Privacy Preservation and Authentication Protocol for BBU-Pool in C-RAN Architecture*

Byomakesh Mahapatra[1], Awaneesh Kumar Yadav[1], Shailesh Kumar[1], and Ashok Kumar Turuk[1]

Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Odisha, India
{514cs6020, 217cs2312, 518cs1014, akturuk}@nitrkl.ac.in

Abstract. The cloud radio access network (C-RAN) is a new generation centralized collaborative base station (BS) growth over a traditional data center for handling voices, videos and data services over a single platform. The C-RAN uses virtualization and cloud computing technology for handling both real and non-real time data. The C-RAN consists of a distributed RF unit and a centralized baseband unit (C-BBU) which performs data processing and controlling activity. As the BBU-Pool consists of a set of virtual machine (VM) controlled by a hypervisor and a host operating system, there are more chances of security threats and identity theft at the C-BBU. In this paper, we have proposed privacy preservation and authentication protocol (PPAP) to secure the BBU-pool from different internal and external attacks. The proposed protocol secures the C-BBU from guest OS, host OS, DoS, and migration attack. The proposed protocol is simulated with the help of two security tools Automated Validation of Internet Security Protocols and Applications (AVISPA) and SCYTHER tools. The simulation result shows that the protocol is secure and able to handle the associated VM more securely in the BBU-pool.

Keywords: BBU-pool · C-RAN · Hypervisor · Security · Virtual Machine

1 Introduction

The growth of IoT and other data-centric wireless network leads to the increase in traffic load on the BS. To encompass this increasing load the number of the cellular BS should be increased, which again leads to an increase in cost incurred and network complexity [1]. The C-RAN is considered to be a new alternative to overcome this limitations. The C-RAN architecture reduces the capital expenditure (CAPEX) and operational expenditure (OPEX) to a greater amount by using the cloud computing technology and virtualization technology at the radio access network platform. The C-RAN provides a collaborative radio access network platform for accessing different base band signal over a virtualized base

* Supported by organization x.

band unit (V-BBU) [2]. The C-RAN architecture (Fig. 1) consists of a distributed radio unit also known as Remote Radio Head (RRH) where number of user entity (UE) are linked by sharing a wireless channel. The base band signal received by the RRH unit are again down converted and send to a centralized unit known as Base Band Unit (BBU), where all the signal processing and controlling activity is carried out. The C-BBU is growth over a cloud platform which consists of some physical hardware, virtual machine (VM), and a hypervisor for performing controlling and interfacing activity. The development of this new technology leads to a more complex platform interm of data-processing and security concern. As in this new C-RAN technology the C-BBU handle voices, video, and data on a single platform by using virtualization technology, it needs more security and authentication then the traditional data-center [3]. In [4], the authors have described different key security challenge in C-RAN and provides many proposed solution to overcome this limitation. Authors in [5], give a complete overview of the security challenges in the cloud computing environment. They have also focused on two main possible attacks i.e. host OS attack and guest OS attack in a virtualized data center. But all previous papers have limited to the analysis part instead of practical protocol implementation. To fill this void we have proposed a new authentication protocol for BBU of a C-RAN architecture. Different validation tools validated the protocol after performing the simulation to a number of iteration.

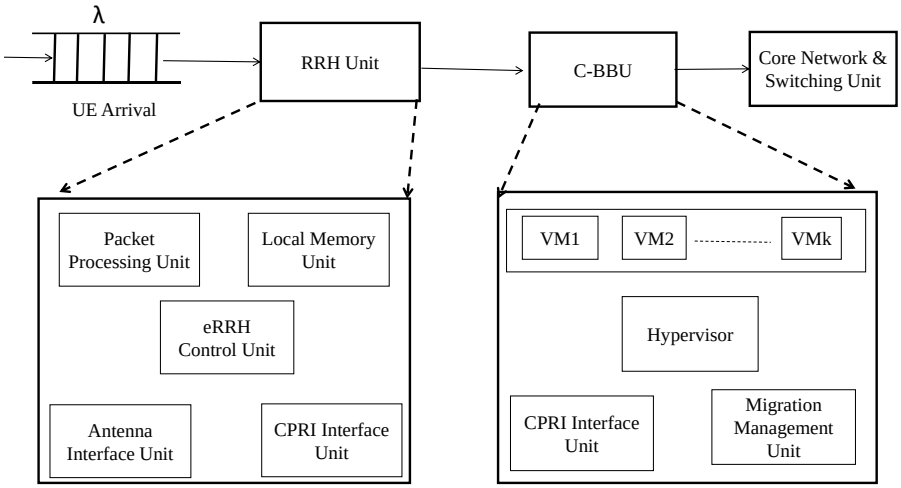

Fig. 1. Architecture of C-RAN

1.1 Architecture of C-RAN:

Based on the functionality the whole architecture of C-RAN is divided into following sub-unit which are as follows:

- *Remote Radio Head RRH:* The RRH is a RF unit which send and resend the Uplink/Downlink signal through a set of RF channel towards the UE and C-BBU.
- *Centralized Base Band Unit C-BBU:*The C-BBU perform all the controlling and signal processing activity in the C-RAN. This unit consists of a number of VM, which are created with the help of a guest operating system (OS). The guest OS or VM are controlled by another application run over a host OS known as hypervisor or virtual machine manager (VMM) as shown in Fig.2.
- *Fronthaul and Backhaul connection:* The Fronthaul and Backhaul are wired or wireless, where the former one is use for signal transmission between RRH and BBU and later one is use for signal transmission between BBU and core network.

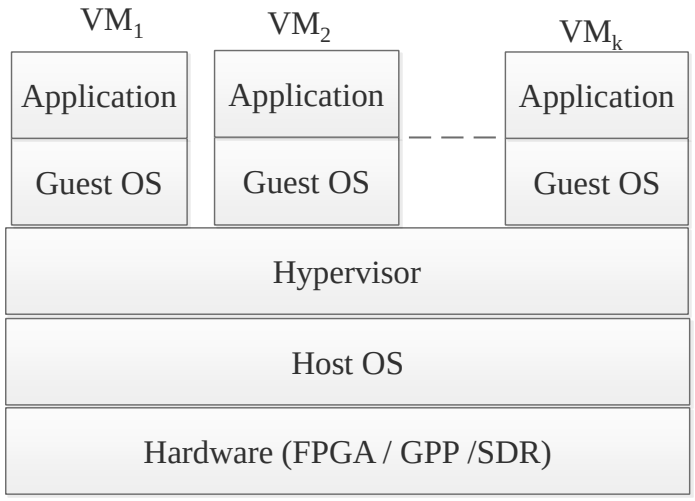

Fig. 2. Layer Architecture Virtualized C-BBU

1.2 Advantage of Virtualization at C-BBU:

The use of virtualization technique at the C-BBU offered many substantial advantage to the RAN world such as:

- **Collaborative Radio Access:** As The virtualized base station V-BS uses a single platform to provide services to different cellular operators interm of infrastructure as a services (IaaS), bring many services to a common platform.
- **Services Isolation:** The use of different VM by the different cellular operators to provide a services isolation between the VM on a single platform. This isolation also provide a secured base band processing without interfering the other VM services:
- **Easy maintenance and fast recovery:** As all the base band signals are processed in one platform at a centralized location it is easy to maintain all the resources with in a short recovery period.
- **Cost effective and secured services:** The centralization brings down different incured cost to a greater extend. Again the introduction of centralized authentication and key agreement protocol simplify the VM authentication process [5, 13].

1.3 Security Challenges in virtualized C-BBU:

The development in virtualization in RAN technology adds many security challenges at the C-BBU. The attacker attacks the hypervisor of C-BBU through either host OS or guest OS. There are various types of attacks are possible at the C-BBU of C-RAN like DDoS attack, man-in-the-middle attack, honeypot attack, and guest-to-guest at both the host and the guest OS. The prime objective of this paper is to find out the different possible attacks and find out the corresponding solutions for this attacks[6, 7]. The different form of attacks at the C-BBU are given as follows:

- *Direct host attack:* In this attack the attacker attacks on the hypervisor by taking the advantage of the vulnerability and security holes present in the host OS. Through this attack attackers main aim is to take control over the hypervisor as well as the host OS [9].
- *Indirect host attack:* In this attack, the hypervisor gets attacked by a unauthorized user, by creating unauthorized VM over a host OS. Due to the effect of compromised VM other VM present in the same host and control by the same hypervisor can also get affected [8].
- *Migration Attack:* This is another form of man-in-the-middle attack. This attack occurs at the C-BBU during the migration of the VM from one host to other. The attacker exploits the security protocol and vulnerability of the network and imposes some malicious code to the target VM. When the affected VM enter the BBU-pool, it compromised the whole system and get access the full resource [11].
- *DoS attack:* In denial-of-service attack the attacker can compromised the hypervisor or host OS by sending large number of VM creation request controlled by fake user. A compromised hypervisor unable to maintain the large number of requests, it will busy only managing the huge requests instead of serving request. This creates an unbalanced resources utilization condition at the BBU-pool [12, 14].

2 Proposed Security protocol and Authentication procedure

As the BBU growth over a datacentric environment with the help of a cloud computing technology, VM and hypervisor security is the prime factor for establishing an end-to-end connection. The proposed PPA protocol preserves the privacy of the VM and hypervisor for proper resources utilization and to increase the quality of services (QoS). Fig.3 shows a complete flow chart for hypervisor key management and BBU utilization in a C-RAN. The whole process is carried out through three different phases:

1. **VM Request Phase:** In VM request phase the user request to the hypervisor to create a VM. The hypervisor analyzed all the circumstances of the host in term of physical resources availability and utilization of each BBU. If the hypervisor found a suitable condition for creating new VM then only it accepts the request and starts the authentication procedure for this new request.
2. **VM Registration and Authentication Phase:** In this phase, the new VM is registered itself to the hypervisor based on the VM allocation policy of the BBU-pool. The registered VM is then authenticated by using our proposed privacy preservation and authentication protocol (PPAP). This proposed protocol has a key distribution center (KDC) for distributing the key among the VMs which are associated with the hypervisor. This KDC authenticates the VM with respect to hypervisor based on the computing challenge response. When the challenge key and the response challenge key of the KDC and VM respectively match each other then the VM authentication process is completed.
3. **Host Utilization Calculation Phase:** After allocating a specific number of VM to the host, the hypervisor each time updates the utilization of the BBU-pool before assigning the new VM to the host. When the host utilization reached a threshold value, the hypervisor will generate an alert message to the host OS to either stop accepting new VM request or perform load balancing by using a load balancing technique. During this period the hypervisor continuously monitoring each VM and host for proper resources utilization and authentication.

3 Propose Protocol for Authentication and Verification

The propose protocol is used for both UE and VM authentication and verification process. The key distribution center (KDC) used the secret key for the authentication process that is shared by KDC to UE and VM.

3.1 Step 1: UE authentication and verification step:

In this step a user requests to create a VM. The hypervisor authenticates the legitimacy of the usre request with the help of a key distribution center (KDC) function. The detail authentication procedure are as follows:

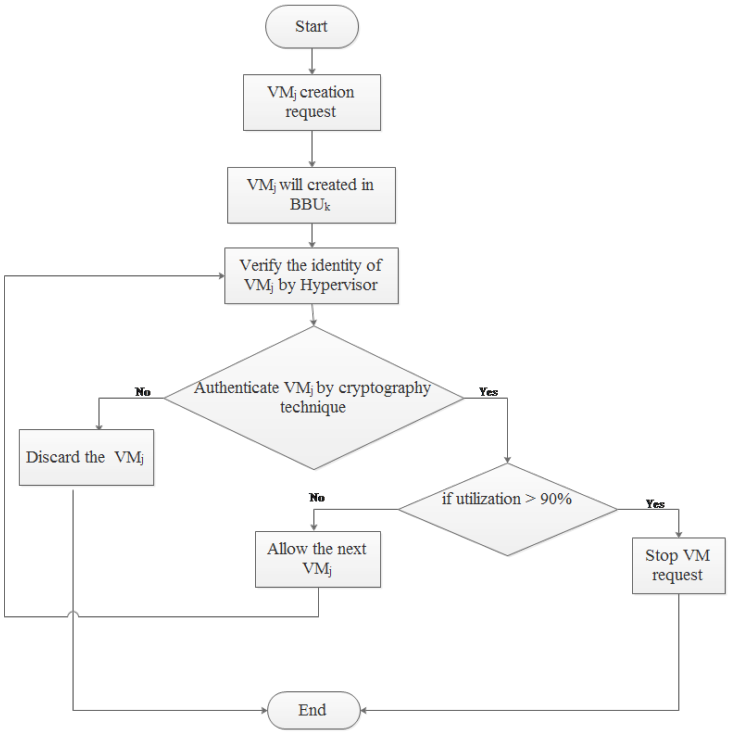

Fig. 3. Architecture of C-RAN

Table 1. Symbols and Abbreviations

Symbols and Abbreviations	
Symbols	Definition
KDC	Key Distribution center
KDF	Cryptographic function (Key Derivation Function)
UE	User entity
HOS	Host Opereting system
VM	Virtual machine
sk	the shared secret key
r	Random number
AUTN	Authentication token (Nonce)
K_{asme}	MME Intermediate key(access security managment entity)
RES/XRES	Response/expected response
CH/RCH	Challenge/responsed challenge

– If UE wants to create the VM, it will send a VM creation request to the host OS with a unique identity UE_{id}.

– After accepting the request from the UE, host OS will verify the legitimacy of the user request and send it to the KDC for the verification of the user request by sending the identities (UE_{id}, HOS_{id}).
– The KDC will accept the request and computes the response for the verification process with the help of secret key, shared between UE and KDC.

$$RES = (r)_{sk}. \tag{1}$$

– After computing the RES, KDC will send it to the host OS with (RES, r, $AUTN$). Where $AUTN$ is the authentication token act as real time nonce for the verification of session.
– Host OS keeps the computed response for further verification process and send (r, $AUTN$) to user.
– After accepting the (r, $AUTN$), UE will also computes the expected response with the help of shared secret key of user and send it to the host OS for verification.
– Now host OS will accept the the expressed responce $XRES$ and verify it with RES

$$If(XRES == RES) \tag{2}$$

Then secret key shared between user entity and KDC is same, it means user is authenticated and will allow to create a VM otherwise it will simply reject the VM creation request.

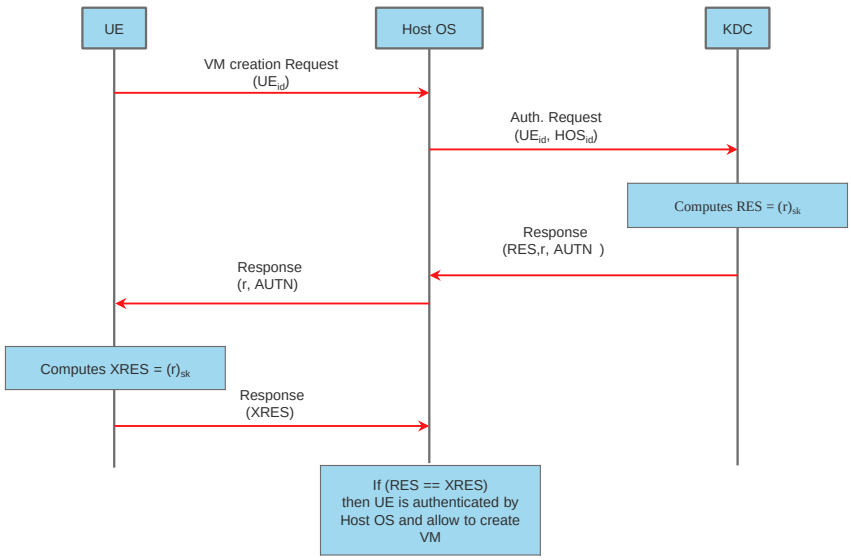

Fig. 4. Protocol for UE Authentication by host OS with a KDC function

3.2 Step2 : VM authentication and verification step:

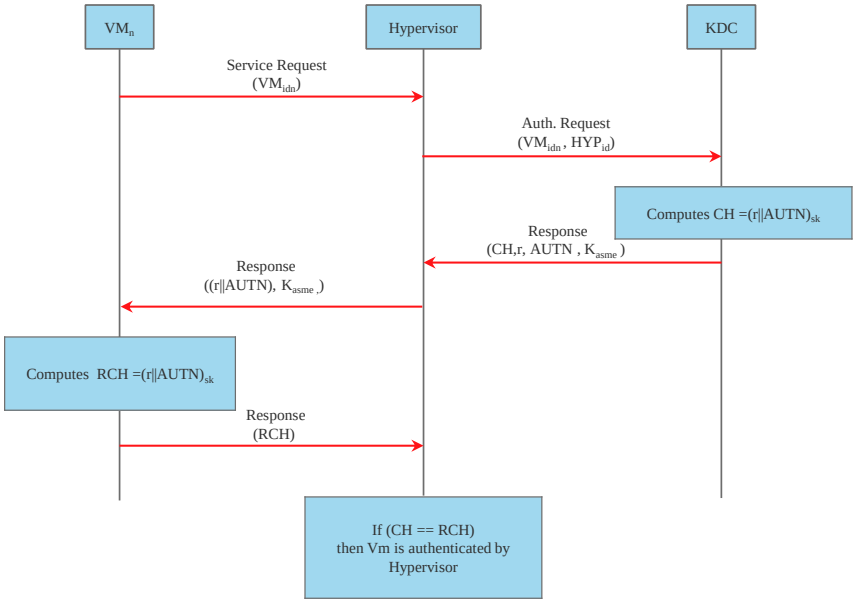

Fig. 5. Protocol for VM Authentication by the host OS with the help of KDC function

After creating the VM, the authentication and key preservation process is carried out by the KDC and associated hypervisor. The authentication process is carried out as shown in Fig.5. The steps are described as follows:

- VM will request for service to the hypervisor by sending identity VM_{idn}.
- After accepting the request from the VM, hypervisor will verify the legitimacy of the VM through the KDC. So it will send the verification request to the KDC by sending the identities(VM_{idn}, HYP_{id}).
- Now KDC will accept the request and computes the response for the verification with the help of secret key shared between VM and Hypervisor and also generate the K_{asme} Calculated for the further process of verification

$$CH = (r||AUTN)_{(sk)}. \tag{3}$$

$$K_{asme} = KDF(sk, HYP_{id}, r). \tag{4}$$

  K_{asme} = Access security management entity used to secure the verification process when CH or RCH gets compromised by attacker.
- After computing the CH, KDC will send it to hypervisor with (r, $AUTN$,K_{asme}, CH).

– Hypervisor keeps the computed challenge CH and send (r, $AUTN$, K_{asme}) to VM.
– After accepting the (r, $AUTN$, K_{asme}), virtual machine will also compute the response challenge and send it to the hypervisor for verification.
– After accepting the RCH, it will verify

$$If(CH == RCH) \tag{5}$$

Then secret key shared between VM and Hypervisor is same, it means VM is authenticated and will grant the service request to the Hypervisor otherwise simply suspend the server request.

3.3 Result and Simulation

We have simulated the proposed protocol in two security tools Automated Validation of Internet Security Protocols and Applications(AVISPA) and SCYTHER for the validation and verification.

– The protocol simulation is carried out with the help of AVISPA tool in a Linux environment, with a system setup of 8GB RAM with a 64 bit OS. The protocol simulation is carried out in following steps[10]. This proposed protocol was tested and validated in two modes of the AVISPA tool i.e. On The Fly Mode (OFMC) and Constraint-Logic-based Attack Searcher (CL-AtSe).

Fig. 6. Simulation result of UE authentication in OFMC back end and CL-atSe back end of AVISPA tool

The protocol simulation is also carried out with the help of SCYTHER tool in a Linux environment. Fig.8, show that the proposed protocol is un-effected by the possible attacks by securing the VMs and its associated hypervisor.

Fig. 7. Simulation result of VM authentication in OFMC back end and CL-atSe back end of AVISPA tool

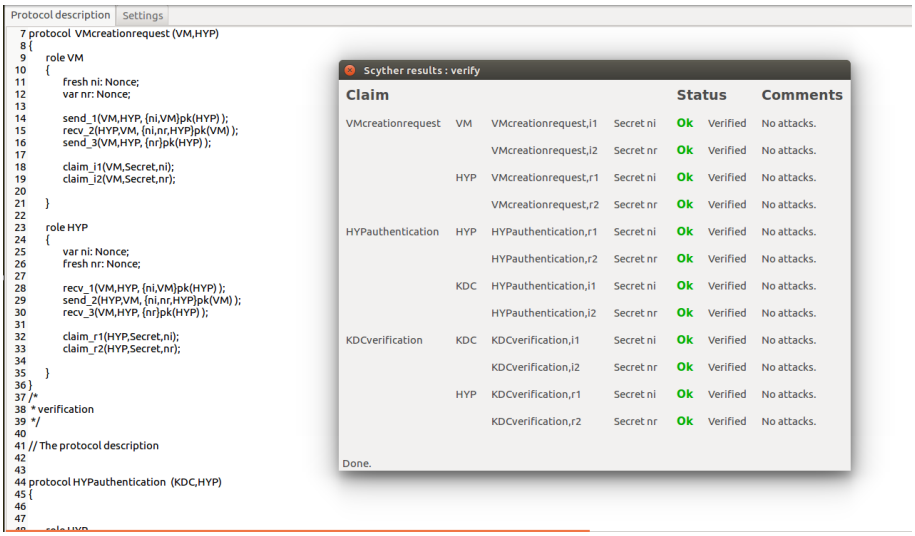

Fig. 8. Simulation result of VM authentication in SCYTHER tool

4 Conclusion

The use of virtualization and cloud computing technology for the radio access network services tremendously increasing for next-generation cellular and data network. As the C-RAN uses a single cloud platform to provide services to many cellular and network operator VM and hypervisor security are the key challenge for infrastructure provider. In this paper, we have described some key security

challenge for the next generation BBU-pool and provided some solution to this challenges. Our proposed protocol is secured and reduces the possible attack to a greater a extend by securing the VM as well as the hypervisor. The proposed protocol can be used for the practical scenario in the BBU-pool.

References

1. Cisco, Visual Networking Index, Global Mobile Data Traffic Forecast Update, 20152020 White Paper(2016).
2. Wu, J., Zhang, Z., Hong, Y. and Wen, Y.: Cloud radio access network (C-RAN): a primer. IEEE Network, **29(1), pp.35-41. (2015)**.
3. Mahapatra, B., Kumar, R., Kumar, S. and Turuk, A. K.: A real time packet classification and allocation approach for C-RAN implementation in 5G network, 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, pp. 1-6 , (2018). doi: 10.1109/RAIT.2018.8389092
4. Tian, F., Zhang, P., and Yan, Z., A Survey on C-RAN Security, in IEEE Access, **vol. 5, pp. 13372-13386, (2017).**
5. Xiao, Z., and Xiao, Y., Security and privacy in cloud computing, Mobile Networks and Applications, **vol. 15, no. 2, pp. 843-859, (2012)**
6. Park, Y. and Park, T.: A Survey of Security Threats on 4G Networks, IEEE Globecom Workshops, pp. 1-6, (2007). doi: 10.1109/GLOCOMW.2007.4437813
7. Bian, K., Park, J.M: MAC-layer misbehaviors in multi-hop cognitive radio networks, US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006), pp. 228-248, (2006).
8. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou, G.: A survey on jamming attacks and countermeasures in WSNs, in IEEE Communications Surveys & Tutorials **vol.11, no.4, pp. 42–56, (2003)**.
9. Hyde, D.: A survey on the security of virtual machines. Dept. of Comp. Science, Washington Univ. in St. Louis, Tech. Rep (2009).
10. Armando, A., Basin, D., Boichut, Y., Chevalier,Y., Compagna,L., Cullar, J., Drielsma, P. H., Ham, P. C., Kouchnarenko, O., Mantovani,M., and Mdersheim, S.: The AVISPA tool for the automated validation of internet security protocols and applications, International conference on computer aided verification, pp. 281–285, (2005). https://doi.org/10.1007/1151398827.
11. Zhang, M. and Jain, R.: Virtualization security in data centers and clouds.(2011), In HTTP://WWW. CSE. WUSTL. EDU/ JAIN/INDEX. HTML
12. Douligeris, C. and Mitrokotsa, A.: DDoS attacks and defense mechanisms: a classification, " Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, pp. 190–193, (2003). doi: 10.1109/ISSPIT.2003.1341092
13. Lin, Y., Shao, L., Zhu, Z., Wang, Q., and Sabhikhi, R. K. : Wireless network cloud: Architecture and system requirements, in IBM Journal of Research and Development, **vol. 54, no. 1, pp. 4:1-4:12, (2010)**.
14. Sonar, K., H Upadhyay, H.: A survey: DDoS attack on Internet of Things. International Journal of Engineering Research and Development, **vol 10(11), pp. 58–63, (2014) .**