参赛队员姓名：舒烨

中学：上海市世界外国语中学

省份：上海市

国家/地区：中华人民共和国

指导教师姓名：李建华、伍军

论文题目：Binary Reed-Solomon Coding Based Secure Distributed Storage Scheme and Test-Bed for Information-Centric Fog Networks

Binary Reed-Solomon Coding Based Secure Distributed Storage Scheme and Test-Bed for Information-Centric Fog Networks

Ye Shu

***Abstract*—Fog computing is an emerging architecture for processing, storing, and controlling the data at the edge of the networks, which is becoming a popular technology for Internet of Things (IoT). As a next-generation networking architecture, Information-Centric Network (ICN) has been introduced into networked fogs to establish efficient data exchange based on name, caching, content features, etc., which gives the IoT an opportunity to store the huge geo-distributed data at the edge of the networks and be less dependent on the Cloud, thus fulfilling the delay-sensitive needs of the end-users. Nevertheless, efficient distributed storage is a must for information-centric fog networks, because of the huge content exchange and geo-distributed data. In addition, the secure data exchange is a must for the distributed storage. To address the aforementioned challenges, this paper proposes an efficient storage scheme by integrating Binary Reed-Solomon erasure code with ICN mechanism in fog networks. The data are encoded into named data blocks and are distributed as well as stored into distributed fog nodes, which can provide fault-tolerance capabilities. The fog network performs information-centered with horizontal fog-to-fog communications to retrieve the data blocks efficiently. Moreover, an secure data exchange protocol is proposed for the distribute data storage. Simulation results prove the efficiency and advantages of the proposed distributed storage scheme. Finally, a test-bed is proposed to further evaluate the feasibility and efficiency of the proposed scheme.**

Index Terms — Fog computing; Distributed Storage; Information-Centric Networks (ICN); Internet of Things (IoT)

Table of Contents

I. Introduction

Fog computing refers to a networking architecture in which data are distributed, stored, and computed near the users in end-user devices instead of in centralized data-centers, i.e. in the edge of the network [1]. Compared to its predecessor, Cloud Computing, fog computing is particularly useful in addressing the problems involving geographical distribution, large-scale distributed systems, or those requiring low and predictable latency. It can be viewed as an extension at the edge near user side in the network of Cloud Computing to provide faster computing, storage, and networking experiences to end-users. With the recent advancements of communicating technologies such as 5G and Li-Fi, fog computing is becoming a popular choice for Internet of Things (IoT).

On the other hand, Information-Centric Networking (ICN) is a future Internet architecture based on named data objects (NDOs) which provides highly scalable and efficient distribution of content [2]. It replaced the where question in the current host-to-host communications with the what question in the network architecture based on NDOs. While today's Internet is mostly used to distribute and retrieve information, ICN aims to make this process more efficient by making the communications information-based. The communications are initiated by receivers who request NDOs and is made available by senders who possess NDOs.

Currently, using Information-Centric Networking to construct network for fog computing has becoming a trend, as being referred in [3], [6], [11] and many more. As stated in [3], the information-centric communication empowered the fog nodes with content-based

communication and further benefits the end-users with built-in mobility supply, simplifying the fog node distribution, shortening the communication latency, and making the communications more efficient. There are numerous benefits of implementing fog computing with Information-Centric Networking. The request-driven and connectionless feature of the ICN well suits the mobility of end users across different Fog Nodes (FNs). For example, if a user is on a moving car or a train and is requesting a certain information from the Information-Centric Fog Network, one would constantly switch between FNs and FNs since that person is traveling at a high speed. Without worrying loss of data during reestablishment process of connections in the conventional host-to-host network, all that person needs to do is to resend a request for the information. Then, the cached information requested would be sent to that person's car via a new connection with a new FN. A more detailed solution can be found in [10].

Fog computing is often implemented into Internet of Things (IoT), due to its similarities in utilizing the sensors locating at the edge of the Internet. As the IoT generates immense size of data of immeasurable value in geographically-dispersed edges of the Internet, it becomes a great burden for the edge networks to store these data. These data can be used to provide information for the system to run in the real-time or be used to analyze patterns for future optimization of the system. Hence, these data need to be accessed by users or requested entities at a low latency and a high reliability. Conventionally, the data are uploaded to the cloud servers and downloaded on-demand. However, this exerts not only a great waste of bandwidth resources but also huge latency during the redundant upload and download process. Instead of uploading the data to the Cloud, the IoT can store them at the edge servers, or the FNs. Since the FNs are not as stable as Cloud Servers and may result in data loss or data unavailability during a downtime, the storage reliability needs to be improved to store data at longer time intervals. To better store these geo-distributed data reliably at the edge of the IoT, the idea of applying the concept of distributed storage into Information-Centric Fog Network originates.

In distributed storage systems, erasure codes are used to prevent data from losing during node failures and to reduce storage overhead exerted by replications [8]. Among them, Binary Reed-Solomon (BRS) Code is a (n, k) regenerating erasure code [4][5]. Compared to other codes of the same kind, such as the Reed-Solomon code that encodes data through multiplication over the Galois field, and the Cauchy Reed-Solomon Code, which converts the Galois field arithmetic in RS code into exclusive or operations, the BRS code is faster in encode and decode speed [8]. Its (n, k) property, which is being proved in [5], ensured the data integrity even in the situation of nodes unavailability. It suggests that only k numbers out of n data blocks can be used to recover the data. On the other hand, the security of data exchange affects both the data storage and usage. Thus, security is a critical issue for the distributed storage, which provides protection for the data storage and retrieval.

In this paper, we proposed a storage scheme to address a solution to the problems stated above by integrating a specific type of erasure code named BRS Code with the Information-Centric Fog Network architecture. We use BRS code to encode the data and restore data

from redundant Fog nodes if any nodes have gone offline. The idea of information-centric communication is used in the data searching and indexing processes to make the process more efficient both in time and in network bandwidth resources. The rest of the paper is organized as follows. Section II discusses and reviews related works. Section III details the scheme and workflow of the proposed scheme. Section IV presents the secure data exchange protocol, while Section V evaluates and analyzes the scheme by simulation experiments. Section VI gives the testbed. Finally, Section VII concludes this paper.

II. Related Works

In this section, we introduce existing researches on fog computing, Information-Centric Networking, and Information-Centric Fog Networks.

As a new and promising paradigm, fog computing has caught the interest of many researchers and being implemented with various research directions, especially those focusing on delay-sensitive, context-aware, and location-aware applications or data protection at the edge of the network. To keep the sensitive data generated by IoT devices secure, [12] designed a scheme that integrates the computing resources of fog computing with storage capabilities of Cloud Computing, in which data are pre-processed at the edge servers, and then uploaded to the Cloud servers. To fulfill the objectives of processing and storing latency-sensitive data, [13] proposed an efficient scheme that supports data sharing between smart devices at the edge of the IoT. However, the scale of the IoT network is being limited in the scheme and is considered to be unfeasible to store and process a large amount of data generated by large-scale Fog Networks in the real situation. Similar to our scheme, [6] and [7] also attempts to combine the idea of distributed storage and fog computing to improve the data storage reliability of fog computing by encoding the data with erasure codes. However, their data is still uploaded to the Cloud, which is not an effective solution to the problem of latency and waste in bandwidth resources. In addition, [18] models the relationship between the service popularity and computing cost in Fog-enabled Industrial IoT with Zipf's law, and then designs a resource-partitioning scheme in which FNs can actively partition their resources for the use of popular Industrial IoT services.

On the other hand, ICN is a scheme for an Internet more capable of effective content distribution. In order to support host mobility, one general solution for ICN would be employing the publish/subscribe communication model [14]. A user interested in an information subscribes to it, while a user possessing the information publishes it. One significant benefit of the publish/subscribe model is the disjoint of the operations in time and space [15]. These properties well support the need of mobility over the network, since mobile nodes can simply reissue a former subscription for information on the go after switching nodes, and the network would be able to direct these subscriptions to nearby caches rather than remote origins [2]. This is a key enabler for ICN to be implemented in fog computing since the connections between users and Fog Nodes are often not persisted in time. The mobility feature of ICN enables users to switch between different FNs and simply reissue their interest when traveling.

There are also quite a few papers that combine the fog computing with ICN. Nguyen et al. proposed an inter-FN connection scheme based on ICN in [3], in which they utilize the horizontal Information-Centric dataflow to enrich the Fog layer with name-based communication, content caching, built-in mobility support, thus reducing the FNs' dependency on the Cloud. The Information-Centric Fog Network has also been applied to real-life scenarios, such as E-Health in [11], in which Guibert et al. uses ICN to extend the networks of fog-computing E-Hospitals and to share data between different Fog networks. The combination of fog computing and ICN provides low latency processing, shorter delays, and local storage opportunities, which meet the key requirements for E-Health.

To address the security issue in the network architecture, the concept of fog networks has been utilized in information-centric networks in [17] to provide a low-latency, content-aware security service filtering scheme for social networks at the edge of the network, which significantly improves the security of information-centric networks. Additionally, [16] proposes a security authentication scheme for big data analysis-based cluster management in Software-Defined Networks, which ensures the validity of the data sources and improves the performance of applications running in SDN by using ant colony optimization.

III. Distributed Storage System for IC-Fog Networks

This scheme is based on the idea of fog computing, which is proposed by Bonomi in [1]. In his idea, fog computing is a three-level architecture composed of cloud, Fog Nodes (FNs), and sensors. The introduction of ICN among the Fog Nodes in [3] reduces the data offloading from FNs to the Cloud.

For example, as depicted in Fig 1, if a person in the town wants to access the security camera footages in his house, the data can directly be passed to through the ICN between FNs, rather than through the cloud. This reduces the latency for him to receive the information. On the other hand, more data is stored at the FNs. However, due to the present storage unreliability at FNs [9], FNs are only considered as a transient storage method for data. This architecture certainly puts more pressure on the FNs for storage reliability.

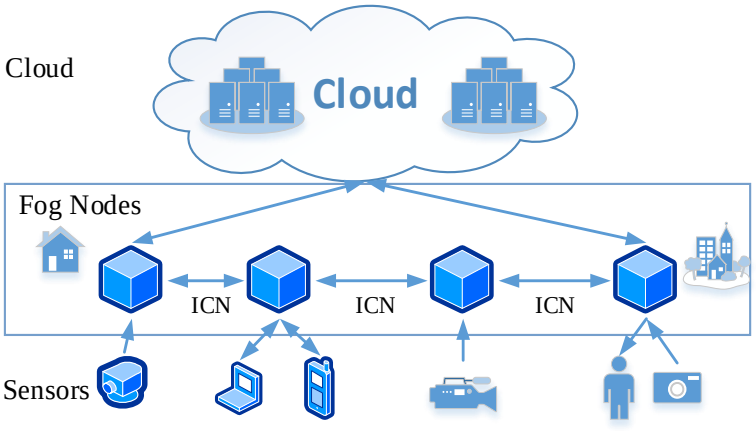

Fig. 1. The three-layered architecture of the Fog Network

With the goal to make the data storage at the FNs more reliable over a longer time interval, we proposed this scheme on the storage of Information-Centric Fog Network. This scheme mainly applies changes to the second layer, the FNs, and extends their storage ability by applying a horizontal ICN network that enables the exchange of data blocks created by BRS code. The implementation of BRS code as an erasure code generates parity data blocks and sacrifices the storage capacity for the reliability of data.

A. Basic Architecture

This scheme defines two layers of FNs out of all the FNs in an ICN network. They are respectively named the Data Nodes, and the Name Nodes, shown in Fig 2.

The data generated are encoded using Binary Reed-Solomon (BRS) code into data blocks and are distributed and stored in different Data Nodes. This process is done automatically by the edge servers and the sensors connected to it which uploads the data.

The Name Node works as a cached index for the named data blocks stored in Data Nodes. It is comparatively nearer to end-users and is the first node that user access upon retrieval of information. Theoretically, any Fog Nodes can be a Name Node, if it is near to the users and can process information received from users and data nodes. The implementation of the concept of Name Node ensures that users get the information at the lowest possible latency and are less likely to suffer from a downtime since any nodes can be a Name Node.

Upon receiving a request packet from the user, the Name Node would first query its cached index, if no results are found, it would send a request packet to data nodes. It is then the architecture of Information-Centric communication took place. The detailed procedure for exchanging data would be discussed in Section C, while the detailed coding and decoding method for the data blocks are discussed in Section B.

B. Distributed Data Storage based on BRS Code

The storage scheme we proposed is based on the idea of a distributed storage system. The data generated is first divided into k numbers of source blocks and is then encoded using Binary Reed-Solomon code into m numbers of parity blocks. The data blocks of $n = k + m$ in total numbers are distributed into different FNs and are retrieved upon a request. Due to the (n, k) property of BRS codes, any k numbers of data blocks would be sufficient to recover the data.

The encoding process is detailed below. After the data generated is uploaded to the nearest FN, it is first divided into k source blocks, each block is of L bits length and is represented by the following polynomial

$$s_i(\mathrm{z}) = \sum_{j=0}^{L-1} s_{i,j} z^j \tag{1}$$

where $s_{i,j}$ represents the $(j+1)^{\text{th}}$ bit of s_i, and $i \in [0, k-1]$. Then, m parity blocks are

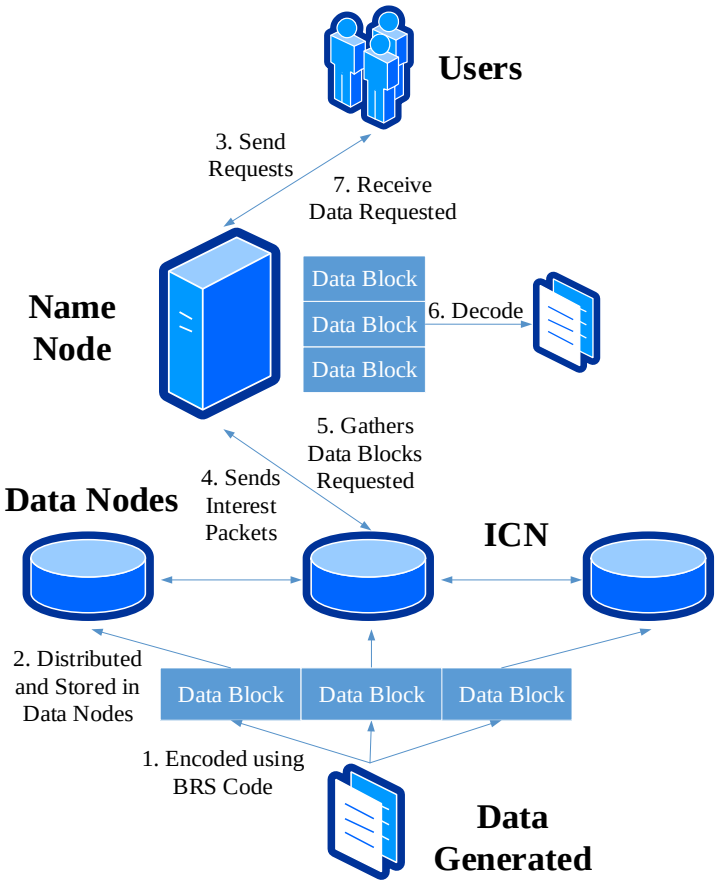

Fig. 2. The basic architecture of the storage system

generated from the source blocks using BRS code at the node receiving this data.

$$m_i(\mathrm{z}) = \sum_{j=0}^{k-1} v_{i+1,j+1} s_j(\mathrm{z}) \tag{2}$$

Accordingly, the corresponding matrix notation of the source data and the parity data would be

$$\begin{bmatrix} s(z) \\ m(z) \end{bmatrix} = \begin{bmatrix} I(k) \\ V(z) \end{bmatrix} s(z) \tag{3}$$

where $I(k)$ is a $k \times k$ identity matrix, and $V(z)$ is a $m \times k$ Vandermonde matrix with $v_{i,j} = z^{(i-1)(j-1)}$. In equations above, $s_{i,j} z^j$ represents the rightwards shift of $s_{i,j}$ with an offset of j. In this way, $n = k + m$ blocks are obtained, which are named after original data followed by an identification number and are distributed into the data nodes and stored.

On retrieval of information, any k number of arbitrary data blocks can be used to recover the original information, in case some FNs are unavailable for exchanging data. The

decoding process can be done with an efficient Zigzag decoding method. After subtracting the remained source blocks from the parity blocks, at least one bit of existing information is shared among parity blocks, which can directly be deduced. Even in the extreme condition which all source blocks have failed, leaving only parity blocks available, the original data can still be recovered using XOR operations, which is illustrated in [5] and [8].

C. *ICN-based Data Exchange for Distributed Storage*

The data exchange is at the horizontal level between FNs, which are constituted by two types of nodes — the Name Node, and the Data Node. The Name Node, which the user directly communicates with, oversees the communication between users and FNs, while the Data Node stores data and exchanges data within the Fog Network. Any FNs inside the Fog Network can be a Name Node if it can communicate with users. The introducing of the Name Node in our scheme benefits the user and the data exchange process in the following ways.

1) Bridge for User-Network Communication: The Name Node works as a bridge for the end-users to get connected to the ICN network of the FNs, it receives the users' requests and sends it to other FNs in ways of ICN interest packets. The user may or may not communicate with the Name Node in the form of ICN interest packets and data packets, which enables conventional equipment to enjoy the benefit of Information-Centric Fog Network, giving the end-users more flexibility to choose from the equipment they use.

2) Shorter Latency Due to the Caching Policy: On retrieval of information, the Name Node automatically caches the catalog of the Data Nodes available, and data blocks, if possible. Hence, on the next retrieval, one would not suffer from the latency of communicating with different Data Nodes in the Information-Centric Fog Network and could directly download the data from the cached data in the Name Node.

3) Flexibility and Efficiency over the Network: The user is only required to communicate with the Name Node once and leave all the locating and decoding work to the Name Node and other FNs in the network, which all happen in an efficient Information-Centric Network. Besides, any FN near the user can be a Name Node, which provides flexibility and mobility for the users as the users are free to switch between the FNs nearest to them during traveling. This switching process also benefits the efficiency since users can communicate to the nearest FN with shorter latency and larger bandwidth.

The communication is based mainly on two types of packets, the Interest Packet, and the Data Packet. The Interest Packet is generated and sent by users who demand a certain content and contains the name of that content. The Interest Packet is forwarded upstream in the ICN until its data source replies with a Data Packet. The Data Packet contains the name of the content, the data itself, as well as digital signature and signed info that clarifies its credibility. The communication process for retrieving a certain required information is depicted in Figure 3 and detailed below.

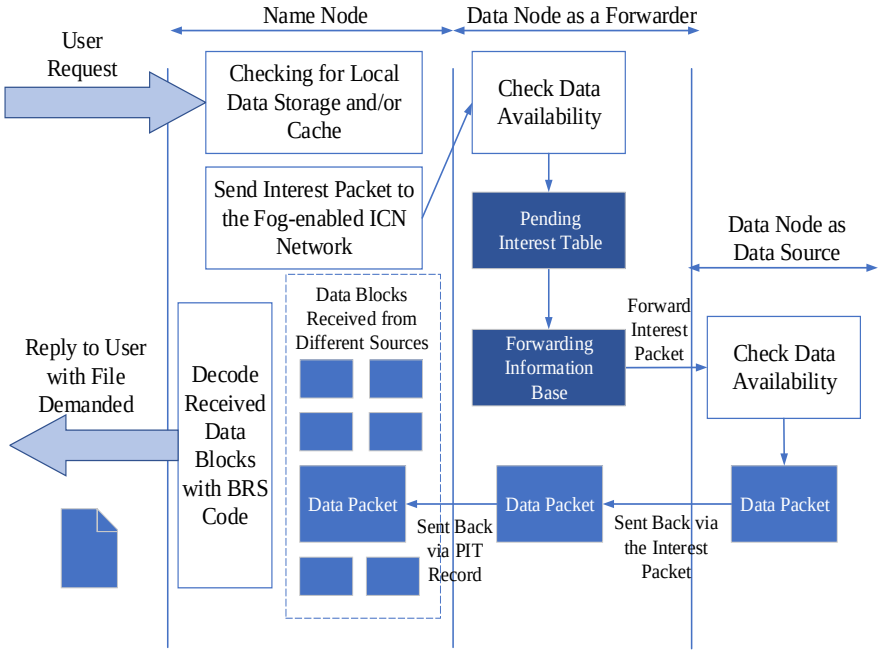

Fig. 3. The Information-Centric Data Exchange for Distributed Storage

When the user demands a certain data, one would connect to its nearest FN. This FN, serving as the bridge for the user to access the Information-Centric Fog Network, is named the Name Node. When a user request arrives at the Name Node, a longest-match lookup is done on the data stored or cached locally. If there exists a matching data, it would be sent back to the user. If not, the Name Node would generate a minimum of k numbers (since the decoding process requires the presence of at least k out of n data blocks) of Interest Packets demanding different data blocks encoded from the data demanded by the user. The Interest Packet is then sent upstream to other FNs in the Fog Network, which are known as Data Nodes.

As a Data Node receives an Interest Packet, it would conduct a longest-match lookup on the data stored or cached. Again, if there exists matching data, it would be sent back in the form of an ICN Data Packet, with the demanded data block stored in it, and the Interest Packet is discarded, or consumed, as it is now satisfied by a Data Packet downstream. If not, the Data Node would first look up the Pending Interest Table (PIT). The PIT keeps tracks of previously forwarded Interest Packets and their requesters. Since only the Interest Packets are propagated upstream, by looking into the PIT, the Data Node would ensure that no duplicate requests are sent upstream. If there is a match in the PIT, which suggests that an identical Interest Packet has already been propagated upstream, the Data Node would discard the newly received Interest Packet and append its requester to the requester list in the PIT. If there is no match in the PIT records, the Data Node would add the Interest Packet and the requester to PIT records before it checks for Forwarding Information Base (FIB) records. The FIB stores the potential sources of the Interest Packet. Upon looking up the FIB for potential data sources, the requester would be removed from the potential sources

list in the FIB (since the requester would not generate an Interest Packet for data it already owns). The Interest Packet is then forwarded to all the potential sources recorded in the FIB.

The processing procedure of Data Packet simply follows the trace of the Interest Packer back to its original requester(s). A longest-match lookup is first conducted on the Data Packet in data stored or cached locally. If a match exists, the newly received Data Packet may be a duplicate of previously received and forwarded Data Packets and is discarded. If there does not exist a match, the Data Packet is cached locally and is looked up in PIT records. Then, the Data Packet is forwarded downstream to all the FNs on the requester's list. After receiving a minimum of k numbers of demanded data blocks, the Name Node decodes the received data blocks by shifting and XOR operations to recover the original data file demanded by the user. The data is then replied to the user as demanded.

IV. Data Exchange Protocol

As a distributed architecture, the proposed storage scheme in information-centric fog networks controls many fog nodes through the mobile communication network. On account of the secure data exchange protocol, the data are transferred under the security protection. As shown in Fig. 4, the secure data exchange protocol is proposed specifically for a pub/sub service. Pub/sub pattern is used in the communication to obtain a more dynamic network topology and greater network scalability. Firstly, based on the username/password in addition to a dynamic password, a mutual authentication between sender node and receiver node is established. Next, key distribution is implemented to initialize the data exchange process and to update the secret key. Then, the secret key is distributed to the participators.

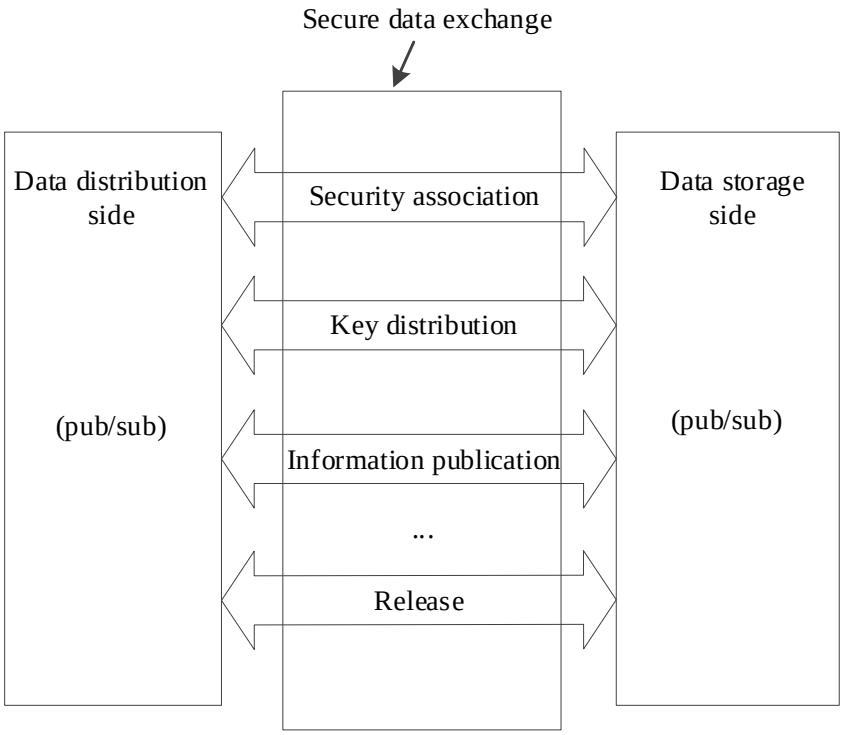

Fig. 4. Sequence of proposed data exchange protocol

Finally, the content is encrypted based on the secret key given. The ciphertext, which is encrypted by the secret key, is exchanged until release. Data receiver node and data sender node are severed as publishers or subscribers, respectively.

The secure data exchange protocol is shown in Fig.5. The notations used in the protocol are shown in Table I. In the security association, *RN* is a challenge number randomly created and distributed to distributed storage nodes in information-centric fog networks. Here, the hash function is used to generate the new password towards an integration of *RN* and original password. The created time of message *TIM* is added to prevent the replay attack. By using hash-based message authentication code (HMAC), the publisher calculates the digital digest for request parameters with created time message. Next, original message *M*, *TIM* and *HMAC(M)* are combined and sent to the subscribers. Then, the subscriber computes *HMAC(M)'* using HMAC algorithm and derives *M* as well as *TIM*. Moreover, it also verifies *HMAC(M)* and *HMAC(M)'*.

Table I Symbols used in secure authentication protocol

Symbol	**Explanation**
Distr	Content distribution node
Sto	Content storage node
TIM	The created time of message against replay attack
(M_1, M_2)	Concatenation of two messages
HMAC(M)	MAC calculation for message *M* based on hash function for authentication
RN	A challenge number
ReqFeatures	Parameters involved in the request
ResFeatures	Parameters involved in the response

In the process of secure data exchange, a group-wise key distribution service based on KCT (Key-Chain Tree) is adopted with self-healing ability. Self-healing phase works in case of broadcast packets loss to some participants. When storage fog node roles are changed after distributed storage, key updating phase is implemented.

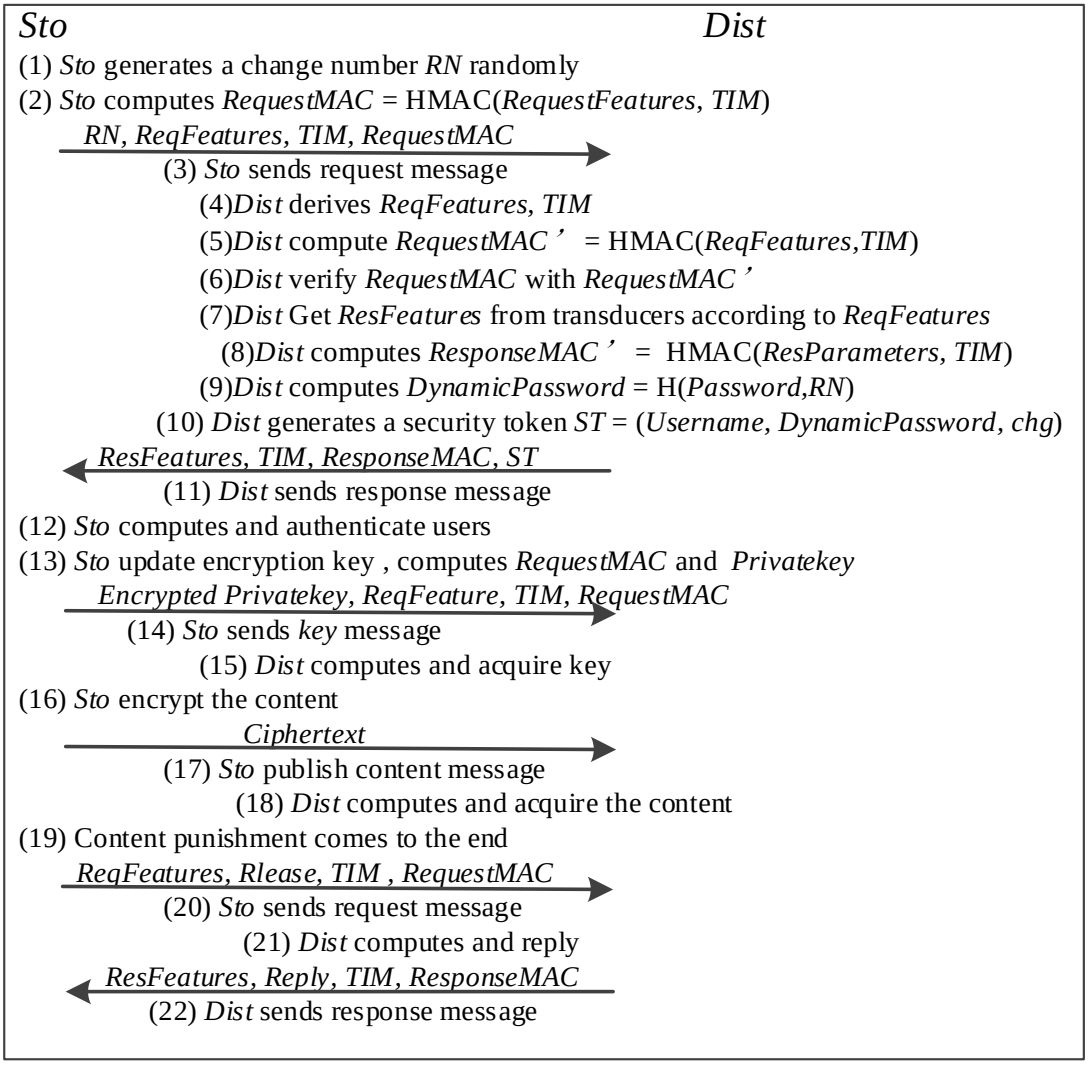

Fig. 5. Proposed data exchange protocol

V. Simulation and Analysis

In this section, we simulated the encode and decode process of this scheme to evaluate its performances. The BRS code is implemented with C++ programming language, which is run on the platform of Intel i5-6200U processor running at 2.40 GHz with 8 Gigabytes of RAM.

A. *The Effect of Failed Blocks on Storage Efficiency*

Firstly, the effect of failed block numbers on decode speed is measured. The block size of 65536 KB is taken as an example and the parameters of m and k are controlled such that the data are split and encoded into a fixed number of blocks. The number of failed blocks is then increased to measure the decode speed.

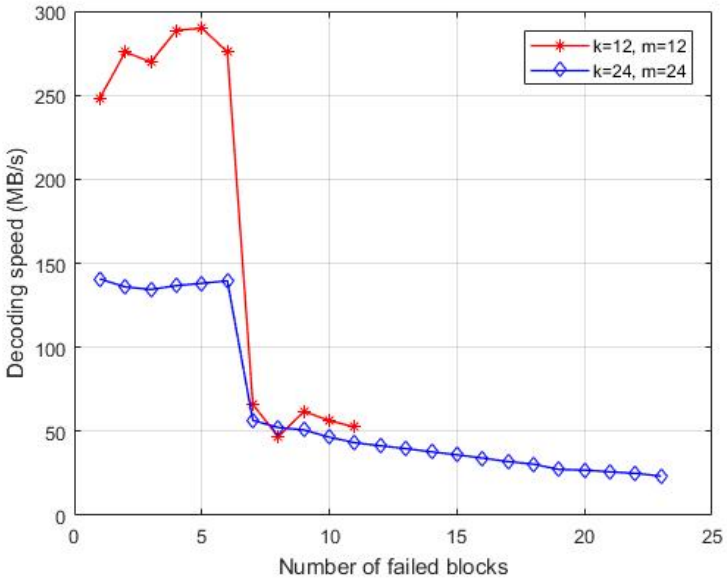

Fig. 6. Effect of failed blocks on storage efficiency

As observed, the decode speed is related to the number of original data blocks k and the number of parity blocks generated m with low numbers of failed blocks. The speed keeps at a constant rate for the range of [1,6] failed blocks, and decreases sharply at the seventh lost block, then converges to the same rate regardless of k and m.

B. *The Impact of Block Sizes on Storage Efficiency*

The number of original blocks k and the number of parity blocks m is kept constant with $k = 3, m = 3$, the number of lost blocks is kept at one. The size of each block is then increased to measure the encode and decode speed.

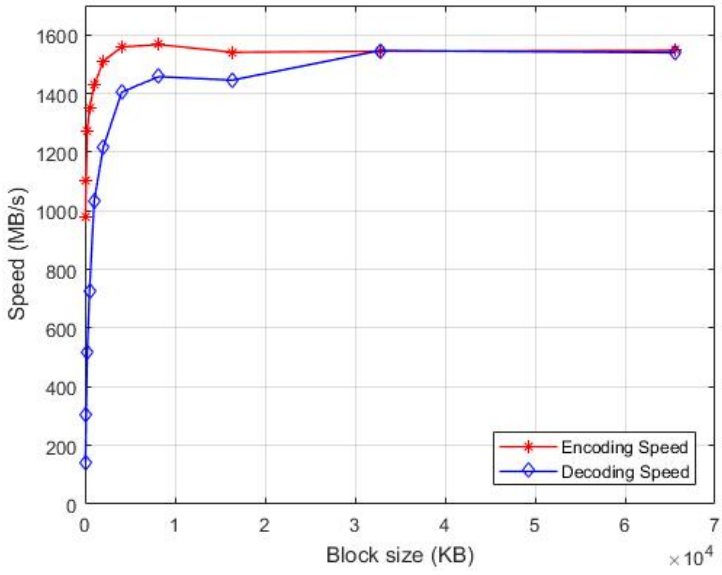

Fig. 7. The impact of block sizes on storage efficiency

As observed, the encode and decode speed increased dramatically when the block sizes are small, and eventually converges at a comparatively high rate.

VI. Test-Bed Platform

Here, a testbed is designed to evaluate the architecture of information-centric fog networks and to enable further researches in physically enabling the architecture. We employ Raspberry-Pis to setup our physical testbed with a relatively low cost. The testbed uses IP network to realize a virtual information-centric networking overlay. Each node within the testbed is considered as a fog node, which consists of several hosts.

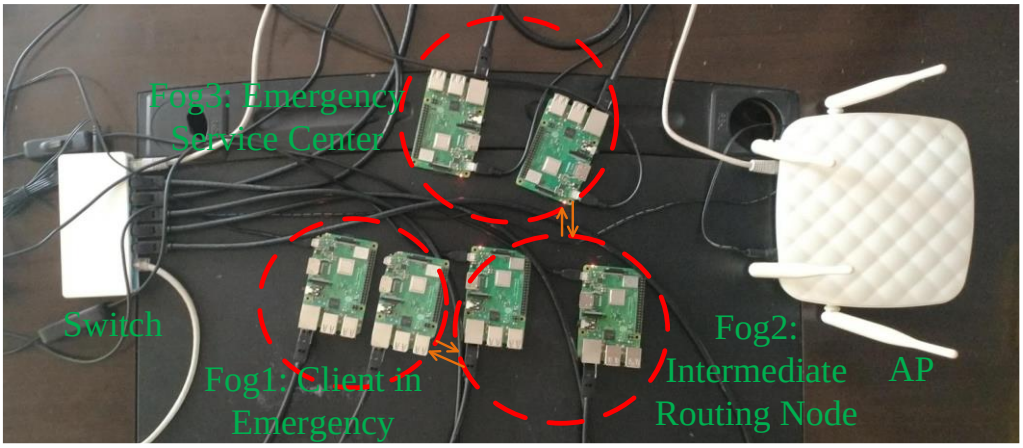

Fig. 8. Test-bed of the proposed scheme

To perform the evaluation and comparisons, we first assumed that the amount of data in each module of the fog nodes is the same. We include 32 sub-modules in each fog node, and in each sub-modules one test data is taken. In the evaluation, three scenarios are considered. Scene 1: the module name is in the request and secure distributed storage is performed. Scene 2: there is no module name in the request but there is traditional storage in the system. Scene 3: there is no module name in the request and there is secure traditional storage in the system. In each of these three scenes, the delay time is tested. The result is shown in Fig. 9: the proposed secure distributed storage scheme is more efficient than traditional storage.

VII. Conclusion and Future Work

In IoT, vast amounts of geographically-distributed data are stored and exchanged at the edge of network, which are capable of responding to end-users' delay-sensitive needs, but are also less reliable than the Cloud considering the limited storage availability of Fog Nodes. To address this problem, we proposed a storage scheme for fog computing, which integrates Binary Reed-Solomon erasure codes for distributed storage at the FNs and Information-Centric Network for efficient content exchange in fog computing. Moreover, a secure data exchange protocol is proposed to guarantee security for the data exchange within the distributed storage. Finally, a test-bed is developed for evaluation of experiment platform in the reality. The proposed scheme shows higher efficiency than traditional storage schemes. Through the scheme, we aim to make storage at the edge of network more

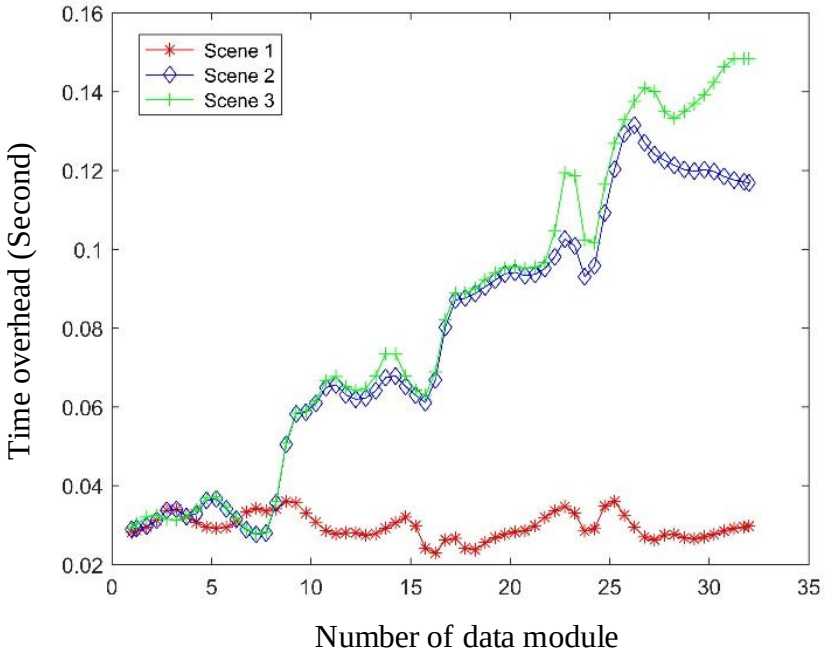

Fig. 9. Time overhead evaluation based on Test-bed

reliable and secure, thus realizing the benefits of fog computing to a more practical and applied level. Nevertheless, this scheme also faces great challenges brought by the unique features of fog computing. The heterogeneous physical connections between Fog Nodes, the limited computing resources to encode and decode the data files, etc.; there is still much left to be done to realize a concrete storage scheme for Information-Centric Fog Networks, even to realize this network architecture.

VIII. REFERENCES

[1] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, “Fog computing: A platform for Internet of Things and analytics,” in Big Data and Internet of Things: A Roadmap for Smart Environments. New York, NY, USA: Springer, 2014, vol. 546, pp. 169–186.

[2] G. Xylomenos, C.N. Ververidis, V. Siris et al., "A survey of information-centric networking research", IEEE Commun. Surv. Tutor., vol. 16, no. 2, pp. 1024-1049, 2014.

[3] D. Nguyen, Z. Shen, J. Jin, and A. Tagami, “ICN-Fog: An information-centric fog-to-fog architecture for data communications,” in Proc. IEEE Glob. Commun. Conf. (Globecom), Singapore, Dec. 2017.

[4] H. Hou, K. W. Shum, H. Li et al., “BASIC regenerating code: Binary addition and shift for exact repair,” *2013 IEEE Intl. Symp. on Information Theory*, pp. 1621-1625, 2013.

[5] J. Chen, H. Li, H. Hou et al., “A new Zigzag MDS code with optimal encoding and efficient decoding,” 2014 IEEE Intl. Conf. on Big Data, 2014.

[6] J. Zhou, T. Wang, M. Bhuiyan, and A. Liu, “A Hierarchic Secure Cloud Storage Scheme based on Fog Computing,” IEEE 15th Intl. Conf. on Dependable, Autonomic and Secure Computing, pp. 470-477, 2017.

[7] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, Y. Liu, “A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing”, IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 3-12, Feb. 2018.

[8] P. Lu, Z. Huang, S. Luo, H. Li, and J. Chen, “Evaluating the Performance of Erasure Codes,” 2015 3rd Intl. Conf. on Advanced Cloud and Big Data, pp. 213-218, 2015.

[9] M. Aazam, S. Zeadally, and K. Harras, “Fog Computing Architecture, Evaluation, and Future Research Directions,” IEEE Commun. Mag., vol. 56, no. 5, pp. 46-52, 2018.

[10] H. Nakazato et al., “On-path resolver architecture for mobility support in information-centric networking,” GC Wkshps, 2015.

[11] D. Guilbert, J. Wu, S. He, M. Wang, and J. Li, “CC-Fog: Toward Content-Centric Fog Networks for E-Health”, 2017 IEEE 19th Intl. Conf. on e-Health Networking, Applications and Services, 2017.

[12] J. Fu, Y. Liu, H. Chao, B. Bhargava, Z. Zhang, “Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing” IEEE Trans. Ind. Informat., in press.

[13] M. Mollah, M. Azad, A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted Internet of things", IEEE Cloud Computing, vol. 4, no. 1, pp. 34-42, 2017.

[14] P. T. Eugster, P. A. Felber, R. Guerraoui, and A. Kermarrec, “The many faces of publish/subscribe,” ACM Computing Surveys, vol. 35, no. 2, pp. 114–131, June 2003.

[15] Y. Huang and H. Garcia-Molina, “Publish/subscribe in a mobile environment,” Wireless Networks, vol. 10, no. 6, pp. 643–652, November 2004.

[16] J. Wu, M. Dong, K. Ota, J. Li, Z. Guan, “Big Data Analysis based Security Cluster Management for Optimized Control Plane in Software-Defined Networks,” IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 27-38, 2018.

[17] J. Wu, M. Dong, K. Ota, J. Li, Z. Guan, “FCSS: Fog-Computing-based Content-Aware Filtering for Security Services in Information-Centric Social Networks,” IEEE Transactions on Emerging Topics in Computing, DOI: 10.1109/TETC.2017.2747158, pp. 1-12, 2017.

[18] G. Li, J. Wu, J. Li, K. Wang, T. Ye, “Service Popularity-based Smart Resources Partitioning for Fog Computing-enabled Industrial Internet of Things,” IEEE Transactions on Industrial Informatics, DOI: 10.1109/TII.2018.2845844, pp. 1-10, 2018.

IX. 致谢

舒烨同学自 2017 年 10 月份至今，参与上海交通大学网络空间安全学院李建华教授以及伍军教授的研究生组会，参与研究领域覆盖新型网络架构的通讯、存储、及安全。

在导师指导下，我阅读了大量计算机网络和通讯领域的研究论文，并自学了分布式存储和信息交换安全协议的相关知识。

这篇研究成果，从课题选题、设计，到其中的完成过程和实现细节，都得到了指导老师们的悉心指点。在老师们的点拨和栽培下，历经一年的努力和奋斗，这份研究成果方才最终问世。

从被动地接受老师传授的知识，到主动地确立自己的研究方向，自主在领域内探索自己感兴趣的知识，独立地思考问题并与导师讨论，这于我而言，是一个质的飞跃。这一过程中，是导师的循循善诱激发了我从事研究的兴趣，为我今后的学术研究之路做了铺垫。

在此，向二位导师表示衷心的感谢！

舒烨

舒 烨

Ye Shu
ye_shu2017@stu.swfla.org / shuye02@outlook.com
Shanghai World Foreign Language Academy, Shanghai, China

SUMMARY

International Baccalaureate Diploma Program Learner who is interested in Computer Science.

ACTIVITIES

Independent Researcher October 2017 – Present

上海交通大学网络空间安全学院

- 参与网络空间安全学院的研究生组会
- 研究领域覆盖 Fog Network, Information-Centric Network 等新型网络架构的通讯、存储、及安全
- 作为第一作者研究 Information-Centric Fog Network 的存储机制，论文被 IEEE 会议录用

Staff & Onsite Tech Support & Hardware Team Leader April 2018 - July 2018

THE Hack 2018 (https://www.thehack.org.cn)

- 联合主办方成员、团队高贡献成员
- On-site Tech Support
- 负责：Hardware Checkout System, 选手提问系统, 评审系统的编写/部署/维护
- 硬件团队（比赛全程硬件设施审批、追踪、统计）leader
- 选手导师：负责在选手提问系统上回答选手的技术性提问

社长 / President May 2018 – August 2019

Computerization 世外信息化社 (a.k.a. C 社)

- 参与开发/维护校园信息化平台 SAM 系统
- 与世外学生会合作，解决了社团教室的管理空白问题、新社团/五星社团/末尾社团答辩的投票和统计问题、学生事务中心的申请受理问题，降低手续繁琐程度，提高学生会的工作效率。
- 与慈善晚会Charity合作，解决拍卖的实时出价和竞价问题
- 组织程序设计讨论、NOIP 校内培训、离散数学/线性代数讨论
- 促成了与 Techomedia 拓科传媒、世外数学社等社团及与学生会的深度合作
- 正在主导开发校内社团 SaaS 平台项目

副社长 / Vice President May 2018 – August 2019

Techomedia 拓科传媒

- 华东最大的学生科技媒体
- 两名副社长之一
- 推文部&技术部 总负责人，参与全部科技推文的审稿
- 独立撰写了 4 篇推文、参与共同撰写了 11 篇推文、最高单篇阅读 39000+
- 为线下活动提供技术支持（包括但不限于 workshop/Hackathon/采访）

副社长 / Vice President May 2018 – August 2019

WFLA Math Club 世外数学社

- 三名副社长之一
- 数学建模竞赛的赛前培训及辅导的主讲人之一
- 独立负责计算机辅助数学学习的社团内部培训

ACHIEVEMENTS

IEEE International Workshop on Computer -Aided Modeling Anal ysis and Design of Communication Links and Networks (IEEE CAMAD 2018) Sept. 2018

Barcelona, Spain

- 作为第一作者的英文研究论文被会议全文录用并发表
- 论文标题：*Binary Reed-Solomon Coding Based Distributed Storage Scheme in Information-Centric Fog Networks*

National Economics Challenge June 2018

World Final (Hosted in New York, United States) - David Ricardo Division

- 1st Place Finish in the Overall Team Awards (China)
- 1st Place Finish in Microeconomics Round (International)
- 1st Place Finish in the Quiz Bowl China Round
- 2nd Place Finish in the Quiz Bowl International Round
- 4th Place Finish in the Critical Thinking Round (International)

The Center for Education in Mathematics and Computing April 2018

Galois Contest

- Group IV (Scores 33 out of 38)
- Certificate of Distinction (≥ World Top 25%)

American Mathematics Competition 10 Feb. 2018

- Honor Roll (World Top 2.5%)
- Has advanced into American Invitational Mathematics Examination

20th Annual High School Mathematical Modeling Contest Nov. 2017

- Honorable Mention

The Mathematics League Nov. 2017

- World Top 100

National Economics Challenge 2017 April 2017

China Final (hosted in Shanghai, China) - Adam Smith Division

- Team leader

The Center for Education in Mathematics and Computing April 2017

Fryer Contest & Pascal Contest

- School Champion (Fryer)
- Group II (Scores 36 out of 38)
- Certificate of Distinction (≥ World Top 25%)

United States Academic Decathlon China 2017 Feb. 2017

- Team leader
- Certificate of Achievement (for team leaders)

Student of the Week Sept. 2016

- For exemplifying character that promotes a healthy learning environment for Elite Citizens of High Caliber
- In International Division, Shanghai Pinghe School

李建华，博士、教授（二级）、终身教授、博士生导师。现任上海交通大学网络空间安全学院（信息安全工程学院）院长，信息内容分析技术国家工程实验室主任，教育部网络安全管理监控与服务工程技术研究中心主任，上海市信息安全综合管理技术研究重点实验室主任，主要研究领域包括：信息内容安全管理、网络攻防与信息系统检测评估、网络安全管理、密码学及应用。现任中国网络空间安全协会副理事长，中国网络空间安全协会人才教育培养工作委员会主任委员，上海市网络安全管理协会名誉会长，教育部信息安全教学指导委员会副主任委员，中国能源研究会网络安全技术研究中心主任，上海市信息化专家委员会专家，曾担任国家 863 计划首席专家/管理专家，科技部国家电子政务重大工程总体组组长/专家，国家保密局顾问专家，上海世博会安保顾问专家，中央网信办第一，二届全球互联网大会安保专家，北京奥运会、上海世博会安保顾问专家，入选首批国家百千万人才计划，获国务院有突出贡献特殊津贴，上海市优秀学科带头人，上海市十大科技精英，上海市科技领军人才，曾入选 2007 年度美国 ISC2 亚洲有影响力的信息安全专业领导人。获 2017 年度中央网信办、教育部“全国优秀教师”荣誉，获国家科技二等奖 1 项，国家级教学成果奖 1 项，省部级科技进步一等奖 5 项，省部级二等奖 4 项，省部级三等奖 4 项，省部级教学成果一等奖 2 项，发表 EI/SCI 收录论文 267 篇，出版教材专著 16 部,并担任国际 Communication security, Internet security, computer survey 及电子学报、通信学报、信息安全学报，网络安全学报等期刊编委及审稿人，担任多个国家重点实验室和国家工程实验室学术委员会委员等。

伍军，上海交通大学信息内容分析技术国家工程实验室副主任，网络空间安全学院副研究员，上海市浦江人才计划专家。博士毕业于日本早稻田大学，曾任日本国立产业技术综合研究所（AIST）博士后特别研究员，早稻田大学国际信息通信研究院特聘研究员，2013 年 9 月至今在上海交通大学任教。主要研究领域为：物联网技术及其安全、云计算/雾计算技术及其安全、下一代互联网及其安全、大数据技术及其安全等。在 IEEE Transactions TII、TETC、TNSM、TBD、T-CE 等期刊和 IEEE INFOCOEM、GLOBECOM、ICC 等会议发表论文 120 余篇，其中 40 余篇 SCI、60 余篇 EI，申请 30 项发明专利；与美国加州大学伯克利分校的诺贝尔奖获得者 Daniel M. Kammen 教授等合著 Wiley/IEEE 英文著作一本；主持了国家自然科学基金、上海市战略新兴产业项目、国家电网科技部重点课题、华为技术有限公司重大课题、公安专项资金、上海市科委等 10 余项项课题。参与中国国家 973、863 课题、国家自然科学基金重点项目、日本学术振兴会（JSPS）课题等科研项目。担任包括 GLOBECOM、ICC、WICON 在内的 10 余个国际会议的 TPC 成员，并担任 SCI 期刊 IEEE Access 的副编辑，SCI 期刊 IEEE Sensors Journal、Sensor 等期刊的专刊责任编辑。任物联网国际标准 IEEE P21451-1-5 标委会主席、中国核设施信息安全专业委员会理事、机械工业出版社“高等教育网络空间安全规划教材”编委会委员。入选中央网信办“网络安全学科建设及教师培养”赴美培训团。

本参赛团队声明所提交的论文是在指导老师指导下进行的研究工作和取得的研究成果。尽本团队所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果。若有不实之处，本人愿意承担一切相关责任。

参赛队员：舒烨　　指导老师：李建华、伍军

2018 年 **9** 月 **14** 日

本参赛团队声明所提交的论文是在指导老师指导下进行的研究工作和取得的研究成果。尽本团队所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果。若有不实之处，本人愿意承担一切相关责任。

参赛队员：舒烨、　　　　指导老师：李建华、任宇

2018 年 9 月 14 日