Chang *EURASIP Journal on Wireless Communications and Networking* (2016) 2016:174
DOI 10.1186/s13638-016-0675-4

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

An integrated testing system for IPv6 and DNSSEC

Hung-Chang Chang

Abstract

IPv6 protocol, which should replace the actual IPv4 protocol, brings many new possibilities and improvements considering simplicity, routing speed, quality of service, and security. In comparison to IPv4, IPv6 improves mechanisms for assuring a secure and confidential transfer of information. DNS has been extended to provide security services (Domain Name System Security Extensions (DNSSEC)) mainly through public key cryptography. We propose a new approach to DNSSEC that may result in a significantly more efficient protocol. We introduce a new strategy to build chains of trust from root servers to authoritative servers. The techniques we employ are based on symmetric-key cryptography. With the depletion of IPv4 address and rampant information security threat, IPv6 and DNSSEC are widely deployed in recent years, but there is no platform that can integrate all relevant detection information and technical information and provide advice for officers concerned in Taiwan. This paper implements an Auxiliary Deployment System for IPv6 and DNSSEC and presents the results of preliminary testing and statistics which can help technology and promoting staff to do evaluation, promotion, and debugging on IPv6 and DNSSEC deployment easily.

Keywords: IPv6, DNSSEC, Security testing

1 Introduction

The Internet protocol (IP) address is the necessary network protocols for each individual computer to access the Internet. Before 2013, almost all computers are connected to the Internet via Internet Protocol Version 4 (IPv4) addresses, but unfortunately, with the growth of the Internet population, the use of IPv4 addresses has become less and less. In other words, IP is facing the problem of depletion. Actually, IPv4 address exhaustion has been anticipated since the late 1980s, and as unexpectedly, the top-level exhaustion occurred on January 31, 2011 [1–3] and the RIR (Regional Internet Registries) and the APNIC's (Asia-Pacific Network Information Centre) exhaustion on April 15, 2011, and some parts of the world have already exhausted their IPv4 allocations [4–6], and the remaining RIRs are expected to deplete their pools within a few years [5]. To deal with the long-anticipated problem of IPv4 address exhaustion, Internet Protocol Version 6 (IPv6) was developed by the Internet Engineering Task Force (IETF) in 1996 that started with RFC 1883.

Correspondence: alex@ms.szmc.edu.tw
Department of Information Management, Shu-Zen Junior College of Medicine and Management, Kaohsiung, Taiwan

Table 1 shows the population of the world over the years with regular Internet penetration. Whether we can find in Asia, Europe, or elsewhere, Internet use is increasing. In Asia, the Internet population between 2000 and 2012 had increased by 841.9 %. Additionally, the latest data of Internet population is 167,335,676 which accounts for less than one fifth of the total population in Africa. It is worth noting that during these years, Africa has grown 3606.7 % (Table 1).

Figure 1 shows the Internet population in Taiwan between December 2006 and December 2012. Even though the growth of Internet population has slowed down, but for IT-big countries, like Taiwan, it has high speed and stable network environment which are necessary things (Fig. 1).

Internet population increased rapidly in all regions, but IP which can be directly connected to the Internet is limited. Thus, it is particularly important to promote IPv6. On June 8, 2011, top websites and Internet service providers around the world, including Google, Facebook, Yahoo!, Akamai, and Limelight Networks joined together with more than 1000 other participating websites in World IPv6 Day for a successful global-scale trial of the new Internet Protocol, IPv6 [7]. On June 6, 2012, the

Springer Open

© 2016 Chang. **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Table 1 World Internet usage and population statistics

World Internet usage and population statistics						
June 30, 2012						
World regions	Population (2012 est.)	Internet users Dec. 31, 2000	Internet users latest data	Penetration (% population)	Growth 2000–2012 (%)	Users % of table (%)
Africa	1,073,380,925	4,514,400	167,335,676	15.6	3,606.7	7.0
Asia	3,922,066,987	114,304,000	1,076,681,059	27.5	841.9	44.8
Europe	820,918,446	105,096,093	518,512,109	63.2	393.4	21.5
Middle East	223,608,203	3,284,800	90,000,455	40.2	2,639.9	3.7
North America	348,280,154	108,096,800	273,785,413	78.6	153.3	11.4
Latin America/Caribbean	593,688,638	18,068,919	254,915,745	42.9	1,310.8	10.6
Oceania/Australia	35,903,569	7,620,480	24,287,919	67.6	218.7	1.0
World total	7,017,846,922	360,985,492	2,405,518,376	34.3	566.4	100.0

Reference: Internet World Stats from http://www.internetworldstats.com/stats.htm

Internet Society carried out a World IPv6 Launch day to bring permanent IPv6 deployment for the products and services of the participants [8]. Following the success of the 2011 test day and 2012 launch day, there are more and more government agencies and business organizations to complete the deployment of IPv6.

IPv6 and Domain Name System Security Extensions (DNSSEC) are the next generation of Internet infrastructure. For a more stable and secure network environment, countries around the world are actively promoting the deployment. In view of this, this paper proposes and implements an Auxiliary Deployment System for IPv6 and DNSSEC to help technology and the promoting staff to do evaluation, promotion, and debugging on IPv6 and DNSSEC deployment easily in Taiwan.

The rest of the paper is organized as follows: First, some knowledge and existing tools are introduced in Section 2. Second, the design of Auxiliary Deployment System and its expected results are described in Section 3. Then the implementing process of our system and its demo are given in Section 4. Finally, our conclusion is drawn in Section 5.

2 Background

2.1 IPv6

IPv6 is the latest version of IP, and it is also called Internet Protocol next generation (IPng). IPv6 is intended to replace IPv4 which was developed by the IETF to solve the increasingly serious problem of IPv4 address exhaustion. In Section 2, we introduce the deployment status of Taiwan and around the world.

2.1.1 Status of IPv6 deployment

Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization that coordinates the Internet's global domain name system. The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for managing the Domain Name System (DNS) Root and the numbering system for IP addresses. In February 2011, ICANN assigns IPv4 addresses of the last five groups to five RIRs, including the following: African Network Information Center (AFRINIC), American Registry for Internet Numbers (ARIN), Asia-Pacific Network Information Centre (APNIC), Latin America and Caribbean Network Information Centre

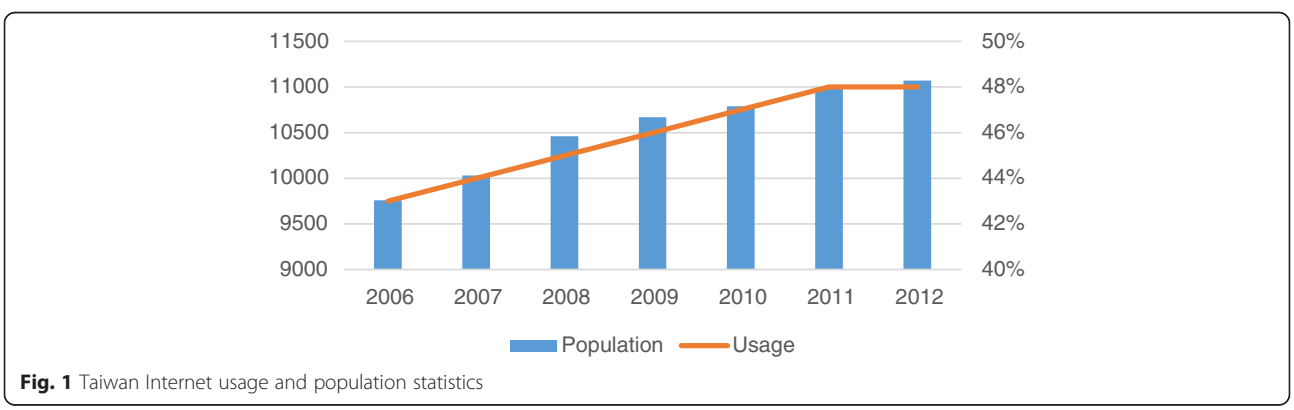

Fig. 1 Taiwan Internet usage and population statistics

(LACNIC), and Réseaux IP Européens Network Coordination Centre (RIPE NCC). At the same time, ICANN declared that the IPv4 address has been exhausted. Figure 2 presents the status of IPv4 allocation over the years.

Figure 2 shows the status of IPv6-enabled users worldwide as measured by Google. We can see that the number of people using IPv6 significantly increased in recent years.

2.2 DNSSEC

The Domain Name System Security Extensions (DNSSEC) has been proposed to deal with the lack of data integrity and validation of data sources by IETF. In Section 2.2.1, how DNSSEC works is introduced, and related research on DNSSEC is summarized in Section 2.2.2. At last, Section 2.2.3 describes the deployment status of Taiwan and around the world.

2.2.1 What is DNSSEC?

DNSSEC is an improved version of DNS-based protocol. DNS' original design did not consider the security issues; the main purpose is to provide convenience for network users to convert domain names to IP addresses. Figure 3 shows the DNS query process.

Due to IP addresses (especially in IPv6) not easily remembered, the DNS has been developed. But DNS provides only the basic mapping services for domain names and IP addresses; hackers can easily tamper with the DNS data or cause the DNS server not to work properly.

According to the research of the past few years, the following problems of DNS were discovered:

Buffer overflow attack is a network attack for DNS software vulnerabilities, not protocol, such as ISC BIND and Windows DNS Server, sometimes also called "flooding attack." Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) are common network attacks; it does not cause data corruption, but users could not properly use the services. Figure 4 shows the architecture of a DDoS attack.

Below we will introduce to the working principle of DNSSEC. While DNSSEC will increase the burden on the server that leads to amplify the effect of these attacks, DNSSEC can avoid its server, becoming an attack tool for hackers. The term "pharming" is a neologism based on the words "farming" and "phishing." Sometimes also called "cache poisoning," it causes the name server to return an incorrect IP address, diverting traffic to another computer (often the attacker's). Figure 5 shows the architecture of a pharming attack.

DNSSEC does not modify the existing mode of operation of DNS, scilicet, DNSSEC does not change the existing DNS query and response processing, but through an extension of the method to achieve the security of DNS. On the basis of the traditional DNS, IETF added some resource records and two header flags into DNS. Below we will explain the newly added records [7–11]:

- DNSKEY
  DNSSEC public key, defined in RFC 4034.
  DNSSEC resource records contain the public key for the zone. They come in two flavors, a zone signing key (ZSK) and a key signing key (KSK). Generally,

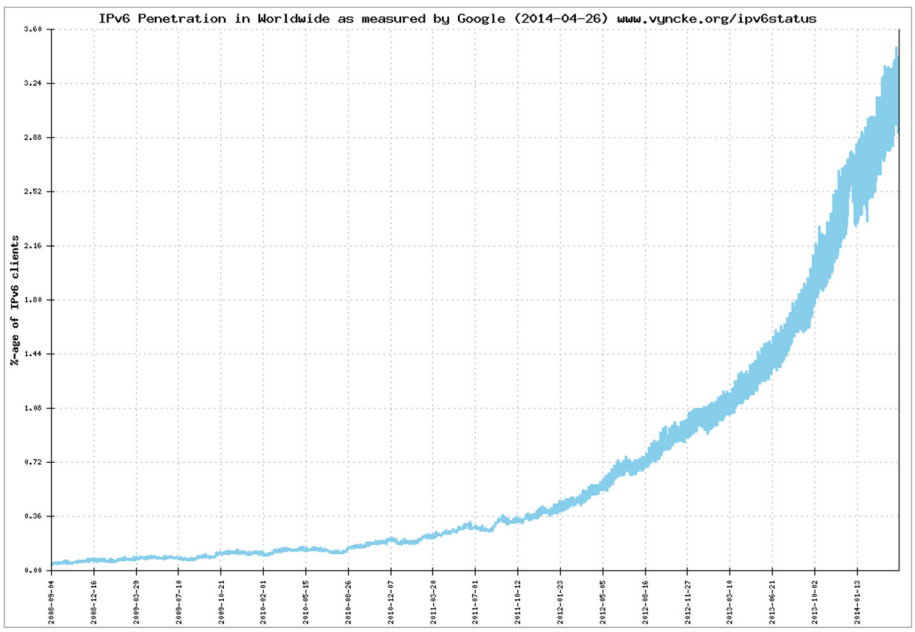

Fig. 2 IPv6-enabled users. Source: https://www.vyncke.org/ipv6status/

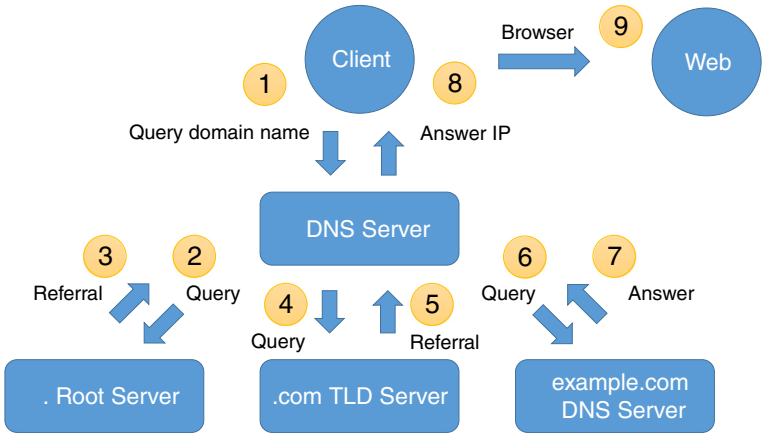

Fig. 3 DNS query process

the KSK signs only certain records within the zone, while the ZSK signs all of the records. You may have as many of each as required for key-rollover protocols or for your needs.

- DS
  Delegation signer, defined in RFC 4034.
  A DS resource records stored key tag, algorithm number, and DNSKEY RR's digest, used in the DNSKEY certification process. DS resource records and its corresponding DNSKEY resource records have the same owner name, but they are stored in different places. DS resource records appear only in the parent zone, such as "example.com." DS resource records are then stored in the "com" zone, and its corresponding DNSKEY resource records are to be stored in the "example.com" zone.
- DLV
  DNSSEC look-aside validation, defined in RFC 4431. The DLV resource record has exactly the same wire and presentation formats as the DS resource record. DLV record does not inherit any of the special processing or handling requirements of the DS record type. Unlike the DS record, the DLV record may not appear on the parent's side of a zone cut. A DLV record may, however, appear at the apex of a zone. For example, a DS record has your zone's name (example.com) while a DLV record has an additional name (example.com.dlv.isc.org.).
- NSEC
  Next secure, defined in RFC 4034.
  NSEC resource records links to the next record name in the zone and lists the record types that exist for the record's name. These records can be used by resolvers to verify the non-existence of a record name and type as part of DNSSEC validation.
- NSEC3
  Next secure ver.3, defined in RFC 5155.
  Like NSEC, NSEC3 resource records can also be used by resolvers to verify the non-existence of a record name and type as part of DNSSEC validation.

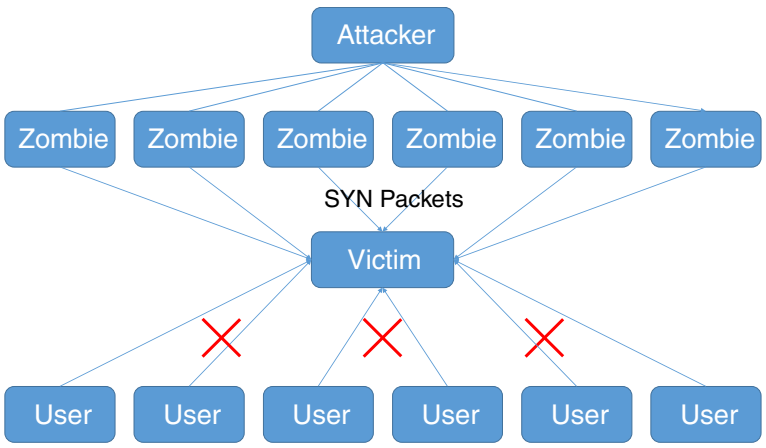

Fig. 4 Architecture of a DDoS attack

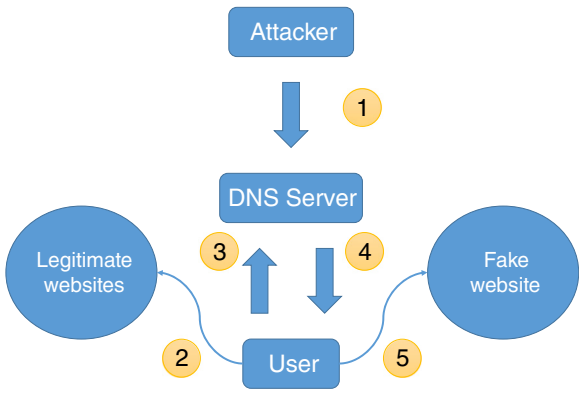

Fig. 5 Architecture of a pharming attack

The NSEC3 resource record links to the next record name in the zone and lists the record types that exist for the name covered by the hash value in the first label of the NSEC3 resource records' own name. NSEC3 resource records have the same functionality as NSEC, except NSEC3 resource records use cryptographically hashed record names to prevent enumeration of the record names in a zone.

- RRSIG
  Resource record signature, defined in RFC 4034. RRSIG holds the digital signature of DNSSEC; resolvers can use public key in DNSKEY resource records to verify it.

DNSSEC works by the use of cryptographic digital signatures which are included in secured zones as resource records. When the client receives a response message, they can determine whether the response message is secured by DNSKEY which is authenticated via a chain of trust. Figure 6 shows the DNSSEC query process.

Simply, DNSSEC is fully compatible with the traditional DNS. And DNSSEC is a set of extensions to DNS which through the mechanism of digital signatures provides the following security guarantees, but not availability or confidentiality.

For data integrity, each DNS zone using DNSSEC requires a pair of keys, namely, "public key and private key," which are generated by the DNS administrator; the private key is kept secret by the administrator, and the public key is published in the zone file used to define DNSKEY resource records. When the data has been modified, the chain of trust would be broken. Through the layers of verification from the end node to the root zone, we believe that the DNS data are correct. Because root zone was managed by hand, it should not be easily hacked theoretically. DNSSEC allows a resolver to validate that a certain domain name does not exist. When returning a negative DNSSEC response, the DNS server usually includes up to two NSEC records or three NSEC3 records. With these record and hashed data of the DNS record, we can know whether it is true that a URL does not exist.

2.2.2 Related research

DNSSEC in the future is an important network infrastructure. In addition to IETF, in many countries some scholars have conducted research and discussion on this.

On May 3 2007, Mark Santcroos and Olaf M. Kolkman published the "DNS Threat Analysis"; they mentioned that although it has the above advantages, DNSSEC does not solve any of the problems that have to do with transport; in fact, since packets are bigger, they consume more resources in the servers and on the wire and impose rules on firewalls. That may provide new vectors for (D)DOS attacks [12]. Moreover, the key management system is also more complex.

In 2005, Wei-An Chen published "The Easy Security Protection and Validation System for DNS Server using DNSSEC" [13], and Shiau-Han Jang published "The Study of Apply DNSSEC to building a Protection Mechanism

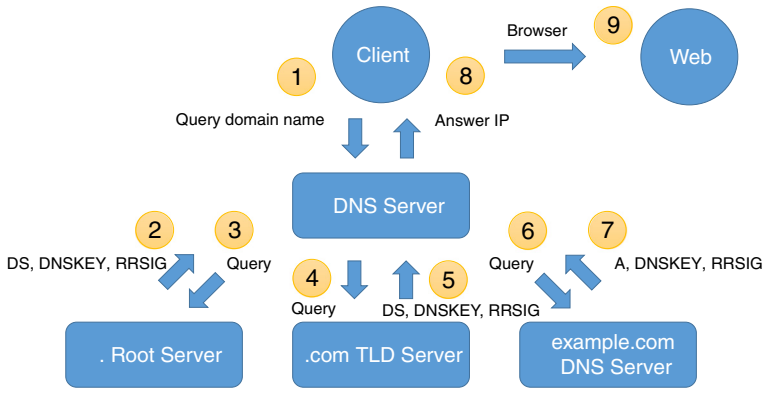

Fig. 6 DNSSEC query process

Table 2 DNSSEC deployment status of TLDs

Domain	Total	Number of support	Percent
Root domains	12	13	100
gTLDs	26	9	35
ccTLDs	253	87	34.39

for DNS Pharming" [14] in 2007. Both discuss and implement DNSSEC system applications.

In 2010, Mantoro, T.; Norhanipah, S.A.; and Bidin, A.F., published "An implementation on Domain Name System security extensions framework for the support of IPv6 environment" [15]. In 2011, papers relating to "against local DNSSEC attacks" [16], "update scheme" [17], "OpenID service" [18], and "mobile peers in HIP networks" [19] have been published in succession. Lin Tao, Liu Wu, Duan Haixin, and Sun Donghong also published "IPv6 Traffic Hijack Test System and Defense Tools Using DNSSEC" [20].

In 2013, Migault, D.; Senecal, S.; Francfort, S.; Herbert, E.; and Laurent, M., proposed "PREFETCHing to Overcome DNSSEC Performance Issue on Large Resolving Platform" to improve DNSSEC performance issues [21].

These studies mentioned above make us more confident that DNSSEC will improve our future network environment, so we should actively promote DNSSEC implementation. Actually, several ISPs have started to deploy DNSSEC-validating DNS recursive resolvers. On May 6, 2013, Google Public DNS has enabled the DNSSEC validation by default.

2.2.3 Status of DNSSEC deployment

In order to solve the traditional DNS problems in security, since 2009, many countries have embarked on the top domain DNSSEC-related experiments, and after more than 1 year of experimental test, in 2011, official succession of import operations of DNSSEC appeared.

According to a survey commissioned by TWNIC commissioned research team in 2013, 13 servers in the root domain have fully supported DNSSEC. In the generic TLDs, i.e., ".com," ".net," and ".org," there are nine domains that support DNSSEC. In country code top-level domains (ccTLDs), there are 87 domains that support DNSSEC, and 4 domains can partially support DNSSEC that accounted for 34.39 % of all 253 still in use in the domain. Table 2 lists the DNSSEC deployment status of TLDs.

Figure 7 shows the DNSSEC deployment status around the world. Figure 8 shows the penetration of DNSSEC on all continents.

2.3 Existing detection platform

Next, we will introduce current testing tools for IPv6 and DNSSEC. For IPv6, there are many tools used to detect IPv6.

Since 2001, CHT-TL IPv6 Testing Lab has provided a test service which was named "IPv6 Ready Logo Program" at present.

While the IPv6 Ready Logo Program provides the detailed examination above, it is not free, and neither is the immediate service. More importantly, the IPv6

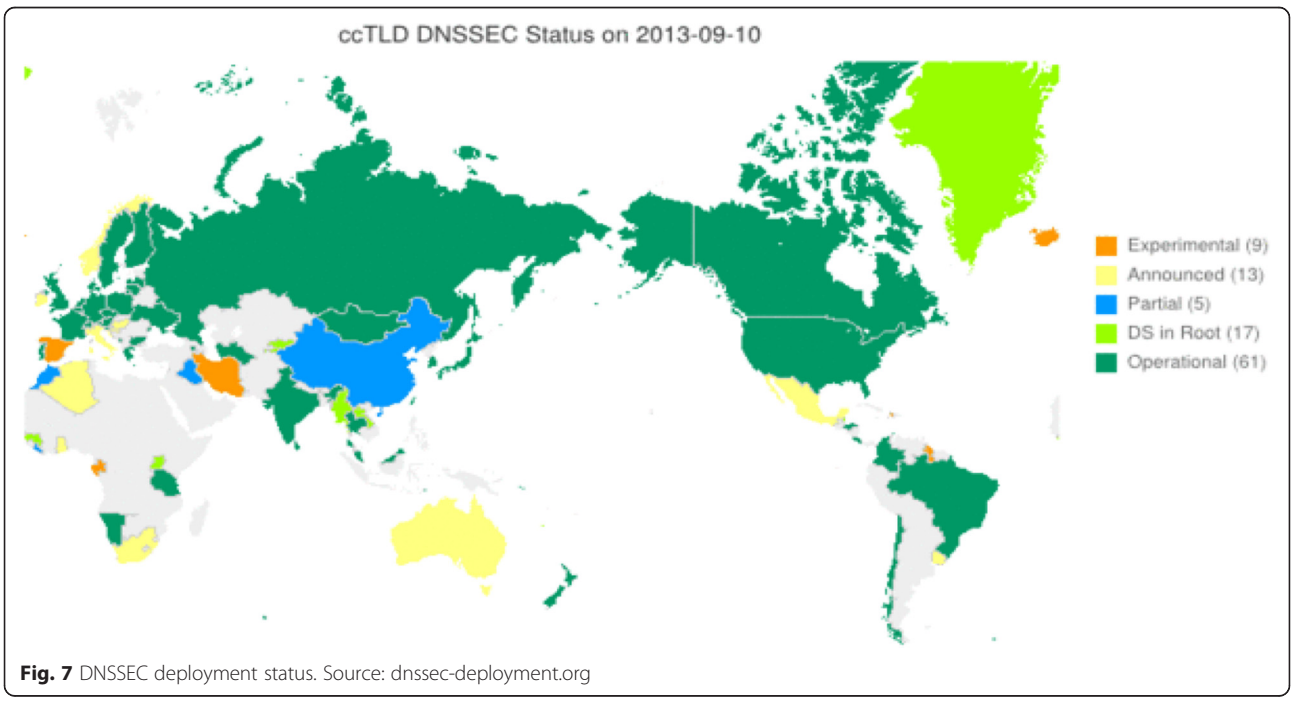

Fig. 7 DNSSEC deployment status. Source: dnssec-deployment.org

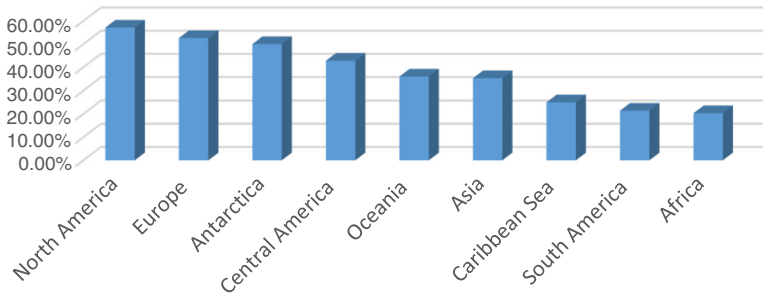

Fig. 8 Penetration of DNSSEC on all continents

Ready Logo Program does not provide the function of statistics and records.

Hexillion also proposed the "CentralOps.net" which is a collection of Internet utilities to test IP and DNS information. Table 3 lists the functions which were provided by CentralOps.net.

CentralOps.net is free for everybody. It does not require login; simply pick a tool on the menu and use it. In addition to these real-time services, CentralOps.net also provides paid services on extended or automated use of its tools. CentralOps.net provides a variety of testing services that has the advantage of instant and free, but also does not provide the functionality of statistics and records.

For DNSSEC, VeriSign launched DNSSEC Debugger which is a web-based tool for ensuring that the "chain of trust" is intact for a particular DNSSEC-enabled domain name since 2011; they provide detailed information for DNSSEC in plain text with a few icons. DNSSEC Debugger has the advantage of instant and free, but it does not provide the functionality of statistics and records. Figure 9 shows the analytical results of National Yunlin University of Science and Technology by DNSSEC Debugger.

3 System design

3.1 Observed objects

To promote IPv6 and DNSSEC in Taiwan, we designed the Auxiliary Deployment System for IPv6 and DNSSEC. Below we will discuss the target objects of the system services.

IPv6 and DNSSEC are the network infrastructure in the future. Because the benefits of IPv6 and DNSSEC for an average user are relatively non-sense, we expect the government to play the role of a leader. In fact, as mentioned in Section 2, the deployment system which TWNIC launched for IPv6 is also designed for each local government. Academic network has been used by many people, including teachers, students, and staff. And each school usually has a variety of server services, such as DNS service, email servers, web servers, FTP servers. Therefore, we believe it is necessary to be promoted on educational institutions. In this paper, educational institutions are classified to state schools and private schools. We can take to explore the future development of both.

To supervise operation of organizations, property, purpose, etc., the nature of the foundation is between the government and the general business, so in addition to the government and schools, this paper also observed

Table 3 The functions on CentralOps.net

Function name	Caption
Domain Dossier	Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.
Domain Check	See if a domain is available for registration.
Email Dossier	Validate and troubleshoot email addresses.
Browser Mirror	See what your browser reveals about you.
Ping	See if a host is reachable.
Traceroute	Trace the network path from this server to another.
NsLookup	Look up various domain resource records with this version of the classic NsLookup utility.
AutoWhois	Get Whois records automatically for domains worldwide.
TcpQuery	Grab a web page, look up a domain, and more.
AnalyzePath	Do a simple, graphical traceroute.

Source: http://centralops.net/co/

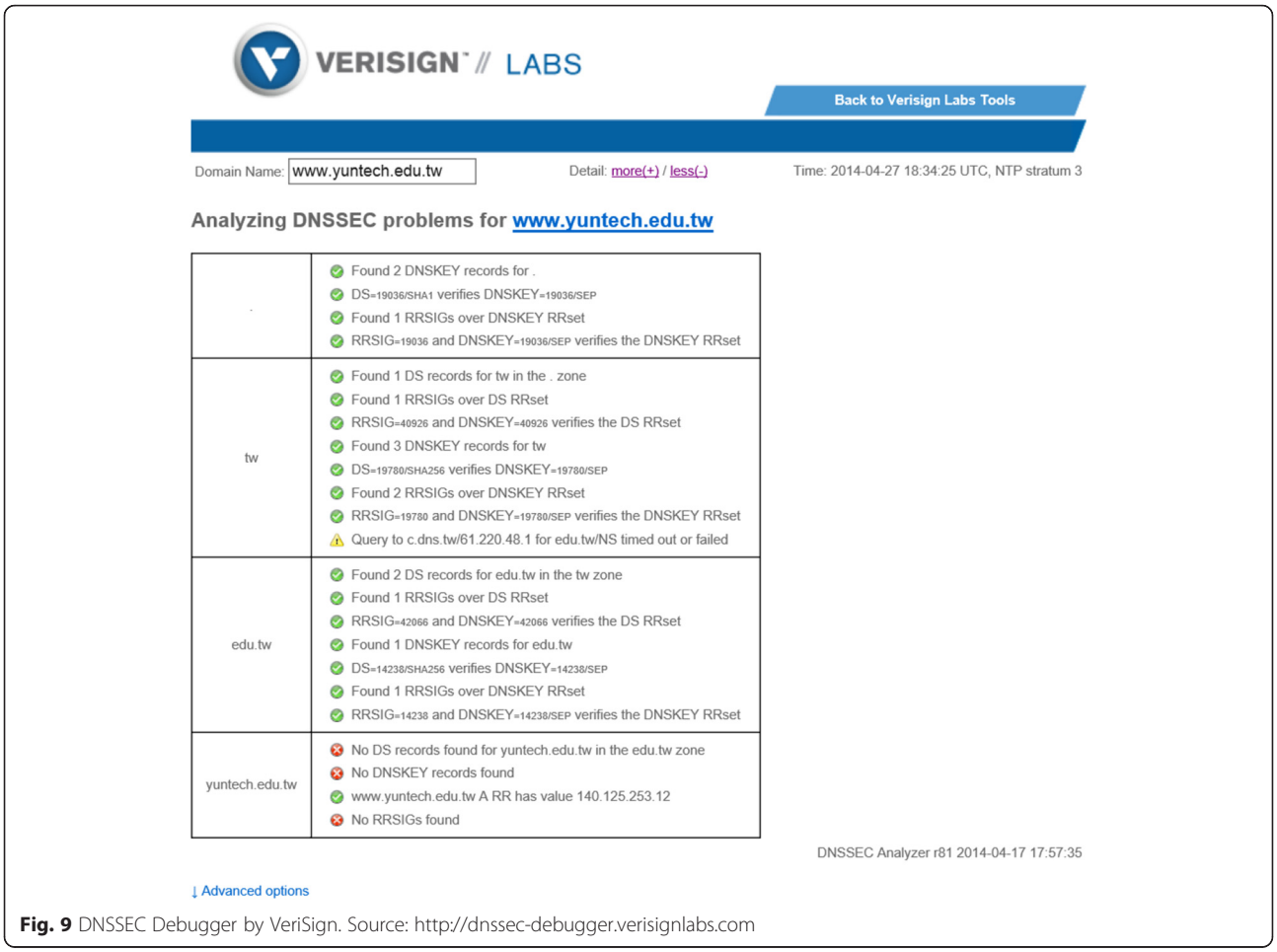

Fig. 9 DNSSEC Debugger by VeriSign. Source: http://dnssec-debugger.verisignlabs.com

the upgrade status of the foundation. Web browsing is a network service that is most commonly used by general users, so we refer to the websites which was Alexa Internet-listed to sort out top 100 traffic websites in Taiwan as our observed object. Table 4 lists the top 10 websites in Taiwan which were listed by Alexa Internet in 2014.

Table 4 Top 10 websites listed by Alexa Internet in 2014

Rank	Host Name
1	Yahoo.com
2	Facebook.com
3	Google.com.tw
4	Pixnet.net
5	Google.com
6	Ettoday.net
7	Gamer.com.tw
8	Youtube.com
9	Mobile01.com
10	Ck101.com

Source: http://www.alexa.com/topsites/countries/TW

Although this system is primarily used to investigate and test the deployment status of domestic units, we still have to detect and record for upgraded status of ccTLDs. In addition, we also collect national development IPv6 and DNSSEC-related information via the Internet.

3.2 Target objects

A project manager is the leader who is responsible for IPv6 or DNSSEC deployment. Project managers can view all the information and modify all the services and personnel data. In ADS, a project manager is termed "admin," a leader of technology or promoting staff in IPv6 or DNSSEC deployment in each area. A district manager can only work through the log information and detection to counseling members in their areas of responsibility. In ADS, a district manager is termed "manager," any person. In addition to the observed objects that were mentioned in the previous section, we also let general users detect objects what they want to do. Users can even choose to perform a complete inspection or testing in general, which can help them to more easily obtain the desired information.

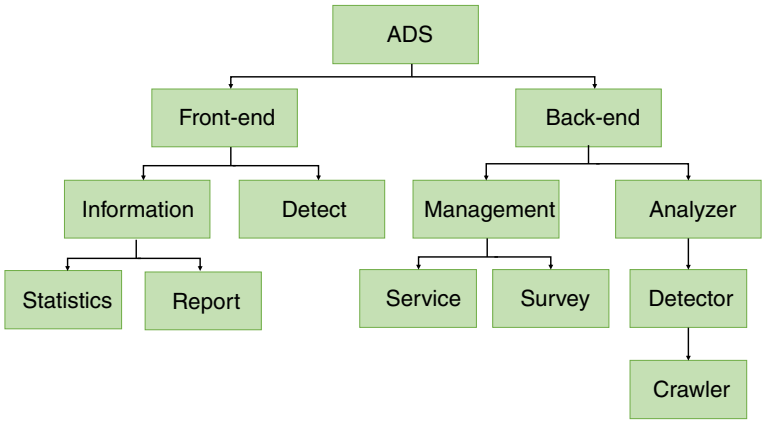

Fig. 10 System framework

3.3 Research framework

To allow all users use the Auxiliary Deployment System for IPv6 and DNSSEC at any time and any place, we designed it as a web-based testing platform. Figure 10 lists our tools for system implementation.

Auxiliary Deployment System for IPv6 and DNSSEC is divided into a front-end and a back-end. The front-end of our system provides many real-time information about IPv6 and DNSSEC and helps guest to debug and detect addresses of their services. Figure 11 shows the schematic diagram of the detection in ADS. Users can perform a complete detection or general detection on demand.

The back-end of our system only allows admin and manger login. A manager is responsible for counseling members to deploy IPv6 and DNSSEC; managers can view statistical information automatically by the system in order to understand what they are responsible for the progress of their work area. Figure 12 shows the deployment status of government services.

In addition to this, mangers can also participate in our survey to let us understand their use situation to improve our system and help in the decision-making, but managers could not modify a member's service data. Managers can only work through the log information

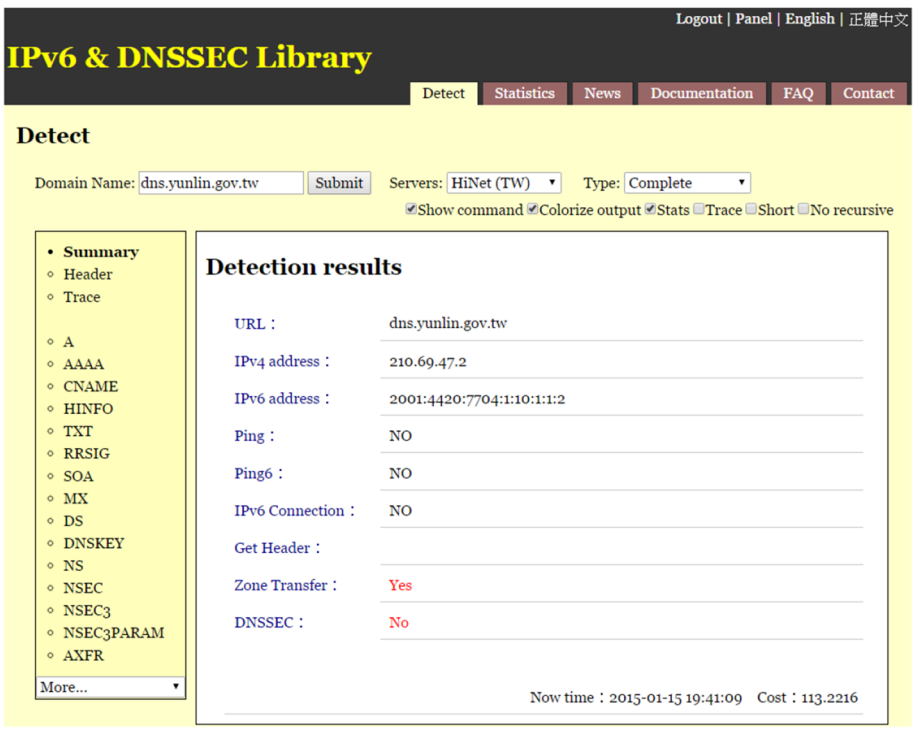

Fig. 11 Schematic diagram of the detection in ADS

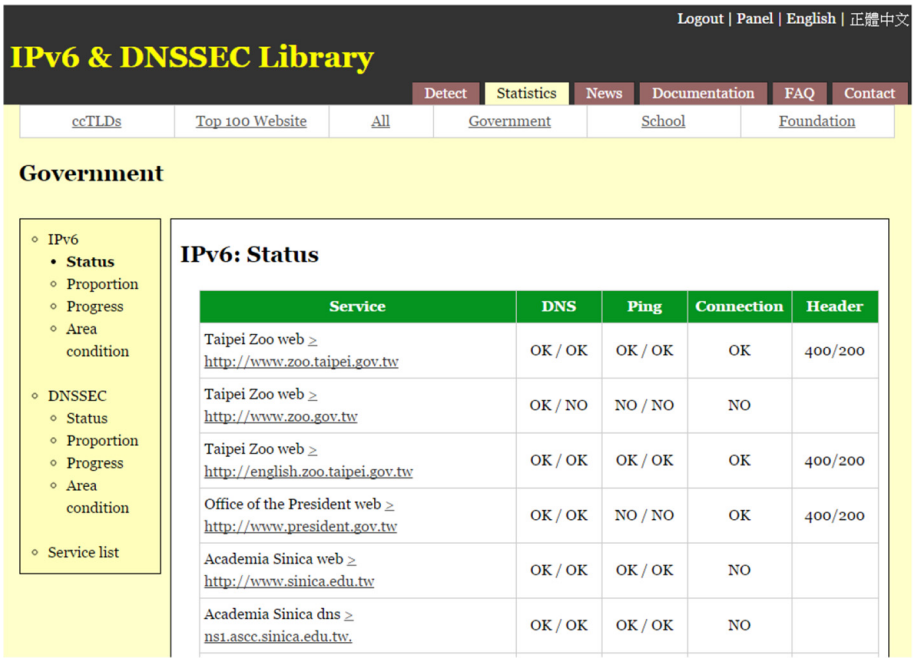

Fig. 12 Deployment status of government services

and detection to counseling a member to upgrade their service to ensure the correctness of this work. Only an admin can modify the service. The admin is the manager's superiors; the admin can manage all members and their services. Figure 13 shows the functional architecture of the back-end of our system.

Detection and statistics are the most important features of this system. Users can use this feature to detect their service to obtain the status of IPv6 and DNSSEC deployment and its environment. When the user wants to view the statistical results, the system will automatically generate plain text and graphical information for users. If the user chooses graphical information, then the user can clearly see the upgrade status of each region.

3.4 Methods

We use the built-in Linux commands "dig," "ping," "nslookup," and others to detect the target address; through the analysis of the target resource records, we can know its deployment status of IPv6 and DNSSEC. For example, if a website has an AAAA resource record and the system could get a header through sending an IPv6 request like a general browser, then the system will determine that the website can support IPv6 connection.

We observe the target object and record their resource record. Then we can analyze these data to estimate the status of deployment of the target objects. Finally, we will refer the results to the relevant personnel. Figure 14 shows the research process of this paper.

In order to satisfy the system requirements, such as system functions and low cost, Auxiliary Deployment System for IPv6 and DNSSEC use the open-source platform and tools for implementation. Table 5 lists our tools for system implementation.

In terms of implementations, first, we will sort out all observed objects to list, then implement a web-based

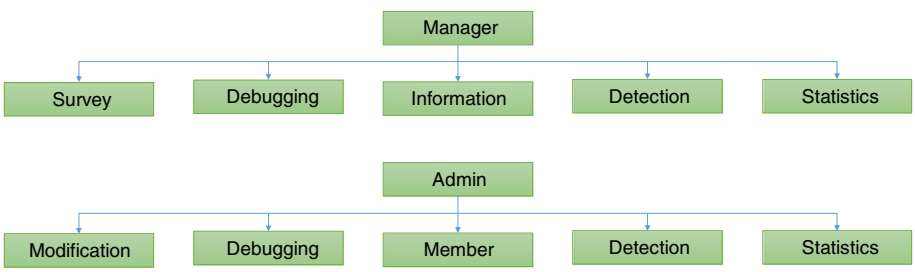

Fig. 13 Functional architecture of the back-end of our system

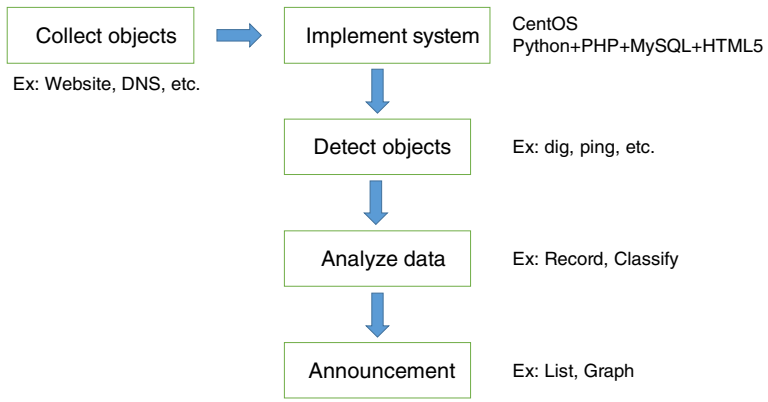

Fig. 14 Research process

platform. The platform provides promoters to promote IPv6 and DNSSEC easily. Promoters can see the information, including deployment progress of a local government, educational institutions, foundation of government, and some famous website. These information were derived from the system automatically detected. Promoters can understand the progress of their area of responsibility development from these information and as debugging and decision.

4 Experimental result

4.1 DNSSEC deployment status of ccTLDs

DNSSEC is a new network security agreement. In order to understand the current status of deployment of the world, this paper also investigated the deployment status of the domestic situation and the deployment of ccTLDs. Figure 15 shows the DNSSEC deployment status of ccTLDs on all continents.

Here, this paper will discuss the situation for DNSSEC deployment of the major regions.

1. Asia-Pacific region
   This area will hold regular DNSSEC workshops and let domain management unit of countries share experiences and exchange technology. And there is the not-for-profit regional Internet registry for the Asia-Pacific region names APNIC (Asia-Pacific Network Information Centre) which provides number resource allocation and registration services that support the global operation of the Internet. Including Japan, South Korea, China, and Taiwan, East Asia has a more complete DNSSEC development than the others in the Asia-Pacific region. These countries have more IT industry and better economic development.
   On the other hand, many countries in the Southern Asia have not yet begun to deploy DNSSEC because some countries have no funds or resources that can provide construction.
2. Europe
   In Europe, the organization responsible for allocating IP addresses is RIPE NCC (Réseaux IP Européens Network Coordination Centre) whose headquarters are in Amsterdam and protected by law in the Netherlands. RIPE NCC is in more than 70 countries worldwide including Russia, the Middle East, and parts of Central Asia; any organizations or individuals can become a member of RIPE NCC. Because the Internet infrastructure in Europe's earlier development and national income per capita is higher than others, most countries in this region have completed the deployment of DNSSEC. The countries that have not yet deployed DNSSEC are more concentrated in southern Europe and the Middle East. The reason should be social instability.
3. Americas
   Only a few countries with large economies of scale in Americas have completed the deployment of DNSSEC. Several countries of the Caribbean and Latin America have not yet deployed DNSSEC. There are two organizations responsible for allocating network resources. One is ARIN (American Registry for Internet Numbers), which is responsible for North America and parts of the Caribbean, and the other is LACNIC (Latin American and Caribbean Internet Address Registry)

Table 5 Our tools for system implementation

Tool name	Caption
CentOS 7	Linux-based operating system
Python 3.4.2	Used to collect and analyze data
PHP 5.4.16	Used to implement the website of our system
MariaDB 5.5.40	Used to record data
HTML5+CSS3+Javascript	Used to design the user interface

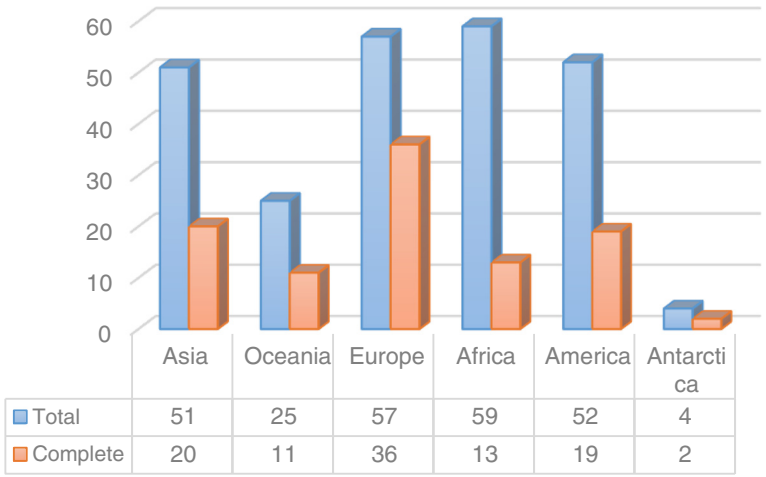

Fig. 15 DNSSEC deployment status of ccTLDs on all continents

which is responsible for Latin America and parts of the Caribbean.

4. Africa
   In Africa, the agency responsible for distribution of network resources is AFRINIC (African Network Information Center).
   Because development is lagging behind, only a few large countries have promoted DNSSEC development in Africa.

5 Conclusions

IPv6 and DNSSEC deployment issues in recent years have been enthusiastically discussed and implemented. Both IPv6 and DNSSEC are indispensable role next-generation systems. For this reason, we introduced related knowledge in the first place and, lastly, proposed an Auxiliary Deployment System for IPv6 and DNSSEC to help our government to more easily promote deployment.

To make the deployment of IPv6 and DNSSEC easier, we designed a web-based system which named Auxiliary Deployment System for IPv6 and DNSSEC for promoters and any person who want to use these. This system is divided into a front-end and a back-end. At the front-end, users can see some information about IPv6 and DNSSEC including news, reports, and various statistics. In addition, users can also detect any domain name to determine whether it supports IPv6 or DNSSEC via complete detection or general detection that the users choose. At the back-end, an admin can manage any services of each organization and carry out some investigation to improve system integrity and understand the needs of users. In addition to interaction with the users, the system also detects a task for service list every hour that is established by our crawler module.

The Auxiliary Deployment System for IPv6 and DNSSEC greatly reduces the complexity of deployment tasks which has many advantages, including a friendly interface, real-time information, integration, security, and free. In the future, we will actively use the system in IPv6 and DNSSEC deployment. Besides the practical application of our system, we will also do data mining of detected records for the associated research.

Author's information
Hung-Chang Chang received the Ph.D. degrees in Information Management from the National Yunlin University of Science and Technology, Taiwan. He is currently an assistant professor at the Department of Information Management, Shu-Zen Junior College of Medicine and Management, Taiwan. Most of his research areas are information security, software programming, and IoT design.

Competing interests
The author declare that he has no competing interests.

Received: 29 March 2016 Accepted: 12 July 2016
Published online: 27 July 2016

References

1. L Smith, I Lipner, *Free pool of IPv4 address space depleted*, 2011. Number Resource Organization
2. Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied, Major Announcement Set on Dwindling Pool of Available IPv4 Internet Addresses https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf
3. ICANN, nanog mailing list. Five /8s allocated to RIRs – no unallocated IPv4 unicast /8s remain https://books.google.com.tw/books?id=H70iDAAAQBAJ&pg=PA115&lpg=PA115&dq=ICANN,+nanog+mailing+list.+Five+/8s+allocated+to+RIRs+%E2%80%93+no+unallocated+IPv4+unicast+/8s+remain&source=bl&ots=PWlalmdqNd&sig=1rzoAP-4vRgPvkluh-NKDxpeDls&hl=zh-TW&sa=X&ved=0ahUKEwiSrM75-onOAhXlmJQKHQucDKkQ6AEILTAC#v=onepage&q=ICANN%2C%20nanog%20mailing%20list.%20Five%20%2F8s%20allocated%20to%20RIRs%20%E2%80%93%20no%20unallocated%20IPv4%20unicast%20%2F8s%20remain&f=false
4. Huston, Geoff. "IPv4 Address Report, daily generated". Retrieved 16 January 2011.Two /8s allocated to APNIC from IANA". APNIC. 1 February 2010. Retrieved 3 February 2011.
5. APNIC, *Two /8s allocated to APNIC from IANA*, 2010
6. APNIC, *APNIC IPv4 address pool reaches final /8*, 2011

7. ISC: DNS and DNSSEC Terminology (2010). Retrieved 02.15, 2014, from https://dlv.isc.org/about/dnssec_records
8. JH-Software: DNS Record types. V52 (2013). Retrieved 02.12, 2014, from http://www.simpledns.com/help/v52/index.html
9. R Arends, R Austein, M Larson, D Massey, S Rose, *RFC 4034: resource records for the DNS security extensions*, 2005
10. M Andrews, S Weiler, *RFC 4431: the DNSSEC lookaside validation (DLV) DNS resource record*, 2006
11. B Laurie, G Sisson, R Arends, D Blacka, *RFC 5155: DNS security (DNSSEC) hashed authenticated denial of existence*, 2008
12. Mark Santcroos, Olaf M. Kolkman, "DNS Threat Analysis", 3 May 2007. Retrieved from NLnet Labs website: http://www.nlnetlabs.nl/downloads/se-consult.pdf
13. W-A Chen, *The easy security protection and validation system for DNS server using DNSSEC*, 2005
14. S-H Jang, *The study of apply DNSSEC to building a protection mechanism for DNS pharming*, 2007
15. T Mantoro, SA Norhanipah, AF Bidin, *An implementation on domain name system security extensions framework for the support of IPv6 environment"*. Multimedia computing and systems (ICMCS), 2011 international conference on, 2011, pp. 1-6–7–9. ISBN 978-1-61284-730-6
16. S-J Chu, *Lightweight resource record distribution scheme against local DNSSEC attacks*, 2011
17. C Shu-Lun, *Efficient DNSSEC resource record update scheme*, 2011
18. C Meng-Huan, *A DNSSEC-based OpenID service*, 2011
19. C-C Yu, *Authenticating mobile peers in HIP networks with DNSSEC trust chain*, 2011
20. T Lin, W Liu, H Duan, D Sun, *IPv6 traffic hijack test system and defense tools using DNSSEC"*. Internet technology and applications (iTAP), 2011 international conference on, 2011, pp. 1-5–16–18. ISBN 978-1-4244-7253-6
21. D Migault, S Senecal, S Francfort, E Herbert, M Laurent, PREFETCHing to overcome DNSSEC performance issue on large resolving platform", in *IEEE international conference on trust, security and privacy in computing and communications*, vol. 12th, 2013. ISBN: 978-0-7695-5022-0/13

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Immediate publication on acceptance
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com