Cha *et al. EURASIP Journal on Wireless Communications and Networking* (2017) 2017:63
DOI 10.1186/s13638-017-0843-1

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Global experimental verification of Docker-based secured mVoIP to protect against eavesdropping and DoS attacks

ByungRae Cha[1], JongWon Kim[1], HaeMin Moon[2] and SungBum Pan[3*]

Abstract

The cloud-computing paradigm has been driving the cloud-leveraged refactoring of existing information and communications technology services, including voice over IP (VoIP). In this paper, we design a prototype secure mobile VoIP (mVoIP) service with the open-source Asterisk private branch exchange (PBX) software, using Docker lightweight virtualization for mobile devices with the immutable concept of continuous integration and continuous deployment (CI/CD). In addition, the secure mVoIP service provides protection against eavesdropping and denial-of-service (DoS) attacks, using secure voice coding and real-time migration. We also experimentally verify the quality of the secure voice and the associated communication delay over a distributed global connectivity environment to protect against eavesdropping and real-time migration to mitigate DoS attacks.

Keywords: Docker, Secure mVoIP, Virtualization, Communication verification test, Eavesdropping/DoS attacks

1 Introduction

Recently, cloud computing has become one of the hottest keywords in the information and communications technology (ICT) sector [1]. Cloud computing is a kind of Internet-based computing service that provides shared computing resources (computing, networking, and storage) and data to computers and other devices on demand. In addition, Docker lightweight virtualization (i.e., containerization) is quickly emerging from the Linux camp. Cloud computing is a means of innovation to change an enterprise's business environment, allowing it to evolve into an IT service model. When associated with a business, cloud computing can add value through business agility, operational efficiency, and infrastructure stability. In addition, the existing legacy application software can be made to evolve in the IT service model through the stability of the IT infrastructure. The existing ICT service and solution provider can add value in the move from a hardware (HW)-centric approach to a software (SW)-centric approach. The ability to constantly grow by evolving the service delivery approaches that generate stable revenue is important. In summary, the exploding cloud-computing paradigm has been driving the cloud-leveraged refactoring of existing ICT services. In this paper, to check the merit of a cloud native computing paradigm, we select the example of secure mobile voice over IP (mVoIP). That is, we attempt to apply the power of cloud computing to improve the security of voice communications in smartphones. We attempt to support secure mVoIP as a software-as-a-service (SaaS) application. Thus, we design prototype secure mobile VoIP services with the open-source Asterisk private branch exchange (PBX) SW by employing Docker lightweight virtualization for mobile devices with the immutable concept of continuous integration (CI)/continuous delivery (CD) [2, 3]. In addition, the proposed secure mVoIP service supports protection against eavesdropping and denial-of-service (DoS) attacks using secure voice coding and real-time migration. We also experimentally verify the quality of the secure voice and the associated communication delay over a distributed global connectivity environment in a domestic/international zone to protect against eavesdropping and real-time migration to mitigate DoS attacks.

*Correspondence: sbpan@chosun.ac.kr
[3]Department of Control and Measuring Robot Engineering, Chosun University, Gwangju, South Korea
Full list of author information is available at the end of the article

Springer Open

© The Author(s). 2017 **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.

2 Related work

In this section, we describe the related basic concepts of mVoIP, voice over long-term evolution (VoLTE), security aspects, and service quality in VoIP, Docker lightweight virtualization with CI/CD to implement a secure mobile VoIP, 5G, and Cisco Application Centric Infrastructure (ACI).

2.1 mVoIP, PBX SW Asterisk, and VoLTE

VoIP [4] is a methodology that combines technologies to deliver voice communication and multimedia sessions over the Internet (Internet protocol (IP) networks). VoIP systems employ signaling protocols and session controls to control the voice signaling, setup, and tear down of the communication calls (Fig. 1). It transports an audio stream over IP networks using special media delivery protocols to encode voice, audio, video with specific audio codecs, and video codecs as digital streamable media. The various codecs exist to optimize the media streaming based on the application requirements and network bandwidth; some of the implementations rely on narrowband and compressed speech, while others support high-fidelity stereo codecs. VoIP is available on smartphones, PCs, and other Internet-enabled devices. However, due to the current political and social situation, eavesdropping security incidents are on the rise. In particular, the US NSA has been suspected of tapping the German Chancellor's phone for more than 10 years, and it has recently been confirmed that the Chinese leaders have also been the target of eavesdropping. To support secure voice communication using VoIP, we examine the ways of guaranteeing the quality of service (QoS) of VoIP and surveying security issues associated with VoIP. The minimum response strategy and network tuning for specific parameters (e.g., packet loss, packet delay in transmission, jitter, and others) are required to guarantee the QoS of voice communication over the IP network. mVoIP is an extension of VoIP with mobility support [5]. Two types of communication are generally supported: (i) short-range or campus communication with cordless/digital enhanced cordless telecommunications (DECT)/physical coding sublayer (PCS) protocols where all base stations are linked into the same local area network (LAN) and (ii) wide-area communications using 3G/4G/5G protocols.

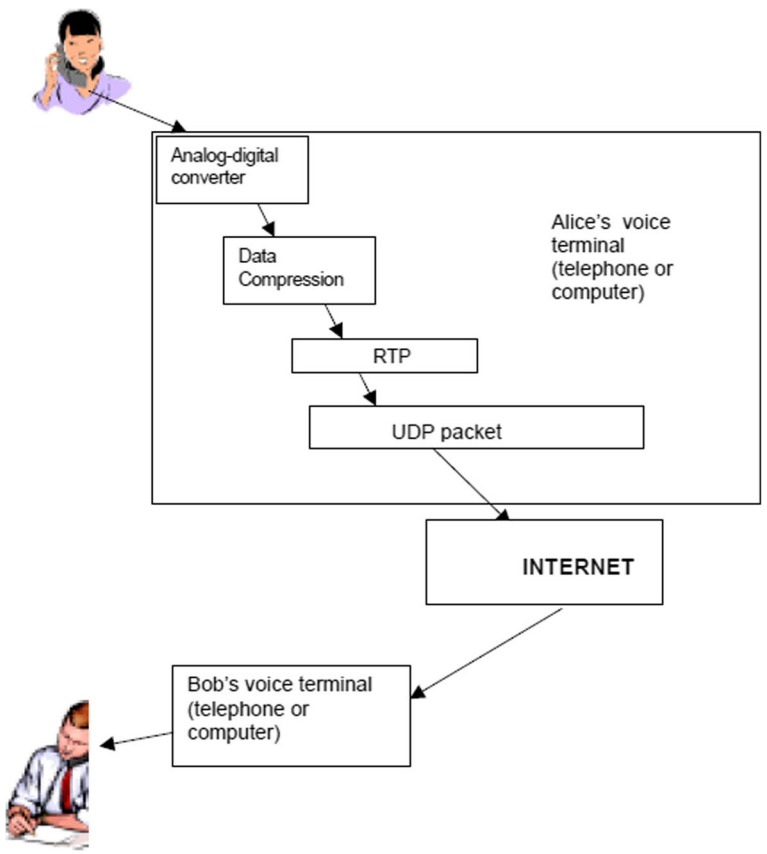

Fig. 1 Voice data processing in a VoIP system [10]

There are several methodologies that allow a mobile handset to be integrated into a VoIP network. One implementation turns the mobile device into a standard session initiation protocol (SIP) client, which uses a data network to send and receive SIP messaging and the real-time transport protocol (RTP) for the voice traffic. This methodology requires minimum support from a mobile handset and high-speed IP communication. The standard VoIP protocols (typically SIP) can be used over any broadband IP-capable wireless network connection. Lastly, Asterisk [6] is a SW implementation of a telephone PBX; it allows attached telephones to make calls to one another and to connect to other telephone services, such as the public switched telephone network (PSTN) and VoIP services. Its name is inspired by the asterisk symbol "*."

VoLTE is a network-based IP Multimedia Subsystem (IMS) with specific profiles for the control plane and media plane of a voice service on LTE as defined by the GSMA in PRD IR.92 [7]. The result of this approach is voice service (control and media planes) delivery as a flow of data within the LTE data bearer. This means that there is no dependency on (or, ultimately, requirement for) maintaining the legacy circuit-switched voice network. VoLTE has a greater capacity for voice and data, up to a factor of 3 compared with 3G universal mobile telecommunications systems (UMTS), and up to a factor of 6 compared with 2G global systems for mobile communications (GSM). Furthermore, it saves bandwidth because VoLTE's packet headers are smaller than in unoptimized VoIP/LTE [8].

2.2 Security issues and service quality of VoIP

Ruck [9] and the National Institute of Standards and Technology (NIST) [10] published documents on the security and QoS of VoIP. They noted 10 security issues relating to VoIP security as follows.

- Issue 1: VoIP traffic might be Internet bound.
- Issue 2: Gateway security options for VoIP are limited.
- Issue 3: Patching problems.
- Issue 4: VoIP security is only as reliable as the underlying network security.
- Issue 5: Many call-processing systems run on common operating systems (OSs), and they have their own security issues to worry about.
- Issue 6: DoS takes down telephony.
- Issue 7: Eavesdropping on calls using VOMIT or SipTap.
- Issue 8: Spam over IP telephony (SPIT).
- Issue 9: More ports open means more ports to secure.
- Issue 10: Wireless phones require advanced wireless security.

NIST summarized these problems into seven items for QoS issues in VoIP: latency, jitter, packet loss, bandwidth and effective bandwidth, throughput speed, power failure and backup systems, and QoS implementations for security.

With regard to VoIP security, in this study, we focus on eavesdropping (issue 7) and DoS attacks (issue 6). Eavesdropping is secretly listening to the private conversations of others without their consent. DoS attacks are an attempt to make a machine or network resource become unavailable to its intended users, such as temporarily or indefinitely interrupting or suspending the services of a host connected to the Internet.

2.3 Docker lightweight virtualization technology and CI/CD

Docker [11] is an open-source project that automates the integration and deployment of applications inside software containers by providing an additional layer of abstraction and automation of OS-level virtualization on Linux. To avoid overhead from starting and maintaining virtual machines, Docker uses the resource isolation features of the Linux kernel such as cgroups and kernel namespaces, and a union-capable filesystem such as aufs and others to allow independent "containers" to run within a single Linux instance. The Linux kernel's namespaces support mostly isolates an application's view of the operating environment, (e.g., user IDs, process trees, network, and mounted file systems), while the kernel's cgroups provide resource limiting (e.g., CPU, memory, block I/O, and network). Recently, there has been a trend to replace the hypervisor [12] with Docker for virtualization. Figure 2 illustrates the differences between hypervisor and Docker.

CI means that whenever a developer checks in code to the source repository, a build is automatically triggered as shown in Fig. 3. If the build and automated unit tests are successful, CD takes this one step further by automatically deploying the application to an environment for more in-depth testing.

Figure 4 presents the registration step, payment step, key distribution step, and deployment step from the secure mVoIP service. It is shown that user A registers their information and makes a payment (see Fig. 4 (1)). The key distribution system sends the public key of user A to the storage server and the private key to user A (see Fig. 4 (2) and (3), respectively). Note that secure shell (SSH) with a session based on public key cryptography is used in the registration step. Figure 4 also presents the deployment of PBX using Docker virtualization. User A accesses the storage server using the private key and downloads the Docker-based PBX container as SaaS (see Fig. 4 (4) and (5)). Then, user A sets up the downloaded PBX container (see Fig. 4 (6)), and finally, user A sends the mVoIP app to user B (see Fig. 4 (7)) to enable the secure voice communication.

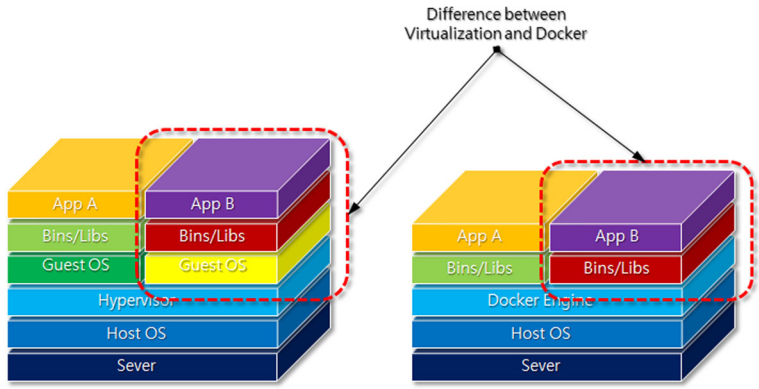

Fig. 2 Difference between virtualization (with hypervisor) and containerization (with Docker)

2.4 5G wireless systems and Cisco ACI

The 5G technology [13, 14] will provide further services and added benefits to the world compared with 4G. It will provide very high bandwidth, which the user will not have experienced previously. It also has many advanced features which makes it a powerful tool for wireless communication. By pushing 5G into VoIP-enabled devices, users will experience a level of data transmission and call volume as never before. Moreover, 5G technology will offer high QoS in many fields such as product engineering,

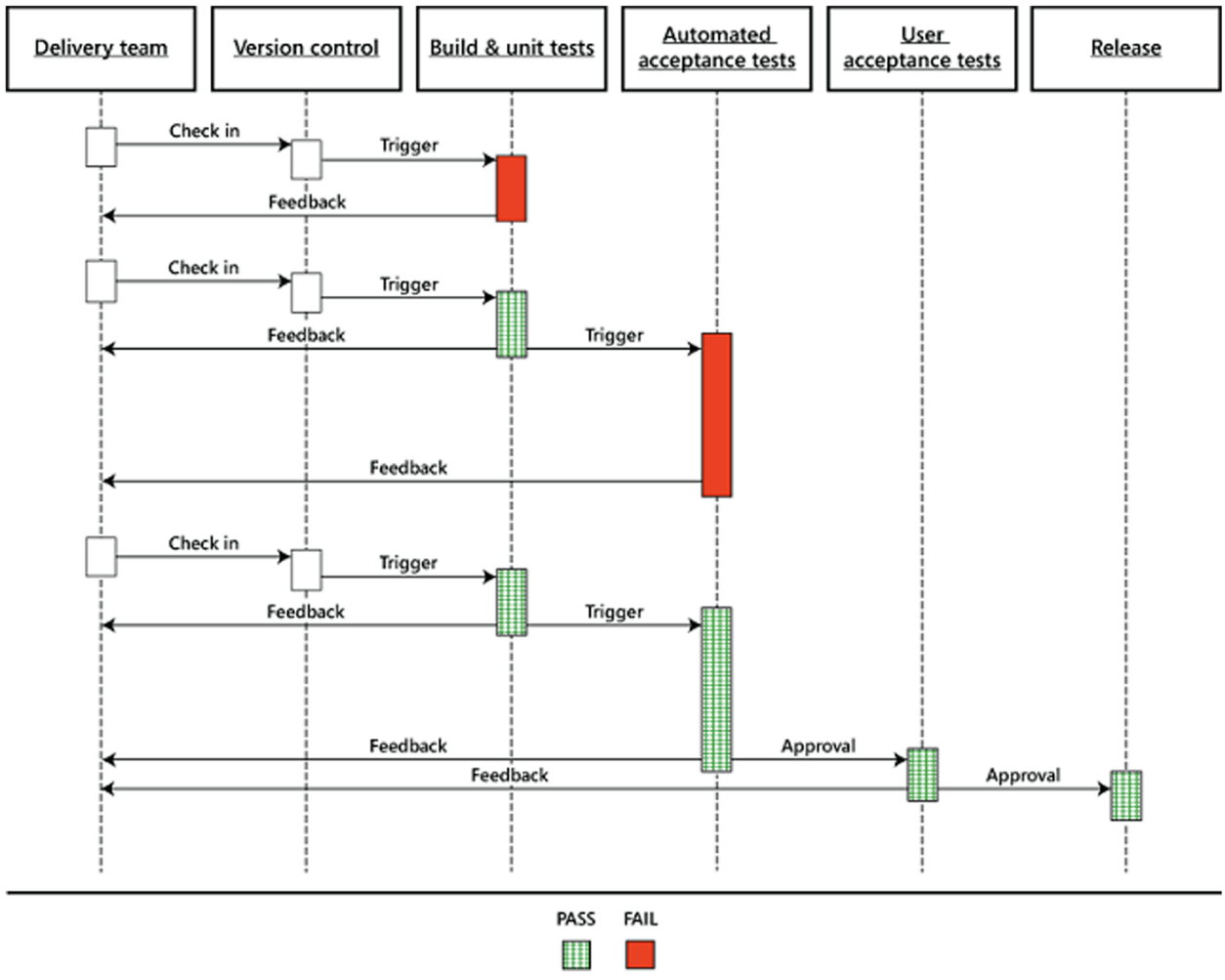

Fig. 3 Detailed diagram of CI processing

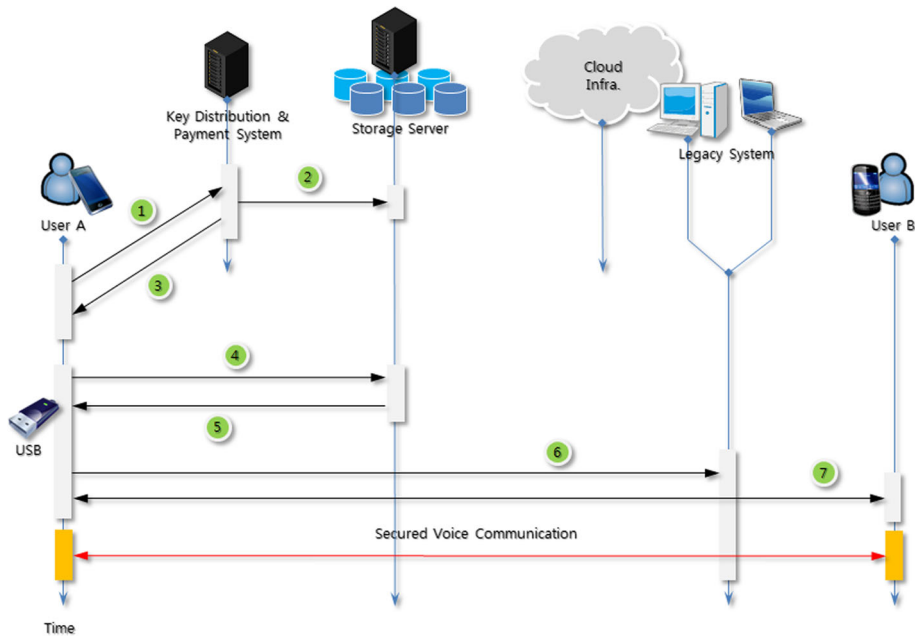

Fig. 4 Concept diagram of the registration and deployment of a secure mVoIP service

Internet of Things (IoT), Internet of Everything (IoE), All to One (AtO), Industrial IoT (I2oT), and electronic transactions (e-payments, e-tickets, and e-transactions).

IT departments and the associated businesses are looking for cloud automation tools and software-defined networking (SDN) [15] architectures to:

- Accelerate application delivery
- Reduce operating costs
- Greatly increase business agility

Cisco Application Centric Infrastructure (ACI) [16] is a comprehensive SDN-based architecture. The policy-based automation solution of Cisco ACI supports a business-relevant application policy language and provides greater scalability through a distributed enforcement system and greater network visibility. These benefits are realized through the integration of physical and virtual environments under one policy model for networks, servers, storage, services, and security.

3 Design and implementation of Docker-based secure mVoIP with CI/CD

To support CI/CD with lightweight virtualization for secure mVoIP, the secure mVoIP based on Docker can be implemented by utilizing the open-source PBX SW Asterisk with HW on a single board or PC instance of high-performance servers. Figure 5 shows the HW platform testbed of the PBX SW Asterisk from single-board

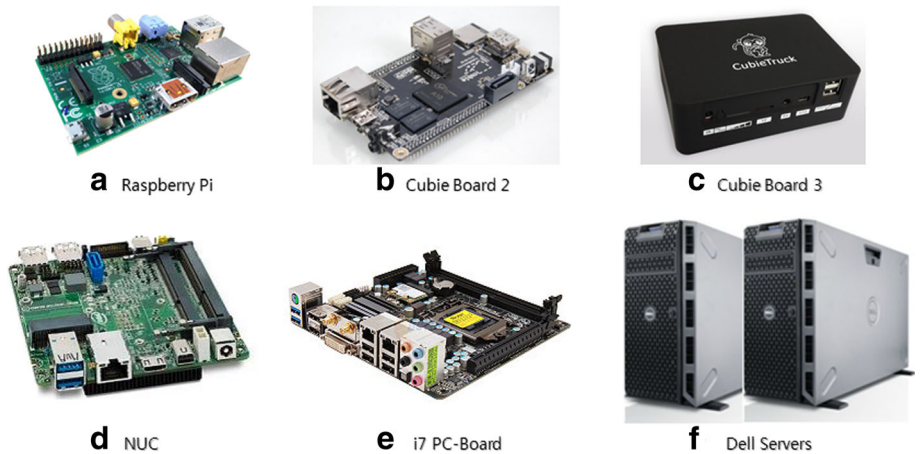

Fig. 5 HW platform testbed of the PBX SW Asterisk. **a** Raspberry Pi. **b** Cubie-Board 2. **c** Cubie-Board 3. **d** NUC. **e** i7 PC board. **f** Dell servers

Raspberry Pi 2 to Dell servers. The single-board Raspberry Pi 2, Cubie-Board 2, and Cubie-Board 3 are standalone-based mVoIP platforms. The Intel NUC, Intel i7 PC, and Dell servers are cloud and Docker-based mVoIP platforms. Figure 6 shows the architecture of the Docker-based PBX SW Asterisk [6] and dashboard FreePBX [17]. As shown in Fig. 6, Dockerfile [18] keywords used to generate the Docker image are presented. Docker can build images automatically by reading the instructions from a Dockerfile, a text file that contains all the commands, in order, needed to build a given image. Dockerfiles support the functions of CI/CD. Dockerfiles adhere to a specific format and use a specific set of instructions.

To support a secure mVoIP app (cf. issue 7 in Section 2.2), Fig. 6 (a) shows the continuous delivery server with generated images using the Dockerfile. Figure 6 (b) shows the architecture of the Docker-based PBX SW Asterisk and dashboard FreePBX in the backend server. As shown in Fig. 6 (c), Dockerfile keywords used to generate the Docker image are presented. The functions of the Dockerfile support CI/CD. The idea behind CI/CD is that we should create jobs that perform certain operations such as building, testing, delivering, and deploying. Those jobs should be linked together to create a CI/CD pipeline.

The main concept of Docker is the immutable infrastructure concept that extends CI/CD as shown in Fig. 6, and the features of the immutable infrastructure are summarized as follows: manageability, scalability, testability, and portability. Figure 6 (d) and (e) show the user interface (UI) screen of the secure mVoIP app based on an Android device for a secure voice communication service. In particular, to prevent eavesdropping on calls using VOMIT or SipTap, Fig. 6 (d) shows the secure key generation process to support secure voice communication including the steps of voice sampling, white-noise removal, and secure key generation [19].

4 Verification of the secure voice test to protect against eavesdropping and the global communication test of secure mVoIP

In this section, we perform verification testing between the user's original voice and the user's secure voice for respectively real voice communication and secure voice communication testing of global and domestic communication environments using the developed secure mVoIP based on Docker.

4.1 Verification of the secure voice test to protect against eavesdropping

We performed the verification testing of secure voice communication to protect against eavesdropping using an Android-based secure mVoIP app and Docker-based PBX SW Asterisk with a PC to support lightweight virtualization. Figures 7 and 8 show the verification of

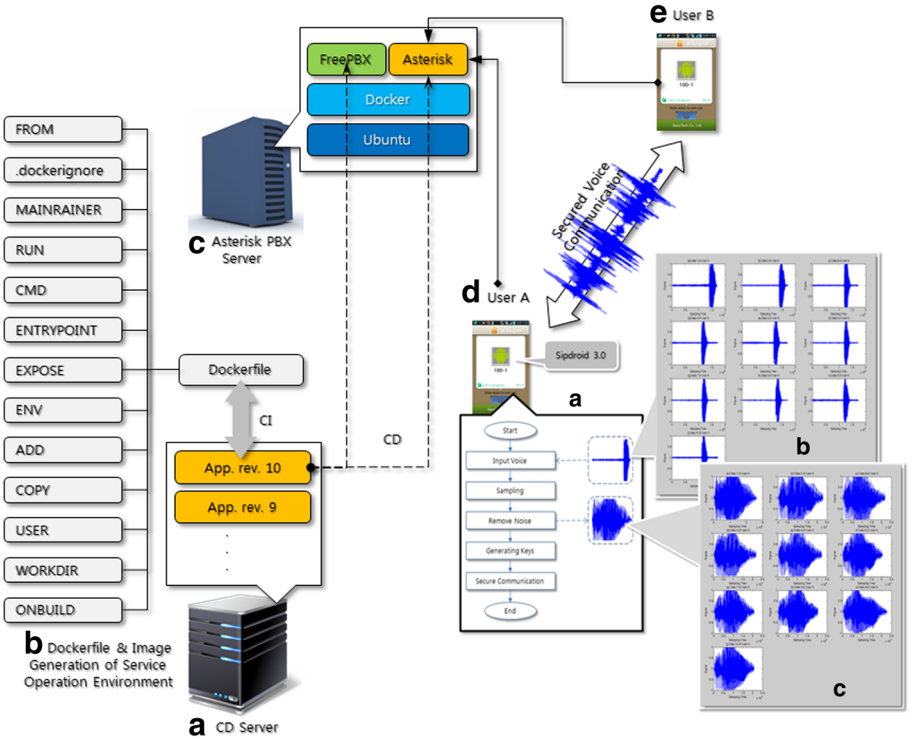

Fig. 6 Diagram of the immutable infrastructure for Docker-based secure mVoIP. *a* CD server. *b* Dockerfile and image generation of service operation environment. *c* Asterisk PBX server. *d* User A. *e* User B

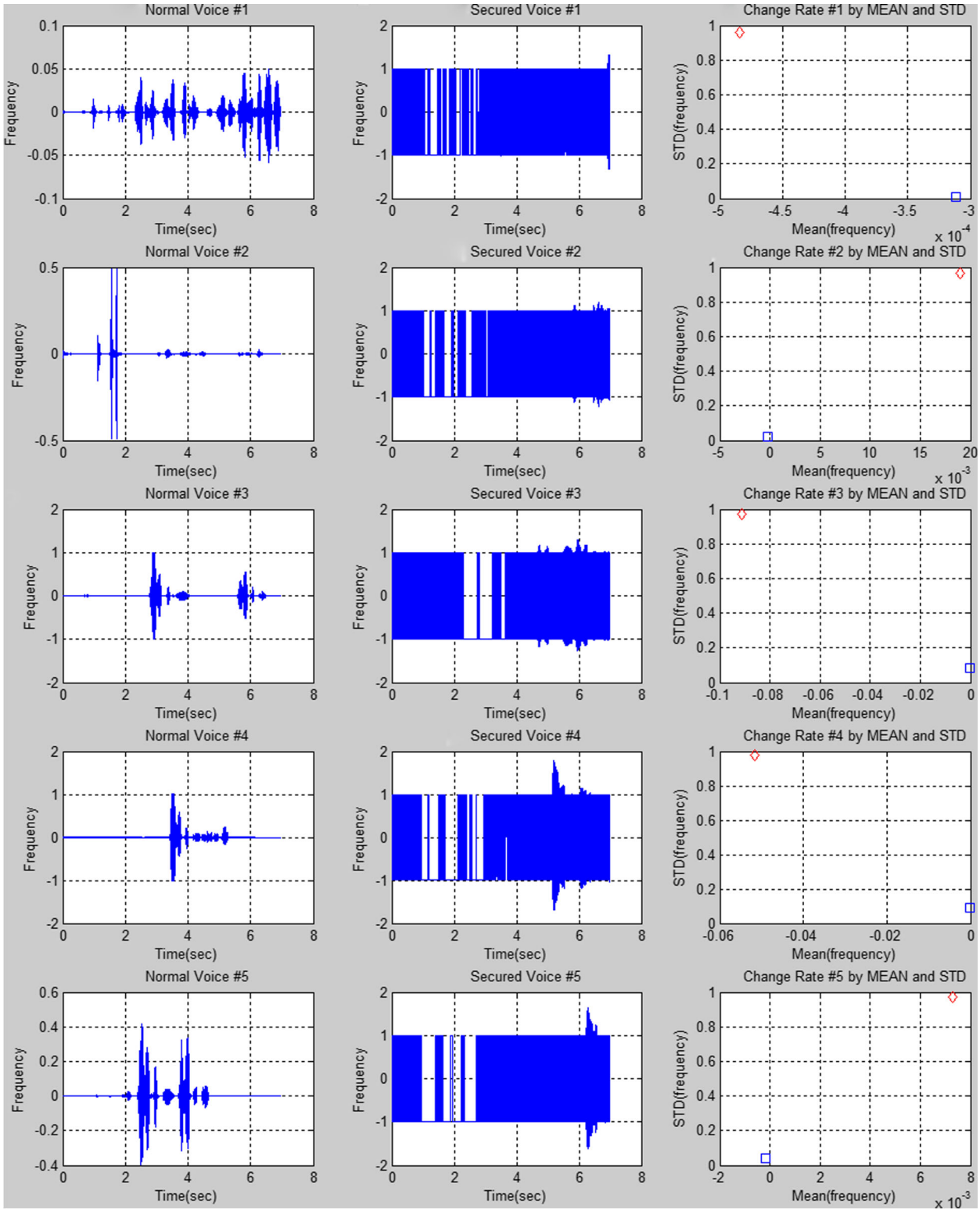

Fig. 7 Original and secured voices (user A)

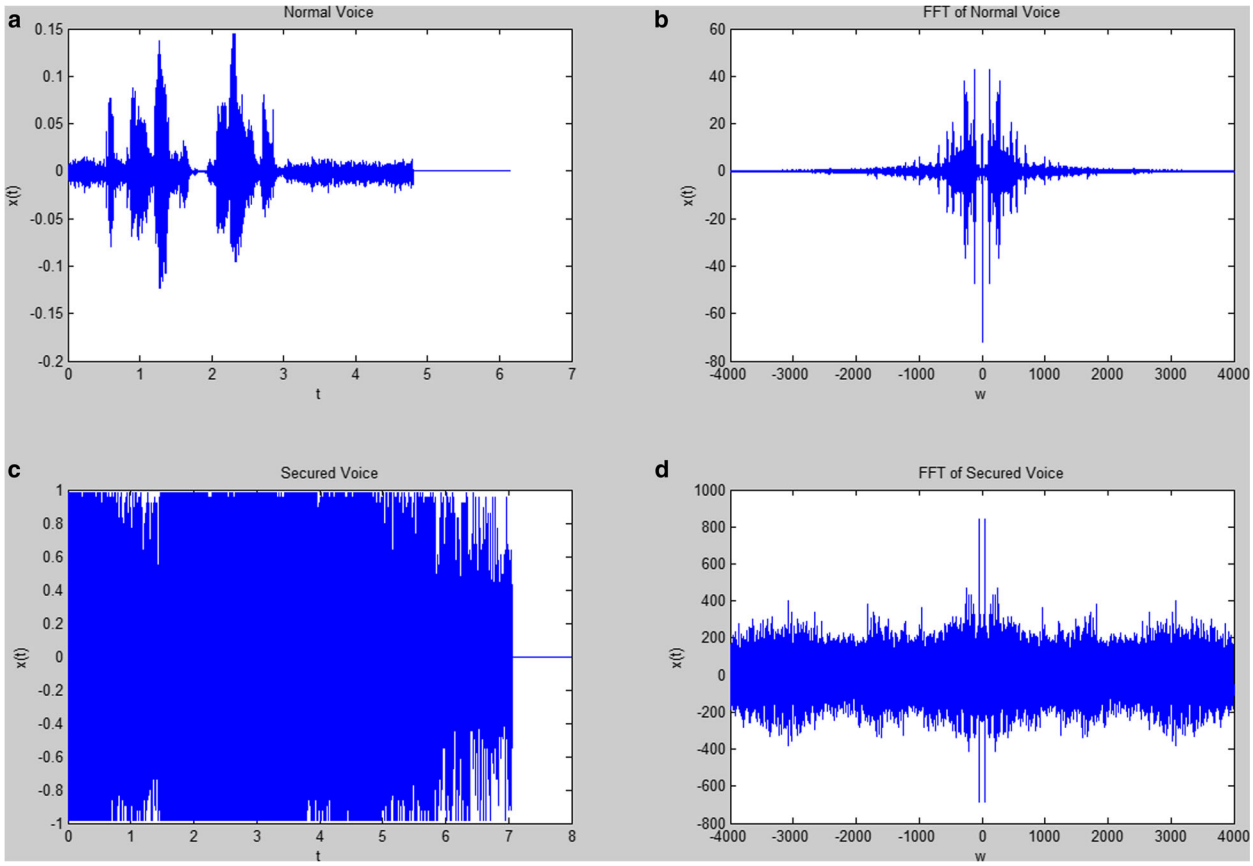

Fig. 8 Original and secured voices and their FFT versions. **a** Normal voice. **b** FFT of normal voice. **c** Secure voice. **d** FFT of secure voice

the secure voice test to protect against eavesdropping by original voice and secure voice. Figure 7 presents the user's original voice and the user's secure voice through the secure mVoIP app. The third column of Fig. 7 shows the locations of the original voices (blue squares) and the secure voices (red diamonds) with regard to the average (x-axis) and standard deviation (y-axis) to demonstrate objectivity. The distances between original voice and secure voice intuitively demonstrate the security of voice communication. Figure 8 shows the user's original voice and secure voice. Figure 8a, b present respectively the original voice and fast Fourier transformation (FFT [20]) signal of the original voice. Figure 8c, d present respectively the secure voice and FFT signal of the secure voice. Figure 9 presents a comparison between original voices and secure voices (mean and standard deviation), and Fig. 10 shows the distribution comparison between original voice and secure voice by FFT.

4.2 Verification of the domestic voice communication test

The domestic real voice communication test of the secure mVoIP was conducted between the metropolitan areas of Seoul, Daejeon, Daegu, Gangneung, or Jeju Island and Gwangju metro-city as shown in Fig. 11. The real voice two-way communication speed is approximately distributed in the range from 133 to 145 ms as shown in Table 1. Figure 12 shows the results of 100 iterations of the network traffic delay test between secure mVoIP apps in Gwangju metro-city.

4.3 Verification of the voice communication test in South-East Asia

The real voice communication test of the secure mVoIP in South-East Asia was conducted between Malaysia, Myanmar, or Okinawa and Gwangju metro-city as shown in Fig. 11. Table 2 presents the real voice communication test results between Gwangju metro-city and Okinawa. The real voice two-way communication speed is approximately distributed in the range of minimum 78 ms and maximum 181 ms. The real voice communication speed between Gwangju metro-city and Malaysia are approximately distributed in the range of minimum 108 ms and maximum 140 ms as shown in Table 2. In addition, the real voice communication speed between Gwangju metro-city and Myanmar are approximately distributed in the range of minimum 78 ms and maximum 175 ms.

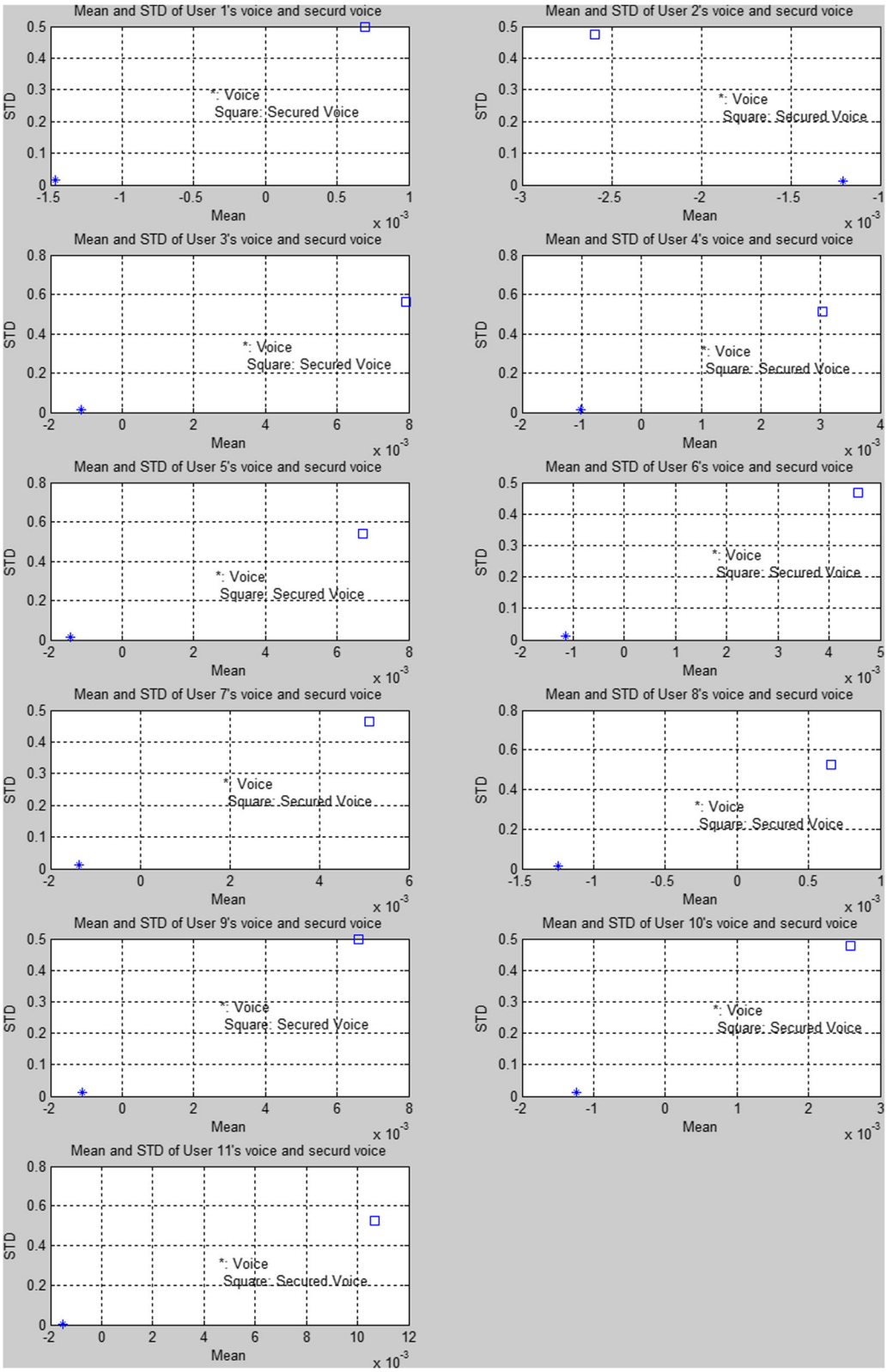

Fig. 9 Comparison between the original voice and secure voice (mean and standard deviation)

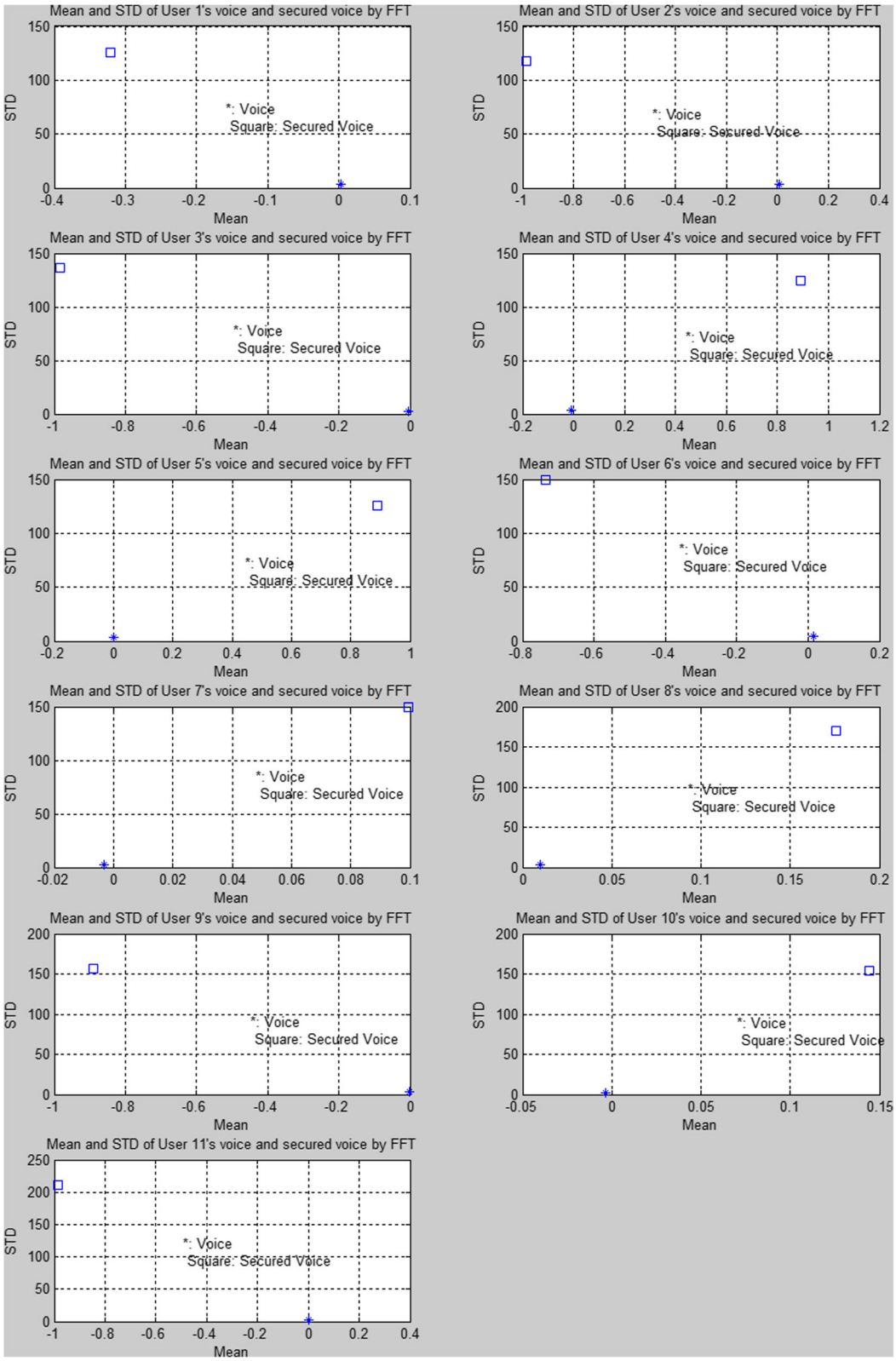

Fig. 10 Distribution comparison between the original voice and secure voice by FFT

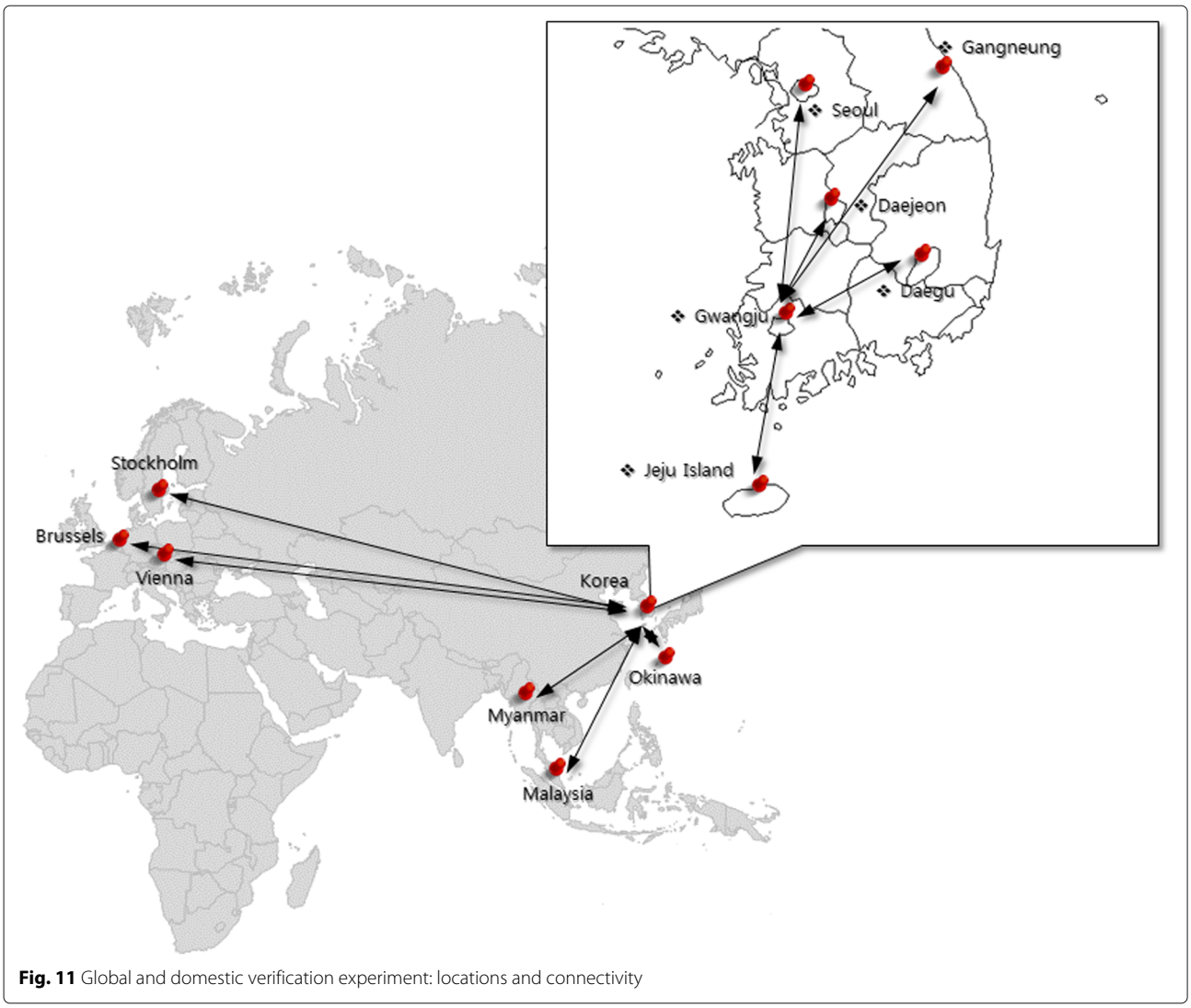

Fig. 11 Global and domestic verification experiment: locations and connectivity

4.4 Verification of the voice communication test in Europe

The real voice communication test of the secure mVoIP in Europe was conducted between Brussels, Stockholm, or Vienna and Gwangju metro-city as shown in Fig. 11. Table 3 presents the real voice communication test results between Brussels, Stockholm, and Vienna and Gwangju metro-city. The real voice two-way communication speed in Europe is approximately 78 ms in all cases. In conclusion, the real voice communication speed of the entire European zone is consistent with that of the real voice communication speed of the South-East Asian zone.

Table 1 Experimental verification of the domestic voice communication test results

Domestic area	Minimum delay time (ms)	Maximum delay time (ms)
Seoul	78	78
Daejeon	78	140
Gangneung	78	140
Jeju Island	133	145

5 Cloud-based real-time migration test of VoIP to mitigate DoS attacks

A cloud-based mVoIP platform has the merits of cloud computing, provisioning, elastic management, and virtualization of resources in the cloud infrastructure. We tested the real-time migration test of mVoIP during voice communication to mitigate DoS attacks and assumed a virtual scenario for any of the DoS attacks (cf. issue 6 of Section 2.2). The strategy to mitigate or avoid DoS attacks is to detour DoS attack traffic using real-time migration among infrastructure resources. Figures 13 and 14 show

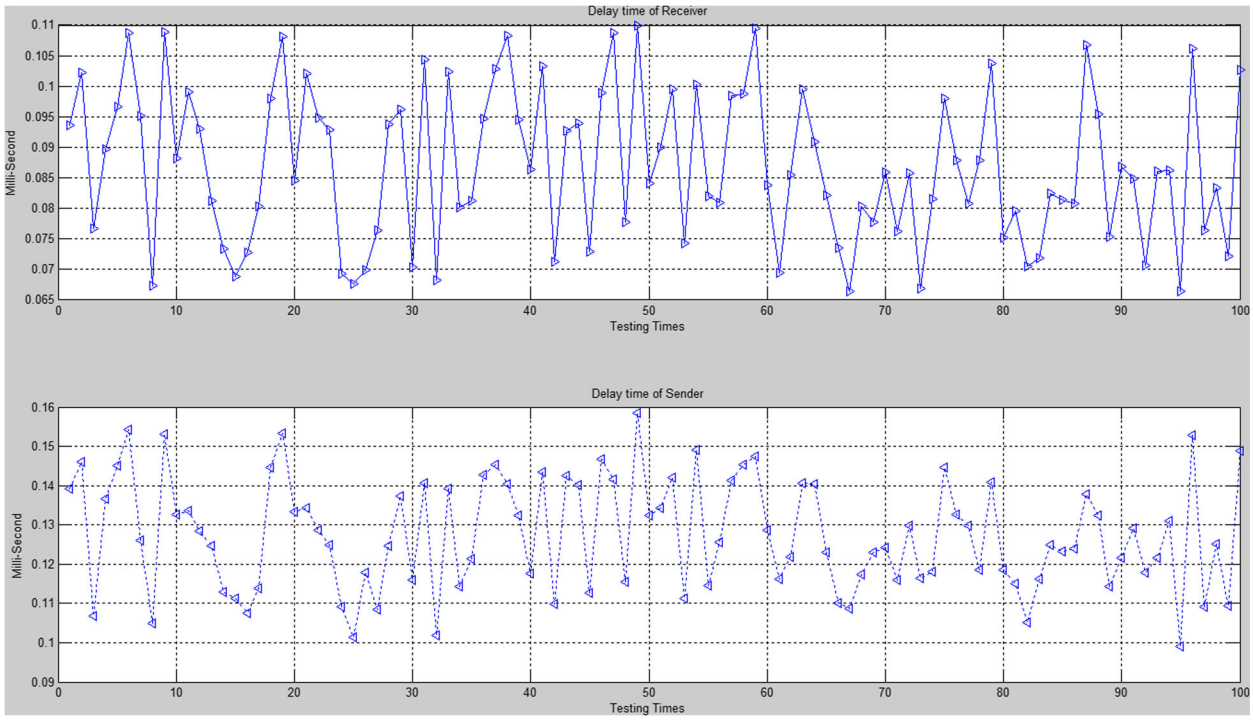

Fig. 12 Network traffic delay test between secure mVoIP apps in Gwangju metro-city

a graph of the network traffic using Cacti [21] and the data communication graph using FreePBX showing the real-time migration between hosts. We observed a much larger amount of network traffic and data communication during real-time migration than during settlement. The real-time migration generates a burst of data types between 15 and 10 s as shown in Fig. 13. In particular, the migration traffic needs a higher level of bandwidth only at the start of the migration as shown in Fig. 14. The amount of real-time migration traffic itself requires less bandwidth, but the absolute priority of real-time migration traffic should be guaranteed as critical traffic to detour/avoid DoS attacks.

6 Conclusions

Recently, the paradigm of the computing environment has changed, and following changes to the communication environment, VoIP technology is being revisited to support various services in the ICT field. In this paper, we designed a prototype secure mVoIP service with the open-source Asterisk PBX SW by employing Docker lightweight virtualization for mobile devices with the immutable concept of CI/CD. In addition, the secured mVoIP service supports protection against eavesdropping and DoS attacks using secure voice coding and real-time migration. We also experimentally verified the quality of the secure voice and the associated communication delay over a distributed global connectivity environment. In particular, the global real voice communication test was conducted in both South-East Asia and Europe. The real voice communication speed of the entire European zone was consistent, and the real communication speed of the South-East Asian zone was variable. We have shown that real-time migration has the potential to provide DoS attack mitigation.

Table 2 Voice communication test result between Gwangju metro-city and South-East Asian locations

Location	Minimum delay time (ms)	Maximum delay time (ms)
Okinawa	78	181
Malaysia	108	140
Myanmar	78	175

Table 3 Voice communication test result between Gwangju metro-city and Europe

Location	Minimum delay time (ms)	Maximum delay time (ms)
Brussels	78	78
Stockholm	78	78
Vienna	78	78

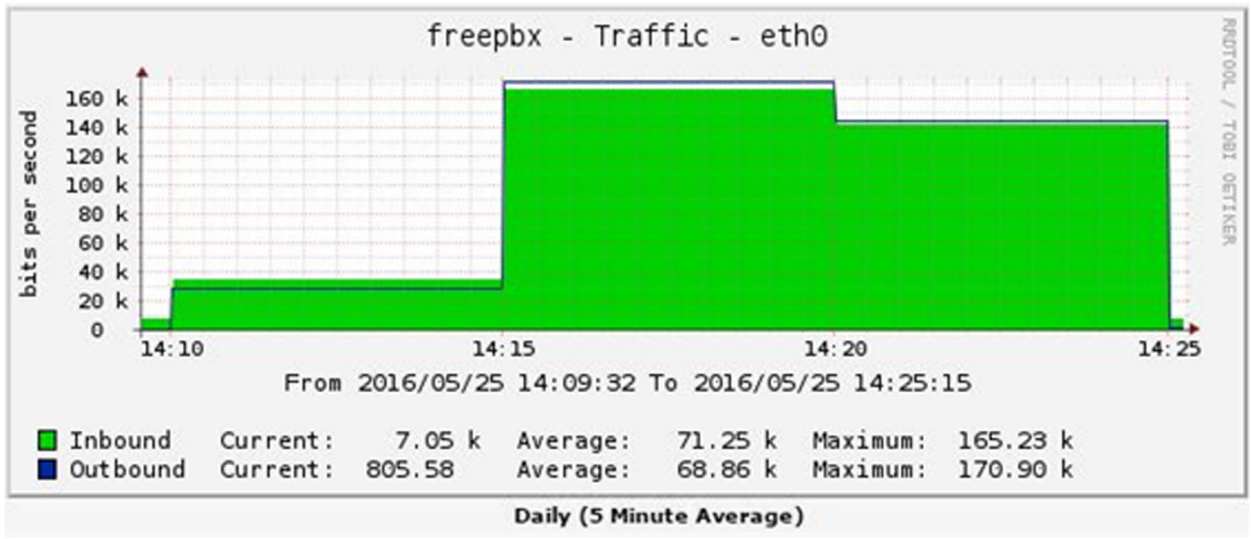

Fig. 13 Network traffic graph using Cacti

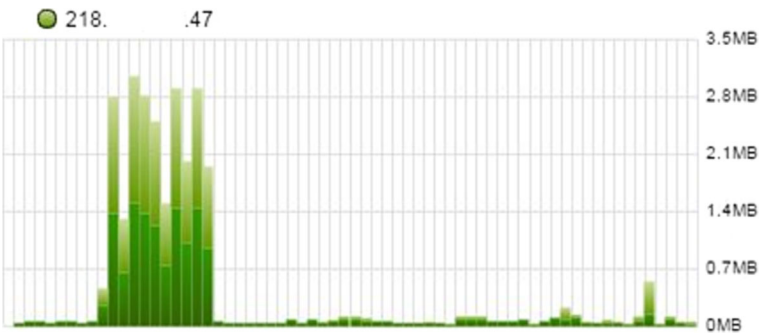

Fig. 14 Data communication graph using FreePBX

Acknowledgements
This work was supported by an Institute for Information Communications Technology Promotion (IITP) grant and funded by the Korean government (MSIP) (no. B0190-15-2030, Web Service User Account Information Management and Spill/Exploit Detection Technology Development) and by the Human Resource Training Program for Regional Innovation and Creativity, through the Ministry of Education and National Research Foundation of Korea (2015H1C1A1035823).

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details
[1]School of Electrical Engineering and Computer Science, GIST, Gwangju, South Korea. [2]Department of Information and Communication Engineering, Chosun University, Gwangju, South Korea. [3]Department of Control and Measuring Robot Engineering, Chosun University, Gwangju, South Korea.

Received: 29 June 2016 Accepted: 20 March 2017
Published online: 04 April 2017

References

1. Gartner Group. http://www.gartner.com/. Accessed 28 Mar 2017
2. CI/CD. https://www.docker.com/use-cases/cicd. Accessed 28 Mar 2017
3. CI/CD. http://www.asp.net/aspnet/overview/developing-apps-with-windows-azure/building-real-world-cloud-apps-with-windows-azure/continuous-integration-and-continuous-delivery. Accessed 28 Mar 2017
4. VoIP. http://www.voip-info.org/wiki/view/What+is+VOIP. Accessed 28 Mar 2017
5. Mobile VoIP. https://www.mobilevoip.com/. Accessed 28 Mar 2017
6. Asterisk. http://www.asterisk.org/. Accessed 28 Mar 2017
7. N Russell, Official document IR.92 - IMS profile for voice and SMS. GSMA (2015)
8. E Elkin, The secret value of VoLTE. TMCnet (2014)
9. M Ruck, Top ten security issues with voice over IP. 2010 White Paper Series, Technology Consultants and Network Engineers (2010)
10. DR Kuhn, TJ Walsh, S Fries, Security considerations for voice over IP systems. NIST Special Publication 800-58, 1-91 (2005)
11. Docker. https://www.docker.com/. Accessed 28 Mar 2017
12. Hypervisor. https://en.wikipedia.org/wiki/Hypervisor. Accessed 28 Mar 2017
13. A Aryaputra, N Bhuvaneshwari, in *Proceedings of the World Congress on Engineering and Computer Science 2011 Vol II*. 5G- the future of mobile network, (2011), pp. 19–21
14. X Li, A Gani, R Salleh, O Zakaria, The future of mobile wireless communication networks. International Conference on Communication Software and Networks, 554–557 (2009)
15. SDN. https://www.opennetworking.org/sdn-resources/sdn-definition. Accessed 28 Mar 2017
16. Cisco ACI. http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html. Accessed 28 Mar 2017
17. FreePBX. https://www.freepbx.org/. Accessed 28 Mar 2017
18. Dockerfile. https://docs.docker.com/engine/userguide/eng-image/dockerfile_best-practices/. Accessed 28 Mar 2017
19. BR Cha, SJ Shim, S Park, JW Kim, Secured mVoIP service over cloud and container-based improvement. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, 791–795 (2015)
20. Fast Fourier transformation (FFT). http://mathworld.wolfram.com/FastFourierTransform.html. Accessed 28 Mar 2017
21. Cacti. http://www.cacti.net/. Accessed 28 Mar 2017

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