Received January 9, 2017, accepted February 2, 2017, date of publication March 6, 2017, date of current version April 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2678510

LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context

QIXU WANG[1], DAJIANG CHEN[1,2], (Member, IEEE), NING ZHANG[2], (Member, IEEE), ZHEN QIN[1], (Member, IEEE), AND ZHIGUANG QIN[1], (Member, IEEE)

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Corresponding author: D. Chen (dajiang.chen@uwaterloo.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada, Major International (Regional) Joint Research Project of China National Science Foundation under Grant 61520106007, in part by NSFC under Grant under Grant 61502085, Grant 61133016, Grant 61272426, Grant 61428203 and Grant 61379117, and in part by the China Postdoctoral Science Foundation funded project under Grant 2015M570775.

ABSTRACT Due to massive mobile terminal devices and ubiquitous communication, the Internet of things (IoT) has become an inevitable trend. Given that the fifth generation (5G) wireless networks expects to drive the proliferation of the IoT and may extend the access functions and systems of the IoT, it makes the IoT a vitally important part in future 5G wireless networks. Simultaneously, the limit of the bandwidth and power of the 5G would adversely affect the widespread promotion of the IoT. However, wireless caching techniques could remarkably resolve this issue. Recently, using fog nodes to improve the capacity of caching has become a trend in caching system. However, node-based caching systems may suffer from malicious access and destruction. To protect caching from sabotage and to further ensure its reliability, we propose a new lightweight label-based access control scheme (LACS) that authenticates the authorized fog nodes to ensure protection. Specifically, the LACS can authenticate the fog nodes by verifying the integrity of the shared files that are embedded label values, and only the authenticated fog nodes can access the caching service. The analysis shows that the proposed scheme is verifiable (the malicious fog node cannot cheat the caching server to pretend to be a legal node) and efficient in both computation and verification. Moreover, simulation experiments show that the LACS can reach the millisecond-level verification and it has a good accuracy.

INDEX TERMS 5G, Internet of things, fog node, caching, access control, authentication.

I. INTRODUCTION

As the next-generation of mobile networks, the target of 5G is to increase the network's capacity to be 1000 times greater than 4G [1], [2]. This means that 5G would be perfectly suitable to dispose the increasing number of wireless devices and omnipresent network access [3]. Without a doubt, such an improvement can better accommodate the Internet of Things (IoT) in the 5G network [4]. However, compared huge amounts of terminal equipment access and communication overhead with limited bandwidth and power, there is an obvious paradox in 5G network [5]. For example, in Fig. 1, numerous IoT-based devices ubiquitously connect to the core 5G network, making the backhaul become the bottleneck. Fog nodes with caching and computing capabilities [33], [45], [46]) can alleviate the backhaul traffic, which makes mobile networks achieve long-term sustainability. These fog nodes form a wireless distributed caching infrastructure. More concretely, the fog nodes are deployed in local positions and are assumed to have (1) large storage capacity, and (2) localized, provision low-latency service [33], [45]. They can alleviate congestion in backhaul traffic by temporarily storing the most popular content in a cache locally. However, since fog nodes can be deployed by users, it is possible for malicious users to deploy illegal fog node. Meanwhile, it is worthy to investigate how to prevent illegal access to caches to ensure the reliability of caching services. Hence, the improvement in the service and prevention of malicious access to caching becomes increasingly important.

Access control technology has the great potential prevent illegal access and ensure the reliability by preventing unauthorized user form accessing the data [7]. One traditional

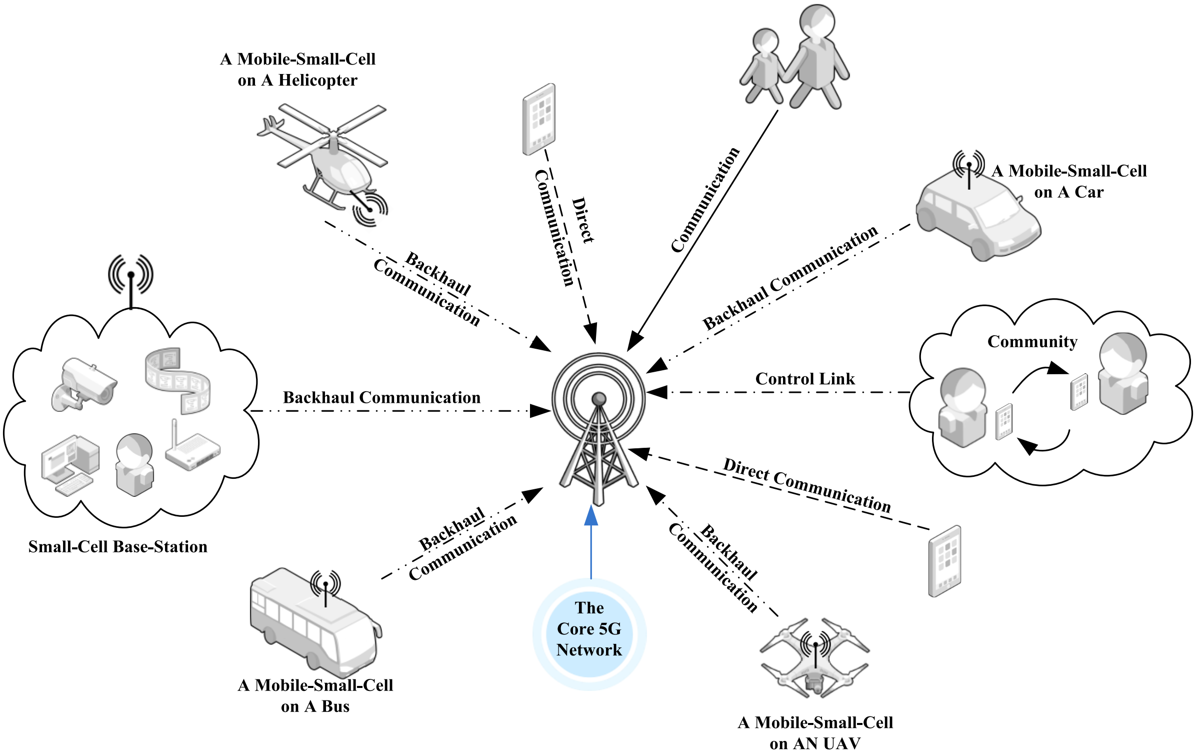


FIGURE 1. The framework of IoT-based 5G context.

access control method is called discretionary access control technology, which is based on the access control list [8], [9]. However, it is unpractical to store the access control list into each terminal devices in the context of the IoT-based 5G caching network. The reasons are as follows: (1) the IoT terminal devices usually do not have sufficient storage capacity (e.g., the RFID tags [6]); and (2) due to the uncontrollability of the communication delay in IoT networks, it would cause the protocol to timeout and stop. Another access control method is the attribute based access control technology (ABAC), in which a large number of complex rules are used to implement fine-grained access control [10], [11]. However, its complex structure of access control outweighs the burden of managing the encryption key in both storage and a computationally limited environment. Therefore, ABAC is also not an optimal choice to efficiently achieve access control [12].

Subsequently, the lightweight access control is a method to solve the access control issues effectively in the context of the IoT-based 5G network. One solution is to authenticate the services and applications from the Cloud, which can reduce the storage and computation requirement to the IoT terminal devices [13]. Another method is to verify the integrity of sharing secrets in order to simplify the authentication [14]. This verifies the data integrity to authenticate user instead of using the access control structure. This characteristic benefits the IoT-based environment, which lacks memory and computation capability.

In this paper, we focus on the caching security and efficiency issue in the IoT-based 5G context and we propose a solution named the lightweight label-based access control scheme (LACS). There are two parts of our scheme, including the verifier (caching server) and prover (caching fog node). It should be noted that adversaries may sit among nodes. First, the verifier uses an one-way function to generate the labels, which are embedded into encrypted files. Second, the verifier uses a pseudo-random function to permute the position of the file blocks. After sharing the processed file, the verifier challenges the prover by requiring the response in random locations. Finally, the verifier checks the label values and outputs the result. The proposed scheme can authenticate users by using verifying data integrity. A simulation experiment shows that LACS can achieve good accuracy. The runtime of the verification phase has been confined to a millisecond, and the expected effect is achieved.

The major contributions are summarized as follows.

1) A new lightweight label-based access control scheme (LACS) is proposed to ensure reliability in the IoT-based 5G caching context. It authenticates the fog nodes by verifying data integrity in the caching context. Theoretical studies show that the proposed scheme is verifiable and efficient in both computation and verification.
2) To provide feasibility and availability, a simulation experiment of the proposed scheme with a detailed analysis is presented. The experimental results show

that the probability to detect an adversary is approximately 100% after 3 rounds of challenge. Moreover, the results also show that the LACS can reach the millisecond-level verification. This feature makes LACS suitable and practical in the general IoT-based 5G caching context.

This paper is organized as follows. In Section 2, related works are discussed. In Section 3, we give the overview of our LACS scheme. The detailed architecture of the proposed scheme is introduced in Section 4. Section 5 provides the security analysis of the scheme. A performance evaluation is demonstrated in Section 6. Finally, we make conclusions in Section 7.

II. RELATED WORK

Recently, the IoT security in the 5G context has drawn increasing attention [37]–[39], especially in the study of access control [40], [41]. To resolve the access control problem in the IoT-based 5G caching environment, traditional public key infrastructure can be adopted in the data encrypting process which allows owner to encrypt data by adopting the public key of users before upload. However, this method would cause a set of problems: (1) For data owners, it is absolutely necessary to obtain the user's public key so that they enable data encryption; and (2) many storage overhead would be spent because of the same plaintext with different public keys [15]. To improve these disadvantages, Sahai and Waters proposed an attribute-based encryption (ABE) scheme [16], which gave the first concept of the ABE scheme. Goyal *et al.* proposed a key-policy attribute based encryption (KP-ABE) scheme [17] that built the access policy into the user's private key and described the encrypted data with the user's attributes. Then, several schemes were proposed based on the ciphertext-policy attribute-based encryption (CP-ABE) scheme [18]–[22]. However, all the above schemes are based on the bilinear map and their deployment ability is limited by the shortage of most IoT terminal devices' computation and storage capacity (e.g., numerous RFID passive tags [42]).

In the IoT context, towards the access control challenge, the Trusted Platform Module [23] offers promise by providing strong guarantees, for example, with respect to the device identity [24] and configuration [25], which access control mechanisms can leverage. All of these solutions are based on hardware equipment, which increases the required budget. Furthermore, the mechanisms used the SHA-1 algorithm to encrypt the secret are vulnerable to attacks, which had already been abandoned by Google [43] and Microsoft [44] enterprises, because of insecurity.

In the Cloud-IoT environment, only a few solutions were proposed. In some exceptional circumstances, such as medical emergencies [26], wider access may be desirable, as specified by "break-glass policies". Mechanisms are required to enable flexible access control policies to be defined by different parties, while are also capable of identifying and resolving potential policy conflicts. Another case is that an access control scheme's vulnerability was discovered in a consumer lighting system, which allowed an attacker to issue lighting commands (causing a blackout) by masquerading as an user-device [27]. The cloud-deployed policy enforcement components must be able to dynamically switch among control schemes to enable context-aware coordination when/where appropriate, e.g., to adapt security levels based on a perceived risk [28]. Yao *et al.* proposed a lightweight cipher-text access control mechanism for mobile cloud storage in [13]. Hernández-Ramos *et al.* constructed an access control solution with a cryptographic based method that achieved the management of certificates, authentication, and authorization [29].

Usually, in the 5G context, access control technology is used in channel access control management. I. K. Son *et al.* developed the FD-MAC access control scheme on mmWave-based small cells [30]. A medium access control protocol to user equipment was presented in [31]. Nikopour *et al.* proposed the access control method to increase spectral efficiency [32]. In the caching domain, most researchers focused on developing new and efficient caching solutions [33]. Negin Golrezaei *et al.* proposed the FemtoCaching scheme, which deployed distributed caching helpers [34]. Similarly, the fog nodes can implement caching technique better [47], [48]. Based on the caching fog node scheme, we propose our LACS solution in this paper. LACS can prevent malicious fog nodes from accessing caching services by authenticating them and achieve the access control goal.

III. LACS OVERVIEW

In this section, we present an overview of our LACS scheme including the network model and design goals.

A. NETWORK MODEL

As shown in Fig. 2, we consider a 5G system with a caching technique involving three participants, which are the caching server (CS), caching fog nodes and service users.

The caching fog node would estimate which contents need to be cached and then send the determined contents to the caching sever. After the process above, the caching server can directly cache the contents. However, malicious fog nodes may deliberately send the false information and make them appear as the real determined contents to the cache sever, which can cause the invalidation and destruction of the high speed communication. Therefore, in this paper we design our scheme so that the CS provides caching service and concurrently enforces access control on caching fog nodes. It bootstraps the entire system during the initialization step and makes service users trust the CS. Meanwhile, the CS can verify the caching fog nodes, and revoke the malicious node that failed to pass the access control policy.

1) The fog node is designed to deal with the low-bandwidth backhaul problem in the wireless distributed caching infrastructure [34], [47]. It disposes the conflicting interests among different users, and reports the content that needs to be cached.

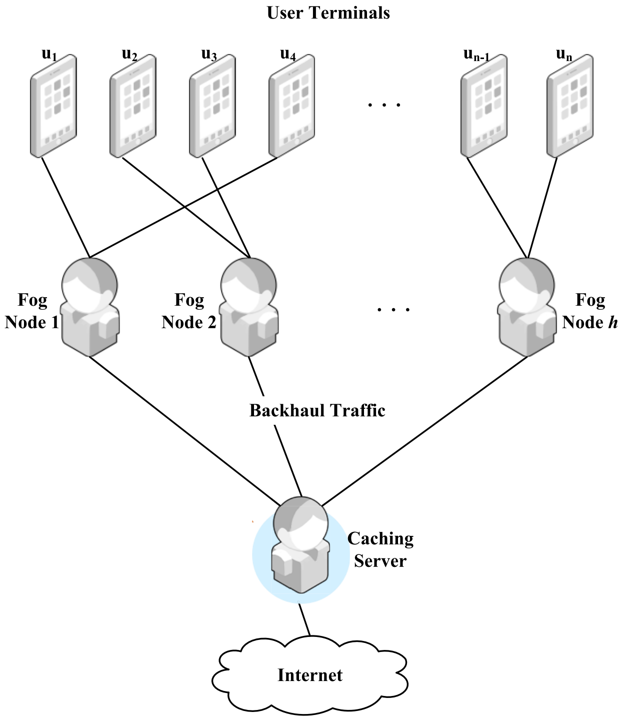


FIGURE 2. Network model.

2) Users refer to a large number of user equipment, which include smart phones and other devices in the radio access network (RAN). We denote them as $U = \{u_1, u_2, \ldots, u_n\}$ in this paper.

B. SECURITY MODEL

We define the adversary as stateless in our scheme, which means it does not have previous knowledge and will not store any result after a cache. In the caching service, the adversary would start attacking at both reporting steps and the disposing conflicts of interest step. We hereby define these attacks into two types as (1) a disturbing attack (DA) to the server and (2) an ignoring attack (IA) to the users. In the first type, the adversary would pretend to be a legitimate fog node and intentionally report false caching target contents to the caching server. Consequently, a large amount of junk information in the cache would invalidate the 5G high speed communication. In the second type, the adversary does not consider the users actual demands, but gives conflicting caching target contents back to the sever, which would greatly reduce the effects of the caching service and comparably lead to the destruction of the 5G. These two types of attack make the 5G fail to work thoroughly.

C. DESIGN GOALS

Our design goal is to develop a lightweight access control scheme in a wireless caching environment in this paper.

1) Efficiency Goals: Considering the limited bandwidth and power in the 5G network, our goal is to develop an efficient access control scheme to prevent junk information occurring in caching as early as possible. The proposed scheme should filter the junk information generator (malicious fog node) efficiently and dissipate the limited additional storage, communication, and computational overheads. Meanwhile, its runtime should be confined to be within milliseconds.

2) Security Goals: The security goal is to protect the caching server against the DA and prevent the user requirements from the IA. The proposed scheme should deny the illegal fog node's access request and verify the legitimate fog node's qualification. In addition, the scheme should run efficiently.

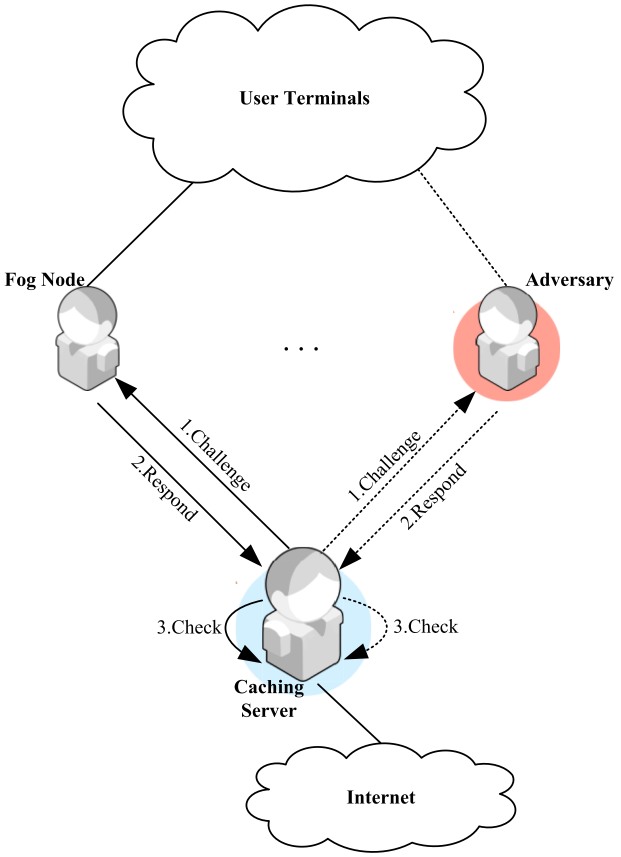


FIGURE 3. The framework of lightweight label-based access control scheme.

IV. THE PROPOSED SCHEME

We propose the LACS scheme in this section. As shown in Fig. 3, an adversary pretends to be a fog node and wants to cache content in the server. Meanwhile, the caching server authenticates fog nodes by verifying them before caching content to successfully detect the adversary.

In our scheme, we use a given file F, which embeds some labels to build the access control technique. For convenience, the notations used in this paper are given in TABLE I.

The LACS consists of the scheme setup, label manipulation, and label-based authentication.

TABLE 1. Notations

Notation	Description
F	the contents of the file
$F^{'}$	the encrypted file
$F^{''}$	the file embedding labels
$\tilde{F}$	the file permuting the position of the labels
$\tilde{F}_{\eta}$	the file adding a unique symbol η
E	a symmetric encryption algorithm
κ	the encryption key based on the symmetric cryptograph
η	the unique file handle symbol to verifier
c	the challenge value
r	the response value for the challenge

1) In the scheme setup step, the caching server uses the setup function to initialize the scheme. After encrypting the file F, we denote it as F'. Then, the server embeds the labels to F', and we denote it as F''.
2) In the label manipulation step, the server permutes the position of the data blocks, and we denote it as $\tilde{F}$. Then, the server uses the encode function to transform the file $\tilde{F}$ into $\tilde{F}_\eta$ and sends the file $\tilde{F}_\eta$ to every legal fog node.
3) In the label-based authentication step, when a fog node attempts to access the caching service, this scheme starts the *Challenges/ Response* mode. Subsequently, the caching server outputs a Boolean variable after checking the label values to assess whether to allow the fog nodes to connect to the service based on the outcome of the check.

A. SCHEME SETUP

To find a proper approach to install the labels to the file F, we use the l - bit block as the basic unit of storage in our scheme. This means that the server divides the F into s chunks with each chunk having b blocks. Namely, the file F has been divided into $s{*}b$ blocks.

There are three steps in the setup phase.

1) The CS applies a fixed-size partition algorithm to divide the F into l - bit blocks.
2) The CS uses the *keygen* function to generate a secret key κ.
3) By applying the key κ, the CS uses the symmetric encryption algorithm E with input F to generate the file F'.

Algorithm 1 illustrates the setup algorithm in the LACS performed by the CS.

B. LABEL MANIPULATION

In this section, we elaborate on our label-based details. Algorithm 2 illustrates the manipulation algorithm in the LACS performed by the CS.

There are three steps to manipulate the label phase.

1) The CS chooses a suitable one-way function f to create n labels, where $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$. Denote $\{L_t\}_{t=1}^{n}$ as $L_t = f\ (\kappa, t)$.
2) The CS embeds these n labels to file F', to yield file F''. Note that for each q queries, our scheme can sustain up to n/q challenges.
3) The CS uses a pseudo-random function g to permute the position of the embedded label blocks, to yield file $\tilde{F}$, where the function $g : \{0, 1\}^j \times \{1, \ldots, b' + n\} \rightarrow \{1, \ldots, b' + n\}$.

Algorithm 1 Setup

```
Procedure: Scheme Setup
The file has been divided into $l$ - $bit$ blocks
CS inputs parameter $\pi$ and applies the function
  $keygen[\pi] \rightarrow \boldsymbol{\kappa}$
if $F$ has already been divided into $l$ - $bit$ blocks then
    CS executes symmetric encryption algorithm $E$ to $F$
else
    CS divides file $F$ into several $l$ - $bit$ blocks
end if
end procedure
```

Algorithm 2 Manipulation

```
Procedure: Label Manipulation
CS runs function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, to get n labels
CS embeds each one label to file blocks
for ($s = 0; s < n; s^{++}$)
    CS embeds label to this block
end for
CS runs random permutation function $g : \{0, 1\}^j \times$
    $\{1, \ldots, b' + n\} \rightarrow \{1, \ldots, b' + n\}$, to get file $\tilde{F}$
CS sends file $\tilde{F}$ to each legal caching fog node
end procedure
```

C. LABEL-BASED AUTHENTICATION

In this phase, the CS can authenticate the status of the caching fog nodes by auditing the data embedded label values. Then, the CS could assess whether to allow the fog node to connect to the caching services based on the outcome of the authentication.

There are four steps in the label-based authentication phase.

1) The CS uses the *encode* function to generate a file handle η as the unique symbol. This function transforms file $\tilde{F}$ into $\tilde{F}_\eta$, where the function *encode* $(\tilde{F}; \kappa)[\pi] \rightarrow (\tilde{F}, \eta)$.
2) The CS uses the output value c of the function *challenge* for file $\tilde{F}_\eta$, where the function $challenge(\eta, \kappa)[\pi] \rightarrow c$.
3) After receiving the challenge value c, the fog node uses the function *respond* to generate a value r for each challenge value c, where the function $respond(c, \eta) \rightarrow r$.
4) The CS uses the function *verify* to determine whether r represents a valid response to challenge c. The function outputs the Boolean variable '1' when verification

succeeds, otherwise it outputs '0', where the function $verify((r, \eta); \kappa) \rightarrow b \in \{0, 1\}$.

According to the details of our scheme we can obtain that the function *challenge* repeats q times, hence, the scheme should generate q different locations for the labels. Moreover, we can see that the dominant overhead is at the pseudo-random permutation step. Algorithm 3 illustrates the authentication algorithm in the LACS performed by the CS.

Algorithm 3 Authentication

```
Procedure: Label-based Authentication
CS runs $encode(\tilde{F}; \kappa)[\pi] \rightarrow (\tilde{F}, \eta)$ to get the file handle $\eta$ and transforms file $\tilde{F}$ into $\tilde{F}_\eta$
CS runs function challenge to output challenge value $c$ for file $\eta$, and sends $c$ to the fog node
The fog node receives the $c$ and runs function respond to generate value $r$, and wants to send $r$ back to CS
if CS receives the value $r$ then
    CS checks the value $r$ valid or not
    if value $r$ is valid then
        CS outputs the Boolean variable '1'
    else
        CS outputs the Boolean variable '0'
    end if
else
    the counter $CT \leftarrow CT + 1$
    if $CT < i$ then
        CS sends challenge value $c$ to the fog node again
    else
        CS outputs the Boolean variable '0'
    end if
end if
end procedure
```

V. SECURITY ANALYSIS

This section discusses the security properties of the LACS.

For the sake of simplicity, we present the two assumptions used in this paper. First, we suppose the one-way permutation algorithm is truly random and the pseudo random number generator outputs true random results. In other words, the probability of the adversary determining the output results by analyzing these algorithms is negligible. Second, we suppose that every block is independent of each other, which means the requests to these blocks are a sequence and makes the foundation of the ball-and-can model in our paper. These ideal assumptions make every block value randomly distributed to the adversary.

We first review some fundamental concepts, that are used throughout this paper.

Theorem 1 [35]: A poly-time POR system $PORSYS[\pi]$ is a (ρ, λ)-*valid* proof of retrievability (POR) if all the poly-time A and for some ζ is negligible in the security parameter j,

$$pr\left[\begin{array}{c} Success^{extract}_{\mathrm{A},PORSYS}(\alpha, \delta, \eta^*) < 1 - \varsigma, \\ Success^{chal}_{\mathrm{A},PORSYS}(\alpha, \delta, \eta^*) \geq \lambda \end{array} \middle| \begin{array}{c} (\alpha, \delta, \eta *) \\ \leftarrow Exp^{setup}_{\mathrm{A},PORSYS} \end{array}\right] \leq \rho .$$

Then we introduce the Chernoff Bounds [36], which is used in the following lemma. Let $X_1, X_2, \ldots, X_\mathrm{N}$ be independent Bernoulli random variables with $\mathrm{pr}[X_i = 1] = p$. Then, for $\mathrm{X} = \sum_{i=1}^{N} X_i$, $\mu = E[X] = pN$, and any $\delta \in (0, 1]$, it is the case that $pr[X < (1-\delta)\mu] < e^{-\mu\delta^2/2}$ and for any $\delta > 0$, it is the case that $pr[X > (1+\delta)\mu] < (e^{\delta} \,/\, (1+\delta)^{1+\delta})^{\mu}$.

The following lemma defines a set of random variables that satisfy the Chernoff Bounds. It also gives the lower bound on the probability that a set of queries respond correctly.

Lemma 1 [35]: Let γ be an odd integer ≥ 1. The probability that a γ-*query* challenger operating over b' blocks correctly outputs every block i for which $p(i) \geq 3/4$ is greater than $1 - b'e^{-3\gamma/72}$.

Define b'' as the total number of blocks which have remaining unused labels, then we can get $b' + q \leq b'' \leq b' + n$. Define ε as the total number of blocks corrupted by the adversary in b'', therefore all of the ε blocks corresponding to that adversary have thrown less than or equal to $\varepsilon b''$ balls into b'' cans.

The next lemma gives the lower bound on the probability that the adversary responds with at least one fault.

Lemma 2: Assume that $\varepsilon b''$ balls are thrown into b'' cans without repetition for $\varepsilon \in [0, 1)$. The adversary has been requested by q different cans, and the can selected at each turn is independent and random. Let the probability that the adversary responds with a fault answer is greater than 1/5. Then, the probability that the adversary responds with at least one fault is greater than $1 - (1 - \varepsilon/5)^q$.

Proof: Let X_i be a Bernoulli random variable, where $X_i = 1$ if the adversary provides an incorrect block on the i_{th} query. The probability that a can contains a ball is $\varepsilon b'' / \, b'' = \varepsilon$, and a can having a ball inside corresponds to the adversary responding with an incorrect block. Since the probability that the adversary responds with a fault answer is greater than 1/5, according to lemma 1, $pr[X_i = 0] < 1 - \varepsilon/5$. We can obtain $pr[X_i = 0 | X_1, \ldots, X_{i-1}, \ldots, X_q = 0] \leq pr[X_i = 0]$. Hence $pr[X_i = 0] < (1 - \varepsilon/5)^q$.

The following theorem gives an upper bound on the probability of generating a 'bad' value by the adversary, where 'bad' means the verifier passes the response from the adversary with a probability of at least λ.

Theorem 2: A polynomial-time *label-scheme*$[\pi]$ is a valid scheme for all adversaries, then:

$$pr\left[Succ^{chal}_{Node}\eta \geq \lambda | \eta \leftarrow Exp^{setup}_{Node}\right] \leq \rho .$$

Proof: Considering the adversary cannot distinguish different blocks by label values and the probability to distinguish which blocks makes up a specific chunk is a random guess. Therefore, we can build the adversary's probability distribution $\{p(i)\}$ through these blocks in the file. Let $p(i) \geq 4/5$

for convenience and build the ball-and-can model with a probability $p(i) \geq 4/5$, where the adversary fails to corrupt the i_{th} block. Consider the adversary successfully corrupting a file block as throwing a ball into a can and every block could correspond to a can. If there is a ball in a can, this block has been corrupted, so that the probability that the adversary successful corrupts the i_{th} block is less than 1/5. If a can does not have a ball in it, this block remains uncorrupted. According to theorem 1 and lemma 2, we can obtain the upper bound.

The following theorem defines the lower bound of the parameters in the Sentinel POR system.

Theorem 3 [35]: Suppose that $\gamma \geq 24(j\ln 2 + \ln b')$. For any $\varepsilon \in (0, 1)$ such that $\mu < d / 2$. *Sentinel-PORSYS*$[\pi]$ is a (ρ, λ)-*valid* POR for $\rho \geq Ce^{(d/2-\mu)}\,(d/2\mu)$ and $\lambda \geq (1-\varepsilon / 4)^q$, where $\mu = n\varepsilon(b' + s) / (b' - \varepsilon(b' + s))$.

Theorem 4 gives the probability of detecting the adversary in our label-based scheme.

Theorem 4: For any $\varepsilon \in (0, 1)$, the *label-scheme*$[\pi]$ is a valid scheme for $\lambda \geq (1 - \varepsilon / 5)^q$, and the probability of detecting the adversary is $pr(detected) = 1 - (1 - \varepsilon/ 5)^q$.

Proof: From lemma 2, we can obtain that for the given value εin the ball-and-can model, the probability that the verifier accepts an illegal access is less than $(1 - \varepsilon / 5)^q$. Therefore, the value ε is valid by satisfying $\lambda \geq (1 - \varepsilon / 5)^q$.

In the following sections, we experiment with different values of ε and are convinced that to reach a higher bound, ε should be a smaller value.

VI. PERFORMANCE EVALUATION

We conduct the simulation experiment to evaluate the performance of our LACS scheme.

A. SIMULATION SETUP

We evaluate the performance of LACS using a desktop computer with a 3.30 GHz Intel CPU, 16GB RAM, and windows 7 OS. To verify the efficiency of the LACS, we utilize a 2 gigabyte (2G) file as an example and divide it into blocks. Each block has a size $l = 128$ bits, which is appropriate for an AES block to resist the brute-force guessing attack. Therefore, the 2G file consists of $b = 2^{27}$ blocks. Let $\varepsilon = 0.01$, meaning the attacker has mastered the 1% of blocks and unused label-values. We generate the labels, verify them with C code, and simulate the caching server and fog nodes in the computer program. According to theorem 3, we use the equation $pr(detected) = 1 - (1 - \varepsilon/ 5)^q$ to evaluate the accuracy of our scheme.

B. SIMULATION RESULTS

In Fig. 4, we compare the partition performances of different block sizes and label numbers. The results show that (1) even though the file size changes, the general trend is the time delay changing along with the block size and (2) in the case of blocks of the same size, the larger file size means a greater time cost.

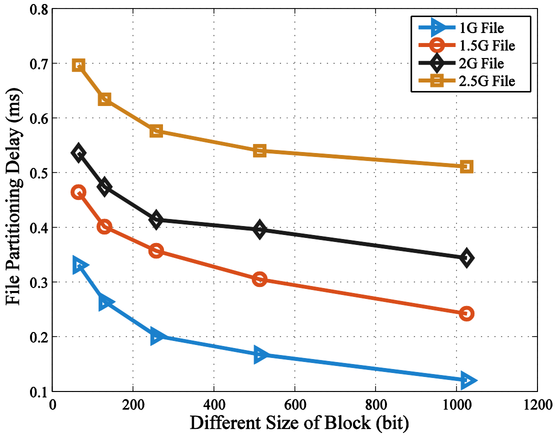


FIGURE 4. File partitioning delay under different size of block.

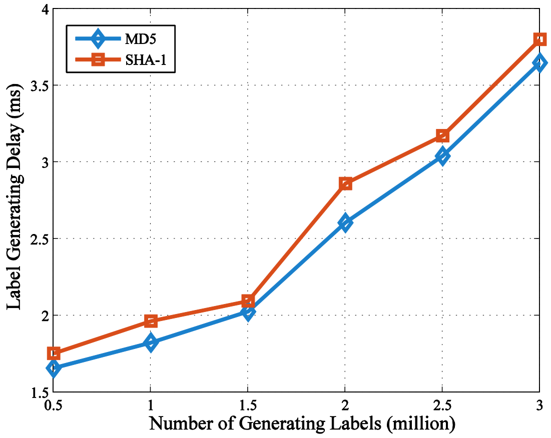


FIGURE 5. Label generating delay under different numbers of labels.

To evaluate the performance of the label generation, we use two common one-way functions, the MD5 and SHA-1. As shown in Fig. 5, the time delay continues to rise with the increase of the label generation number. Through Fig. 5, we can find out that the MD5 is more efficient than the SHA-1 in our scheme environment.

Fig. 6 shows the performance of the embedding label on the different block sizes and label numbers. The general trend is that the time overhead increase with the block size and label number, and larger block sizes means a greater time cost.

In Fig. 7, we compare the permutation performance of different block sizes and label numbers. The results show that (1) even though the label number changes, the general trend is that the time delay changes with the block size and (2) in the case of the same block size, a larger label number means a greater time cost.

Fig. 8 shows the verification performance for different label numbers and block sizes. From Fig. 8, the general trend is that the time overhead increases with the block size and label number. Consistent with the theoretical analysis, a greater label number and larger block size means more time overhead.

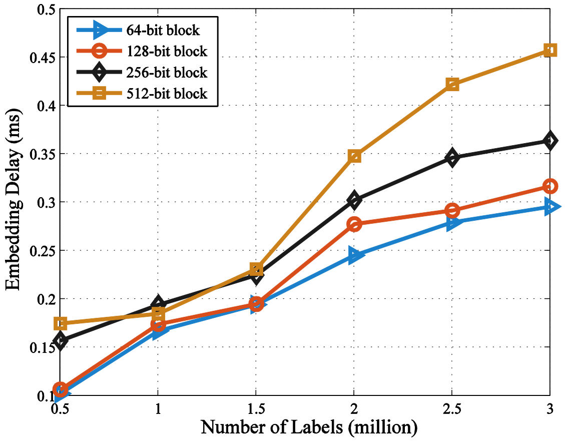


FIGURE 6. Label embedding delay under different numbers of labels.

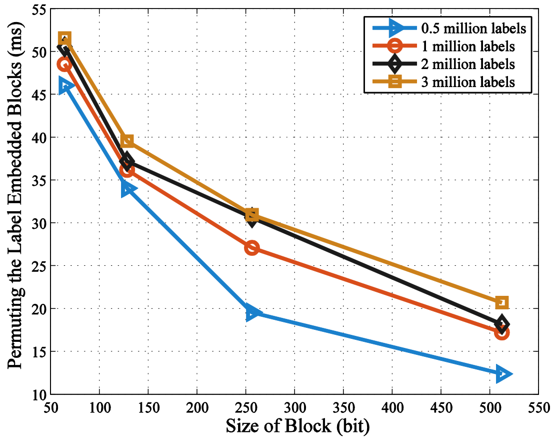


FIGURE 7. Blocks permuting delay under different size of blocks.

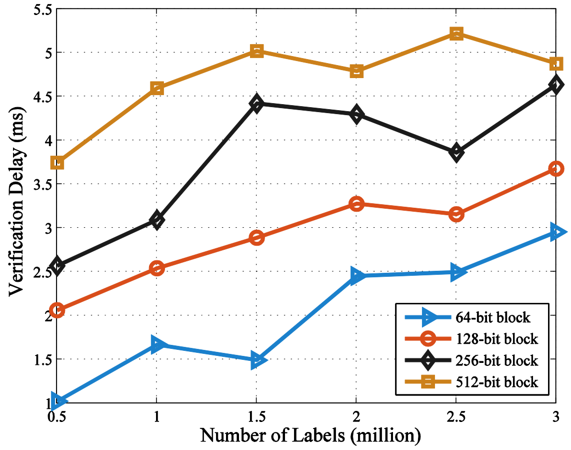


FIGURE 8. Verification delay under different numbers of labels.

In Fig. 9, we compare the verification performance with different fog node numbers and block sizes. The results show that (1) the time cost changes along with the fog node number and (2) for the same fog node number, the larger block size means a greater time cost.

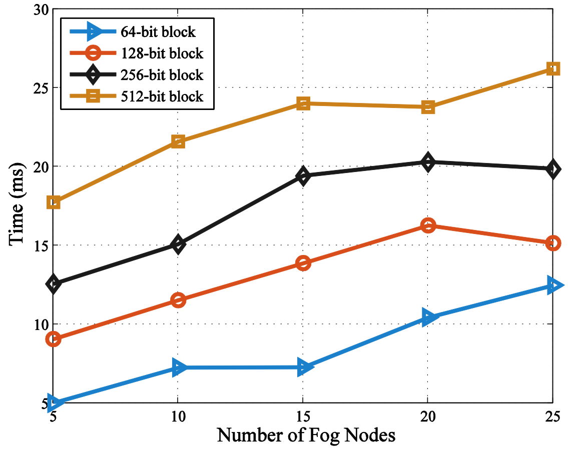


FIGURE 9. Verification performance under different numbers of fog nodes.

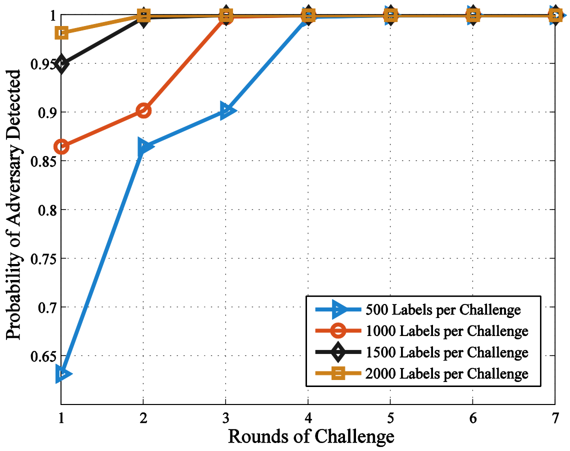


FIGURE 10. Probability of detecting the adversary under different challenge rounds.

Fig. 10 shows the probability of detecting the adversary with our scheme. We compare this probability for different q (e.g., 500, 1000, 1500, and 2000). For example, we suppose $q = 1000$, which means the verifier needs 1000 label-values to audit at one challenge. If the total number of labels is 1000000, the labels would be sufficient for almost three years, and even though the verifier asks the challenge each day. For each challenge, the probability that the attacker can be found is $1 - (1 - \varepsilon / 5)^{q} \approx 86.5\%$. Although such a probability is not very high in a single challenge, it is high enough for the cumulative process. After challenging 7 times, the probability that an attacker is still unfound is less than 1 in 100000. The results show that the LACS can achieve high accuracy with fewer operational steps.

VII. CONCLUSION

In this paper, a new lightweight label-based access control scheme named LACS has been proposed to achieve the reliability protection for the IoT-based 5G caching network. The LACS authenticates caching fog nodes by verifying the integrity of shared files that randomly embed label values. In the proposed scheme, each challenge utilizes the limited label-values. If the total number of labels is assumed to be 1000000 and $q = 1000$, the scheme can support nearly 3 years by implementing one challenge daily. Furthermore, we have proved that the LACS can theoretically ensure caching reliability and security. Finally, the simulation experiments have been provided to evaluate the efficiency of the LACS scheme. The results showed that the LACS can reach millisecond-level verification. These features make LACS suitable and practical for the general IoT-based 5G caching context.

REFERENCES

[1] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[2] N. Zhang, N. Cheng, A. T. Gamage, K. Zhang, J. W. Mark, and X. Shen, "Cloud assisted HetNets toward 5G wireless networks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 59–65, Jun. 2015.

[3] M. R. Bhalla and A. V. Bhalla, "Generations of mobile wireless technology: A survey," *Int. J. Comput. Appl.*, vol. 5, no. 4, pp. 26–32, 2010.

[4] M. Dohler, "The tactile Internet IoT, 5G and cloud on steroids," in *Proc. IET Conf.*, Mar. 2015, pp. 1–16.

[5] A. Loshkarev and A. Markhasin, "Performance modeling and optimization of flexible QoS-guaranteed multifunctional MAC for rural profitable ubiquitous 5G IoT/M2M systems," presented at the Int. Conf. Inf. Sci. Commun. Technol., Nov. 2016, pp. 1–5.

[6] Y.-L. Lai and J. Cheng, "A cloud-storage RFID location tracking system," *IEEE Trans. Magn.*, vol. 50, no. 7, Jul. 2014, Art. no. 3501004.

[7] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Information centric networking in IoT scenarios: The case of a smart home," presented at the IEEE Int. Conf. Commun., Jun. 2015, pp. 648–653.

[8] M. Uriarte *et al.*, "Usable access control enabled by sensing enterprise architectures," in *Proc. 6th Workshop Enterprise Interoperability*, 2015, pp. 1–10.

[9] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[10] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, Feb. 2015.

[11] V. C. Hu *et al.*, "Guide to attribute based access control (ABAC) definition and considerations (draft)," *NIST Special Pub.*, vol. 800, no. 162, pp. 15–26, 2013.

[12] F. Li, Y. Rahulamathavan, and M. Rajarajan, "LSD-ABAC: Lightweight static and dynamic attributes based access control scheme for secure data access in mobile environment," in *Proc. IEEE 39th Annu. IEEE Conf. Local Comput. Netw.*, Sep. 2014, pp. 354–361.

[13] X. Yao, X. Han, and X. Du, "A lightweight access control mechanism for mobile cloud computing," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Apr./May 2014, pp. 380–385.

[14] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "LIVE: Lightweight integrity verification and content access control for named data networking," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 308–320, Feb. 2015.

[15] C.-C. Lee, P.-S. Chung, and M.-S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *Int. J. Netw. Secur.*, vol. 15, no. 4, pp. 231–240, Jul. 2013.

[16] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2005, pp. 457–473.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13thACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.

[18] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2007, pp. 456–465.

[19] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Proc. Inf. Security Pract. Exper.*, 2009, pp. 13–23.

[20] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

[21] L. Ibraimi *et al.*, "Mediated ciphertext-policy attribute based encryption and its application," IN *Porc. Inf. Secur. Appl., Int. Workshop (Wisa)*, Busan, South Korea, 2009, pp. 309–323.

[22] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," in *Proc. Inf. Secur. Pract. Exper.*, 2009, pp. 1–12.

[23] T. Morris, "Trusted platform module," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 1332–1335.

[24] C. Lesjak, T. Ruprechter, J. Haid, H. Bock, and E. Brenner, "A secure hardware module and system concept for local and remote industrial embedded system identification," in *Proc. Emerg. Technol. Factory Autom.*, Sep. 2014, pp. 1–7.

[25] M. Hutter and R. Toegl, "A trusted platform module for near field communication," in *Proc. Int. Conf. Syst. Netw. Commun.*, Aug. 2010, pp. 136–141.

[26] J. Singh and J. M. Bacon, "On middleware for emerging health services," *J. Internet Services Appl.*, vol. 5, no. 6, pp. 1–34, 2014.

[27] N. Dhanjani. (Jan. 2017). *Hacking Lightbulbs: Security Evaluation of the Philips Hue Personal Wireless Lighting System*. [Online]. Available: http://www.dhanjani.com/docs/Hacking%20Lighbulbs%20Hue%20Dhanjani%202013.pdf

[28] R. M. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in *Proc. Int. Workshop Adapt. Secur.*, 2013, pp. 1–6.

[29] J. L. Hernández-Ramos, A. J. Jara, L. Marin, and A. F. Skarmeta, "Distributed capability-based access control for the internet of thing," *J. Internet Services Inf. Secur.*, vol. 3, nos. 3–4, pp. 1–16, 2013.

[30] I. K. Son, S. Mao, Y. Li, M. Chen, M. X. Gong, and T. S. Rappaport, "Frame-based medium access control for 5G wireless networks," *Mobile Netw. Appl.*, vol. 20, no. 6, pp. 763–772, 2015.

[31] Y. Liu, Y. Zhang, R. Yu, and S. Xie, "Integrated energy and spectrum harvesting for 5G wireless communications," *IEEE Netw.*, vol. 29, no. 3, pp. 75–81, May/Jun. 2015.

[32] H. Nikopour *et al.*, "SCMA for downlink multiple access of 5G wireless networks," in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 3940–3945.

[33] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, Mar. 2016.

[34] N. Golrezaei, K. Shanmugam, A. G. Dimakis, A. F. Molisch, and G. Caire, "FemtoCaching: Wireless video content delivery through distributed caching helpers," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1107–1115.

[35] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 584–597.

[36] T. Hagerup and C. Rüb, "A guided tour of Chernoff bounds," *Inf. Process. Lett.*, vol. 33, no. 6, pp. 305–308, 1990.

[37] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.

[38] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[39] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov. 2013.

[40] D. Chen *et al.*, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017, doi: 10.1109/JIOT.2016.2619679.

[41] K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, "An efficient and fine-grained big data access control scheme with privacy-preserving policy," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2016.2571718.

[42] G. Alpár, L. Batina, and W. Lueks, "Designated attribute-based proofs for RFID applications," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy*, 2012, pp. 59–75.

[43] Chris Palmer. (Sep. 2014). *Gradually sunsetting SHA-1*. [Online]. Available: https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html

[44] R. A. Grimes. (Nov. 2016). *Implementing SHA2 in Active Directory Certificate Services (ADCS)*. [Online]. Available: https://gallery.technet.microsoft.com/Migrating-SHA-1-to-SHA-2-82ee3a4e#content

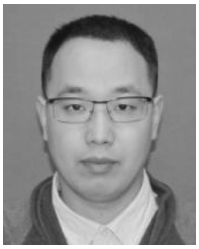
[45] S. Kitanov, E. Monteiro, and T. Janevski, "5G and the Fog—Survey of related technologies and research directions," in *Proc. 18th Medit. Electrotechn. Conf.*, Apr. 2016, pp. 1–6.

[46] K. Intharawijitr, K. Iida, and H. Koga, "Analysis of fog model considering computing and communication latency in 5G cellular networks," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops*, Mar. 2016, pp. 1–4.

[47] I. Abdullahi, S. Arif, and S. Hassan, "Ubiquitous shift with information centric network caching using fog computing," in *Computational Intelligence in Information Systems*. Cham, Switzerland: Springer, 2015, pp. 327–335.

[48] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data*, 2015, pp. 37–42.

QIXU WANG was born in the Neijiang, China, in 1985. He received the bachelor's degree from the School of Computer Science and Technology, Southwest University of Science and Technology, Mianyang, China, in 2009. He is currently pursuing the Ph.D. degree with School of Information and Software Engineering, University of Electronic Science and Technology of China. His research interests include information security, cloud computing, and storage.



DAJIANG CHEN (M'15) received the B.Sc. degree from Neijiang Normal University, Neijiang, China, in 2005, the M.Sc. degree from Sichuan University, Chengdu, China, in 2009, and the Ph.D. degree in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, in 2014. He is currently a Post-Doctoral Fellow with the University of Waterloo, Waterloo, ON, Canada, and with the School of Information and Software Engineering, UESTC. His current research interests include wireless security, physical layer security, information theory and channel coding and their applications in wireless network security and wireless communications.

NING ZHANG (S'12) received the B.Sc. degree from Beijing Jiaotong University, Beijing, China, in 2007, the M.Sc. degree from the Beijing University of Posts and Telecommunications, Beijing, in 2010, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2015. He is currently a Post-Doctoral Fellow with the University of Waterloo, Waterloo, ON, Canada. His current research interests include dynamic spectrum access, 5G, physical layer security, and vehicular networks.

ZHEN QIN (M'13) received the B.Sc. degree in communication engineering from UESTC in 2005, the M.Sc. degree in electronic engineering from the Queen Mary University of London in 2007, and the M.Sc. and Ph.D. degrees in communication and information system from UESTC in 2008 and 2012, respectively. He is currently a Lecturer with the School of Communication and Information Engineering, UESTC. His current research interests include network measurement, wireless sensor networks, and mobile social networks.

ZHIGUANG QIN (S'95–A'96–M'14) is currently the Director of the Key Laboratory of New Computer Application Technology and the Director of UESTC-IBM Technology Center. His research interests include wireless sensor networks, mobile social networks, information security, applied cryptography, information management, intelligent traffic, electronic commerce, and distribution and middleware. Dr. Qin served as the General Co-Chair for the WASA 2011, and Bigcom 2017.