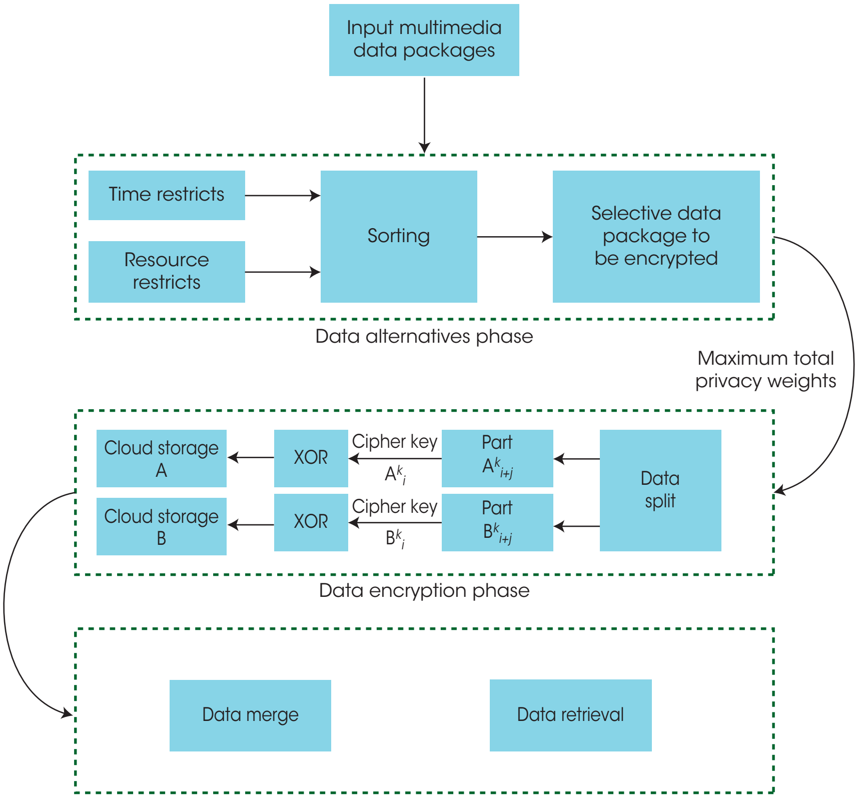

FIGURE 2. The proposed selective privacy-preserving model. Our model contains a data alternatives phase and a data encryption phase.

package with highest security, as well as reasonably allocate encryption resources under constraints. Here, we focus on cases of multiple data packages.

Our proposed selective model must consider three key aspects. First, having both mobile and static nodes is rare in multimedia sensing systems, so the encryption scheme must be designed to avoid heavy loads. Second, the encryption scheme should be able to analyze and resist some attacks using surveillance videos and cooperative applications. Third, a rate-adjustable encryption algorithm is required because of the unstable fluctuation of the multimedia data stream's bandwidth over time. Thus, we introduce a fast multimedia encryption scheme that can adjust the encryption speed in our model. The encryption process can be briefly expressed as

$$CipherD^{k}_{i+j} = PlainD^{k}_{i} \oplus PlainD^{k}_{i+j},$$

where $CipherD^{k}_{i+j}$ is the cipher text of data package with byte k, $PlainD^{k}_{i+j}$ is the plaintext of data package with byte k, and $PlainD^{k}_{i}$ is the generated cipher keys with byte k. The following $(i + j)$ block of data packages can be protected by the prior i block of data packages. The length of block j is controllable for speed adjustment.

Mulitmedia Privacy Protection

Here, we describe our selective model for data encryption to protect privacy in a multimedia system, focusing on our selective privacy-preserving and data-split-based encryption methods.

Selective Privacy-Preserving Method

To upgrade the privacy-protection level and maximize the total privacy weights under resource and time constraints, we propose a selective privacy-preserving method (see Algorithm 1 in Figure 3). Here, we first simplify the multimedia big data system and define some system parameters.

Large-scale multimedia data streams flow in this system; we define the amount of data streams in a particular time as l. The set $D = \{D_1, D_2, \ldots D_l\}$ is denoted as different data streams in a particular time. We assume the data stream bandwidths are stable in a particular time, defining those bandwidths as $b = \{b_1, b_2, \ldots b_l\}$.

Under different encoding standards, multimedia data can be encrypted by different encryption schemes. We denote $E_k = \{E_{k1}, E_{k2}, \ldots E_{kl}\}$ as selected encryption schemes that are used to protect privacy data. Different privacy data encryption schemes have different data encryption rates and security levels, and they are important performance indexes for protecting privacy data. The set $v = \{v_1, v_2, \ldots v_l\}$ represents data encryption rates, where $0 \leq v_i \leq 1$. The data encryption rate is affected by different data encryption types, such as identity-based encryption, attribute-based encryption, proxy re-encryption, and homomorphic encryption. The data encryption rate can be acquired automatically according to the pre-known data package size and encryption type. The set $s = \{s_1, s_2, \ldots s_l\}$ represents the security levels of encryption schemes, where $0 \leq s_i \leq 1$ and $s_i = S_{E_{ki}}(v_i)$.

In addition, we introduce $w = \{w_1, w_2, \ldots w_l\}$ to express the privacy weight value of each type of data package. The privacy weight value is a criterion to categorize various privacy incidents into different levels based on the incident's characteristics. For instance, in a real-time video streaming case to monitor one person's location status, the privacy weight values vary according to location characteristics. If that person goes to the shopping mall or other public places, the location data is automatically set to low privacy weight values. If the person goes home, the location data is automatically set to high privacy weight values.

```
Input: $x_i$, $w_{x_i}$, $N_{x_i}$, $T^1_{x_i}$, $T^0_{x_i}$, $T_m$, $M$, $v_j$
Output: $\{Z\}$, $max \sum_{i=1}^{l} (w_{x_i} * N^1_{x_i})$, $max \sum_{i=1}^{l} (v_i * w_i)$
set $\{Z\} = \phi$; set $i = 0$;
set $\lambda_{x_i} = \frac{w_{x_i}}{T^1_{x_i}}$;
start with the $x_i$ with the highest priority;
repeat
    Select $x_i$ according to the descend order of $\lambda_{x_i}$ value;
    for $\forall\, x_i$, $1 \leq i \leq N_{x_i}$ do
        if $\tau > T^1_{x_i} - T^0_{x_i}$ then
            Add one $x_i$ to $\{Z\}$;
            $\tau = \tau - T^1_{x_i} + T^0_{x_i}$;
        else
            Break
        end
        $i = i + 1$;
    end
until $\sum_{j=1}^{l} (b_j * v_j) > M$, or
    $\sum_{m=1}^{l} (T^1_{x_m} * N^1_{x_m}) + \sum_{n=1}^{l} (T^0_{x_n} * N^0_{x_n}) > T_m$;
```

FIGURE 3. Algorithm 1—the selective privacy-preserving algorithm. It is designed for maximum total privacy weights, taking both resource and time constraints into consideration.

The size of multimedia big data grows even larger in a multimedia system. However, the computation and energy resources are limited in network nodes, which might restrict the protection of privacy data. To increase the reliability of privacy protection and reduce encryption delays under resource constraints, the input of our proposed encryption scheme on network nodes must be less than the extreme value M, which means we need to satisfy the following expression:

$$\sum_{i=1}^{l} (b_i * v_i) \leq M.$$

We introduce three types of privacy data encryption schemes: full encryption, specific security-level encryption, and no encryption, represented as E_f, E_{sec}, and E$_n$, respectively. None of the three include data without encryption or with very low encryption rates, which can be overlooked. According to the encryption types for privacy data, we define the throughput of each type on network nodes as M_f, M_{sec}, and M_n. If input data throughput satisfies

$$\sum_{i=1}^{l} (b_i * v_i) > M_{sec},$$

data streams with higher privacy weight values are protected by E_{sec} schemes, while the others are left with no encryption. On the contrary, if input data throughput satisfies

$$\sum_{i=1}^{l}(b_i * v_i) \le M_{sec},$$

all of the data is protected by E_{sec} schemes at first. We then select more significant data and allocate redundant resources to the data, replacing the E_{sec} scheme with full encryption E_f.

To study total privacy weight values, we introduce an objective function for optimization:

$$\Phi_1(w_1, w_2, \ldots, w_l, s_1, s_2 \ldots s_l),$$

where $s_i = S_{E_{ki}}(v_i)$, $i \in [1, 2, \ldots, l]$; thus, s_i has relationships with encryption scheme E_k and data encryption rate v. So, we can write the objective function as

$$\Phi_1 (w, v, E_k).$$

Given the resource constraints, the optimization functions for maximizing total privacy weight values can be expressed as

$$max\ \Phi_1(w, v, E_k),$$
$$s.t.\ \sum_{i=1}^{l}(b_i * v_i) \le M.$$

However, in this optimization function, it is difficult to carry out the analytical expressions for every encryption scheme E_k. So, we select three aforementioned types of privacy data encryption schemes here—E_f, E_{sec}, and E_n. In the E_f scheme, encryption rate $v = 1$ and $s_i = S_{E_f}(v_i) \in (0,1]$. In the E_{sec} scheme, encryption rate $v = 1$ and $s_i = S_{E_{sec}}(v_i) \in (0,1]$. In the E_n scheme, encryption rate $v = 0$ and $s_i = S_{E_n}(v_i) = 0$. In all, a constant set $\{S_{E_f}$, $\mathrm{S}_{E_{sec}}$, $0\}$ is denoted as a security score for the three encryption schemes.

To better explore the optimization functions, we study a further simplified situation, in which we consider only two encryption schemes, E_f and E_n. This is a 0-1 knapsack problem, and the encryption type can be determined only by v. If $v = 1$, the full encryption scheme E_f is selected. Otherwise, the E_n scheme is used, which means privacy data will not be encrypted or will be encrypted at a very low rate. Next, the objective function $\Phi_{SEC}(w, v, E_k)$ is simplified to $\Phi_{SEC}(w, v)$. We use an approximate linear analytical model to assume

$$\Phi_1(w,v) = \frac{\sum_{i=1}^{l}(S_{E_k} * v_i * w_i)}{\sum_{i=1}^{l} w_i},$$

where S_{E_k} is from a constant set and

$$\sum_{i=1}^{l} w_j$$

has a fixed value that can be calculated at a particular time. Therefore, *max* $\Phi_1(w,v)$ is equivalent to

$$max \sum_{i=1}^{l}(v_i * w_i).$$

Finally, the simplified optimization functions for maximizing total privacy weight values at a particular time can be written as

$$max \sum_{i=1}^{l}(v_i * w_i),$$
$$s.t. \sum_{i=1}^{l}(b_i * v_i) \le M.$$

Having discussed resource constraints issues, we now explore how to acquire the maximum total privacy weight value under time constraints. Here, $x = \{x_i\}$ and $N = \{N_{x_i}\}$ represent data package types and the amount of data in every data package type, respectively, while w_{x_i} represents the privacy weight values of every data package. $T_{x_i}^1$ and $T_{x_i}^0$ are denoted as operation time for data with and without encryption, respectively, in package type x_i. Our goal is to maximize the total privacy weight value under time constraint T_m, which is expressed as

$$max\ \Phi_2\left(N_{x_i}, w_{x_i}\right) = \sum_{i=1}^{l}(w_{x_i} * N_{x_i}^1),$$

$$s.t.\ T_{sum} = \sum_{m=1}^{l}(T_{x_m}^1 * N_{x_m}^1) + \sum_{n=1}^{l}(T_{x_n}^0 * N_{x_n}^0) \le T_m,$$

where $\{x_m\}$ and $\{x_n\}$ represent encrypted and non-encrypted data packages, respectively.

In the data sorting process, we introduce a value λ_{x_i}, defined as

$$\lambda_{x_i} = \frac{w_{x_i}}{T^1_{x_i}},$$

where alternative priority is related to privacy weight value and the operation time of data package x_i. A time scope is also denoted as $[0, \tau]$, in which τ can be written as

$$\tau = T_m - \sum_{i=1}^{l} (T^0_{x_i} * N_{x_i}).$$

Next, the privacy data selective encryption process starts. The encryption order is decided according to λ_{x_i}. The data package with the highest λ_{x_i} value is encrypted first. This execution process will not stop unless the whole data package's encryption is completed or the time remaining is shorter than the operation time $T^1_{x_i}$ for the next data package.

We define the time remaining as T_r, which is related to the operation time for all data with and without encryption in package type x_i. When the data package x_i is allocated to be encrypted, the operation time with non-encryption ought to be added to T_r. At this point, T_r can be written as

$$T_r = \tau - \Sigma(T^1_{x_s} * N_{x_s}) + \Sigma(T^0_{x_s} * N_{x_s}),$$

where x_s represents the selected data packages, and $T_r \le \tau$. The selective encryption process ends when any remaining data package's operation time $T^1_{x_i}$ is higher than T_r. The output value is $max \sum_{i=1}^{l} (w_{x_i} * N^1_{x_i})$.

In all, taking both resource and time constraints into consideration, the expression of maximum total privacy weight values can be summarized as

$$max\ \Phi = \alpha\Phi_1 + (1 - \alpha)\Phi_2,$$

$$s.t. \sum_{i=1}^{l} (b_i * v_i) \le M,$$

$$s.t. \sum_{m=1}^{l} (T^1_{x_m} * N^1_{x_m}) + \sum_{n=1}^{l} (T^0_{x_n} * N^0_{x_n}) \le T_m,$$

where α can be adjusted according to different limited extents in resource and time. When time constraints impact the multimedia system more than resource constraints, we denote $\alpha \le 0.5$; otherwise, $\alpha > 0.5$.

```
Input: $P^k_{i+j}, A^k_{i+j}$
Output: $\alpha^k_{i+j}, \beta^k_{i+j}$
randomly generate one data package $A^k_{i+j}$ to start;
set $j = 0$;
repeat
    Generate cipher keys $A^k_i$;
    for $\forall A^k_{i+j}, 1 \le j \le u$ do
        if $A^k_{i+j} \neq \phi$ and $A^k_{i+j} \le P^k_{i+j}$ then
            $B^k_{i+j} = P^k_{i+j} - A^k_{i+j}$;
            $\alpha^k_{i+j} = A^k_i \oplus A^k_{i+j}$;
            $\beta^k_{i+j} = B^k_i \oplus B^k_{i+j}$;
        else
            break
        end
        $j = j + 1$;
    end
until Complete the last data package encrypting in buffer;
```

FIGURE 4. Algorithm 2—the data-split-based encryption method algorithm. Input data packages to be encrypted are first randomly split into two separate components and then transmitted to different cloud storage servers.

Data-Split-Based Encryption Method

Having studied our approach for maximizing total privacy weight values and security scores under resource and time constraints, we now explore data-split-based encryption approaches to better utilize limited resources and time, while also avoiding heavy load and high latency (see Algorithm 2 in Figure 4). The user's privacy data includes massive amounts of sensitive information, consisting of a string of data packages x_{i+j}. P_{i+j} is denoted as the input data packages to be encrypted. P_{i+j} are first randomly divided into two separated components, A_{i+j} and B_{i+j}, shown as

$$B_{i+j} = P_{i+j} - A_{i+j},$$

where $A_{i+j} \neq \phi$ and $A_{i+j} \le P_{i+j}$ are assumed.

Next, A_{i+j} and B_{i+j} are transmitted to cloud storage server 1 and cloud storage server 2, respectively, which prevents initial user data from directly leaking to cloud operators. The

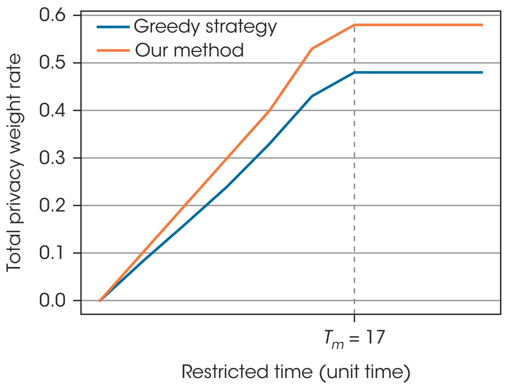

FIGURE 5. Total privacy weight rate curve under time constraints. The total privacy weight rate within T_m using our method is higher than using the greedy strategy.

randomly separated components and generated cipher key values are always unknown, which can greatly deter malicious attackers and protect privacy. The efficient data split mechanism guarantees data retrievability without heavy overload and latency. Next, a cipher key is generated by the plaintext of prior block i to protect the following $i + j$ block, in which $j \in [1, u]$. The parameter u can be adjusted to control the encryption rate. The rate-adjustable encryption strategy can effectively deal with fluctuations in the dynamic multimedia data stream bandwidth over time. We use the generated cipher key to do XOR operations with A_{i+j} and B_{i+j}, which can be written as

$$\alpha_{i+j}^{k} = A_i^k \oplus A_{i+j}^{k},$$
$$\beta_{i+j}^{k} = B_i^k \oplus B_{i+j}^{k},$$

where α_{i+j}^{k} and β_{i+j}^{k} are the cipher texts of a data package with byte k; A_{i+j}^{k} and B_{i+j}^{k} are the plaintexts of a data package with byte k; and A_i^k and B_i^k are the generated cipher keys with byte k. Finally, the α_{i+j}^{k} and β_{i+j}^{k} cipher texts are stored in cloud storage server 1 and cloud storage server 2, respectively. This encryption method can effectively solve data package loss issues. If one data package is missing, the following data package will not be affected and can continue to do encrypted operations.

Our proposed selective privacy-preserving method chooses the encrypted data pack's security level in the data alternative phase. When we have completed the data encryption phase and want to retrieve data from cloud servers, we know the security level of the data pack to be decrypted, so we simply take the encrypted data from cloud storage server 1 and cloud storage server 2 and execute XOR operations with the primary generated cipher keys, expressed as

$$\gamma_{i+j}^{k} = A_i^k \oplus \alpha_{i+j}^{k},$$
$$\eta_{i+j}^{k} = B_i^k \oplus \beta_{i+j}^{k}.$$

Then, γ_{i+j}^{k} is added to η_{i+j}^{k} to obtain the original data packages and this completes the privacy data decryption process.

Performance Simulation

We conducted simulations to verify the performance of our proposed selective privacy-preserving model. All the simulations were conducted using Python in a Sony server equipped with 8-core CPU, 9 Gbytes of memory, and Mongo DB. We installed a VMWare workstation and an Ubuntu 15.04 LTS Server to simulate the cloud environment.

Performance of Data Alternatives

In the data alternatives phase, we evaluated our proposed selective privacy-preserving method's performance by setting up a simulation based on four different types of data packages ($Q_1 - Q_4$) to be encrypted. The number of data packages for each type is Q_1: 3, Q_2: 4, Q_3: 2, and Q_4: 2. The privacy weight of each type of data package is defined as Q_1: 2.5, Q_2: 2, Q_3: 1.2, and Q_4: 1. The operation time of each type of data package varies. We also introduce a specific restricted time T_m in this simulation. When T_m is set as a 17-unit time, our method can generate the following data encryption plan: encrypt 4 Q_2, encrypt 1 Q_1, encrypt 1 Q_3, and do not encrypt Q_4, meanwhile, a greedy algorithm can generate the following strategy: encrypt 3 Q_1, encrypt 1 Q_2, and do not encrypt Q_3 and Q_4.

We simulated the curve of the total privacy weight rate for encrypted data packages under restricted time T_m using our proposed method and compared it with the greedy algorithm. As Figure 5 shows, the total privacy weight rate within T_m using our method can reach up to 59 percent, while the rate using the greedy strategy is 48 percent. Thus, our approach's total privacy weight rate is 11 percent higher than the greedy strategy, which shows superior performance.

Figure 6 shows the tradeoff between resource and time costs for pursuing a constant total privacy weight value in the data alternative process. The blue curve shows the relationship between resource cost and α, while the green curve shows the relationship between time cost and α. As the figure shows, when α ranges from 0.36 to 0.6, we obtain an optimized area for balancing resource and time costs. That is, if we control α between 0.35 and 0.6, we can acquire maximum total privacy weight values while taking both time and resource constraints into consideration.

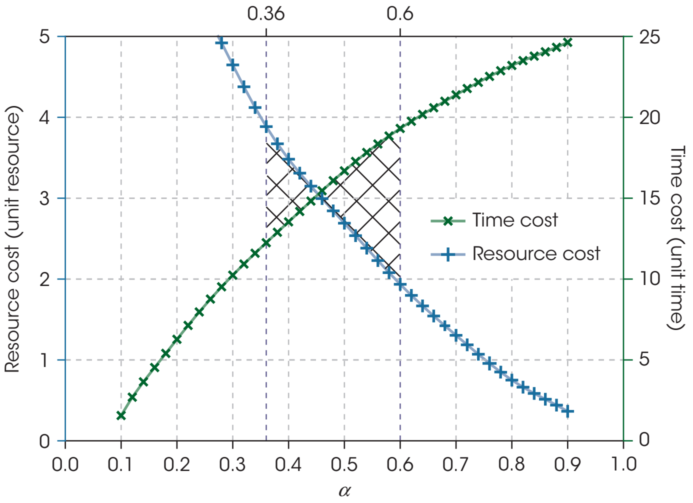

FIGURE 6. The tradeoff between resource and time costs. An optimized area for balancing resources and time can be obtained when α ranges from 0.36 to 0.6.

Performance of Data Encryption and Retrieval

In the data encryption and retrieval phase, we evaluate our proposed data-split-based encryption method by simulating the operation time with different input data sizes. Figure 7 shows a comparison of the operation times of our data encryption and data retrieval methods with the Advanced Encryption Standard (AES)[8,9] for data encryption, with input data sizes of 10, 50, and 250 Mbytes. Our data encryption method has the shortest operation time, while our data retrieval method's time is a bit longer; both of our methods have a lower operation time than AES. Figure 8 shows similar results when the input data sizes are 1 and 5 Gbytes. With the increase of input multimedia data size, the operation time for data encryption and retrieval grows exponentially.

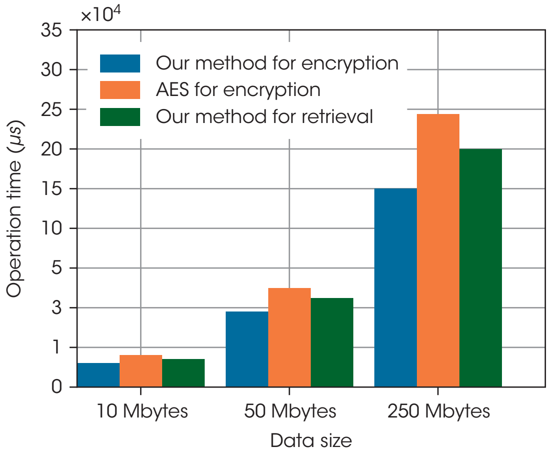

FIGURE 7. The comparison of operation time with data sizes of 10, 50, and 250 Mbytes. Both our proposed data encryption method and data retrieval method have a lower operation time than the Advanced Encryption Standard (AES).

Multisource and heterogeneous multimedia data are generated throughout the entire multimedia network. The network QoS must be considered owing to network heterogeneity. The size of multimedia data boosts rapidly and can even reach Terabytes, so higher throughput and quicker responses are required. Our future research will focus on promoting the robustness of the privacy preserving method in a realistic multimedia data environment. MM

Acknowledgments

This work is supported by the National Natural Science Foundation of China (NSFC 61572262, 61772286, 61533010, 61373135, 61571233, and 61532013); the National

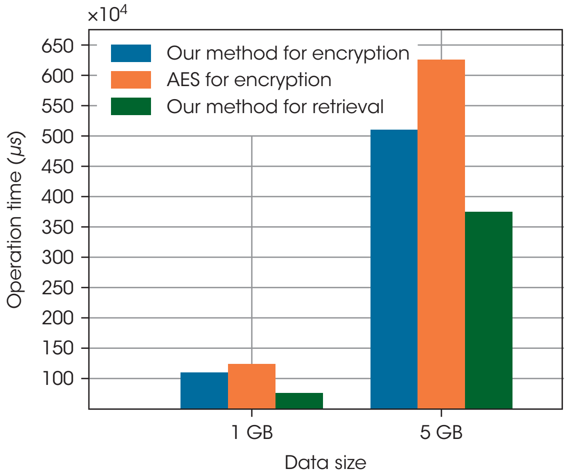

FIGURE 8. The comparison of operation time with data sizes of 1 and 5 Gbytes. Both our proposed data encryption method and data retrieval method have a lower operation time than AES.

China 973 Project (2015CB352401); the NSF of Jiangsu Province (BK20141427); and the China Postdoctoral Science Foundation (2017T100297, 2017M610252).

References

1. C. Zhu et al., "Multi-Method Data Delivery for Green Sensor-Cloud," *IEEE Comm,* vol. 55, no. 5, 2017, pp. 176–182.
2. S. Pudlewski, A. Prasanna, and T. Melodia, "Spatio-Temporal Analysis for Human Action Detection and Recognition in Uncontrolled Environments," *IEEE Trans. Mobile Computing*, vol. 11, no. 6, 2012, pp. 1060–1072.
3. K. Wang et al., "Strategic Anti-Eavesdropping Game for Physical Layer Security in Wireless Cooperative Networks," *IEEE Trans. Vehicular Technology*, vol. PP, no. 99, 2017; doi: 10.1109/TVT.2017.2703305.
4. K. Wang et al., "Big Data Analytics for System Stability Evaluation Strategy in the Energy Internet," *IEEE Trans. Industrial Informatics*, vol. 13, no. 4, 2017, pp. 1969–1978.
5. D. Liu et al., "Compressed-Sensing-Enabled Video Streaming for Wireless Multimedia Sensor Networks," *Int'l J. Multimedia Data Engineering and Management* (IJMDEM), vol. 6, no. 1, 2015, pp. 1–8.
6. Y. Yan, M. Shyu, and Q. Zhu, "Negative Correlation Discovery for Big Multimedia Data Semantic Concept Mining and Retrieval," *Proc. IEEE 10th Int'l Conf. Semantic Computing (ICSC)*, 2016, pp. 55–62.
7. K. Wang et al., "Wireless Big Data Computing in Smart Grid," *IEEE Wireless Comm.*, vol. 24, no. 2, 2017, pp. 58–64.
8. A. Alahmadi et al., "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard," *IEEE Trans. Information Forensics and Security*, vol. 9, no. 5, 2014, pp. 772–781.
9. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields," *IEEE Trans. Very Large Scale Integration Systems*, vol. 19, no. 1, 2011, pp. 85–91.

Huining Li is a doctoral student in information acquisition and control at Nanjing University of Posts and Telecommunications in Nanjing, China. Her research interests include big data analysis, information and network security, and energy management. Li received a B.Eng in electronic science and technology from Nanjing University of Information Science and Technology (NUIST). Contact her at huinli@outlook.com.

Kun Wang (the corresponding author) is a research fellow in the Department of Computing at Hong Kong Polytechnic University and a full professor in the National Engineering Research Center of Communications and Networking, Nanjing University of Posts and Telecommunications. His research interests include big data, wireless communications and networking, the smart grid, the energy Internet, and information security technologies. Wang received a PhD in computer science from the School of Computer Science & Technology at Nanjing University of Posts and Telecommunications. He is a senior member of IEEE. Contact him at kwang@njupt.edu.cn.

Xiulong Liu is a postdoctoral fellow in the Department of Computing at The Hong Kong Polytechnic University. His research interests include wireless sensing, ubiquitous computing, and the Internet of Things. Liu has a PhD in computer science from the School of Computer Science and Technology, Dalian University of Technology, China. He is a member of IEEE. Contact him at xiulongliucs@gmail.com.

Yanfei Sun is a professor in the College of Telecommunication and Information Engineering, Nanjing University of Posts and Telecommunications. His research interests include the future network, the industrial Internet, big data management and analysis, and intelligent optimization control. Sun received a PhD in communication and information systems from the Nanjing University of Posts and Telecommunications. Contact him at sunyanfei@njupt.edu.cn.

Song Guo is a professor in the Department of Computing at The Hong Kong Polytechnic University. His research interests include cloud and green computing, big data, wireless networks, and cyber-physical systems. Guo received a PhD in computer science from University of Ottawa. He is a senior member of IEEE, an IEEE Communications Society Distinguished Lecturer, and a senior member of ACM. Contact him at song.guo@polyu.edu.hk.