Received: 31 May 2019 | Revised: 21 July 2019 | Accepted: 11 August 2019
DOI: 10.1002/ett.3779

SPECIAL ISSUE ARTICLE

WILEY

Credible and economic multimedia service optimization based on game theoretic in hybrid cloud networks

Tengfei Cao[1,2] | **Lujie Zhong**[3] | **Han Xiao**[1] | **Chengru Song**[1] | **Shujie Yang**[1] | **Changqiao Xu**[1]

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China

[2]Department of Computer Technology and Applications, Qinghai University, Xining, China

[3]Information Engineering College, Capital Normal University, Beijing, China

Correspondence
Changqiao Xu, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China.
Email: cqxu@bupt.edu.cn

Present Address
Changqiao Xu, No.10, Xitucheng Road, Haidian District, Beijing City, China

Funding information
National Natural Science Foundation of China, Grant/Award Number: 61871048, 61872253 and 61762074; BUPT Excellent PhD Students Foundation, Grant/Award Number: CX2018208; Open Foundation of State key Laboratory of Networking and Switching Technology (BUPT), Grant/Award Number: SKLNST-2019-2-04; Chunhui Plan of Ministry of Education, Grant/Award Number: z2016081; Qinghai University, Grant/Award Number: SY201907

Abstract

The cloud network has the advantages in efficiently offloading the large-scale Internet traffic, which is considered as a promising architecture to provide the satisfactory multimedia services for mobile users. However, most current studies lack the joint consideration of economic and security of services in hybrid cloud networks. In this paper, a novel multimedia service optimization mechanism is proposed hereby to meet the user's requirements mentioned above while guaranteeing the reliability of service. Firstly, a credible scheme is designed to help the mobile users distinguish the reliable cloud providers. Meanwhile, a blockchain-based content credibility approach is further designed to guarantee the reliability and integrity of video contents. Moreover, a noncooperative Stackelberg game model is presented to maximize the profit of each party. Furthermore, the equilibrium of this game is achieved by the methods of backward induction and gradient descent. Finally, extensive simulations demonstrate that our solution has efficient performance in terms of secure service ratio, utility, service pricing, etc.

1 | INTRODUCTION

With the rapid development of wireless communication technologies and the popularity of mobile devices, a variety of multimedia services, such as interactive live video, immersive media, online gaming, etc, have sprung up.[1,2] These large-scale multimedia applications have led to an exponential growth in wireless network traffic and increasingly account for 82% of mobile Internet traffic in 2022.[3] This growth trend puts tremendous pressure on the current mobile network. To

This paper is recommended from INFOCOM ICCN 2019.

TABLE 1 Comparison of existing works

Literatures	Credible	Cost	Multimedia	Hybrid clouds
Hybrid cloud applications[16-19]	No	Little	No	Yes
Multimedia service in clouds[20,21]	No	Little	Yes	No
Service security[22-24]	Yes	No	Little	Little
Pricing optimization[25-28]	No	Yes	No	Little
Our proposed method	Yes	Yes	Yes	Yes

tackle this issue, the cloud network as a potential solution provides a beam of light to the conflict between transmission performance and quality of experience.[4,5] In particular, edge clouds (ECs) have the natural advantage to efficiently mitigate redundant transmissions from central cloud (CC)[6,7] and provide satisfactory quality of service for mobile users (MUs).

Although cloud networks can solve the problem of large-scale traffic offloading, it still faces several crucial challenges. Firstly, both the CC and ECs need to pay cost such as bandwidth and energy to satisfy the diversified service demands of mobile users.[8-10] Thus, it is necessary to investigate an economic incentive approach to coordinate CC and ECs, where the revenue and consumption should be considered to determine the pricing strategy for each party. Secondly, the ECs are managed by different operators. Due to the fragility of management, some ECs are more vulnerable while facing external attacks, which leads to untrustworthy services.[11,12] At the same time, the video contents obtained by MUs are still vulnerable to modification, castration, and deletion.[13,14] Therefore, the credibility of each cloud and service content also should be taken into account to guarantee the security of multimedia service in hybrid clouds. Motivated by the above aspects, economic and credible multimedia services are essential for mobile users in hybrid cloud networks.

Even though the existing solutions provide valuable insights in service optimization, most of them lack the joint consideration of economic and security of services in cloud networks, which is urgent to be resolved (a detailed overview of the state of the art is presented in Section 2). For this purpose, a novel service optimization mechanism based on Stackelberg game is proposed hereby to effectively achieve the above targets, which is a significant extension of our previous work.[15]

The main contributions of this paper are listed as follows.

- A credible service provider evaluation scheme is designed according to the interactive behavior to help the mobile users identify the reliable cloud providers, which is inferred by direct credibility and indirect credibility.
- A blockchain-based content credibility approach is further presented to indicate whether the video content is reliable and has not been tampered with, which is calculated by a carefully crafted smart contract to audit the video possession and history records.
- A noncooperative Stackelberg game model is proposed between mobile users and cloud service providers, where the equilibrium of the game is analyzed by the methods of backward induction and gradient descent.
- Extensive simulations are conducted to evaluate the performance of the proposed method. Experiment results validate the effectiveness of our solution in terms of secure service ratio, utility, pricing, and service requirements.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 presents the system model in cloud networks. Section 4 proposes the credible multimedia service mechanism. Section 5 formulates the optimization problem. Section 6 provides the analysis of the game process. Section 7 conducts the simulation experiment. Section 8 concludes this paper.

2 | RELATED WORK

Service optimization and application methods in cloud networks recently attracted the growing attention from the scientific community. In this section, related works on those subjects are summarized and qualitatively compared to our approach (see also Table 1).

2.1 | Cloud network applications

Extensive application research has been conducted on cloud networks. Pan and McElhannon[16] propose the method that an edge cloud node has an offload effect to the central cloud computing platform while lacking the consideration of collaboration between these service clouds. Rimal et al[17] point out central cloud and edge cloud can coexist and complement each other in cloud networks, playing a mutually supportive role. Weinman[18] considers that the future network is a hybrid cloud architecture and the distributed edge cloud will complement the central cloud. As each user has the price-optimized statistics across multiple clouds, these hybrid clouds can be proven to be economically optimal through the dynamic pricing strategy. Zeng et al[19] investigate a green fog computing platform in the cyberphysical system, which jointly considers service data rates, load balancing, and replica deployment to provide the energy-efficient service composition. Jin and Wen[20] propose a novel network function virtualization–based multimedia cloud system, including end-to-end and layered view perspectives. The authors further describe the architecture ranging from the optimal resource provision to automated optimization. Experimental results show that the cost of multimedia services provided by network function virtualization–based cloud system can be substantially reduced. Imagane et al[21] design an edge cloud system based on the OpenStack deployment. This system utilizes the grained service slicing and chaining to achieve the efficient and low-latency multimedia service provisioning.

Based on the above overview, it can be observed that service applications in cloud networks have recently been extensively studied. However, most of the previous works did not consider the service reliability of applications in cloud networks.

2.2 | Service optimization management

There are increasing researches on service optimization in cloud networks. Nie et al[22] consider highly of the security in cloud platform, but their main purpose is to solve the information privacy rather than the reliability of cloud nodes. Chen et al[23] quantitatively analyze the impact of credibility by stochastic geometry and set the trusted node as high priority to ensure the security of service. Jimenez et al[24] propose a new hybrid cloud architecture to manage the multimedia resource. The hybrid platform combines multiple cloud computing models and considers both the levels of QoS and the security of cloud environment. Nevertheless, due to the imbalance of interests of all parties, the economic services cannot be effectively guaranteed. Zeng et al[25] investigate how to reduce the overall cost for purchasing the services from edge clouds. The authors jointly consider the data scheduling and the network resource allocation without any prior knowledge. The tradeoff between the queue backlog and the service cost is achieved by using the Lyapunov optimization. Liu and Liu[26] propose a price-based Stackelberg game method to optimize the offloading problem of computing task in edge clouds. First, a unified and differentiated pricing algorithm is developed to maximize the revenue of the edge cloud. Then, the users make offloading decisions to minimize their latency and payment cost based on this pricing strategy. Yuan et al[27] investigate a profit maximization approach based on the hybrid heuristic optimization to discover the law of variation of service prices in hybrid clouds over time. This method can dynamically schedule all arriving tasks for execution in hybrid clouds while ensuring latency constraints for delay tolerant services. Zeng et al[28] present a novel deep reinforcement learning–based edge computing resource management framework. Based on the framework, the authors design a mobile autonomously perceived service migration strategy according to the user mobility pattern, which can minimize the operation cost of services.

Although insightful views have been presented, it is worth noting that few of them coordinate the service security and cost effectiveness of providers and users in hybrid clouds. In comparison, our focus is on jointly optimizing these two aspects, aiming to attain the multidimensional service optimization on both sides.

3 | SYSTEM MODEL

In this section, we describe the system model in hybrid cloud networks, including the network model and popularity-based cost model. For sake of clarity, Figure 1 briefly summarizes the flow chart of the proposed method herein.

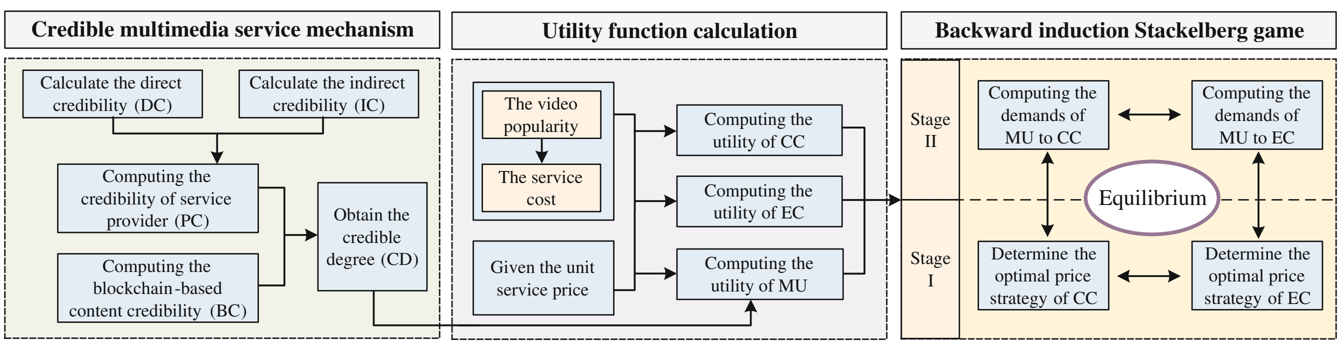

FIGURE 1 Multimedia service optimization flow chart

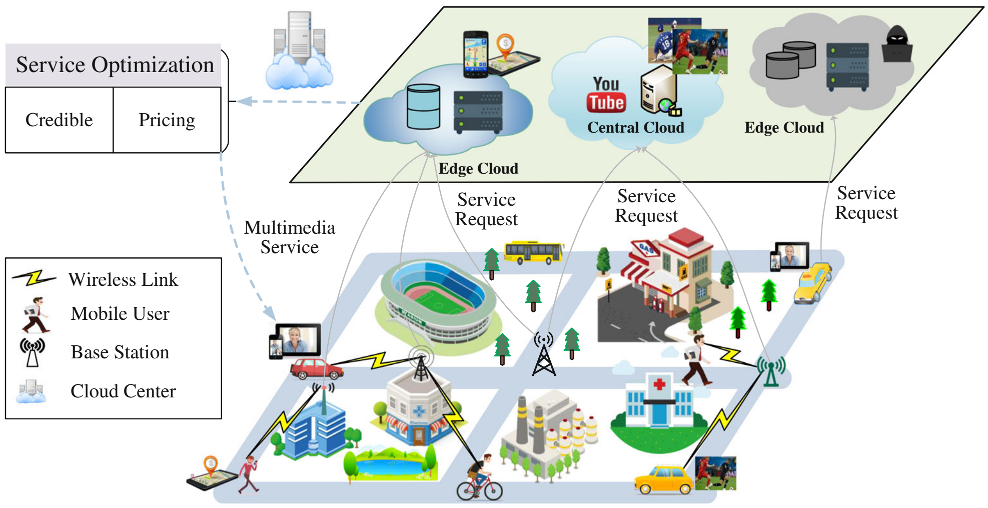

FIGURE 2 Multimedia services in hybrid cloud network scenario. CC, central cloud; EC, edge cloud; MU, mobile user

3.1 | Network Model

A hybrid cloud network scenario is considered, where multiple ECs execute the offloaded data for the CC (see Figure 2). We assume that both ECs and CC can provide streaming services to MUs. Specifically, we assume that CC in cloud networks can serve for all MUs, denoted by n_0. The other cloud service providers $\mathcal{N}_e = \{1, 2, \dots, n_e, \dots, N\}$ represent ECs. Meanwhile, the mobile users, denoted by $\mathcal{M} = \{1, 2, \dots m, \dots, M\}$, are able to access the CC and EC simultaneously. For convenience, we further let $\mathcal{N} = \{n_0\} \cup \mathcal{N}_e$ denote the set of all providers and let n denote an arbitrary service cloud, where $\forall n \in \{n_0, n_e\}$.

We assume the coverage area of ECs is disjoint. We use the indicator I to indicate whether MU m is within the coverage area of EC n_e. The indicator calculation is shown in Equation (1)

$$I_{mn_e} = \begin{cases} 1, \text{if user } m \text{ in EC } n_e, \\ 0, \text{otherwise}. \end{cases} \tag{1}$$

It is worth noting that provider CC serves for all MUs. Thus, the indicator of CC satisfies: $I_{mn_0} = 1$.

3.2 | Popularity-based cost model

We consider the cloud network system has constant video bitrate requests by mobile users. We assume there are Q different types of videos in cloud network system, with $\mathcal{Q} = \{1, 2, \dots q, \dots, Q\}$. We suppose that video contents are split in segments and all segments are assumed to be with equal size.[29] For video content q, the set of segments is defined by $\mathcal{S}_q = \{\text{seg}_{1,q}, \text{seg}_{2,q}, \dots \text{seg}_{i,q}, \dots \text{seg}_{S,q}\}$. Moreover, each user usually completes the entire video service through multiple requests. Moreover, let q_{mn} represent the amount of video segments requested by MU m to provider n. Thus, the number of video segments requested by user m in a single timeslot will be less than the total number of video segments (ie, $q_{mn} \leq |\mathcal{S}_q^m|$).

We assume each type of videos has a different measure of popularity reflected by the probability of requests for it. Similar to previous research works,[30,31] the distribution of user requests for videos is defined by a general Zipf distribution as

$$z(q) = \frac{\Omega}{q^\gamma}, q = 1, \dots, Q, \tag{2}$$

where $\Omega = 1/\sum_{q' \in \mathcal{Q}} \frac{1}{q'^\gamma}$, γ denotes the exponent characteristic of the Zipf distribution, with $0 < \gamma < 1$. The videos are ranked by their popularity in cloud networks, and let video q denote the qth popular video, ie, $q = 1$ means the most popular video while $q = Q$ denotes the least popular video.

The more video services offered by service clouds, the more profits can be earned by them. Moreover, the more popular the video is, the less service cost is incurred by clouds. Thus, the service clouds are more willing to provide more of

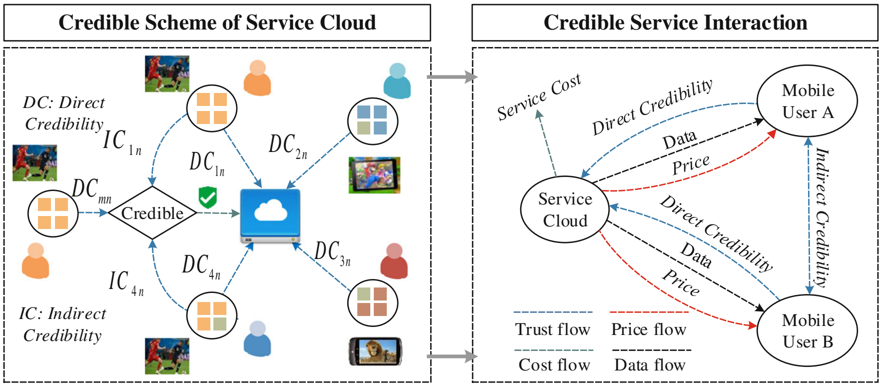

FIGURE 3 Credible scheme of service cloud

the popular videos to MUs. In this case, the service cost of videos provided by cloud n can be defined to be inversely proportional to the popularity as

$$c_n = \frac{c_n^0}{z(q)}, \tag{3}$$

where c_n^0 denotes the unit service cost of cloud n. Without loss of generality, we define it as a fixed initial value associated with the caching cost of cloud servers. Besides, we observe that if the value of q is smaller, the service cost c_n will be lower. We assume that the service cloud has no priority for the requesting videos and has all types of videos.

4 | CREDIBLE MULTIMEDIA SERVICE MECHANISM

In this section, we elaborate the proposed credible mechanism. Firstly, the credibility scheme of service cloud is presented to help calculate the security of the service provider. Then the blockchain-based content credibility is introduced to identify the credibility of the service videos.

4.1 | Credible scheme of service cloud

As the service providers (CC and ECs) are deployed by different cloud operators, some providers are honest to provide multimedia services, while others may conduct malicious attack to threaten mobile users. Namely, the honest providers' services are trustful, while the malicious providers may be not credible. Therefore, to provide credible multimedia services for mobile users, the credibility of each provider needs assessment. The credibility can be evaluated by two aspects, including direct credibility and indirect credibility (as shown in Figure 3), which are denoted by DC_{mn} and IC_{mn}, respectively.

4.1.1 | Direct credibility (DC)

According to the number of interactions between the MUs and providers, one MU can obtain the current subjective assessment of direct credibility to the provider. We define the direct credibility by two aspects: positive credibility and negative credibility. First, we denote the assessed credibility via the previous interaction as v_{mn}^k, with $0 \leq v_{mn}^k \leq 1$. In addition, with consideration that the influence of interaction interval, the value of credibility needs to multiply by $\log(\frac{\omega}{t-t_k}+1)$, where t and t_k represent the current and kth interaction time, respectively. ω denotes the decay influence factor, with $\omega > 0$. Then, the positive credibility and negative credibility can be defined as

$$C_{mn}^{\text{Positive}} = \sum_{k=1}^{K} v_{mn}^k \log\left(\frac{\omega}{t-t_k}+1\right), \tag{4}$$

$$C_{mn}^{\text{Negative}} = \sum_{k=1}^{K} (1-v_{mn}^k) \log\left(\frac{\omega}{t-t_k}+1\right), \tag{5}$$

where K denotes the number of interactions between MU m and provider n. Based on the Equation (4,5), the direct credibility of MU m to provider n can be calculated by Equation (6)

$$DC_{mn} = \frac{\sigma \cdot C_{mn}^{\text{Positive}}}{P_{mn}^{\text{Positive}} + \eta \cdot C_{mn}^{\text{Negative}} + \psi}, \tag{6}$$

where ψ is the uncertain factor and σ and η are the positive weight factors. From Equation (6), we can observe that as the number of interactions between MU m and the trusted cloud n increases, the direct credibility of this cloud will continue to raise. Conversely, if cloud n experiences untrustworthy behavior in a service interaction, his credibility will decrease rapidly.

4.1.2 | Indirect credibility (IC)

In general, the more intimate the relationship, the more trustworthy the MU is. The credible MUs will provide trustful recommendations. Therefore, when one MU enters the scope of a new EC, he can utilize the direct evaluation of the surrounding MUs and the relationship in this EC as an indirect credibility. The indirect credibility of each MU can be defined as

$$IC_{mn} = \frac{\sum\limits_{m'=1, m' \neq m}^{M} DC_{m'n} r_{mm'} I_{m'n}}{\sum\limits_{m'=1, m' \neq m}^{M} I_{m'n}}, \tag{7}$$

where $r_{mm'}$ denotes the relationship degree between MU m and MU m'. The relationship degree of MUs can be represented by matrix R

$$R = \begin{bmatrix} r_{11} & \dots & r_{1m} \\ \dots & \dots & \dots \\ r_{m1} & \dots & r_{mm} \end{bmatrix} \\ \text{s.t. } 0 \leq r_{mm'} \leq 1, \forall m, m' \in \mathcal{M}, \tag{8}$$

where $r_{mm'} = 0$ denotes that these two MUs have little social relationship and $r_{mm'} = 1$ indicates that the social relationship between the two MUs is very close.

4.1.3 | Credibility of service provider (PC)

Then, the value of credibility about MU m to service cloud n can be determined by jointly considering direct credibility (DC) and indirect credibility (IC). The credibility of MU m to cloud n can be defined as

$$PC_{mn} = \varphi_{mn} \cdot DC_{mn} + (1 - \varphi_{mn}) \cdot IC_{mn}, \tag{9}$$

where φ_{mn} denotes the weight factor of DC_{mn}, with $0 \leq \varphi_{mn} \leq 1$. Then, we use variable ε to represent a trusted threshold, and when the value of PC is greater than this threshold, it is considered to be trustworthy. On the contrary, it means that it is not credible.

4.2 | Blockchain-based content credibility (BC)

Despite the fact that the credibility of service clouds can be calculated through multiple interactions, the service content obtained by MUs is still vulnerable to modification, castration, and deletion. When tackling with the content credibility, video files are large in size, and will be divided into larger amount of segments than a normal file during transmission. This will result in a heavy calculation. Therefore, we focus on the issue of the credibility of video segments delivered to MUs by different service clouds. We present a blockchain-based credibility calculation scheme, which utilizes a carefully crafted smart contract[32] to audit the video content through querying and calculating the current video possession and history records from the service cloud, thus producing a credibility index indicating whether the content is credible. The whole procedure of calculating the credibility of the service cloud is illustrated in Figure 4.

The proposed blockchain-based scheme is operated by means of a smart contract deployed on a trusted public chain. The smart contract deployed on the blockchain can be described as Figure 5.

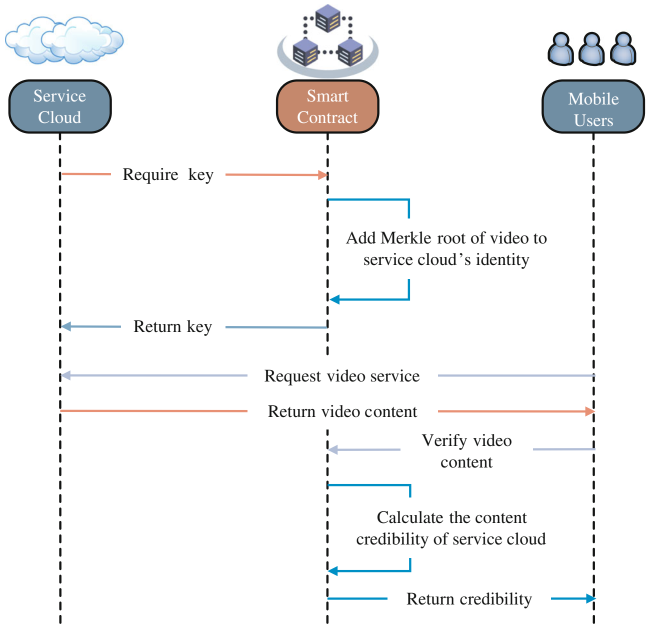

FIGURE 4 Blockchain-based credibility calculation procedure

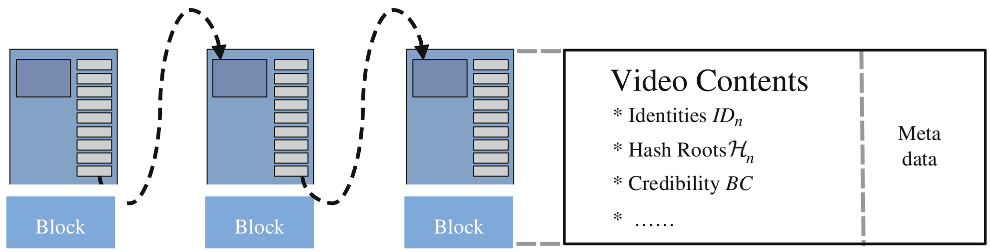

FIGURE 5 Smart contract on blockchain

When service cloud n distributes a video to MUs, the segments of the video should be encrypted. Hence, the service cloud n first requires a key from the smart contract to encrypt the video content. Meanwhile, the smart contract needs to verify the identity of the requesting service cloud. Before verification, if the identity ID_n of service cloud n is not enrolled, we enlist it in the identity array, which yields $\mathcal{I} = \{ID_0, ID_1, \ldots ID_N\}$. When the smart contract returns a certain key to service cloud n, it empowers the service cloud to provide the video by adding it to the playing list of ID_n. The encryption and decryption procedure of video segment $s_{i,q}$ can be described as Equation (10)

$$\begin{aligned} L_{i,q} &\equiv s_{i,q}^{kb} (\text{mod } n^+), \\ L_{i,q}^{kv} &\equiv \left(s_{i,q}^{kb}\right)^{kv} (\text{mod } n^+), \end{aligned} \tag{10}$$

where $L_{i,q}$ and $s_{i,q}$ denote the encrypted and original video segments, respectively. n^+ is a large positive integer, and kb and kv are public key and private key, respectively.

After the above procedure, service cloud n is qualified to distribute the videos. However, when MU m retrieves video q from cloud n, no prior knowledge for him to know whether cloud n is authorized. Besides, MU m needs to validate whether the video content is modified through transmission. For this reason, we adopt hash function $H(.)$ to achieve this goal as it is particularly sensitive to modifications. Specifically, the open addressing method[33] can be embraced to implement the hash function.

Since videos are delivered through segmentation, it is computationally heavy to verify each segment for MUs. Therefore, we utilize the Merkle tree hash method to verify which segment of the video is modified. Merkle tree[34] is a binary tree that each root is a hash value calculated from its children. As a result, the root of the Merkle tree could represent the whole video. Any modification will result in a different hash root. The procedure of building a Merkle tree is defined as Equation (11)

$$\begin{aligned} h_{\text{root}}^q &= H\left(H\left(x_l^q\right) \Big\| H\left(x_r^q\right)\right), \\ x_i^q &= H(L_{i,q}), \end{aligned} \tag{11}$$

where h_{root}^q is the root hash value of video q. x_i is the hash value of video segment $L_{i,q}$. Total hash roots owned by cloud n compose the authorized playing list $\mathcal{H}_n = \{h_n^1, h_n^2, \dots h_n^q, \dots\}$.

The credibility of video q provided by cloud n can be categorized to three situations, including both video q and cloud n are registered on the blockchain, only cloud n is enrolled, and the identity of cloud n is not signed up. Therefore, we can calculate the content credibility based on blockchain as:

$$BC_n^q = \begin{cases} 1, & \text{if both the video and cloud are enrolled,} \\ \lambda f_{\text{norm}}\left(\sum_{q=1}^{Q'} \zeta_{nq}\right), & \text{else if only cloud is enrolled,} \\ 0, & \text{otherwise cloud is not enrolled,} \end{cases} \tag{12}$$

where λ is a balancing parameter. $f_{\text{norm}}(x)$ is an interval function between $[0, 1]$, which satisfies $f_{\text{norm}}(x) = \frac{1}{1+x^{-1}}, x > 0$. Q' denotes the total categories of videos owned by cloud n, with $Q' \in Q$. ζ_{nq} denotes the credibility of video q provided by cloud n, which is a positive constant.

The procedure ends with a message dispatched to the service cloud n declaring the capability of delivering the video q. Afterwards, when MU m requests to fetch the video services, it first poses a query to the smart contract to acquire the credibility of video q provided by cloud n. The smart contract is responsible of validating both the video content and the identity of the cloud, and then, the specific credit score will be returned to the MU. The design of smart contract is described in Algorithm 1.

Algorithm 1 Blockchain-based content credibility algorithm

Enrollment:
Input: The identity of certain service cloud ID_n, the set of identity array $\mathcal{I} = \{ID_0, ID_1, \dots ID_N\}$.
Output: Boolean value of whether the service cloud is enrolled.
Search $\mathcal{I}$ for ID_n
if ID_n is in $\mathcal{I}$ **then**
  Return True
else
  Return False
end if
Validate:
Input: The set of Hash roots of cloud n is $\mathcal{H}_n = \{h_n^1, h_n^2, \dots h_n^{Q'}\}$,
  hash h_{root}^q of video content q obtained by MU m from service cloud n.
Output: Boolean value of whether the hash root is in the registered array.
Search $\mathcal{H}_n$ for h_{root}^q
if h_{root}^q is in $\mathcal{H}_n$ **then**
  Return True
else
  Return False
end if
Calculate Credibility:
Input: Requested video hash h_{root}^q, identity of service cloud ID_n
Output: Calculate BC_n^q of the video content via Equation (12),
Return BC_n^q

4.3 | Credible degree calculation of multimedia service

When MU m requests video content q from service provider n, the credible degree of multimedia service can be determined by the joint consideration of provider credibility (PC) and blockchain-based credibility (BC). Thus, the credible degree (CD) can be defined as

$$CD_{mn}^q = \lambda_{PC} \cdot PC_{mn} + \lambda_{BC} \cdot BC_n^q, \tag{13}$$

where λ_{PC} and λ_{BC} denotes the positive parameters of PC_{mn} and BC_{mn}, respectively.

5 | PROBLEM FORMULATION

In this section, with the credible service mechanism, a game theoretic paradigm for multimedia services among one central cloud, one edge cloud and MUs is explored to improve the MU's service experience in hybrid cloud networks, where the interaction process between these three parties is modeled by the Stackelberg game. We first describe the utility function of each player. Then, we present the optimization strategy for the three parties.

5.1 | Utility function

Here, MUs will request the multimedia services from the nearby providers CC and EC simultaneously after assessing the credible degree of these service providers. In order to obtain benefits and pay for the cost, each provider first determines the unit service price; then, MUs will purchase the required services from them. To satisfy the requirements of each party, we need to introduce the utility function for CC, EC, and MUs in the following.

5.1.1 | Utility of CC

The utility of provider CC is defined as

$$U_{n_0} = P_{n_0} - C_{n_0}, \tag{14}$$

where P_{n_0} and C_{n_0} represent service revenue and service cost of provider CC n_0, respectively.

Intuitively, the more services the MU requests, the more the revenue of CC is. Therefore, we define the revenue function P_{n_0} of CC as

$$P_{n_0} = p_{n_0} \sum_{m=1}^{M} q_{mn_0} I_{mn_0}, \tag{15}$$

where $p_{n_0} \in [0, p_{n_0}^{\max}]$ is the unit service price, which is a nonempty convex and compact subset of the Euclidean space. q_{mn_0} is the number of video segments requested by MU m to service cloud CC.

According to the popularity-based cost scheme, the service cost function is defined as

$$C_{n_0} = c_{n_0} \sum_{m=1}^{M} q_{mn_0} I_{mn_0}, \tag{16}$$

where c_{n_0} denotes the service cost of the qth popular video provided by CC.

5.1.2 | Utility of EC

Similarly to CC, the utility of provider EC n_e can be defined as

$$U_{n_e} = P_{n_e} - C_{n_e}, \tag{17}$$

$$P_{n_e} = p_{n_e} \sum_{m=1}^{M} q_{mn_e} I_{mn_e}, \tag{18}$$

$$C_{n_e} = c_{n_e} \sum_{m=1}^{M} q_{mn_e} I_{mn_e}. \tag{19}$$

5.1.3 | Utility of MU

Here, MUs prefer to purchase credible services from the more trusted providers; hence, the utility function of MU m can be defined as

$$\begin{aligned} U_m = \lambda_m \log\left(1 + CD_{mn_e}^{q} q_{mn_e} + CD_{mn_0}^{q} q_{mn_0}\right) \\ - p_{n_e} q_{mn_e} - p_{n_0} q_{mn_0}, \end{aligned} \tag{20}$$

where λ_m denotes the service satisfaction factor of MU m.

5.2 | Optimization strategy

The optimal strategies of the three players are analyzed based on their utility functions. Since each party is selfish, the optimization target of three players can be transformed to the maximization of benefit problem.

5.2.1 | Problem 1

For provider CC, the maximum utility can be formulated as

$$\begin{aligned} &\max_{p_{n_0}} \ U_{n_0}(p_{n_0}, q_{mn_0}) \\ &\text{s.t.} \sum_{m=1}^{M} q_{mn_0} \le E_{n_0}, \end{aligned} \tag{21}$$

where E_{n_0} represents the transmission capability of CC n_0.

5.2.2 | Problem 2

Similarly, the optimization problem of provider EC is formulated as

$$\begin{aligned} &\max_{p_{n_e}} \ U_{n_e}\left(p_{n_e}, q_{mn_e}\right) \\ &\text{s.t.} \sum_{m=1}^{M} q_{mn_e} \le E_{n_e}, \end{aligned} \tag{22}$$

where E_{n_e} represents the transmission capability of EC n_e.

5.2.3 | Problem 3

Finally, for requester MU, the optimization problem is formulated as

$$\begin{aligned} &\max_{q_{mn_0}, q_{mn_e}} \ U_m\left(q_{mn_0}, q_{mn_e}, \mathbf{p}\right) \\ &\text{s.t.}\ q_{mn_0} + q_{mn_e} \le |S_q^m|, \end{aligned} \tag{23}$$

where $|S_q^m|$ represents the total amount of video segments requested by MU m and $\mathbf{p} = \{p_{n_0}, p_{n_e}\}$.

6 | GAME OPTIMIZATION

A two-stage noncooperative Stackelberg game is presented to analyze the interactions between the providers and MUs. The objective is to calculate the Stackelberg equilibrium according to the optimization strategy of the leaders (service clouds) and the followers (MUs). In addition, the backward induction method and gradient iteration algorithm are utilized to achieve the Nash equilibrium in this game.

6.1 | Game analysis

When the service price is determined by clouds, MUs need to determine the quantity demand from the service clouds. Note that the determination of MUs is not only affected by the unit service price of CC but also influenced by EC's price strategy. We present a noncooperative game $G =< \mathcal{M}, \mathcal{N}; U_{n_0}, U_{n_e}, U_m >$ to analyze the pricing competitions among CC and ECs, where the solution of the game is a Nash equilibrium.

Definition 1 (Stackelberg equilibrium). Let $p_{n_0}^*$ and $p_{n_e}^*$ denote the pricing solutions for Problem 1 and Problem 2, respectively. In addition, let $q^* = \{q_{mn_0}^*, q_{mn_e}^*\}$ denote a requirement solution for Problem 3. Then, we can get a

Stackelberg equilibrium $(p_{n_0}^*, p_{n_e}^*, q_{mn_0}^*, q_{mn_e}^*)$ for the game $G = \{\mathcal{M}, \mathcal{N}; U_{n_0}, U_{n_e}, U_m\}$ when the strategy profile satisfies the following conditions:

$$\begin{gathered} U_n\left(p_n^*, q_{mn}^*\right) \geq U_n\left(p_n, q_{mn}^*\right), \\ U_m\left(q_{mn_0}^*, q_{mn_e}^*, \mathbf{p}^*\right) \geq U_m(q_{mn_0}, q_{mn_e}, \mathbf{p}^*), \\ \forall m \in \mathcal{M}, \forall n \in \{n_0, n_e\} \quad . \end{gathered} \tag{24}$$

We utilize a backward induction method to achieve the Nash equilibrium of the Stackelberg game. In stage II, based on the initial service price and credible degree, we study the optimal decision of MUs on the amount of service demand in order to solve Problem 3. In stage I, according to the requirement decision of MUs $q^* = [q_{mn_0}^*, q_{mn_e}^*]$, we further investigate the optimal strategy of providers CC and EC on the service price. In this case, we can solve Problem 1 and 2 for the optimal price $\mathbf{p}^*$.

6.2 | Strategy analysis of MUs in stage II

To solve the Problem 3, each MU targets the maximization of the utility by deciding its optimal requirement.

6.2.1 | Case 1 CC

We first take the derivative of the utility function (23) of MU m with respect to q_{mn_0} as

$$\frac{\partial U_m}{\partial q_{mn_0}} = \frac{\lambda_m CD_{mn_0}^q}{1 + CD_{mn_e}^q q_{mn_e} + CD_{mn_0}^q q_{mn_0}} - p_{n_0} \quad . \tag{25}$$

Then, the second derivative of MU m with respect to q_{mn_0} is calculated as in Equation (26)

$$\frac{\partial^2 U_m}{\partial {q_{mn_0}}^2} = -\frac{\lambda_m {CD_{mn_0}^q}^2}{\left(1 + CD_{mn_e}^q q_{mn_e} + CD_{mn_0}^q q_{mn_0}\right)^2} < 0 \quad . \tag{26}$$

Obviously, Equation (26) implies that the utility function of MU m exists a maximum value. Then, let the first derivation Equation (25) be equal to zero; we can calculate the optimal service demand ${q_{mn_0}}^*$ of MU m to the provider CC

$${q_{mn_0}}^* = \max\left[\frac{\lambda_m}{p_{n_0}} - \frac{1 + CD_{mn_e}^q q_{mn_e}}{CD_{mn_0}^q}, 0\right] \quad . \tag{27}$$

6.2.2 | Case 2 EC

We take the derivative of the utility function of MU m with respect to q_{mn_e}

$$\frac{\partial U_m}{\partial q_{mn_e}} = \frac{\lambda_m CD_{mn_e}^q}{1 + CD_{mn_e}^q q_{mn_e} + CD_{mn_0}^q q_{mn_0}} - p_{n_e} \quad . \tag{28}$$

Similarly to Case 1, the optimal service demand ${q_{mn_e}}^*$ of MU m to the provider EC can be calculated as

$${q_{mn_e}}^* = \max\left[\frac{\lambda_m}{p_{n_e}} - \frac{1 + CD_{mn_0}^q q_{mn_0}}{CD_{mn_e}^q}, 0\right] \quad . \tag{29}$$

According to the optimal service demands of above two cases, we note that the demands to provider is proportional to the credible degree and is inversely proportional to the service price. Moreover, if the amount of service demands from EC is reduced, the amount of requirements from CC will increase.

6.3 Strategy analysis of providers in stage I

When the optimal strategy of requirement of MUs is obtained, the price strategy of services will be determined in Stage I. We first re-evaluate the providers' utility function according to the demand strategy (27, 29) as

$$U_{n_0} = (p_{n_0} - c_{n_0}) \sum_{m=1}^{M} \left[\frac{\lambda_m}{p_{n_0}} - \frac{1 + CD^q_{mn_e} q_{mn_e}}{CD^q_{mn_0}} \right] I_{mn_0} \quad , \tag{30}$$

$$U_{n_e} = (p_{n_e} - c_{n_e}) \sum_{m=1}^{M} \left[\frac{\lambda_m}{p_{n_e}} - \frac{1 + CD^q_{mn_0} q_{mn_0}}{CD^q_{mn_e}} \right] I_{mn_e} \quad . \tag{31}$$

From Equation (30, 31), we can note that the utility of the providers depends not only on its own price but also on the amount of the MU's demands to another provider. In fact, the price decision of these two parties is affected between each other.

In this case, we make use of the best response to find the Stackelberg equilibrium point. When the price strategy of EC is given, the best respond function of CC can defined as

$$p_{n_0} = R\left(p_{n_e}\right) \quad , \tag{32}$$

where p_{n_e} denotes the unit service price of provider EC.

Afterwards, we need to analyze and prove the existence and uniqueness of the Nash equilibrium through the following theorems.

Theorem 1 (**Existence**). *There exists at least one Nash equilibrium for provider CC in the game.*

Proof of Theorem 1. Since the unit price p_{n_0} is continuous, bounded, and closed (see Equation (15)), we calculate the first derivative of utility function u_{n_0} with respect to p_{n_0} as

$$\frac{\partial U_{n_0}}{\partial p_{n_0}} = \sum_{m=1}^{M} \left[\frac{\lambda_m c_{n_0}}{{p_{n_0}}^2} - \frac{1 + CD^q_{mn_e} q_{mn_e}}{CD^q_{mn_0}} \right] I_{mn_0} \quad . \tag{33}$$

Then, the second derivative of u_{n_0} is calculated as

$$\frac{\partial^2 U_{n_0}}{\partial {p_{n_0}}^2} = -\sum_{m=1}^{M} \left(\frac{2\lambda_m c_{n_0}}{{p_{n_0}}^3} \right) I_{mn_0} < 0 \quad . \tag{34}$$

Equation (34) implies that the utility function of u_{n_0} is a concave function. Namely, the game exists at least one Nash equilibrium.[35] Thus, Theorem 1 is proved. □

In order to obtain the optimal price of u_{n_0}, we solve the first derivation of Equation (33) as

$$\sum_{m=1}^{M} \left[\frac{\lambda_m c_{n_0}}{{p_{n_0}}^2} - \frac{1 + CD^q_{mn_e} q_{mn_e}}{CD^q_{mn_0}} \right] I_{mn_0} = 0 \quad . \tag{35}$$

Then, the optimal price of CC can be determined

$$p^*_{n_0} = R(p^*_{n_e}) = \sqrt{\frac{\sum_{m=1}^{M} \lambda_m c_{n_0} I_{mn_0}}{\sum_{m=1}^{M} \left(\frac{1}{CD^q_{mn_0}} + \frac{CD^q_{mn_e} q_{mn_e}}{CD^q_{mn_0}} \right) I_{mn_0}}} \quad . \tag{36}$$

Theorem 2 (Uniqueness). *The noncooperative game has a unique Nash equilibrium for CC.*

Proof of Theorem 2. From Theorem 1, we know that there exists a Nash equilibrium for CC. Let $p_{n_0}^*$ be the optimal price for provider CC, which satisfies the best response function (32). Then, we need to prove that Equation (36) is a standard function.

Definition 2. A function $R\left(p_{n_e}^*\right)$ is standard if, for all $p_{n_e}^* > 0$, the following properties are satisfied.[36]

- Positivity: $R\left(p_{n_e}^*\right) > 0$;
- Monotonicity: If $p_{n_e}^* \geq \left(p_{n_e}^*\right)'$, then $R\left(p_{n_e}^*\right) \geq R\left(\left(p_{n_e}^*\right)'\right)$;
- Scalability: For all $\alpha > 1$, $\alpha R\left(p_{n_e}^*\right) > R\left(\alpha p_{n_e}^*\right)$.

1. Proof of positivity

As the amount of demand by MUs is usually positive, the positivity property is satisfied for the best response function $R\left(p_{n_e}^*\right) > 0$.

2. Proof of monotonicity

According to the Equation (29), let $\Theta_{mn_e} = \frac{1}{CD_{mn_e}^q} + \frac{CD_{mn_0}^q q_{mn_0}}{CD_{mn_e}^q}$. Then, optimal service demand ${q_{mn_e}}^*$ of MU m to EC can be redefined as

$$ {q_{mn_e}}^* = \max\left[\frac{\lambda_m}{p_{n_e}} - \Theta_{mn_e}, 0\right] . \tag{37} $$

Substitute the ${q_{mn_e}}^*$ into the optimal price of CC, Equation (36) can be rewritten as

$$ p_{n_0}^* = \sqrt{\frac{\sum_{m=1}^{M} \lambda_m c_{n_0} I_{mn_0}}{\sum_{m=1}^{M}\left(\frac{1}{CD_{mn_0}^q} + \frac{CD_{mn_e}^q}{CD_{mn_0}^q}\left(\frac{\lambda_m}{p_{n_e}} - \Theta_{mn_e}\right)\right) I_{mn_0}}} . \tag{38} $$

From Equation (32, 38), it can be observed that p_{n_e} is proportional to the price of $R(p_{n_e})$. Thus, the monotonicity is proved.

3. Proof of scalability

Since $R\left(p_{-n_0}^*\right)$ and $R\left(\alpha p_{-n_0}^*\right)$ are positive real numbers, to prove the scalability, $\alpha R\left(p_{n_e}^*\right) - R\left(\alpha p_{n_e}^*\right)$ can be converted to the following formula:

$$ \frac{\alpha R\left(p_{-n_0}^*\right)}{R\left(\alpha p_{-n_0}^*\right)} = \sqrt{\frac{\sum_{m=1}^{M}\left[\frac{\alpha^2}{CD_{mn_0}^q} + \frac{\alpha CD_{mn_e}^q}{CD_{mn_0}^q}\left(\frac{\lambda_m}{p_{n_e}} - \Theta_{mn_e}\right)\right] I_{mn_0}}{\sum_{m=1}^{M}\left[\frac{1}{CD_{mn_0}^q} + \frac{CD_{mn_e}^q}{CD_{mn_0}^q}\left(\frac{\lambda_m}{p_{n_e}} - \Theta_{mn_e}\right)\right] I_{mn_0}}}. \tag{39} $$

As $\alpha > 1$ and Equation (39) > 1, $\alpha R(p_{-n_0}^*) > R\left(\alpha p_{-n_0}^*\right)$. Thus, the proof of scalability is completed.

According to the above proofs, the best response function (36) is a standard function. Namely, the noncooperative game has a unique Nash equilibrium for provider CC.[36] Similarly to CC, the best response function $p_{n_e} = R\left(\mathbf{p}_{n_0}\right)$ for EC also has a unique Nash equilibrium. □

6.4 | Gradient-based iteration algorithm

Based on the above analysis, a gradient-based iteration algorithm (GIA) is designed for the two stage Stackelberg game (see Algorithm 2).

Algorithm 2 Gradient-based iteration algorithm

Input: The set of providers $\mathcal{N} = \{n_0\} \cup \mathcal{N}_e$, n_0 denotes CC, other providers denote ECs;
The set of MUs $\mathcal{M} = \{1, 2, \dots m, \dots, M\}$ and the iteration time $\mathcal{T} = \{0, 1, \dots t, \dots, T\}$.
Output: The optimal price strategy of $p_n^*, \forall n \in \{n_0, n_e\}$.
for $t \leq T$ **do**
  for $m = 0$ to M **do**
    MU m constantly requests the video services from the cloud service providers
    for $n = 0$ to N **do**
      Calculate the credibility of service provider (PC) from MU m to cloud n via Equation (9)
      Calculate the blockchain-based content credibility (BC) via Equation (12)
      Calculate the credible degree (CD) of multimedia service via Equation (13)
    end for
    for $n = 0$ to N **do**
      if Make the first decision on price **then**
        Decide the price via Equation (36)
        Decide the amount of requirements from m to provider n via Equation (27)
      else
        $p_n(t+1) = p_n(t) + \mu \nabla U_n(p_n)$
      end if
    end for
  end for
  Until $(p_n(t) - p_n(t-1))/p_n(t-1) \leq \varepsilon$
  Until p_n is not changed, $p_n^* = p_n$.
end for

6.4.1 | Analysis of GIA

The target of GIA is to achieve the optimal price strategy based on the credible service mechanism. The novelty of this algorithm is to incorporate the idea of gradient descent in the best response function, which can achieve the Nash equilibrium more quickly with less computing power. Firstly, MU m computes the credibility of service cloud n through the credible mechanism. Then, MU m calculates the credibility of the content q provided by cloud n through the blockchain method. In addition, MU m determines whether to request the video services from cloud n according to the value of credible degree. Furthermore, the two-step Stackelberg game begins to execute. Cloud n first makes the decision on the service price by Equation (36). Next, MU m determines the quantity required based on the credibility and service price of cloud n in Equation (27). Afterwards, we use the gradient-based descent method to achieve the best game equilibrium, in which μ denotes the step size. $\nabla U_n(p_n)$ denotes the price gradient with $\frac{\partial U_n}{\partial p_n}$. ε indicates the threshold of the price change strategy (eg, $\varepsilon = 10^{-4}$). The algorithm eventually terminates until the price is not falling or the price gradient is less than the threshold ε.

6.4.2 | Algorithm complexity

The complexity of GIA is $\mathcal{O}(|\mathcal{M}||\mathcal{N}|)$, which is proved as follows. For each iteration time, the algorithm complexity is mainly determined by the sets of MUs and cloud providers. We know that the numbers of MUs and cloud providers are $|\mathcal{M}|$ and $|\mathcal{N}|$, respectively. Thus, the algorithm complexity is $\mathcal{O}(|\mathcal{M}||\mathcal{N}|)$.

7 | PERFORMANCE EVALUATION

In this section, extensive numerical simulations have been conducted to demonstrate the superiority of our proposed scheme. We first introduce the simulation environment. During the experiment, we assume that there are 1 CC, 8 ECs, and 30 MUs in hybrid cloud networks. The request process of the video service is continuous. The assessed credibility of MUs is initialized with $v_{mn}^k \in [0, 1]$. The provider CC is considered to be credible, and ECs are trusted with a certain probability and set with different values. The service price of CC is more expensive than ECs. As the distance of CC is

TABLE 2 Simulator parameter setting

Parameter	Value	Parameter	Value
ε	0.6	ω	10
σ	1	η	0.5
ψ	0.2	φ_{mn}	0.7
λ_m	1	μ	0.2
λ_{PC}	0.5	λ_{BC}	0.5

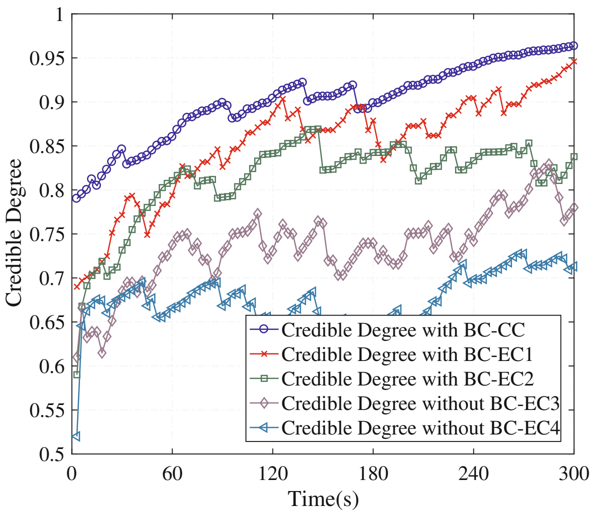

FIGURE 6 Credible degree vs time. BC, blockchain-based credibility; CC, central cloud; EC, edge cloud

farther than EC, the service consumption of CC is assumed to be higher. All simulations are performed over 300 seconds. The main parameters are shown in Table 2.

7.1 | Credible degree analysis

We first perform the credible degree analysis of the proposed method. One CC and four ECs are selected for the credible degree experiments. Among them, cloud CC, EC1, and EC2 are registered on the blockchain, while the identity of cloud EC3 and EC4 are not signed up. In addition, the credibility of these service providers (PC) are initialized to 0.8 (CC), 0.7 (EC1), 0.6 (EC2, EC3), and 0.5 (EC4), respectively. After massive experimental tests, we found that when the credibility of service provider is greater than 0.6, the number of service untrustworthy behaviors will be less, and the service quality is relatively stable; thus, we set the credible threshold of service providers to 0.6 (ie, one provider with the credibility greater than 0.6 is considered to be trusted; otherwise, it is not credible).

Figure 6 shows how the changes of the credible degree by a MU to these service clouds over time. It can be seen that the trust curves of CC, EC1, and EC2 gradually increase as the number of interactions rises. This is because all of them belong to the high-trust service clouds, and more frequent interactions will lead to higher trust. We can further observe that the credible degree of EC3 is significantly lower than EC2; this is because EC3 lacks the security check function for the video content it owns. Moreover, it is observed that the jitter of EC4 is more intense than EC3. This is because the security protection of EC4 is weaker than EC3, resulting in more vulnerable and more frequent untrustworthy behavior. This case ultimately leads to a decline of the EC4's credibility.

7.2 | Service demand under different price strategies

Then, we analyze the service demands of MUs through different price strategies of hybrid clouds. We first set the initial unit price of CC to be twice that of EC. Moreover, the credibility of CC is set higher than EC. Figure 7 shows the changes in MU's service demand under different provider pricing strategies. We can observe that the MU's demand and provider's pricing fluctuates dramatically at the beginning. As the game process evolves, the demand and pricing curves will gradually stabilize. In addition, from the enlarged view of the timeline 240 to 300, we know that the MU's demands is inversely proportional to the provider's pricing, and when the pricing of one provider (eg, CC) increases, the MU's demands for another provider (eg, EC) will be larger. Until the game reaches equilibrium, the requirements and pricing strategies of all parties will not change. Besides, note from Figure 7 that although the average price trend of CC is higher than EC, the

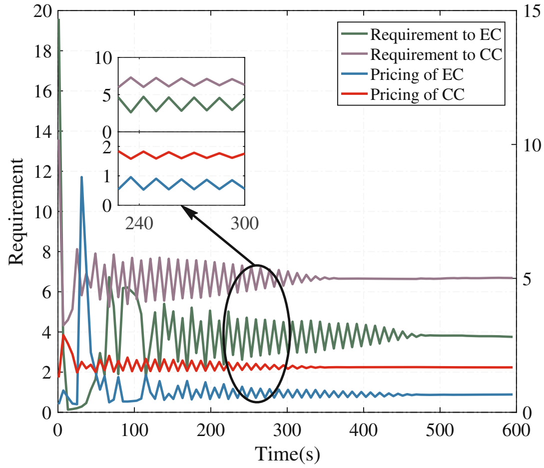

FIGURE 7 Requirement vs pricing. CC, central cloud; EC, edge cloud

demand for CC will be higher than that of EC; this is because MUs would rather spend more money to purchase higher credible services from cloud provider CC.

7.3 | Secure service ratio analysis

We contrast the *safety service ratio*(*SSR*) of the proposed method with the latest caching secure method,[12] social secure method,[23] and random method.

Safety service ratio (SSR): The proportion of credible segments that can be acquired on service clouds to the total amount of video segments requested by the MU. Thus, SSR can be defined as $\mathrm{SSR}(t) = \frac{\widetilde{S(t)}}{S(t)}$, where $\widetilde{S(t)}$ denotes the number of credible video segments obtained by the MU during timeslot $[0, t]$ and $S(t)$ denotes the total amount of segments requested by the MU during the same time.

The proportion of trusted ECs in cloud networks is set from 40% to 80%. Figure 8 shows that as the growth of the trusted proportion, the SSR of four methods will gradually increase and tend to be consistent. Specifically, the SSR of the caching security method is relatively low because it ignores the security check of the content. The quality of experience of users will degrade due to the modification, castration, and deletion of contents. In addition, the social secure strategy uses nodes with intimate relationships to perform reliable services. This method can achieve better security within close range; however, it excessively relies on social relationships in networks, which has serious limitation. Finally, the proposed method is superior to the other methods under the same trusted proportion. This is because our approach jointly considers the credibility of providers and the security of the content. It is worth noting that when the trusted proportion is relatively low, the advantages of our method will be more obvious.

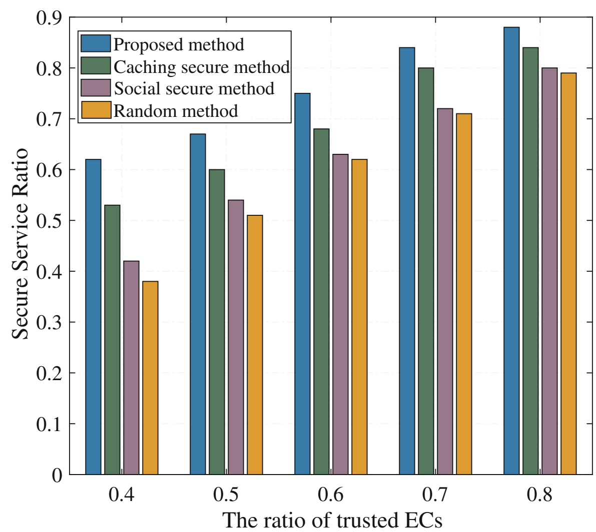

FIGURE 8 Secure service ratio. EC, edge cloud

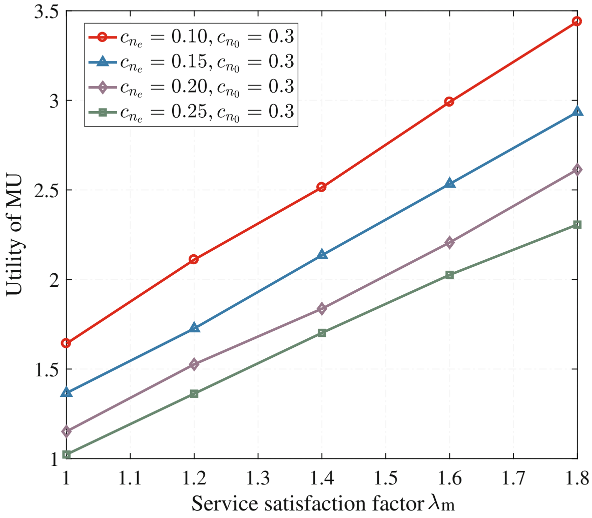

FIGURE 9 Utility of mobile user (MU)

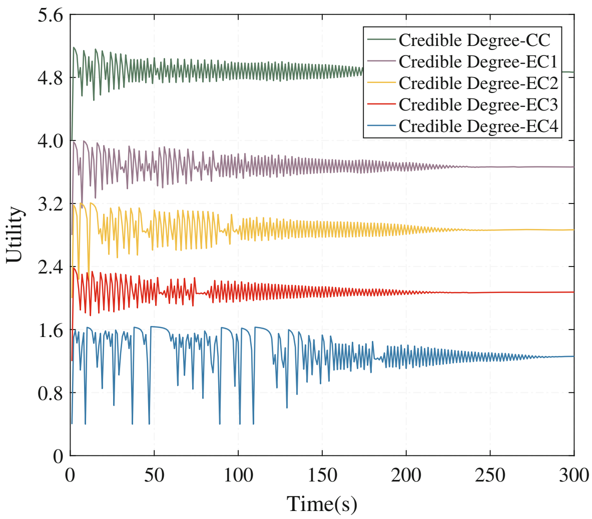

FIGURE 10 Utility of hybrid clouds. CC, central cloud; EC, edge cloud

7.4 | Utility analysis of MU

Figure 9 shows the utility of MU under different satisfactory factor and cost consumption. As the factor λ_m increases, the MU's utility gradually rises. This is because λ_m characterizes the MU's satisfaction with the credible service. When the value of λ_m is larger, the service satisfaction is higher, and the MU's utility is also increased. Moreover, when the unit cost consumption of the EC's service is reduced, the MU's utility will also increase. The reason is that the service price of the EC will decrease as the cost consumption of the EC decreases (see Equation (38)), causing the increase of MU's utility eventually (see Equation (20)).

7.5 | Utility analysis of hybrid clouds

Figure 10 shows the utility of hybrid clouds under different credible degree. The credibility setting of service clouds is the same as in Figure 6. We observe from Figure 10 that as the credible degree of service clouds increases, so does the utility of these clouds. The reason is that the service credibility is proportional to the service price (see Equation (36)). When the cost of service clouds is the same, the service utility of clouds is proportional to the service credibility. As shown in Figure 10, the service utility will start to jitter at the beginning and will gradually stabilize as time goes by. This is because as the service interaction continues, the service credibility of hybrid clouds will change, which will result in a change in the service utility. However, with the arrival of the game equilibrium, both credibility and utility will be stable.

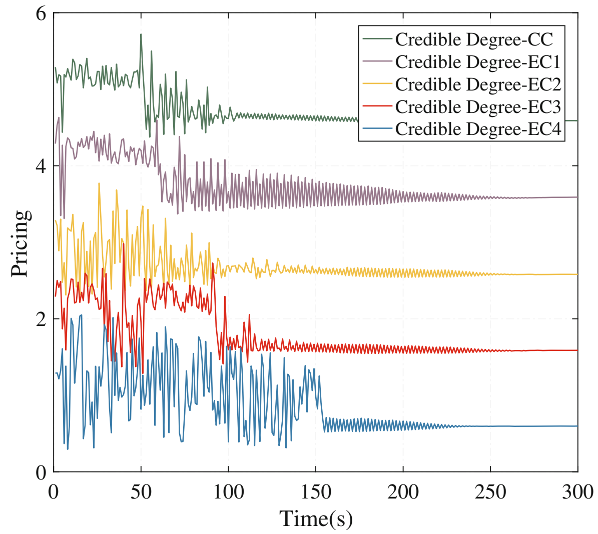

FIGURE 11 Pricing of hybrid clouds. CC, central cloud; EC, edge cloud

7.6 | Pricing analysis of hybrid clouds

Figure 11 shows the pricing strategies of hybrid clouds under different credible degree. Similar to the service utility, as the service credibility increases, so does the pricing of service clouds. In addition, we note that the lower the credibility of the service cloud, the greater changes of the pricing strategy at the initial stage. This is because low-security service clouds are more vulnerable to external attacks, which will lead to poor user satisfaction. In this case, the service cloud must maintain the utility by reducing the price of the service. Besides, it can be seen that the higher the security of the cloud, the faster the pricing strategy will be confirmed. This is because the more reliable the service cloud, the more stable its trust will be; thus, the game equilibrium will converge more quickly.

8 | CONCLUSIONS

This paper presents the mechanism to deliver multimedia content in hybrid cloud networks, where both the CC and EC can provide service to MUs, competitively and collaboratively. Firstly, a secure scheme is designed by the interactive behavior to evaluate the service cloud's credibility. Secondly, a blockchain-based credibility method is further proposed to indicate whether the video content owned by service clouds is reliable. Afterwards, the Stackelberg game model based on the credible mechanism has been investigated to depict the interaction among the cloud providers and MUs. Furthermore, the equilibrium of the game is obtained by the methods of backward induction and gradient descent, so as to maximize the secure and economic profit of each party. Finally, extensive simulations prove that the credibility and economy of multimedia service can be effectively guaranteed in our method.

ACKNOWLEDGMENTS

This work is supported by National Natural Science Foundation of China under grants 61871048, 61872253, and 61762074, by BUPT Excellent PhD Students Foundation under grant CX2018208, by Open Foundation of State key Laboratory of Networking and Switching Technology (BUPT) under grant SKLNST-2019-2-04, by Chunhui Plan of Ministry of Education under grant z2016081, and by experimental education teaching research project of Qinghai University under grant SY201907.

ORCID

Shujie Yang https://orcid.org/0000-0002-9597-2659
Changqiao Xu https://orcid.org/0000-0003-1467-1086

REFERENCES

1. Zhang X, Zhu Q. Hierarchical caching for statistical QoS guaranteed multimedia transmissions over 5G edge computing mobile wireless networks. *IEEE Wirel Commun*. 2018;25(3):12-20.
2. Xu C, Zhang P, Jia S, Wang M, Muntean G-M. Video streaming in content-centric mobile networks: challenges and solutions. *IEEE Wirel Commun*. 2017;24(5):157-165.
3. Cisco. *Cisco Visual Networking Index: Forecast and Methodology*. 2017-2022 Technical Report. 2019.
4. Wang C, Jayaseelan A, Kim H. Comparing cloud content delivery networks for adaptive video streaming. In: Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD); 2018; San Francisco, CA.
5. Tran TX, Hajisami A, Pompili D. Cooperative hierarchical caching in 5G cloud radio access networks. *IEEE Network*. 2017;31(4):35-41.
6. Liu T, Li J, Shu F, Guan H, Yan S, Jayakody DNK. On the incentive mechanisms for commercial edge caching in 5G wireless networks. *IEEE Wirel Commun*. 2018;25(3):72-78.
7. Zhang K, Leng S, He Y, Maharjan S, Zhang Y. Cooperative content caching in 5G networks with mobile edge computing. *IEEE Wirel Commun*. 2018;25(3):80-87.
8. Chen X, Li W, Lu S, Zhou Z, Fu X. Efficient resource allocation for on-demand mobile-edge cloud computing. *IEEE Trans Veh Technol*. 2018;67(9):8769-8780.
9. Xu C, Quan W, Zhang H, Grieco LA. GrIMS: green information-centric multimedia streaming framework in vehicular ad hoc networks. *IEEE Trans Circuits Syst Video Technol*. 2018;28(2):483-498.
10. Yang S, Qiu X, Xie H, Guan J, Liu Y, Xu C. GDSoC: green dynamic self-optimizing content caching in ICN-based 5G network. *Trans Emerg Telecommun Technol*. 2018;29(1):1-15.
11. Yan J, Wu D, Wang R. Socially aware trust framework for multimedia delivery in D2D cooperative communication. *IEEE Trans Multimed*. 2019;21(3):625-635.
12. Xu Q, Su Z, Zhang K. Game theoretical secure caching scheme in multi-homing heterogeneous networks. In: Proceedings of the 2018 IEEE International Conference on Communications (ICC); 2018; Kansas City, MO.
13. Wang M, Xu C, Chen X, Hao H, Zhong L, Yu S. Differential privacy oriented distributed online learning for mobile social video prefetching. *IEEE Trans Multimed*. 2019;21(3):636-651.
14. Kumar M, Verma H, Sikka G. A secure lightweight signature based authentication for cloud-IoT crowdsensing environments. *Trans Emerg Telecommun Technol*. 2019;30(4):1-15.
15. Cao T, Xu C, Xiao H, Zhong L. Credible and economic multimedia service optimization in cloud network. In: Proceedings of the 2019 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); 2019; Paris, France.
16. Pan J, McElhannon J. Future edge cloud and edge computing for internet of things applications. *IEEE Internet Things J*. 2018;5(1):439-449.
17. Rimal BP, Van DP, Maier M. Mobile-edge computing versus centralized cloud computing over a converged FiWi access network. *IEEE Trans Netw Serv Manag*. 2017;14(3):498-513.
18. Weinman J. The economics of the hybrid multicloud fog. *IEEE Cloud Comput*. 2017;4(1):16-21.
19. Zeng D, Gu L, Yao H. Towards energy efficient service composition in green energy powered cyber-physical fog systems. *Future Gener Comput Syst*. 2018;PP(99):1-9.
20. Jin Y, Wen Y. When cloud media meets network function virtualization: challenges and applications. *IEEE MultiMedia*. 2019;PP(99):1.
21. Imagane K, Kanai K, Katto J, Tsuda T, Nakazato H. Performance evaluations of multimedia service function chaining in edge clouds. In: Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC); 2018; Las Vegas, NV.
22. Nie W, Xiao X, Wu Z, Wu Y, Shen F, Luo X. The research of information security for the education cloud platform based on AppScan technology. In: Proceedings of the 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom); 2018; Shanghai, China.
23. Chen X, Zhao Y, Li Y, Chen X, Ge N, Chen S. Social trust aided D2D communications: performance bound and implementation mechanism. *IEEE J Sel Areas in Commun*. 2018;36(7):1593-1608.
24. Jimenez JM, Diaz JR, Lloret J, Romero O. MHCP: multimedia hybrid cloud computing protocol and architecture for mobile devices. *IEEE Network*. 2019;33(1):106-112.
25. Zeng D, Zhang J, Gu L, Guo S. Stochastic scheduling towards cost efficient network function virtualization in edge cloud. In: Proceedings of the 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON); 2018; Hong Kong.
26. Liu M, Liu Y. Price-based distributed offloading for mobile-edge computing with computation capacity constraints. *IEEE Wirel Commun Lett*. 2018;7(3):420-423.
27. Yuan H, Bi J, Tan W, Li BH. Temporal task scheduling with constrained service delay for profit maximization in hybrid clouds. *IEEE Trans Autom Sci Eng*. 2017;14(1):337-348.
28. Zeng D, Gu L, Pan S, Cai J, Guo S. Resource management at the network edge: a deep reinforcement learning approach. *IEEE Network*. 2019;33(3):26-33.
29. Cao T, Xu C, Wang M, Chen X, Zhong L, Muntean G-M. Family-aware pricing strategy for accelerating video dissemination over information-centric vehicular networks. In: Proceedings of the 2018 IEEE International Conference on Communications (ICC); 2018; Kansas City, MO.
30. Hajimirsadeghi M, Mandayam NB, Reznik A. Joint caching and pricing strategies for popular content in information centric networks. *IEEE J Sel Areas Commun*. 2017;35(3):654-667.
31. Xu C, Jia S, Wang M, Zhong L, Zhang H, Muntean G-M. Performance-aware mobile community-based VoD streaming over vehicular ad hoc networks. *IEEE Trans Veh Technol*. 2015;64(3):1201-1217.

32. Delmolino K, Arnett M, Kosba A, Miller A, Shi E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In: *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*. Berlin, Germany: Springer; 2016:79-94.
33. Purcell C, Harris T. Non-blocking hashtables with open addressing. In: *Distributed Computing: 19th International Conference, DISC 2005, Cracow, Poland, September 26-29, 2005. Proceedings*. Berlin, Germany: Springer; 2005:108-121.
34. Xu J, Wei L, Zhang Y, Wang A, Zhou F, Gao C. Dynamic fully homomorphic encryption-based Merkle tree for lightweight streaming authenticated data structures. *J Netw Comput Appl*. 2018;107:113-124.
35. Arrow KJ, Debreu G. Existence of an equilibrium for a competitive economy. *Econometrica*. 1954;22(3):265-290.
36. Yates RD. A framework for uplink power control in cellular radio systems. *IEEE J Sel Areas Commun*. 1995;13(7):1341-1347.

How to cite this article: Cao T, Zhong L, Xiao H, Song C, Yang S, Xu C. Credible and economic multimedia service optimization based on game theoretic in hybrid cloud networks. *Trans Emerging Tel Tech*. 2022;33(8):e3779. https://doi.org/10.1002/ett.3779