Cloudification and Security Implications of TaaS

Mehrnoosh Monshizadeh
Nokia Research, Finland
Department of Comnet, Aalto University, Espoo, Finland
mehrnoosh.monshizadeh@nokia.com
mehrnoosh.monshizadeh@aalto.fi

Zheng Yan
The State Key Lab of ISN, Xidian University, Xi'an, China
Department of Comnet, Aalto University, Espoo, Finland
zyan@xidian.edu.cn
zheng.yan@aalto.fi

Leo Hippeläinen, Vikramajeet Khatri
Nokia Research, Finland
leo.hippelainen@nokia.com
vikramajeet.khatri@nokia.com

***Abstract*—Cloud computing has got attention of telecommunications operators as a potential cost saver, because it enables sharing computing resources within network infrastructure and between operators. The concept of Telecommunications network as a Service (TaaS) has been proposed as a renovation direction of mobile operators. However, information security which is one of the major challenges of the cloud computing should be seriously investigated and discussed in order to realize TaaS in practice. For this purpose, we review new threats introduced by TaaS and discuss prevention mechanisms to resist them. Based on the cloud deployment model, we further propose a security framework, "Cloud Security Framework for Operators (CSFO)" in order to support TaaS. We also go through open research issues about security related to TaaS and propose future research focus.**

Keywords— Cloud computing, IaaS, PaaS, SaaS, TaaS, SDN, NFV, SLA, CSFO.

I. INTRODUCTION

Due to the vital role of mobile operators in providing Internet services and the fast growth of cloud computing technology, mobile operators have considered reforming themselves as one of the cloud providers for networking services. Telecommunications Service Providers (TSP), especially Mobile Network Operators (MNO) have invested huge amount of resources on maintenance and expansion of their infrastructures while cloud providers such Amazon and Google selling their services at the expense of telecom operators.

A physical mobile network can host several network operators called Mobile Virtual Network Operators (MVNOs). Each MVNO can have its own support systems or they may become customers of a mobile virtual network enabler (MVNE). An obvious development is to implement MVNE services using cloud computing.

Since November 2012 European Telecommunications Standards Institute (ETSI) has hosted industry specification group for Network Function Virtualization (NFV). The idea is to apply mainstream IT virtualization technologies to specify standardized network elements, which can be run in a cloud service and can be used as building blocks to create communication services [1]. This would enable cloud based centralized network elements, which are logically separate per each MVNO, but can share software and still use operator specific data.

Both MNVE and NFV can be considered to run mostly on cloud layers. We can also call it as an applied platform for telecommunications, which provides Telecommunication network as a Service (TaaS).

Obviously, the mobile operators can benefit from cloudification by sharing physical resources. The new technology can also make easier for new companies to enter not only telecommunications service provider market place but also as software vendor for virtualized network functions and perhaps also as cloud service provider. On the other hand with the help of network data intelligence, the operators could share the critical information (like customer segmentation) with third parties (with privacy preservation) to extend their business in order to gain additional profits.

The cloudification of mobile operators may introduce several advantages, but security is still one of the biggest challenges. Due to resource sharing, a disturbance or cyber attack (data leakage and data corruption) can spread to harm several seemingly separate mobile operators. A bad apple in the basket should not spoil others. Although traditional prevention mechanisms such as backup-recovery, encryption, Intrusion Detection System (IDS), IPSec and secure protocols can be used, we still need to confront new security challenges for implementing TaaS [2].

In this paper, we review new threats introduced by TaaS and discuss prevention mechanisms to resist them. Based on the cloud deployment model, we propose a security framework, Cloud Security Framework for Operators (CSFO) in order to achieve TaaS security. We also go through open research issues about security related to TaaS and propose future research trends.

The rest of the paper is organized as follows. Section 2 briefly reviews related work. We introduce the concept of cloudification of mobile operators and present a new part TaaS in cloud architecture in Section 3. In Section 4, we discuss the security challenges of TaaS. In Section 5, we discuss TaaS deployment and propose a framework to mitigate deployment security. In Section 6, we further discuss current open issues along with suggestions on future research trends. Finally, conclusion is presented in the last section.

978-1-4799-9907-1/15/$31.00 ©2015 IEEE

DOI : 04.IJIS.2015.1.5

II. Related Work

Suo et al. [3] recommended incorporating current security technologies including authentication, access control and encryption in the cloud platform to avoid any attacks. They also highlight the need for backup and restore functionality to restore the data of both networks and users in case of any unexpected failure. They suggest using behavioral authentication in contrast to traditional authentication with credentials, certificate or key based authentication.

Scott-Hayward et al. [4] have done a survey on Software Defined Network (SDN) security. A centralized controller in the SDN infrastructure can be a target of Denial of Service (DoS) attack. Thus, Transport Layer Security (TLS) should be used for the communications between switches and control planes. This study recommended using a middle box approach where traffic from the control plane should be directed and a dynamic security policy should be enforced on all flows to avoid any fraudulent flows. One proposed mechanism is comparing the security authorization of providers of new rules with the conflicting rule providers and make a decision whether to pass such a flow or not.

Nokia whitepaper [5] recommends mutual authentication and firewall (FW) to be used in all Virtual Machines (VMs), and encryption as per need. In order to prevent VM images from being compromised, software signature and trusted boot concepts should be utilized. Infrastructure and hypervisor must be hardened, secure Application Programming Interface (API) techniques must be used at northbound API in SDN, and IPSec or TLS should be used at controller-switch communication to avoid DoS attacks in SDN. Considering the adoption of SDN and NFV in a cloud environment, the white paper suggested applying all possible security measures. However the security requirements for each individual layer are not discussed.

Alcatel-Lucent whitepaper [6] recommends security mechanisms including hypervisor introspection and centralized security management for NFV deployment. Depending on the deployment model, identity and access management, security zones, FWs, hypervisor introspection and hardening must be applied to prevent unauthorized access. Regarding DoS attacks, virtual load balancers and virtual Domain Name System (DNS) servers should be utilized. A secure key storage should be provided using specialized Hardware Security Models (HSM) so it is not accessible and visible by third-party virtual Network Functions (vNF). Various security aspects for NFV were discussed in this paper, but security requirements for each layer in cloud are not discussed.

Recent Celtic Plus project SEED4C has developed secure cloud demonstration prototypes based on a network of hardware secure elements and hardened virtual machines. SEED4C proposes computer aided security modeling, automated deployment of security settings to the target system, run-time enforcement of security policies on top of mechanisms available on the target VM (e.g., SE Linux or iptables) and automated security assurance. The primary solution to create secure system is to deny all connections unless explicitly allowed. In order to create more trust, there is an automatic and continuous testing of the security measures and reporting if a problem is found. Secure logging and anomaly detection are used as a last defense line, which detect intruders if they somehow manage to pass though the primary protections. SEED4C proves that model based security design is doable and can be translated automatically to run-time configuration. However, neither SEED4C systematically list attack scenarios nor provides solutions to protect services against each attack scenarios [7].

ETSI NFV has a working group focusing on security problems. They have categorized security issues to host security, infrastructure security, virtualization network function (VNF) / tenant security, trust management and regulatory concerns. Their work covers many if not all aspects of the domain [8].

Schoo et al. [9] applied homomorphic cryptography, policy enforcement and anomaly detection for protection of cloud content. The security in cloud as general was discussed in this paper without considering security requirements for each layer.

Modi et al. [10] surveyed security challenges and solutions at different layers of cloud. Several types of attack such as DoS, man-in-the-middle, metadata spoofing, phishing and backdoor channel on VMs and hypervisor are discussed. Also prevention and detection techniques such as IDS/IPS for spam identification, FW for authentication and authorization, secure APIs and protocols e.g., Secure Sockets Layer (SSL) and VM isolation are recommended solutions in this paper.

Ali et al. [11] carried out a survey regarding security issues in cloud computing and its mitigation solutions. In this paper author concentrated mostly on the hypervisor and virtualization challenges such as misconfigurations, VM image sharing, VM escape and so on. Later on, they explained how discussed risk could lead to unauthorized access (e.g. man-in-the-middle, IP-spoofing) or malicious attacks (e.g. DoS).

Most of the related work covers security requirements of cloud as a general, and only few cover security requirements at each layer of cloud but none of them cover the security requirements for TaaS.

III. Cloudification Of The Network Operators

According to National Institute of Standard and Technology (NIST) [12], cloud computing is a process to enable on-demand access to a shared pool of configurable resources such as storage, applications and services, which can be rapidly provisioned and released with minimum provider interaction. On-demand service, broad network access, rapid provision, resource pooling and measured services are the main characteristics of this process.

The shift to cloud computing technology introduces diverse delivery models to telecom operators. In this transition, mobile operators could act as cloud network providers and based on common characteristics such as geographical zone and availability, offer networking services either to end user or other operators. For this purpose we introduce a new functionality called TaaS.

TaaS is a platform for creating functionalities to be used for commercial MNO business. TaaS is composed of software, hardware and application functions (also known as vNFs) as

DOI : 04.IJIS.2015.1.5

outlined by NFV industry standards. The combination of these functions is proposed as TaaS and could be sold as a service product to emerging MNOs or MVNOs.

Fig. 1 shows the TaaS stacks in the cloud layers.

TaaS platform hosts various mobile operators. Each mobile operator has interconnection with cloud layers (IaaS, PaaS and SaaS) depending upon on the type of services it provides to the customers.

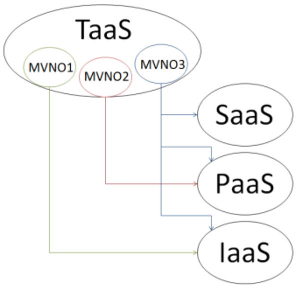

Fig. 1. TaaS Stack

Infrastructure as a Service (IaaS) provides virtualized infrastructures. Mobile operators can rent out their network elements, storage resources, computing system and licenses to other operators.

Platform as a Service (PaaS) is an interface between applications in SaaS and VMs in IaaS. PaaS controls VMs. This virtual platform is provided to developers for programming and web management. This programming could be related to network optimization, adding new features and so on. The main added value for PaaS comes from providing easy to use mechanism to deploy customer's software applications to the cloud service and providing scaling for server capacity.

Software as a Service (SaaS) is an application layer that provides different kinds of application software services to mobile operators, when they are relying on cloud base services. The applications can be used for bandwidth control, Quality of Service (QoS) management, network configuration, system backup and so on.

The proposed software stack can be implemented in a combination of cloud deployment model: public cloud, private cloud, community cloud and hybrid cloud. The combination is based on security consideration and will be discussed in next section.

IV. Security in TaaS

Security is the main issue of cloud services provided for mobile operators. Due to cloud characteristics such as virtualization and multi-tenancy, application sharing and open source software, the associated security threats like authentication, information leakage and data corruption are also growing in the TaaS cloud environment.

On the other hand, due to the open nature of IP in mobile technologies, these networks are potential targets of cyber-attackers to intrude services and cause problems to the end users and mobile operators. Although in later phases, extensions like IPSec and Authentication Authorization Accounting (AAA) have been added into mobile network implementation, security is still a main challenge in cloud computing due to the inconsideration in initial design of the Internet [13, 14].

To fulfill security requirements such as availability, integrity, authentication and authorization, we need to address TaaS vulnerabilities. For this purpose we classify TaaS security issues into three main aspects.

A. *Data Security*

Mobile operators that act as cloud providers are responsible for their customer data protection. The customers are either end users or other mobile operators. Herein we define data vulnerabilities based on the security requirements.

1) Authentication and authorization: It refers to access control mechanism that is used against unauthorized access or privilege logging. In this scenario, an attacker tries to modify, corrupt, steal and intercept the data of Control Plane (CP) and User Plane (UP). In addition to account control, telecom operators that act as cloud provider should also consider other aspects of data protection.

2) Integrity: It points out data correctness whether the data has been modified or corrupted. Malicious codes could be distributed by both insider and co-tenant or via external attackers on data storages [15]. Data encryption, data isolation, secure protocols and intrusion detection could support data integrity and prevent data modification and corruption.

Another aspect of data integrity is data leakage prevention that could be achieved by data sanitization [14, 16, 17] (encryption and data cleanup). Since multiple tenants may share the same infrastructure or VM e.g., virtual Home Subscriber Server (vHSS), therefore cloud service provider is responsible for a complete data cleanup before handing over VM to the next tenant.

3) Availability: It covers the basic concepts of security such as data recovery and resource availability. Availability could be achieved via load balancing, redundancy and data backup to prevent data loss. Threats such as DoS should be prevented by intrusion detection mechanism.

In addition to discussed security requirements, legal aspects such as security warranties and compensation agreements among operators belonging to TaaS looks necessary. On the other hand, location of the cloud provider [18] (where the parent company is registered) is important since different countries have diverse laws; regardless of data centers location, in special circumstances, authorities could have access to customer data.

B. *Hypervisor & VM Security*

Concept of virtualized threats refers to every kind of attack against availability, integrity and confidentiality of the hardware and software in a virtualized mobile network. There are three elements in a virtualized network: hypervisor, VMs (virtual hardware and images) and applications; all these

DOI : 04.IJIS.2015.1.5

elements should be adequately secured against unauthorized access, change and destruction.

In a virtualized mobile network, hypervisor itself is not directly connected to any end user, and threats arise through malicious VMs mostly, therefore having a reliable hypervisor requires secure VMs. While traditional security techniques such as IDS, antivirus and FWs are still applicable for virtualized networks; isolation could be an important approach towards security of VMs. Isolation will ensure that if one VM would be attacked, other VMs wouldn't get infected [11, 19].

There are different methods such as security zones and traffic separation for VM isolation. VMs with similar functionality and security requirements could be grouped in same hardware. Each zone could be controlled by different access list defined in FW or dedicated IDS and so on. DeMilitarized Zone (DMZ) is an example of security zones. Traffic separation is another method for VM isolation; similar to traditional networks, traffic with different characteristics, functionality (e.g., CP and charging) and security requirements would be assigned to different Virtual Local Area Networks (VLANs) or Virtual Private Networks (VPNs), in this case sensitive traffic would be separated [5].

After discussing virtualized network security concerns now we go through security requirement such as authentication, availability and integrity.

1) Authentication and Authorization: It refers to mechanism such as certificate based authentication that should be utilized to avoid unauthorized access. Keys and signatures must be stored in a secure storage such as HSM [6] to make it invisible to third parties. Hardening should be applied to infrastructure layer and wherever needed to block any backdoor access. Virtual FWs must be used inside VMs and proxy and traditional FWs must be used where needed to prevent unauthorized traffic. Backup must be maintained for all VMs so that data can be restored in case of failure. AAA should be maintained by logging actions from each VM and modules; and logs should be stored in a safe storage so that in case of attack or failure, logs shouldn't be affected and would help revealing the root cause. Encryption must be used so that data is not readable to unintended party even if it is accessed without authorization. Security policy should be enforced to make sure that all users in cloud have similar security policy and are in line with Service Level Agreement (SLA) [20].

2) Integrity: It refers to protection against threats on virtualized network. These threats could vary from attacking different virtual machines such as virtual Mobility Management Entity (vMME), vHSS, and their virtual functions, misconfigurations or abuse of resources, corrupting operating systems, switches and management software (in SDN), and inducing any kind of malicious applications.

3) Availability: It can be improved by applying techniques such as load balancing, redundancy and data backup as discussed earlier.

C. Application Security

Another aspect of virtualized network security refers to protection against threats that are related to an application server or a web server connected to the Internet.

Based on the concept of SaaS, software applications should be accessible over the Internet that makes security a very critical challenge for mobile operators. Beside the mechanisms such as data encryption, access control and authentication, back up and redundancy, mobile operator could implement sensitive applications that do not require end user intervention (such as billing application) using PaaS that is accessible only to limited professional users among mobile operators [21].

D. SDN & NFV Security

In addition to three main aspects of TaaS security (data security, hypervisor and VM security, application security) here we discuss other security and threats of cloud computing therefore TaaS.

It should be considered that introducing new technologies normally brings new security challenges as well. Except for the security issues of SDN and NFV that are new technologies for supporting TaaS, other security threats and their detection-prevention mechanisms are almost similar to traditional networks. However, traditional network implementations rely on dedicated hardware and private connections between network elements. Their control plane connections are not exposed to public, unless there is somewhere a configuration error. Traditional network has survived quiet well until today and will continue to survive with very little security awareness.

SDN is a new approach to separate UP and CP in mobile networks. Based on its functionality, it can be considered in IaaS (SDN switch) or in PaaS (SDN controller). SDN controller in mobile networks only carries CP (MME, or Serving/Public Data Network Gateway (S/P GW) VMs), and is located in PaaS. In this case, SDN is an interface between infrastructure and application layer. SDN in its switching functionality (S/P GW VM) only carries UP and considers part of infrastructure layer. UP and CP use OpenFlow protocol for communications with each other in SDN. VNFs are running on virtual machines and they provide certain subsection of the whole functionality of a telecommunications network.

From the security point of view, however SDN and NFV concepts bring several advantages such as [22]:

- Centralized management: simpler maintenance and debugging
- Programmability: faster security solution implementation and easy feature deployment
- Cost saving with sharing security techniques and service chaining
- Centralized and virtualized function: centralized monitoring and detection techniques.

They also have disadvantages for mobile networks and therefore for TaaS:

- Centralized controller: potential for single attack

DOI : 04.IJIS.2015.1.5

- Vulnerable southbound interface (OpenFlow) between controller and data-forwarding: degrade network, availability, performance and integrity via DoS attack
- Vulnerable northbound interface between controller and applications
- Programmability: applications have access to controller to program the network
- Reduced isolation of network functions
- Expensive and vulnerable cryptographic keys.

SDN and NFV carries most of the three layers threats such as configuration, authorization and access control, as well as software and images vulnerabilities. Different solutions such as security zone and grouping, isolating applications by VMs and licensing are recommended for NFV security. NFV acts in hypervisor and other parties could see the encryption keys, therefore providing signature beside the keys looks necessary [6]. FW and orchestration both are recommendations for NFV and platform security. On the other hand the Open Networking Foundation (ONF) has identified the southbound interface between controllers and data forwarding devices (SDN switches) as vulnerable. This interface uses OpenFlow protocol that could be vulnerable against spoofing if the authentication between controllers and switches are not implemented correctly or is compromised [22]. Therefore communication between controller and switch must be over TLS or IPSec to avoid eavesdropping, tampering and DoS attacks at controller. Considering SDN, secure API techniques must be utilized at northbound interface.

Fig. 2 shows SDN and NFV security threat vectors on TaaS [22].

- Forged or faked traffic flows
- Attacks on switches
- Attacks on control plane communications
- Attacks on controllers
- Lack of mechanisms to ensure trust between the controller and management applications
- Attacks on administrative stations
- Lack of trusted resources for forensics and remediation
- Attack on virtualized network functions
- Programmability of network via the controller by untrusted applications
- Protocols misbehavior

Finally below are some of the monitoring, detection and prevention techniques that could be used for SDN, NFV and OpenFlow security [22]:

- Deep Packet Inspection (DPI)
- Deep Flow Inspection (DFI)
- Shallow Packet Inspection (SPI)
- Virus scanners
- Intrusion Detection Systems (IDS)
- Firewall (FW)
- Security zones
- Policy enforcement (PCRF) to define access rules and flow rules for access control and authorization
- Secure protocols such as FlowTagging (flow tracking)
- Simple Network Monitoring Protocol (SNMP)
- Remote Monitoring (RMON)
- NetFlow or sFlow
- SDN Monitoring (SDNM)

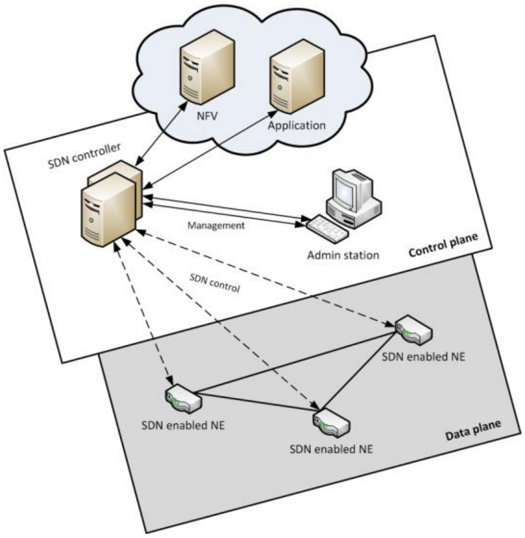

Fig. 2. SDN and NFV threat vectors [22]

E. *TaaS Security Benchmark*

TABLE I. [23-26] shows some of the TaaS threats and their prevention mechanisms. The comparison in this table is based on the discussed cloud domain and security requirements. In this table, all three domains of data, hypervisor and application cover SDN and NFV security.

What matters in cloud computing is the combination of layers and deployment to propose a new security model. This model not only recommends for each layer proper deployment but also emphasizes on specific detection-prevention mechanism for different layers [27].

V. TAAS DEPLOYMENT SECURITY

Fig. 3 shows our proposed security framework for TaaS.

A. *IaaS*

1) Layer point of view: Since infrastructures are fully managed by a mobile cloud provider, the security mechanism is also responsibility of the provider.

The tenants usually have minimum control and interaction on the network elements. They do not have access to the control plane VMs, even though they still could reach some of the network elements such as Home Location Register (HLR) or Policy Control and Charging Function (PCRF) server to pull their subscribers' information (such as subscriber profile, billing information). However, IaaS is less accessible by customers (end users or tenants); still insider attackers need to be highly considered.

For this layer, techniques such as data isolation through VMs, ciphering to protect data against unauthorized access, backup and recovery for data reliability and IDS for preventing malicious attacks should be considered by the cloud provider.

DOI : 04.IJIS.2015.1.5

TABLE I. TAAS SECURITY BENCHMARK

Domain	Requirements						Affected Layer
	Authentication and authorization		**Availability**		**Integrity**		
	Threats	**Prevention**	**Threats**	**Prevention**	**Threats**	**Prevention**	
Data	Unauthorized access and privileged access • Probing • Remote to Local • User to remote • Man-in-the middle attack • IP-Spoofing • Phishing	• AAA • FW • Rule based policy control • Encryption • Hardening • IPSec	Data loss and resources unavailability • Data removal • Unexpected system failure • Abusive use • DoS	• Backup • Redundancy • Load balancing • IDS • FW • AAA • IPSec	Data corruption, tampering and leakage	• FW • AAA • IPSec • IDS • Vulnerability scanning • Encryption SSL/TLS • Data cleanup before switching tenant	SaaS PaaS IaaS
Hypervisor and VM	Unauthorized access and privileged access • Probing • Remote to Local • User to remote • Man-in-the middle attack • IP-Spoofing • Phishing	• AAA • FW • Rule based policy control • IPSec • Hypervisor monitoring • VM isolation	• Image loss • Configuration loss • Misconfiguration • DoS • Abusive use	• Backup • Redundancy • Load balancing • IDS • FW • AAA • IPSec • Configuration test	Data corruption, tampering and leakage • Botnet • Malware	• VM isolation Security zone Traffic separation VLAN and VPN • SSL/TLS • DPI • IDS • FW • AAA • IPSec	PaaS SaaS
Application	Unauthorized access and privileged access • Probing • Remote to Local • User to remote • Man-in-the middle attack • IP-Spoofing • Phishing • spyware • Cookie poisoning • Service injection attack	• AAA • FW • Rule based policy control • IPSec • Encrypting cookie data	• Unexpected system failure • DoS	• Redundancy • Implementing system related applications in PaaS	• Application corruption • Botnet • Malware • Adware • Ransomware	• IDS • Secure coding • Secure browser	PaaS SaaS

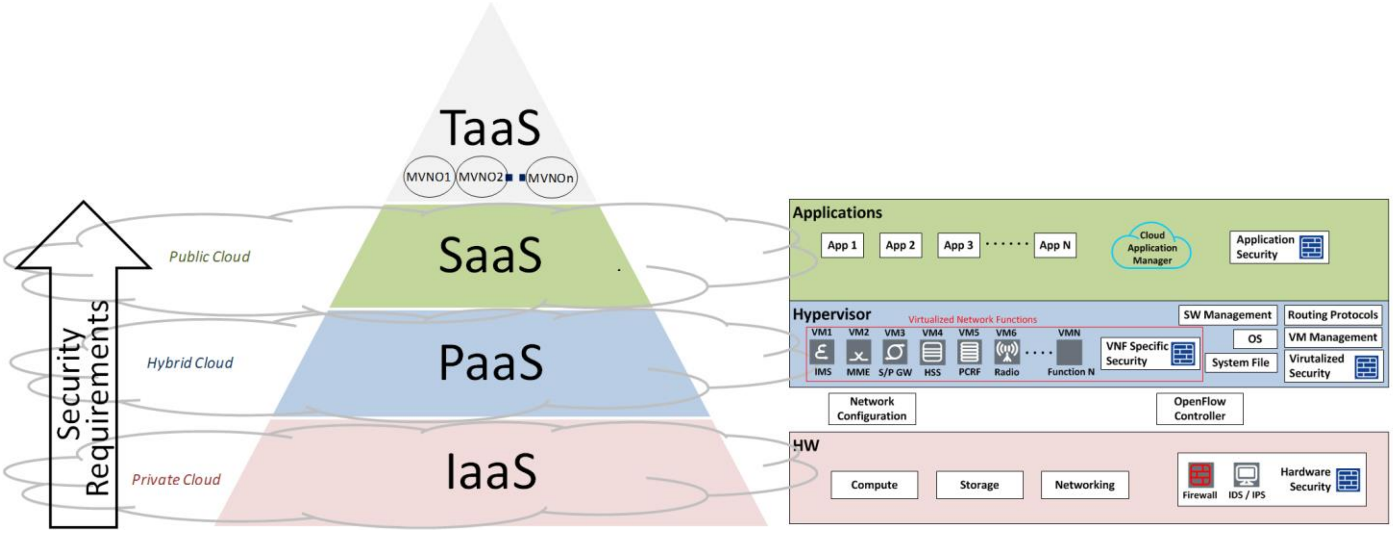

Fig. 3. Cloud Security for Operators

DOI : 04.IJIS.2015.1.5

In Fig. 3, more area is dedicated to IaaS layer to highlight the higher security requirement for this layer.

2) Deployment point of view: Considering high security requirements for infrastructures, limited accessibility, geographic location and high cost of network elements, mobile operators are recommended to use private cloud for this layer.

B. *PaaS*

1) Layer point of view: This layer is normally used by developers to program and run their applications. Generating software bug or file system corruption, unauthorized access or privilege upgrade and denial of service are the security threats that should be considered at this layer.

Strong authentication and access right control is required for this layer to limit user base that can make critical modification to configuration. Logging of all management actions are important to trace misbehaving users and to learn from mistakes. Therefore, a policy control mechanism could evaluate the requested access and decide whether to grant the access to developer or not.

2) Deployment point of view: This layer will be used by limited group of professionals and does not need to be accessible by all end users, therefore community or hybrid deployment for this layer is recommended. Mobile operators could take the advantages of public cloud, while for sensitive part of system software they just provide private cloud.

C. *SaaS*

1) Layer point of view: Since application layer is the closest layer to the end users, they could easily install different kinds of malware or spyware and steal the information or cause the data corruption at this layer. Secure protocols and malware detection methods are some of the prevention mechanisms that should be considered in this layer.

2) Deployment point of view: In order to gain the initial cloud computing benefits, such as elasticity, economies of scale, SaaS should be available to all customers (end users and other tenants) therefore public cloud is recommended for SaaS.

VI. Open Research Issues and Future Work

A. *Future Work*

We need to learn more about specifications and results of ongoing work at ETSI NFV. Proposed TaaS shall implement at least partially security requirements outlined in ETSI NFV specification. TaaS concept needs to be analyzed further and compared with NFV to find commonalities and also to understand how it can be positioned in NFV context.

ETSI NFV compliant open source software implementation OPNFV release Arno became available June 4th, 2015 [28, 29], and it should be analyzed how well it addresses security concerns outlined for TaaS.

A cloud system is distributed over many geographically separate computing sites, and if one site breaks down unexpectedly (e.g., by earth quake or severe cyber attack), it is challenging to leverage such cloud system.

B. *Research Issues*

Although there are many researches on the security concerns of cloud computing, there are still open issues requested further investigation in future studies.

First, various new business opportunities opened by cloudification disruption in the operator domain should be investigated and analyzed if these business opportunities, trigger further technological breakthroughs or not. On the other hand further research is necessary to understand requirements to TaaS and their mutual priorities. It should be studied whether there will be lightweight MVNOs, which operate almost without own staff. To achieve this, the expectations of various stakeholders, like MNOs, MVNOs, equipment vendors and end users in the security domain should be listed.

Second, fighting against governmental cyber war attacks is one of the common concerns among potential target governments, privacy aware end users, and consequently also service providers. Some governments are not financially restricted while preparing cyber attacks and espionage and they may sponsor cracker and hacktivists to leverage their technological curiosity for ideological purposes. For this purpose a novel means at least detecting these attacks as early as possible, or even preventing looks necessary.

Third, cloud computing enables fast update cycles for software components such as VM images. It should be investigated whether lowering quality assurance (testing) effort of finding typical software bugs like buffer overruns is feasible or not. Lowering quality assurance poses risk of enabling vulnerabilities that can enable breaking in to a system. It is important, if such breaches can be detected quickly and also their fixes are distributed before any major damage occurs. On the other side, it is worth considering if the possible development cost savings, and profits from faster time to market exceed potential expenses caused by damages and bug fixing.

Forth, from the end user perspective, one main benefit for MNO cloudification is utilization of higher bandwidth for lower costs. It can also provide flexibility benefits such as on-demand services, dynamic charging patterns for bandwidth fluctuations etc.

Fifth, from legacy perspective, legislation protecting end users against MNO/MVNOs with malicious intentions may be needed in future. Small capital lightweight MVNO may be bought by bad people with malicious intent, and legislation should be introduced to disconnect such malicious MVNOs.

VII. Conclusion

Emerging traditional mobile operators who follow similar interests introduce potential demand for a new service model in cloud computing called TaaS. According to a location based, customer based or service based agreement, mobile operators

DOI : 04.IJIS.2015.1.5

could be grouped to considerably improve their cost structure, time and quality efficiency and therefore their speed to market.

TaaS gives the possibility to understand mobile operator's threats in a wide range and based on their provided cloud layers. While majority of earlier studies have been concentrated only on few threats for specific layer, this paper has discussed the mobile cloud threats in a combined method, for all layers of cloud and from an operator point of view that delivers its services based on the basic cloud infrastructure.

On the other hand, the proposed cloud security model helps mobile operators to understand how to tradeoff and merge their services based on the deployment and importance of the provided services. In Fig. 3, private deployment is assigned to IaaS that requires highest security consideration. For SaaS that is the closest layer to the end users public cloud is recommended. Some of the reasons for this recommendation come from application availability to wide range of end users, scattered end users (geographic location) and roaming condition. Finally hybrid cloud is the proposed deployment for PaaS layer; that means private and public deployment could be considered for provided platforms and based on their sensitivity and security concerns.

Discussed CFSO model in this paper, is a combined security model that considers different threats and vulnerabilities for each layer, their modules, services and protocols, and helps TaaS to find the best combination of deployment solution.

References

[1] M. Chiosi and S. Wright, "Network functions virtualisation - white paper # 3,"ETSI, Darmstadt, Germany, 2014. https://portal.etsi.org/Portals/0/TBpages/NFV/Docs/NFV_White_Paper3.pdf

[2] N. Katica and A. Tahirovic, "Opportunities for telecom operators in cloud computing business," in *MIPRO, 2012 Proceedings of the 35th International Convention,* 2012, pp. 495-500.

[3] Hui Suo, Zhuohua Liu, Jiafu Wan and Keliang Zhou, "Security and privacy in mobile cloud computing," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International,* 2013, pp. 655-659.

[4] S. Scott-Hayward, G. O'Callaghan and S. Sezer, "Sdn security: A survey," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For,* 2013, pp. 1-7.

[5] "Building secure telco clouds (white paper)," Nokia Networks, Tech. Rep. C401-01087-WP-201409-1-EN, 2014.

[6] "Why service providers need an NFV platform (white paper)," Alcatel-Lucent, Tech. Rep. C401-01087-WP-201409-1-EN, 2013.

[7] T. Kekkonen, T. Kanstren and K. Hatonen, "Towards trusted environment in cloud monitoring," in *Information Technology: New Generations (ITNG), 2014 11th International Conference On,* 2014, pp. 180-185.

[8] M. Chiosi, "Network functions virtualisation - introductory white paper," ETSI, Darmstadt, Germany, 2012. https://portal.etsi.org/nfv/nfv_white_paper.pdf

[9] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub and D. Zeghlache, "Challenges for cloud networking security," in *Mobile Networks and Management*, K. Pentikousis, R. Agüero, M. García-Arranz and S. Papavassiliou, Eds. Springer, 2011, pp. 298-313.

[10] C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *The Journal of Supercomputing,* vol. 63, pp. 561-592, 2013.

[11] M. Ali, S. U. Khan and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci.,* vol. 305, pp. 357-383, 2015.

[12] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology,* vol. 53, pp. 50, 2009.

[13] A. Oredope, A. McConnell, C. Peoples, R. Singh, T. A. Gonsalves, K. Moessner and G. P. Parr, "Cloud services in mobile environments ?? the IU-ATC UK-india mobile cloud proxy function," in *Wireless Conference (EW), Proceedings of the 2013 19th European,* 2013, pp. 1-7.

[14] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire and P. R. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security,* vol. 13, pp. 113-170, 2014.

[15] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications,* vol. 34, pp. 1-11, 1, 2011.

[16] A. Kronabeter and S. Fenz, "Cloud security and privacy in the light of the 2012 EU data protection regulation," in *Cloud Computing, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, M. Yousif and L. Schubert, Eds. Springer, 2013, pp. 114-123.

[17] L. F. B. Soares, D. A. B. Fernandes, J. V. Gomes, M. M. Freire and P. R. M. Inácio, "Cloud security: State of the art," in *Security, Privacy and Trust in Cloud Systems*, S. Nepal and M. Pathan, Eds. Springer, 2013, pp. 3-44.

[18] "Cloud service level agreement standardisation guidelines," European Commission, Brussels, 2014. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138

[19] F. Doelitzscher, C. Reich, M. Knahl and N. Clarke, "Understanding cloud audits," in *Privacy and Security for Cloud Computing*, S. Pearson and G. Yee, Eds. Springer, 2012, pp. 125-163.

[20] D. Petcu, "SLA-based cloud security monitoring: Challenges, barriers, models and methods," in *Euro-Par 2014: Parallel Processing Workshops*, L. Lopes, J. Žilinskas, A. Costan, R. Cascella, G. Kecskemeti, E. Jeannot, M. Cannataro, L. Ricci, S. Benkner, S. Petit, V. Scarano, J. Gracia, S. Hunold, S. Scott, S. Lankes, C. Lengauer, J. Carretero, J. Breitbart and M. Alexander, Eds. Springer, 2014, pp. 359-370.

[21] R. Yrjo and D. Rushil, "Cloud computing in mobile networks — case MVNO," in *Intelligence in Next Generation Networks (ICIN), 2011 15th International Conference On,* 2011, pp. 253-258.

[22] E. M. d. Oca and W. Mallouli, *Software Defined Mobile Networks : Beyond LTE Network Architecture*, M. Liyanage, A. Gurtov and M. Ylianttila, Eds. Wiley, 2015, pp. 331-356, in press.

[23] S. Binu and M. Misbahuddin, "A survey of traditional and cloud specific security issues," in *Security in Computing and Communications*, Springer, 2013, pp. 110-129.

[24] Ni Zhang, Di Liu and Yunyong Zhang, "A research on cloud computing security," in *Information Technology and Applications (ITA), 2013 International Conference On,* 2013, pp. 370-373.

[25] B. Chhabra and B. Taneja, "Cloud computing: Towards risk assessment," in *- High Performance Architecture and Grid Computing*, A. Mantri, S. Nandi, G. Kumar and S. Kumar, Eds. Springer, 2011, pp. 84-91.

[26] M. Monshizadeh and Zheng Yan, "Security related data mining," in *Computer and Information Technology (CIT), 2014 IEEE International Conference On*, 2014, pp. 775-782.

[27] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2. 1," *Cloud Security Alliance,* pp. 1-76, 2009. https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[28] *OPNFV Delivers Open Source Software to Enable Deployment of Network Functions Virtualization Solutions*. https://www.opnfv.org/news-faq/press-release/2015/06/opnfv-delivers-open-source-software-enable-deployment-network

[29] *Technical Overview | Open Platform for NFV (OPNFV)*. https://www.opnfv.org/software/technical-overview