# A Credible Food Traceability System Based on Domain Name System Security Extensions

https://doi.org/10.3991/ijoe.v14i04.8385

Yi Liu, Sha Liu, Junyu Wang(✉), Kan Qian, Yiwei Shi, Lirong Zheng
Fudan University, Shanghai, China
junyuwang@fudan.edu.cn

Feng Chen
China Food and Drug Administration, Beijing, China

Ning Kong
China Internet Network Information Center, Beijing, China

**Abstract—**Food safety has drawn worldwide attention because of its enormous impact on human health and social stability. Although traceability systems based on Internet of Things (IoT) can improve the visibility of the food supply chain, the trust service is necessary to ensure the data origin and data integrity. This paper proposes a food traceability system supported by a trust service based on Domain Name System Security Extensions(DNSSEC). A DNSSEC-enabled traceability system is implemented for food safety in China. In the traceability system, the master data and event data of the products is stored in distributed databases owned and managed by the enterprises respectively in the supply chain. Enterprise oriented Internet of Things Information Service (iotIS) is an important component of the distributed traceability system. A trust service for the Internet of Things, iotTS, is proposed to guarantee the data integrity. With this service, it can be ensured that the information stored in the enterprise database is original and has never been manipulated. Lightweight public keys are distributed based on the DNSSEC in this solution. Compared with the existing solutions, the proposed solution has better scalability and credibility.

**Keywords—**EPCIS, data integrity check, DNSSEC, IoT, traceability system

## 1 Introduction

Food safety is a worldwide issue and it has garnered concerns from governments and the society because of its adverse effects to public and household health and interests [1]. Although food safety issues have led to fewer fatalities than those caused by other issues, such as cancer or traffic accidents, traditional and social media can enlarge the social hazards caused by food safety issues. Food safety issues affect the happiness of the people, increase the management cost of governments, evoke the distrust of food safety, and jeopardize the development of both the economy and soci-

ety. Thus, food safety issues will cause far more harm to a society than other issues regarding human health. Many countries have implemented systems for food safety supervision and inspection to reduce the quantity, strength, and impact of food safety incidents and to improve the quality of the food that is delivered to end users [2].

In China, some serious food safety incidents have occurred in recent years [3]. The Chinese government has taken strict measures to guarantee food safety and quality in response to these incidents. In 2015, Chinese central government approved a new version of the Food Safety Law, which is the strictest one in its history, however how to implement the law efficiently with the support of information technology is deserved to research. IoT [4, 5] is a promising technology can make product management more flexible and efficient. In recent years, a lot of research has been made on the food safety and electronic tracking and tracing based on the IoT technology [6]. Existing food safety solutions in China lack unified standards in terms of data capturing, data communication, data processing and data application. Furthermore, the existing solutions have drawbacks in terms of their interoperability, scalability, efficiency and data credibility.

This paper proposes and develops an extendable and trustable IoT-based food traceability system for food safety in China. The platform can not only track and trace food products throughout their life cycle but also provide trust service for the stakeholders throughout their supply chain and help them to form a value-added ecosystem. The proposed system adopts a serialized ID, and the management service of the ID is provided by the "IoT Network Identification Service Platform", which is supported by GS1 China and the China Internet Network Information Center (CNNIC). Both data capture and data communication are standardized to accommodate heterogeneous hardware, software and networks. In the IoT architecture for food electronic tracking and tracing system, the iotIS is an expanded information service based on the Electronic Product Code Information System (EPCIS) standard. The iotIS is compatible with GS1 EPCIS (ISO/IEC 19987:2015, ISO/IEC 19988:2015) standard [7], and adopts the distributed deployment. In addition, the iotIS works together with the Internet of Things name service (iotNS) and Internet of Things directory service (iotDS). IotNS performs heterogeneous translation functions in the framework and iotDS uses the directory mode in the architecture to complete the function of locating iotIS, it is basically consistent with the way that is implemented in the GS1 architecture [8].

The master data and event data through the whole life cycle of the product in the food tracking and tracing system is stored separately in the corresponding enterprise-level iotIS. Based on this infrastructure, we have built a prototype system that can provide an open and credible data service for food safety application developers. Compared with existing solutions, the proposed solution combined the tracking and tracing system with the government food inspection system and third-party food testing systems and defined corresponding standard interfaces, which made the system more credible and extendable.

To ensure the reliability of the food product data, we propose an anti-manipulation data service based on TPA (Third Party Auditor) and DNSSEC trust chain. With the proposed method, it can be ensured that the source of the product data is indeed the

claimed enterprise, and the product data has never been manipulated during transmission. Thus, the responsibility of the food safety can be oriented to the producing enterprise.

The remainder of this paper is organized as follows. We briefly review the background of the trust service on information reliability and the related works in Section 2, and in Section 3, a traceability system framework for food safety in China is proposed. Section 4 introduces the architecture of the proposed trust service, including the essential problems and the solutions. Performance testing of the trust service is presented in Section 5. We give a conclusion and introduce the future work in Section 6.

## 2 Related Works

In the food tracking and tracing system based on the IoT technology, the master data and event data of the products are stored in the iotIS database of the enterprise providing the information. When the clients, such as the downstream enterprises in the supply chain, the supervisors and the customers, query the food product information, it is necessary to ensure that the information is original and has never been manipulated.

The information stored in distributed databases of enterprises is vulnerable to external attack and internal manipulation. The manipulation on the information in the databases can be classified into the following cases:

1. The enterprise modifies the information in the iotIS deliberately.
2. The iotIS is attacked by the hackers, and the information in storage is manipulated or deleted maliciously.
3. The iotIS fails because of hardware breakdown, interrupted storage service, or lost information.

The latter two cases can be prevented by adding redundant resources, multiplying backup or enhancing the system security. While for the first case, it is hard to prevent the enterprise from manipulating the information by itself. For instance, assume that there is a quality issue with the material for a batch of food product. While the enterprise manipulates the information about the material in its own iotIS to avoid the product from being called back and reduce the loss. The customers, downstream enterprises and even the supervisors cannot get the original food information, leading to the spread of the food safety trouble. In the cases similar to this instance, the trust service of food information is necessary.

### 2.1 GS1 e-Pedigree

In the year of 2007, GS1 proposed the e-Pedigree of version 1.0[6] to solve the anti-manipulation issue during the transmission of drugs. The upstream and downstream enterprises in the supply chain compare the information protected by the digital signa-

ture in the e-Pedigree with the actual products and receipts to verify if the receipts and the e-Pedigree are reliable.

In the next step, the research on the e-Pedigree and the information reliability converges in the realization, optimization and content extension of them:

In 2007, a distributed e-Pedigree architecture was proposed. The pedigree information is saved in EPCIS and the complete pedigree is obtained by searching step-by-step [7].

In 2011, an e-Pedigree system for agricultural products production and circulation is proposed [11]. The key information of agricultural production and circulation is saved in the e-Pedigree and is signed to ensure the data not being manipulated.

In 2012, Korea Industrial Strategic Technology Development Program conducted a comparison of 6 e-Pedigree deployment plans and decided to use the e-Pedigree in the drug distribution regulation [12-13]. This program extended the pedigree content based on the GS1 e-Pedigree standard including the temperature and humidity parameters that have to be monitored in the cold chain transport, thus providing the reliable data for the drug safety regulation.

However, there are some limits for the e-Pedigree using for iotIS data protection for food safety.

- e-Pedigree can only prove the data stored in it is not modified or counterfeited, but lots of data is stored in the iotIS database and the e-Pedigree can't prove its integrity. The extended functions of the e-Pedigree XML can add more food safety related information that is stored in the iotIS. In reference paper [11], cold chain sensor data of temperature and humidity is added in iotIS. However, this way is different from our original intention because the e-Pedigree will become a huge centralized database and lead to the difficulties of maintaining. We intend to make a distributed deployment and clear the responsibility of the data subject and decentralize access pressure. Compared with the information in the iotIS database, the information in e-Pedigree is limited.
- As to the GS1 e-Pedigree standard, public key distribution must conform to the X.509 standard. This means that every enterprise engaged in the food safety IoT must apply for public key certification to the CA (certification authority). The CA can authenticate the public key when the e-Pedigree is verified and signed. This method is difficult for the small and medium-sized food production and circulation enterprises, and to apply and use the e-Pedigree is also too complicated.

### 2.2 TPA (Third Party Auditor)

TPA is generally used for the data integrity verification in remote or cloud storage [14-15]. The file is separated into blocks, and whether it has been manipulated is verified by PDP (Provable Data Possession) and POR (Provable Data Possession) methods. The research in this region includes reducing the authentication consumption and privacy protection for the users' data.

However, it is not appropriate to treat the iotIS as cloud storage and perform information verification for the iotIS directly with TPA. There are some differences

between iotIS and cloud storage. The PDP and POR methods used for data integrity verification for cloud storage are more suitable for static data with various patterns. Since the data in iotIS is changing with single pattern, it is reasonable to take the method of TPA as a reference, and conduct the data integrity verification with other methods.

### 2.3 DNSSEC

The secured parsing service based on DNS is deployed in the IoT for food safety. The public key distribution based on the DNSSEC is helpful to decrease the complexity of the system deployment and functioning, and can spare the enterprises from applying certifications from the authorized CA.

DNSSEC realizes the trust chain from the root to each domain name. The reliability and undeniability of each record in the DNS can be ensured with the DNSSEC root maintained by CNNIC (China Internet Network Information Center). Distributed by the records in DNSSEC, the public key can be ensured to be non-manipulated. With the digital signature achieved from the trusted third part such as the iotTS, the decrypted data can be ensured to be the original data submitted by the enterprise.

In the state-of-art, there are some works have been done on using the DNSSEC to distribute keys instead of CA. DMAIL uses DNSSEC resolution to do the authentication between MAIL SERVERs [16]. Distributed IKS architecture uses DNSSEC to query service location [17]. DANE protocol provides authentication for TLS transmission [18]. This paper also adopts such architecture to achieve the lightweight public key distribution.

## 3 System Architecture

This paper proposes and develops a system for food safety in China. This system is based on GS1 keys, an Electronic Product Code Information Service (EPCIS), and a name service and has been used in a national pilot project for food safety in China.

The system is constructed with a hierarchy that includes 3 layers (Fig. 1). At the enterprise level, master data, event data, and transaction data about the food are collected through mobile phones, tablets, computers, barcode scanners and radio frequency identification (RFID) readers. The information will be managed in the enterprise unit, as the China Food Safety Law states that the food enterprise should assume the main responsibility for food safety. All the information provided by the enterprise will be digitally signed with a private key for each food enterprise. The data provided by the food enterprise are stored in a network database, which can be accessed by an interface called iotIS.

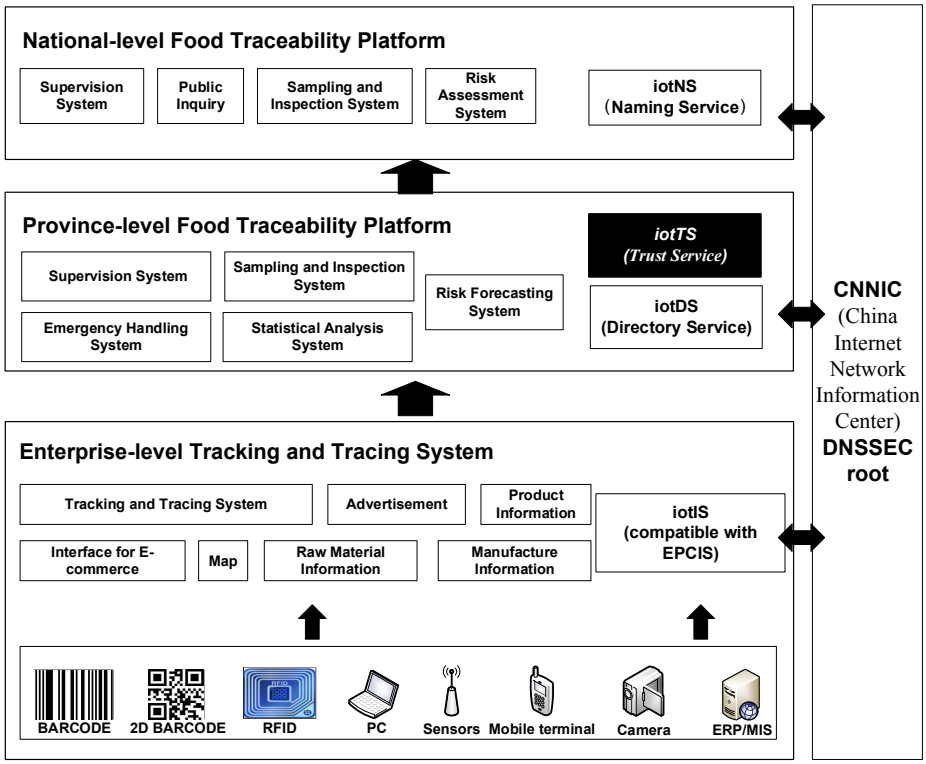


**Fig. 1.** Proposed system hierarchy for food safety in China.

There are several subsystems in the Province-level Platform:

- Province-level Food Safety Supervision System
- Sampling and Inspection System
- Risk Forecasting System
- Emergency Handling System
- Credit Record System
- Statistical Analysis System
- iotDS
- iotTS

According to the China Food Safety Law, the food supervision organization in each province should be responsible for the food safety issues in the province. As a trustable food traceability service, iotTS is be deployed in the provincial platform to protect food traceability data be trustable. Moreover, iotDS is also be deployed in the provincial platform for the characteristics of its third party public service.

There are several subsystems in the National-level Platform:

- National-level Food Safety Supervision System
- Sampling and Inspection System
- Risk Forecasting System
- Statistical Analysis System
- Food Safety Issue Announcement System
- iotNS

In this system, iotIS is a network database for the enterprise-level data, and the service is fully compatible with EPCIS1.1. Additional interfaces are included in the iotIS to meet the requirements of the applications, such as the interface with the China Food and Drug Administration (CFDA) system and the interface for the quality detection system. The name service, iotNS, is provided by the CNNIC. iotDS is deployed to offer the index access of the iotIS Universal Resource Identifier (URI) of each enterprise that the food products go through. The supply chain enterprises deploy their own iotIS and submit an event index automatically to their respective iotDS server. The supply chain enterprises register and maintain their enterprise domain names through the iotNS.

In the proposed architecture of the traceability platform for food safety in China (Fig. 2), the traceability data, environment data, and sampling inspection data are stored in the central database after data filtering and data format normalization. Different service engines will be employed for data processing, including data mining, location-based services (LBS), statistical analysis, decision support, data pushing services, and risk assessment. The platform can support various applications, such as public inquiry, inspection report, risk assessment, early warning, and decision making.

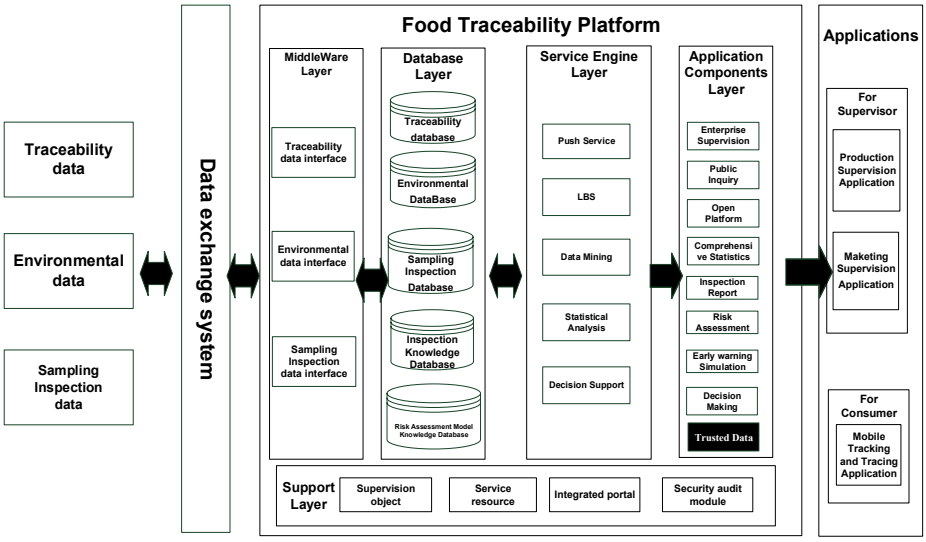


**Fig. 2.** Proposed architecture of the traceability platform for food safety in China.

In this platform, the trusted data system will be presented as an application component to ensure that the food traceability data in the platform is trustworthy. Compared to the existing solutions, this solution combines the tracking and tracing system with the food inspection system and standardizes the interfaces of data capturing, data communication, data processing and data application, which results in better interoperability, scalability, efficiency and data credibility.

## 4 iotTS Information Service

To protect the data in iotIS used for food tracking and tracing system, specific mechanism has to be designed with reference of TPA. In this paper, a methodology of trusted data service, iotTS, is proposed to ensure that the information in the iotIS are non-manipulated and undeniable.

- iotTS is reliable data service provided by a third part. The third part is maintained by government department, supervisor institution or other serving organizations to ensure the fairness, similar with the iotDS which is deployed on the trustable public platform.
- iotTS only stores the digital signatures of the master data and event data in the food tracking and tracing system, thus decreasing the amount of data exchange and effectively protect the data owners' privacy.
- The data of the food products, the digital signatures and the public keys are separately stored in the enterprise database, the iotTS and the domain names protected by the DNSSEC. The data manipulation happened in any parts will be detected by the client during verification.
- The address of the iotTS is maintained and provided by the DNS network. iotTS can be separated.
- The public key is distributed using the DNS of the IoT enterprise with the DNSSEC technology.

The iotTS acts as the trusted third part and provides reliable data service for the important information including the master data and event data stored in it. Through the IoT analytical services running on the DNSSEC, the users can get the address and query the public key of the digital signature and the hash function, thus verifying whether the data from iotIS is manipulated or not.

Figure 3 shows the relationship between iotTS and the other services in IoT.

iotTS provides the following master services:

- Service registration and key generation
- Master data digital signature submission
- Master data digital signature query
- Event data digital signature submission
- Event data digital signature query

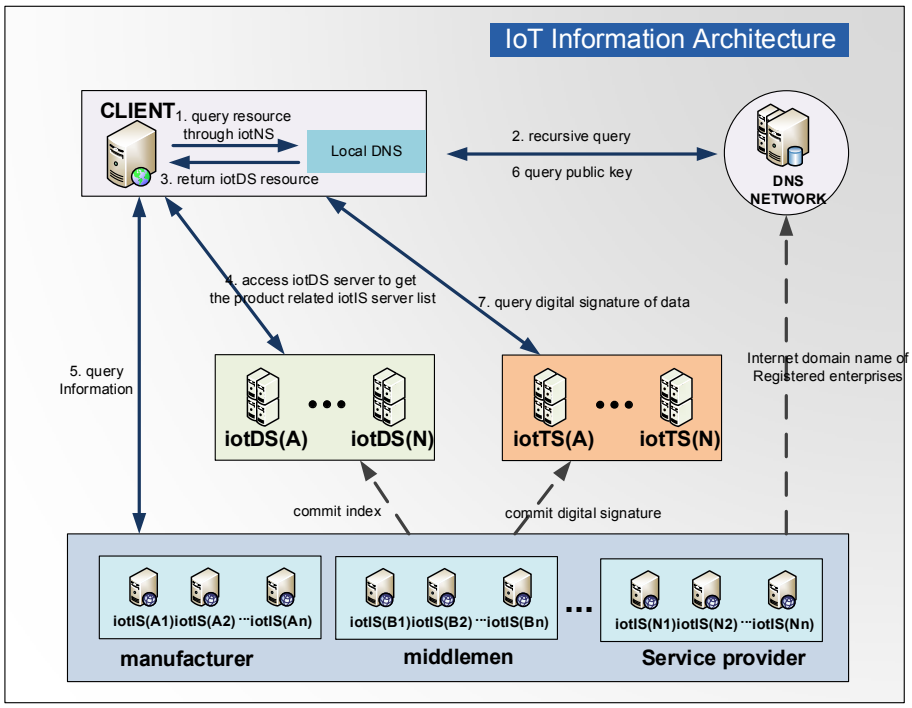


**Fig. 3.** iotTS realized in the IoT architecture.

These are the steps for an enterprise to submit data to the trust service.

- Get an iotTS service registration
- Generate the key pair used in the digital signature and the secret key is used to sign data and the public key is kept in the IoT analytical services protected by DNSSEC.
- Sign the master data using the secret key and submit the digital signature and the secret key number to the iotTS.
- Sign the event data using the secret key and submit the digital signature and the secret key number to the iotTS.

These are the steps for the client to query and verify.

- Obtain all the information of the food throughout its life time via the DNSSEC and iotIS.
- Query the digital signature and key series number of the master data via iotTS
- Query the digital signature and key series number of the event data via iotTS
- Acquire the public key of each digital signature via the DNSSEC.
- Verify if the master data and the event data have been manipulated by decrypting the signature with the corresponding key.

### 4.1 Service Registration and Key Generation

The enterprise user gets a legal domain name via CNNIC. The domain name is called the enterprise domain name in IoT and represents the enterprise. The iotTS service is activated and configured for this domain name. After that the NAPTR record of the enterprise domain name in IoT will contain the enterprise's URL of its iotTS as shown in Table 1.

**Table 1.** NAPTR Records Containing the URL of iotTS

| Order | Pref | Flags | Service | Regexp | Replacement |
|---|---|---|---|---|---|
| 0 | 0 | U | iotTS | !^.*$!http://iotTS service URL! | . |

For instance, the enterprise domain name in IoT of company1 is company1.cniotroot.cn. And the DNS NAPTR of this domain name will contain the URL of the enterprise's iotTS, for example http://company1.iot-ts.cn:6130/service, in the Regexp column as shown in Table 1.

Before using the iotTS service, the enterprise needs to generate the private RSA key for digital signature, and then adds a sub domain name, for example key_name.key.company1.cniotroot.cn, to be used as the public key domain name. The TXT in the public key domain keeps the public key. The enterprise may generate different RSA keys pairs for different products or batches and stores the public keys in the sub domain name. For example, the enterprise company1 generates a pair of RSA keys for one batch of food products and registers the public key domain name as batch1.key.company1.cniotroot.cn. The public key can be stored in the TXT record of the sub domain name. After then, the querying clients can achieve the public key of batch1 in the TXT record in the domain batch1.key.company1.cniotroot.cn.

### 4.2 Digital Signature and Submission for Master Data

The regMasterData method is used by the enterprise to submit the master data signature to its iotTS for storing. The signature of master data is generated with an RSA private key of the enterprise. The items that submitted to the iotTS include the digital signature, the URI of the master data and the public key domain name.

For instance, 001.item.company1.cniotroot.cn is the URI of a product's master data. The master data, including the product name, materials list, quality guarantee period, number of producing standard, quality level and number of the food producing license, are stored in the URI. The enterprise converts the master data to JSON string, then generates digital signature with the private key named item1.

Then the regMasterData method of iotTS is invoked with three arguments. The argument masterID denotes the URI of the master data domain name, thus urn:cniotroot:id:item:001.item.company1.cniotroot.cn. The argument signature denotes the digital signature. The argument keyID denotes the public key domain name, e.g. item1.key.company1.cniotroot.cn.

### 4.3 Query and Verification for Master Data

When the client queries the digital signature of the master data, he should firstly query the NAPTR record to acquire the URL of the iotTS. Then the client invokes the query Master Signature method passing the URI expression as an argument to acquire the digital signature and the public key domain name of the master data. The client queries the TXT record in the public key domain name and acquires the public key correspond to the digital signature.

When the client verifies the master data, the public key is used to decrypt the digital signature and acquire the hash value of the master data. Then the client conducts JSON conversion on the data acquired directly from iotIS and gets the hash value. If the two hash values are identical, it is proved that the master data has never been manipulated.

### 4.4 Digital Signature and Submission for Event Data

RegEvInfo port is used by the enterprise to summit the event data of products to the iotTS. The event data are stored in the iotTSs allocated for the enterprises of different phases. When the food products are in producing phase, the event data are stored in the iotTS of the manufacture enterprise. When the food products are in transmission phase, the event data are stored in the iotTS of the middlemen.

The enterprise makes a signature for the event data after JSON conversion, and submits the signature to the iotTS through the RegEvInfo port. The event data include the event information required by the EPCIS standard and the food safety related information extended by iotIS. After submission, any manipulation on the event data will trigger the food safety alarm.

### 4.5 Query and Verification for Event Data

QueryEvInfo port is used to query digital signature and public key domain name of specific event.

The client firstly acquires the URL of the food product's iotDS via the NAPTR record in the client's iotNS denoted by the DNS. Then the client acquires URLs of the iotISs of all of the phases, and acquires the URL of the iotTS via the NAPTR record in its iotNS.

After that, the client gets the completed event data throughout the whole lift time of the products including the events' IDs by querying the iotISs of each phase.

The client accesses the iotTSs of each phase, passes the events' IDs as argument and gets all of the digital signatures and public key domain names of the events.

By querying the TXT records of the public key domain names, the client can get all of the public keys.

When verifying the event data, the public keys are used to decrypt the digital signatures and get the hash values of all the events. Then conduct JSON conversion on the event data acquired from the iotISs and get all the hash values. After comparing the two groups of hash values one by one, if every pair of them are identical, the event

data are proved not have been manipulated, otherwise there is potential safety issue for the food product.

# 5 Performance Evaluation

After introducing iotTS, the procedures of data submitting and querying are changed. In the phase of data submitting, after capturing the user's data, the iotTS needs to conduct JSON conversion and digital signing on the data; then it submits the ID of the data, the digital signature and the key's name through the port of iotTS. In the phase of querying, two extra DNS accesses are need for the user to obtain the address of iotTS and the public key for decrypting the digital signature. The user needs to access the iotTS to obtain the digital signature as well.

With the growing processing capability of the CPU, the influence of JSON conversion and digital signing performed locally on the performance can be neglected. However, the remote access to DNS service and iotTS will influence the procedures of data submission and query.

In this way, the performance testing includes the following three procedures:

- DNS performance test is done by measuring the time consumption for the client to obtain the public key from the DNS TXT.
- iotTS submit interface performance, to measure the extra time consumption for the iotIS to submit master data or event data.
- iotTS query interface performance, to measure the extra time consumption for the client to query the data.

The test server configuration is 4 CPUs, 4G memory, WEB server is based on IIS7, the database is MYSQL5.5. Test client including QUERYPERF and LOADRUNNER 11.

## 5.1 DNS Performance Test

We add a TXT containing the public key to the DNS. Conduct 120,000 times access to the TXT using the BIND QUERYPERF. The test result is listed in Table 2.

**Table 2.** DNS TXT Access Performance Test

| Item | Result |
|---|---|
| Access times | 119,976 times |
| Test Time | 44.5s |
| Query speed | 2,696times/s |

### 5.2 iotTS Submit Interface Performance

The concurrent test of the submit interface is to gradually increase the number of concurrent, by recording the response time, and then analyze the concurrency performance. The test results for the iotTS submit interface are shown in Figure 4:

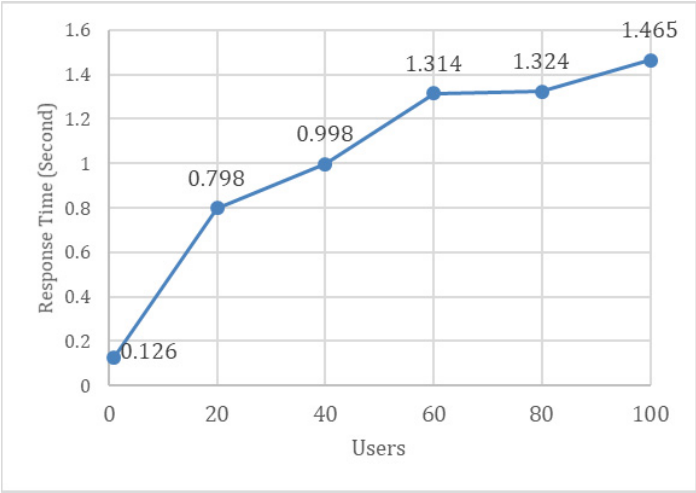


**Fig. 4.** iotTS Submit Interface Performance.

### 5.3 iotTS Query Interface Performance

As well as the methods used in the submit test, we also perform concurrent testing of the query interface. The test results for the iotTS query interface are shown in Figure 5:

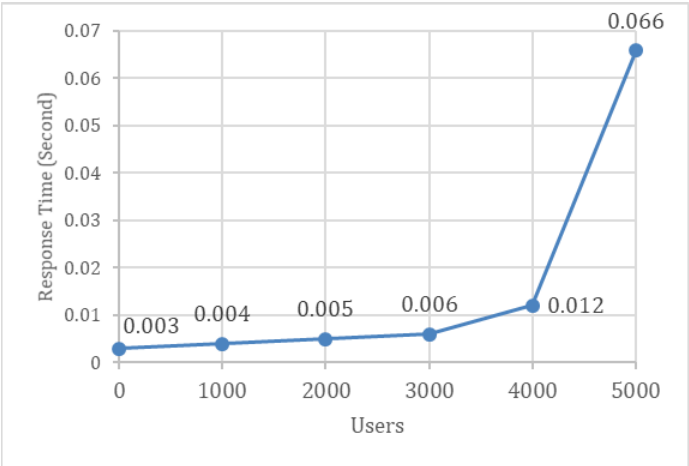


**Fig. 5.** iotTS Query Interface Performance.

### 5.4 Result Analysis

When the number of concurrent data submitted to iotTS is no more than 40 users, the response speed can be obtained within 1 second; when the user is 100, the response speed is less than 1.5 seconds. For the event submission, the delay is acceptable, but for a large number of data submissions waiting time significantly longer, which is to be further improved in the future work.

When the number of concurrent requests is less than 3,000, the response time of iotTS is below 0.006s, and when the user exceeds 3,000, the response performance began decline. If the traceable goods with 5 event including production, inspection, shipping, receiving and retail, when use iotTS in 3,000 concurrent users, the query time increment evaluation is as follows: 0.006 x 5 (with event data) +0.006 (with master data) +0.0064x2 (DNS) =0.0488 seconds, it's almost imperceptible.

## 6 Conclusions

In this paper, a credible food traceability system based on DESSEC is proposed. The proposed iotTS technique provides integrity protection for important information in iotIS. With the public key distribution service based on DNSSEC, certification for the middle and small-sized enterprises with affordable cost is provided.

At the same time, a system architecture for food safety validation is also proposed. The proposed system architecture follows the new Chinese Food Safety Law. It has good scalability and credibility, as it supports interactions with the authorized food safety testing organization. The proposed solution combines the tracking and tracing system with the government food inspection system or a third-party food testing system, and defines standard interfaces, which make the system more credible and extendable.

In the future work, digital signature and verification are to be integrated into iotTS, and the complexity of data submitting and querying will be further reduced.

## 7 Acknowledgment

This work was supported by the National Science & Technology Pillar Program of China (2015BAK36B01), the National Natural Science Foundation of China (61402436).

## 8 References

[1] Y. Gu , W. Han , L. Zheng , B. Jin , Using iot technologies to resolve the food safety problem - an analysis based on chinese food standards, in: Proceedings of WISM, 2012, pp. 380–392.

[2] B. Antunovic, A. Mancuso, K. Capak, V. Poljak, and T. Florijančić, "Background to the preparation of the Croatian food safety strategy," Food Control, vol. 19, no. 11, pp. 1017–1022, Nov. 2008. https://doi.org/10.1016/j.foodcont.2007.10.012

[3] L. He, and Z. Wang, et al. "The method of food safety sampling inspection based on dynamic weight," Math. Modeling Its Appl., vol. 2, no. 3–4, pp. 4–12, 2013.

[4] L. Atzoria, A. Ierab, and G. Morabitoc, "The Internet of Things: A survey," Computer Networks, vol. 54, pp. 2787–2805, 2010. https://doi.org/10.1016/j.comnet.2010.05.010
[5] L. D. Xu, W. He, and S. Li, "Internet of Things in indus- tries: A survey," IEEE Trans. on Industrial Electronics, 2014. https://doi.org/10.1109/TII.2014.2300753
[6] Y. Liu, W. Han, Y. Zhang, L. Li, J. Wang, and L. Zheng, "An Internet-of-Things Solution for Food Safety and Quality Control: A Pilot Project in China," Journal of Industrial Information Integration, vol. 3, pp. 1-7, 2016. https://doi.org/10.1016/j.jii.2016.06.001
[7] EPC Information Services (EPCIS) Version 1.1 Specification, http://www.gs1.org/sites/default/files/docs/epc/epcis_1_1-standard-20140520.pdf.
[8] The GS1 EPCglobal Architecture Framework GS1 Version 1.7, http://www.gs1.org/sites/default/files/docs/architecture/EPC_architecture_1_7-framework-May-2015.pdf.
[9] Pedigree Ratified Standard 3 Version 1.0 as of January 5th, 2007, http://www.gs1.org/sites/default/files/docs/epc/pedigree_1_0-standard-20070105.pdf.
[10] A Distributed ePedigree Architecture, Proceedings of the 11th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'07).
[11] W. Han, Y. Gu, and W. Wang. The design of an electronic pedigree system for food safety. Information Systems Frontiers, 17(2):1-13. 2015. https://doi.org/10.1007/s10796-012-9372-y
[12] Kwang NamGung, Yongjung Choi, Seongjin Park, and Chulwoo Jun, The Development of e-Pedigree Model for Securing Transparent Pharmaceutical Distribution Channel in Korea, G. Lee et al. (Eds.): ICHIT 2012, CCIS 310, pp. 226–234, 2012.
[13] H.S. Kim,H.J. Jeong and H.S. Park, A Study on RFIDIUSN based e-pedigree System for Cold Chain Management, 2012 IEEE International Technology Management Conference, Dallas, TX USA, June 25-27,2012.
[14] Y. Yu et al., "Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767-778, 2017. https://doi.org/10.1109/TIFS.2016.2615853
[15] A. Le, A. Markopoulou and A. G. Dimakis, "Auditing for Distributed Storage Systems," in IEEE/ACM Transactions on Networking, vol. 24, no. 4, pp. 2182-2195, 2016.
[16] Dmail: A Globally Authenticated Email Service, COMPUTER Published by the IEEE Computer Society 2014.
[17] Layering Public Key Distribution Over Secure DNS using Authenticated Delegation, Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005).
[18] The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC6698.

## 9 Authors

**Yi Liu, Sha Liu, Junyu Wang, Kan Qian, Yiwei Shi and Lirong Zheng** are with the State Key Laboratory of ASIC & System (Fudan University), Shanghai Engineering Research Center of Product Traceability, Fudan University, 200433, Shanghai, China

**Feng Chen** is the Professor and Deputy Director General of Information Center for China State Food & Drug Administration, 100053, Beijing, China.

**Ning Kong** is the researcher of China Internet Network Information Center, 100190, Beijing, China.

Article submitted 07 February 2018. Resubmitted 23 February 2018. Final acceptance 31 March 2018. Final version published as submitted by the authors.