Security Threats in Software Defined Mobile Clouds (SDMC)

R. Mythili, and N. Revathi Venkataraman

Abstract– **Future Internet comprises of emerging ICT mega-trends (e.g., mobile, social, cloud, and big data) commands new challenges like ubiquitous accessibility, high bandwidth, and dynamic management to meet the data tsunami requirements. In the recent years, the rapid growth of smartphone business is highly evidenced due to its versatile usage irrespective of location, personality or context. Despite of increased smartphone usage, exploiting its full potential becomes very difficult owing to its typical issues such as resource scarcity, mobility and more prominently the security. Software Defined Networking (SDN), an emerging wireless network paradigm can make use of rich mobile cloud functionalities such as traffic management, load balancing, routing, and firewall configuration over physical abstraction of control planes from data planes. Hence SDN leads to a clear roadmap to Software Security control in Mobile Clouds (SDMC). Further it can be extended to a level of Security prevention. To address in this direction, this paper surveys the relevant backgrounds of the existing state-of-art works to come up with all possible SDMC threats and its countermeasures.**

Index Terms– **Future Wireless Networks, SDMC, Reconfigurable Programming, Security, Threats, Countermeasures.**

I. INTRODUCTION

With the stunning proliferation of mobile devices, the internet users expect ubiquitous connectivity that is remain to be connected anywhere, at any-time and using any device. This has encouraged the service providers to come up with innovative network architectures by incorporating new services. Now, the evolution of the mobile networks almost reaches the fifth generation (5G-Thoeretical).5G technologies expect the delivery of ultra-fast, ultra-reliable network service access. The massive increase of data traffic and connected nodes should be assisted with such services. Emerging technologies such as Software Defined Networks (SDN), Network Function Virtualization (NFV) and Cloud Computing concepts are evolving to address the requirements of these future mobile networks.

The attraction towards the technology Software Defined Networking (SDN) is due to the potential benefits of network management, new network function deployment and network architecture evolvement. And also these benefits could invaluably applied in different networking environments like datacentres, wireless Networks, broadband access networks and campus networks.

Manuscript received March 16, 2016; revised June 6, 2016.

Authors are with the SRM University, India (E-mails: mythili.r@rmp.srmuniv.ac.in, revathi.n@ktr.srmuniv.ac.in).

The explosive growth of smart phones and tablets introduces an inevitable strain on cellular networks, hence experiencing a major network revolution that will shape the design and deployment of networks and its services enormous in numbers for the next decade.

The relentless improvement in cloud capabilities with SDN in Mobile Clouds (SDMC) aims at innovation and development of future converged mobile networks. SDN and NFV [1], [2] combined together leveraging the intelligent services orchestration and dynamic resources management. SDN individually aims at decoupling the networks' control from the data planes. The abstraction of underlying network infrastructure from the control functions is achieved through the logically centralized intelligence network control of SDNs. However, the security needs to be assured and managed in future telecommunication networks depends notably on the introduction of centralized controllers, programmability, the separation of the control and data planes, the introduction of new network functions and even on the new Mobile Virtual Network Operators (MVNO). The future networks' [3] scalability challenges are resolved by providing the Mobile Subscribers with frequent mobility, fine-grained measurement and control, and real-time adaptation.

SDN could give Mobile Operators [4] greater control over their equipment, simplify network management, and introduce value-added services. SDN distributes data-plane rules over multiple, cheaper network switches, reducing the scalability pressure on the packet gateway by can enable carriers and flexible traffic handling. Scalability challenges can be significantly raised with real-time updates to many fine-grained packet handling rules. Forwarding state at individual subscriber level leads to frequent user mobility, and the very fast state change to avoid service disruptions. Fine-grained traffic volume monitoring by switches guarantee to detect when subscribers exceed their usage caps. The QoS network policies [4] must adapt quick data measurement, or transcode content to offer good service during times of congestion. These issues can be addressed by Flexible subscriber policies,
local switch agents, Flexible switch patterns and actions and Remote control of virtualized base-station resources.

The paper describes the roadmap towards the SDMC leveraging SDN technology for uninterrupted services with the Secure Wireless QoS requirements. In section I of this paper, the introduction of SDN in Mobile Clouds with its key benefits & challenges are discussed. In section II, the core concepts of Mobile Cloud Computing (MCC), Software Defined Networks (SDN) and convergence of both as a new inherent view Software-Defined Mobile Clouds (SDMC) is presented. The reference SDMC security architecture with the major security

threats is described in section III of this paper. Moreover Section IV contributes the cogent analysis of various works towards the convergence of future SDMC performance networks. Section V of the study gives the suggestions about the countermeasures of various possible SDMC threats. Finally the last sections conclude all possible SDMC concepts and the future SDMC research challenges for the benefit of early stage motives of this domain of interest.

II. BACKGROUND

A. Mobile Cloud Computing (MCC)

Smartphones became inevitable now-a-days due to the advances in mobile hardware and software which can replace even the tasks of PCs, Digital Cameras & GPS devices also. Apple iphone, Android phones, Blackberry and other latest smartphone users practise the full internet usage, Movies & Other videos, Music and Games. Smartphones also achieve ubiquitous internet access via Clouds along with 3G, 4G/LTE & 5G connections. Built-in cameras, microphones, improved built-in memory capacity including flash and new mobile APPS support the Smartphones to accomplish many interesting sensor-based, location-based GPS applications. The smartphone users made possible on-demand, low cost infrastructure, platforms, and software provided by leading service providers with the Mobile Cloud infrastructure support. Even then, the mobile devices fall of the resource based (Battery life, Storage & Bandwidth) and Communication based (Mobility and Security) challenges. Mobile Cloud Computing (MCC) in computing evolution makes possible to resolve the challenges by integrating mobile computing with Cloud technologies. The Cloud Elasticity Service (CES- Cloud Manager +Application Manager + Cloud Node Manager) and Cloud Fabric Interface (CFI) majorly comprise the MCC Security framework. MCC security threats [Table .IV] can further be classified as threats to mobile devices, threats to cloud platform & application container and threats to communication channels.

B. Software Defined Networks (SDN)

Future Internet comprises of emerging ICT mega-trends (e.g., mobile, social, cloud, and big data) commands new challenges like ubiquitous accessibility, high bandwidth, and dynamic management. Leveraging Software Defined Networking (SDN) leads effective network management and control of all sorts of networks irrespective of size, heterogeneity, and complexity. SDN decouples the network control from the data plane to establish intelligent decision making. Further SDN provisions a convenient platform to do new experimentations with network designs by network programmability. Network abstraction in accordance with security can be achieved through the logical centralization of the network intelligence and state. SDN also provides network security enhancement by means of global visibility of the network state [5], [6]. Hence, the SDN architecture endows networks to actively monitor traffic and diagnose threats hence by facilitating network forensics, security policy alteration, and security service insertion. However the separation of the control and data planes open security challenges [7] like Denial of Service (DoS) attacks, Man-In-Cloud attacks, Flow and Hijacking attacks [Table .IV].

C. Software Defined Mobile Clouds (SDMC)

With the profound complexity of future mobile clouds, more research contributions are needed to resolve the well-known challenges of consistency, replication, unreliability, scalability, availability, portability, security, and privacy. However to attract potential consumers, the service provider has to offer a completely secure environment by targeting all possible security threats. In this regard, a massive amount of work is going on in many research organizations and academia. Still there are some grey areas need to be addressed (i.e.) security and privacy of user's cloud data, security threats by multiple virtual machines, intrusion detection and so on. Proposed cloud security algorithms cannot be directly run on a mobile device due to resource limitations. Hence, researchers are working with the target lightweight security framework, converging towards Software Defined Mobile Clouds (SDMC).

SDN technologies proposed on Mobile Clouds aiming at innovation. The targeted benefit of decoupling the control from data plane [Table. I] can be best effectively utilized, bringing security performance in SDMC. Software decision making logics are deployed on control plane for achieving the required security management. Entire set of services and mobile applications are mapped by the network/distributed operating system in control plane.

D. SDMC APPLICATIONS

In view of the convergence towards future Mobile Networks [8], the popular Mobile operators in the market try to improve their business turnovers. They try to implement the same by information gather of related mobile access networks such as ongoing traffic, bandwidth availability, points of congestion, energy consumption, QoS data, Mobility and most importantly the network vulnerabilities that effects more damages. The gathered network information and the subscriber information related to their profile and behaviour along with the Big Data analysis techniques can provide valuable insights to the network operator for network optimization [Table. I] and innovative personalized applications.

TABLE I.
SDMC APPLICATIONS.

SDMC Application Type	SDN Feature
Directing Traffic through Middle boxes	S/W based Traffic analysis
Monitoring for Network Control & Billing	A Logical centralized controller & view of the N/W
Seamless Subscriber Mobility, Virtual Cellular Operators	Separation of the control plane from the data plane
QoS and Access Control Policies	Dynamic updating & forwarding rules & flow abstraction
Inter-Cell Interference Management	Programmability of the N/W by external applications

An innovative service of multi-screen customization and adaptability can be enabled by the Mobile Service Providers by leveraging the connection prioritization, audio/video

transcoding and quality selection. The network services could also consider the present network conditions, channel information, user profile and devices properties among many other data. SDMC could utilize the following list of Open source tools for deployment of applications, services[Table .II].

TABLE II.
SDMC – OPEN SOURCE TOOLS

Type of the Tool	Name of the Tool
Emulation & Simulation	Mininet,NS-3
Software Switch Platforms	OpenFlow, OpenVswitch,Indigo,OpenWRT
Native SDN	NetIron,Rackswitch,Junos
Controller Platforms	NOX,Open Daylight Floodlight,Beacon,Nodeflow,Flowvisor,Routeflow
Code Verification & Debugging	NICE,Anteater,OFRewind,Wireshark

III. SDMC –REFERENCE SECURITY THREAT MODEL

Leveraging the benefits of logical centralization & separation of control from data plane in Mobile Clouds, SDMC introduces the programmability of security policy automations. SDMC can also respond to the run time network anomalies and spurious traffic conditions. To elaborate these SDN features, the reference SDMC security architecture [Fig.1] constitutes the important functional components as follows:

(1) ***Forwarding Devices:*** Switches, Routers, Virtual Switches, Wireless Access Points are mentioned to be some popular forwarding devices. To achieve high performance SDMC, the issues related to forwarding device to be resolved may be additional flow table entries, buffer space, statistical counters, minimized rules, Optimized routing, packet latency and throughput under diverse load conditions.

(2) ***Controller:*** It is defined as the programmatic interface to the network for implementing network management tasks and offering new functionalities. The layering abstractions are described by the control models. The different controller approaches which can be used are:

- Centralized Vs. Decentralized
- Control Granularity
- Reactive Vs. Proactive policies

The controller related problems are scalability, failure & recovery, QoS in flow-based control, traffic overheads, policy managements etc.

(3) ***Southbound Interface:*** This is the important SDMC component which links the data and control planes. It should always be available and secure. It has to be supported with encrypted transport layer security communication and a certificate exchange between the switches & the controller. There is no exact implementation, granting partial permissions and certificate format currently specified.

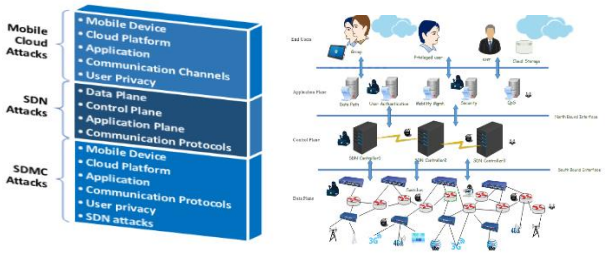

Fig. 1(a) **Fig. 1(b)**

Fig 1. (a) SDMC – Reference Security Threat Model
(b) SDMC – Reference Security Architecture

(4) ***Northbound Interface:*** Communication between controllers/ controller-service to extract the network information & control the network behaviour/policies. There is no standard northbound interface available.

(5) ***Communication Protocols:*** To improve the standard of SDMC, standard communication mechanisms, interfaces and protocols are required.

TABLE III.
SDN PLANES/INFORMATION SECURITY SERVICES

SDN Attack Plane	Availability	Authentication	Authorization	Confidentiality	Integrity
Application	✓	✓		✓	
Northbound	✓	✓		✓	
Control	✓	✓	✓	✓	✓
Southbound	✓	✓	✓	✓	✓
Data			✓	✓	✓

Table. III describes the SDN planes/Information security services for further research considerations. The gathered information of both Mobile Cloud and SDN implementation related attacks will sure support the associated researchers in the similar domains for their expected Wireless QoS achievements.

IV. RELATED WORKS

Recently the mobile population increases as the need of ubiquitous computing everywhere we go. Although the Mobile clouds are preferable in these aspects due to their benefits of low-cost cloud resources, they always suffer by the major drawbacks of Battery, Storage, Bandwidth and Security vulnerabilities. Hence an resource effective technology has to adopted to solve these issues to still improve the Mobile Cloud performances. Now-a- days, SDN becomes the most tuned solution for the future generation mobile computing. The separation of control planes from data planes can be effectively focused for the purpose of overcoming security threats in SDN based Mobile Clouds (SDMC).This section supports in elaborating the various state-of-art works described relevant to the focus [Table .IV].

The state-of-art works includes overview of Mobile Cloud features, Security services at different layers [9], a privacy-aware secure cross-layer reputation [10], a new virtualized mobile cloud service [5] along with provisioning &

configuration. Zhijie Wang, Dijiang Huang proposed a novel distributed Privacy-Preserving Mobile Access Control (DP-MAC) with scalability compromises [11] in which a dual-root model was leveraged to prevent identity theft in case of Mobile device loss. It is also suggested about the Single-Point of Failure (SPOF) attacks through dynamic policy updations by service provider and no records of shared secrets of certificates of Identity Provider. One of the innovative ideas of monitoring & detecting abnormal Mobile Cloud user behaviour is elaborated in [12].

SDN survey of latest developments, three-layer architecture & some open challenges were suggested by Wenfeng Xia, Yonggang Wen in their work [13].Many researchers concentrated the applications of SDN technology in various network control activities in their specific projects. Roberto Bifulco, Ghassan O. Karame suggested a new SDN path towards richer set of services [14] which makes possible of secure location for registered network users. Network control can also have an impact by packet classification through dynamic routing [15] and genetic algorithm based Deep Packet Inspection (DPI) [16]. But it has to be made adoptable for future IPV6 compatible (i.e.) optimized memory access to maximize network traffic throughput. [5] justifies the role of Network traffic, Low variation Passive of state collection and High variation Active of state activity. New protocol namely Application Layer Traffic Optimization (ALTO) [6] can also be practiced to adopt the network abstraction of a large class of rendezvous services. Also possible to establish Network abstraction using management patterns for individual resilience services. It has to be verified for OpenFlow applications with the MiniNet emulator. An alternate architecture iSTAMP[17] proves the highest influence on estimation accuracy by a MAB based flow sampling algorithm.

Most of the comprehensive reviews show that the SDN can most successfully utilize its architectural benefits to enhance the network security of prevention, detection & innovative reactions to threats. On one hand, SDN can be constructively used for enhanced network management but on the other hand the separation of control from data plane itself introduces vulnerabilities into the system [18], [19], [20] and [21]. Analysis of the various threats on all three planes Application, Control & Data and countermeasures [22] are effectively done under ITU-T recommendations for further improvements. Specifically Controller specific issues are discussed in [8]. Hu Yan Nan, Wang Wen Dong were studied the issues of control traffic protection in SDNs and developed a control traffic protection scheme [23] by combining both local rerouting and constrained reverse path forwarding. SDN also being powerful in clouds also with unique extensions like multiple controllers[24], leveraging new protocols of Host Identity Protocol(HIP) & IPSec tunnelling[25],two-level hierarchical SDN/ OpenFlow control plane[26] and specific security issues of Software Defined Mobile Networks(SDMN)[27].

The research community of both academia & industry are trying all possible dimensions to resolve the future internet issues like Ossification, Traffic tsunami. The major obstacles related to the deployment of IPv6 and the IP multicast service difficulties [28] which are addressed are also much useful. It is evidently clear that the future internet requires the technology evolution [29] on capacity, ubiquity and traffic integration of real & virtual worlds. An alternate innovative technology of Follow-Me-Cloud [30] is introduced for better interworking between mobile core network and packet data network. Recent work by Mehiar Dabbagh[31] introduces a new profile-based routing path scanning to minimize the number of probes and the scanning time.

TABLE IV.
SDN-BASED SECURITY MECHANISMS

Reference Nos.	Description
[9],[10], [11] and [12]	Mobile Cloud Security & Privacy issues
[8] ,[21] [43] and [48]	SDN-Security Vulnerabilities & its impact
[22]	SDN plane attacks & Countermeasures
[8],[26]	SDN Controller specific issues
[23]	Traffic control protection in SDNs
[24]	Multiple Byzantine-Resilient SDN controllers
[25]	Leveraging HIP & IPSec protocols
[27]	Security issues in SDN based Mobile Networks
[8] ,[28], [29],[30] and [31]	Future SDN-converged networks
[32] ,[33],[34],[35] and [36]	SDN-based DDoS survey mechanisms
[37],[38],[39],[40] and [41]	SDN-based IDPS
[42],[43] ,[47],[48] and [49]	Popular SDN platform tools

Due to rapid growth of network infrastructure, the most prominent threats of DDoS attacks have been increasing day-by-day. It is of course essential that the DDoS attacks have to be prevented before it happens. DDoS mitigation works exploit the general characteristics and new trends of DDoS in cloud environments [32]. Advanced recent works show some improvements like graphical Bayesian model based DDoS attack detection with dataset shift problems [33], a buffer prioritizing attack solution for controllers namely FlowRanger[34] ,Botnet based network security solutions[35] and defense mechanisms of DDoS flooding[36], sniffer[37] & NFV[38]. Currently the network research community also provisions some anomaly detection systems [39], [40], [41] which will surely strengthen the network domain.

Emerging new network paradigm of SDN has some noteworthy tools to deploy the portable applications. Existing State-of-art papers give the real time demonstration of the popular SDN platforms of GNS & MiniNet[42], Openflow[47],[48], OpenSec[43] and list of some other SDN Switches & Controllers in the market[49]. All of them give material resources [Table .IV] for the SDMC researchers to upgrade their skills.

V. SDMC SECURITY - FUTURE DIRECTIONS

SDN technologies empowers the predominant role in establishing secured wireless networks of Smartphone lifestyle

today (LTE), in the way proper network management and monitoring.

The capacity bottleneck problem of legacy cellular systems can potentially be solved by Device-to-Device (D2D)[30] communication, while it should be flexible and powerful to meet the commercial cellular needs as well as public safety applications.

Due to the separation of the planes, aggregating the control functionality to a centralized system, the Mobile cloud is prone to many new security challenges (i.e.) masquerading attacks.

The Application plane can be affected by the various issues of authentication, authorization, access control and fraudulent security policies. The Control plane is more vulnerable to security attacks like DoS, DDoS, Controller hijacking, Scalability or Availability. The Data plane may react to forge rules, Flooding or Controller-Switch masquerading. The South-bound Interface is inherent mostly to TCP and Man-In-Cloud attacks. The North-bound Interface may have influence on illegal controller and policy manipulations and fraudulent rule insertions [Table .V].

TABLE V.
POSSIBLE SDMC SECURITY THREATS

Security Classification	Types of Threats	Description
Mobile Cloud Threats	Mobile Device Mobile Application Cloud Platform Communication Channels User privacy	Device theft, Virus Attacks, Misuse of Access Rights, DDoS Attacks ,Integrity Standards, Authentication, Legal provisions, Service Incompatibility, Cloud Data Encryption & Decryption, Sensitive Data Marking Model, Data theft risks, Data Access violations
SDN Implementation Threats	Data Plane Control Plane Application Plane Communication Protocols	Flow Table Attacks, Inference Attacks, Device Attacks, Malicious Code Injection, SDN Controller Attacks, Topology/Routing Attacks, DDoS Attacks, Application Threats, TLS/SSL Attacks, IP Spoofing, Man-In-Cloud Attacks, False Rule Injections, Replay attacks, Packet encryption & tunnel bypassing
Software Defined Mobile Cloud(SDMC) Threats	Mobile Device Mobile Application Cloud Platform Communication Channels User privacy SDN Plane Attacks	Misuse of Access Rights, DDoS Attacks ,Integrity Standards, Authentication, Legal provisions, Service Incompatibility, Cloud Data Encryption & Decryption, Sensitive Data Marking Model, Data theft risks, Data Access violations, Flow Table Attacks, Inference Attacks, Device Attacks, Malicious Code Injection, SDN Controller Hijacking Attacks, Topology/Routing Attacks, Application Threats, TLS/SSL Attacks, IP Spoofing, Man-In-Cloud Attacks, False Rule Injections, , Replay attacks, Packet encryption & tunnel bypassing

DDoS Attacks: Among all the threats, DDoS attacks are becoming more prevalent in Mobile Clouds. The DDoS attacks result in availability issues due to flooding, amplification, protocol exploiting, and malformed/ sniffed packets. On one hand, the SDN capabilities like software based traffic analysis, logical centralized control global network view, and dynamic forwarding rules updation make it easy to detect and to react to DDoS attacks rapidly.

With the exhaustive survey, the future of heavy Mobile Cloud Security may fall into the following aspects:

- ✓ **Antivirus as an Off-Device Cloud Service**
- ✓ **Intrusion Detection as Offload Service**
- ✓ **Anomaly-based Detections & Prevention**
- ✓ **Lightweight Mobile Agents**
- ✓ **Enhanced Security Policies**
- ✓ **Device-to-Device Communication**
- ✓

VI. CONCLUDING REMARKS

TABLE VI.
POSSIBLE COUNTERMEASURES FOR SDMC THREATS

Security Classification	Types of Threats	Description
Mobile Cloud Threats	Mobile Device Mobile Application Cloud Platform Communication Channels User privacy	Device theft, Virus Attacks, Misuse of Access Rights, DDoS Attacks ,Integrity Standards, Authentication, Legal provisions, Service Incompatibility, Cloud Data Encryption & Decryption, Sensitive Data Marking Model, Data theft risks, Data Access violations
SDN Implementation Threats	Data Plane Control Plane Application Plane Communication Protocols	Flow Table Attacks, Inference Attacks, Device Attacks, Malicious Code Injection, SDN Controller Attacks, Topology/Routing Attacks, DDoS Attacks, Application Threats, TLS/SSL Attacks, IP Spoofing, Man-In-Cloud Attacks, False Rule Injections, Replay attacks, Packet encryption & tunnel bypassing
Software Defined Mobile Cloud(SDMC) Threats	Mobile Device Mobile Application Cloud Platform Communication Channels User privacy SDN Plane Attacks	Misuse of Access Rights, DDoS Attacks ,Integrity Standards, Authentication, Legal provisions, Service Incompatibility, Cloud Data Encryption & Decryption, Sensitive Data Marking Model, Data theft risks, Data Access violations, Flow Table Attacks, Inference Attacks, Device Attacks, Malicious Code Injection, SDN Controller Hijacking Attacks, Topology/Routing Attacks, Application Threats, TLS/SSL Attacks, IP Spoofing, Man-In-Cloud Attacks, False Rule Injections, , Replay attacks, Packet encryption & tunnel bypassing

The fantasy of Mobile Clouds attracts everyone to experience the resource-sensitive infrastructure with the notable security limitations. In this paper, research aspects of SDN & Mobile Cloud concepts, Security reference architecture, SDMC programming tools, analysis standards of existing security works in the relevant objective are sequenced in way to be useful for building future programmable wireless networks. Through this exhaustive survey, it is seemingly disparate that the SDN technologies can be beneficial in the domain of Mobile Cloud Security in various dimensions like Security threats, Other Vulnerabilities and Attacks specifically DDoS [Table .VI].

More and more security prevention works to be established in SDMC based on the network measures to achieve the required QoS. The survey leaves the identified security paths in the future domain of Software Defined Mobile Clouds and possible paradigm changes that could be implemented for the uninterrupted, high performance wireless QoS achievements.

REFERENCES

[1] Tao Chen, MarjaMatinmikko, "Software Defined Mobile Networks: Concept, Survey, and Research Directions", IEEE Communications Magazine, November 2015.

[2] Malla Reddy Sama, Luis M. Contreras," Software-Defined Control of the Virtualized Mobile Packet Core", IEEE Communications Magazine, February 2015.

[3] Ian Ku, You Lu, Mario Gerla," Software-Defined Mobile Cloud: Architecture, Services and Use Cases",IEEE,2014.

[4] XU Xiaodong, ZHANG Huixin,"SDN Based Next Generation Mobile Network With Service Slicing and Trials", China Communications, February 2014

[5] Mohamed Aslan and Ashraf Matrawy,"On the Impact of Network State Collection on the Performance of SDN Applications", Ieee Communications Letters, Vol. 20, No. 1, January 2016

[6] Vijay K. Gurbani, Michael Scharf,"Abstracting network state in Software Defined Networks (SDN) for rendezvous services", Software Defined Networks, p 6627-32.

[7] Adnan Akhunzada, Ejaz Ahmed," Securing Software Defined Networks:Taxonomy, Requirements, and Open Issues", IEEE Communications Magazine • April 2015

[8] Wei Tan, Jinfang Zhang," SDN-Enabled Converged Networks",IEEE Wireless Communications, December 2014

[9] Abdul Nasir Khan, M.L. Mat Kiah," Towards secure mobile cloud computing: A survey", Elsevier- Future Generation Computer Systems 29(2013) 1278-1299.

[10] Hui Lin, Li Xu, "A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing", Elsevier- Future Generation Computer Systems (2014)

[11] Zhijie Wang, Dijiang Huang, "Towards Distributed Privacy-Preserving Mobile Access Control", Globecom 2014 - Communication and Information System Security Symposium

[12] Taehyun Kim, YeongrakChoi,"Monitoring and Detecting Abnormal Behavior in Mobile Cloud Infrastructure', 2012 IEEE/IFIP 3rd Workshop on Cloud Management

[13] Wenfeng Xia, Yonggang Wen,,"A Survey on Software-Defined Networking", IEEE Communication Surveys & Tutorials, Vol. 17, No. 1, First Quarter 2015.

[14] Roberto Bifulco, Ghassan O. Karame,"Towards a Richer Set of Services in Software-Defined Networks", http://dx.doi.org, 2014

[15] K.GuerraPerez, X.Yang, "Optimized Packet Classification for Software-Defined Networking", IEEE ICC 2014 – Communication and Information Systems Security Symposium.

[16] Mathieu Bouet, J´er´emieLeguay and Vania Conan, "Cost-based placement of virtualized Deep Packet Inspection functions in SDN", 2013 IEEE Military Communications Conference.

[17] Mehdi Malboubi, Liyuan Wang,"Intelligent SDN based Traffic (de)Aggregation and Measurement Paradigm (iSTAMP)",IEEE Conference on Computer Communications,2014

[18] Syed Taha Ali, Vijay Sivaraman,"A Survey of Securing Networks using Software Defined Networking", IEEE Transactions On Reliability.

[19] Mehiar Dabbagh, Bechir Hamdaoui "Software-Defined Networking Security: Pros and Cons", IEEE Communications Magazine, June 2015.

[20] Lisa Schehlmann, Sebastian Abt," Blessing or Curse? Revisiting Security Aspects of Software-Defined Networking", IFIP,2014.

[21] Zhaogang Shu1 & JiafuWan,"Security in Software-Defined Networking: Threats and Countermeasures",Mobile Netw Appl, Springer ,Jan 2016.

[22] Ijaz Ahmad, SunethNamal," Security in Software Defined Networks: A Survey", IEEE Communication Surveys & Tutorials, Vol. 17, No. 4, Fourth Quarter 2015.

[23] HU YanNan, WANG WenDong," On the feasibility and efficacy of control traffic protection in software-defined networks", SCIENCE CHINA-Information Sciences, December 2015, Vol. 58 120104:1–120104:19

[24] He Li, Peng Li," Byzantine-Resilient Secure Software-Defined Networks with Multiple Controllers in Cloud", IEEE Transactions On Cloud Computing, Vol. 2, No. 4, October-December 2014.

[25] Madhusanka Liyanage, IjazAhmad,"Security for Future Software Defined Mobile Networks" in framework of the CELTIC project CP2012 SIGMONA.

[26] Abdelkader Aissioui, Adlen Ksentini ," Toward Elastic Distributed SDN/NFV Controller For 5g Mobile Cloud Management Systems", IEEE Access Special Section Editorial,Vol 3, 2015

[27] Min Chen, Yongfeng Qian," Software-Defined Mobile Networks Security", Mobile NetwAppl(Springer), Jan 2016 , DOI 10.1007/s11036-015-0665-5

[28] Akram Hakiri ,Aniruddha Gokhale,"Software-Defined Networking: Challenges and research opportunities for Future Internet", Elsevier-Computer Networks 75(2014) 453-471.

[29] Antonio Marcos Alberti," A conceptual-driven survey on future internet requirements, technologies, and challenges", J BrazComputSoc (2013) 19:291–311

[30] Tarik Taleb, "Toward Carrier Cloud: Potential, Challenges, and Solutions", IEEE Wireless Communications, June 2014
[31] Mehiar Dabbagh, NaoumSayegh, "Fast dynamic internet mapping", Elsevier- Future Generation Computer Systems 39(2014) 55-66
[32] Qiao Yan, F. Richard Yu," Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE Communications Surveys & Tutorials, Vol. 18, No. 1, First Quarter 2016.
[33] Bing Wang ,Yao Zheng, "DDoS attack protection in the era of cloud computing and Software-Defined Networking", Computer Networks 81 (2015) 308–319
[34] Lei Wei, Carol Fung, "FlowRanger: A Request Prioritizing Algorithm for Controller DoS Attacks in Software Defined Networks", Communications(ICC),June 2015.
[35] Nazrul Hoque, Dhruba K Bhattacharyya ,"Botnet in DDoS Attacks: Trends and Challenges", 10.1109/COMST.2015.2457491, IEEE Communications Surveys & Tutorials.
[36] Saman Taghavi Zargar, James Joshi," A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS)Flooding Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013.
[37] Pin-Jui Chen, Yen-wen Chen, "Implementation of SDN Based Network Intrusion Detection and Prevention System", The 49th Annual IEEE International Carnahan Conference on Security Technology
[38] Ying-Dar Lin, Po-Ching Lin,"An Extended SDN Architecture for Network Function Virtualization with a Case Study on Intrusion Prevention", IEEE Network, May/June 2015.
[39] Syed Akbar Mehdi, Junaid Khalid,"Revisiting Traffic Anomaly Detection Using Software Defined Networking", Springer, 2011.
[40] K. Giotis, C. Argyropoulos, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments", Elsevier-Computer Networks 62(2014) 122-136.
[41] Tsung-Huan Cheng, Ying-Dar Lin," Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems", IEEE Communications Surveys & Tutorials, Vol. 14, No. 4, Fourth Quarter 2012.
[42] Ivan Grgurevic, ZvonkoKavran," Simulation Analysis of Characteristics and Application of Software-Defined Networks".
[43] Adrian Lara Byrav Ramamurthy," OpenSec: Policy-based Security Using Software-defined Networking", DOI 10.1109/TNSM.2016.2517407, IEEE Transactions on Network and Service Management, Globecom 2014 - Communication and Information System Security Symposium
[44] Paul Smith, Alberto Schaeffer-Filho, "Management Patterns: SDN-Enabled Network Resilience Management",EU-funded PRECYSE(www.precyse.eu) & SECCRIT (www.seccrit.eu) projects,IEEE,2014.
[45] He Li, Peng Li , "MoRule: Optimized Rule Placement for Mobile Users in SDN-enabled Access Networks", Globecom 2014 - Wireless Networking Symposium
[46] Mianxiong Dong, He Li, "Rule Caching in SDN-Enabled Mobile Access Networks", IEEE Network, July/August 2015
[47] Masayoshi Kobayashi, Srini Seetharaman, "Maturing of OpenFlow and Software-defined Networking through deployments", Elsevier-Computer Networks 61(2014) 151-175.
[48] Idris Zoher Bholebawa, Rakesh Kumar Jha," Performance Analysis of Proposed OpenFlow-Based Network Architecture Using Mininet", Wireless PersCommun(Springer),July 2015,DOI 10.1007/s11277-015-2963-4
[49] Ivan Pepelnjak," OpenFlow and SDN" @ ipspace.net,NIL Data Communications.

R. Mythili is presently working as an Assistant Professor and pursuing Ph.D at SRM University, India. She has been in academia since from 1999. Her research interests include Cloud Computing, Wireless Security and Software Defined Networking. She started her research on Cloud Computing, slowly converged to current SDN based Mobile Clouds and Security. She is currently working papers on SDN based Mobile Clouds.

N. Revathi Venkataraman is currently working as a Professor at SRM University, India. She received her PhD in Computer Science and Engineering from SRM University in 2013. Her research interests include wireless networks and security, trust computing, wireless ad hoc and sensor network testbed developments which are ongoing research activities funded by Indian Government.