Fraud Threats Disclosure through Cloud Information Security Framework

Theodoros Mavroeidakos
School of Electrical and Computer Engineering
National Technical University of Athens
Heroon Polytechniou 9
GR-15780 Zografou, Greece
Email: el10807@central.ntua.gr

Dimitrios D. Vergados
Department of Informatics
University of Piraeus
80, Karaoli & Dimitriou St.
GR-18534, Piraeus, Greece
Email: vergados@@unipi.gr

***Abstract*—The Cloud Computing (CC) paradigm introduces a highly efficient environment based on the aggregation of novel technologies. The cloud-based services are characterized by enhanced behavior and unique features due to the capabilities facilitated by the particularities of the CC environment such as the scalability. However, because of these particularities, new threats and vectors of attacks emerge. This surface of cloud attacks, is distributed and covered in nature, which can be utilized to stage fraudulent activities. The cyber-incidents that entail fraudulent activities lead to negative effects such as the nefarious usage of CC resources and the abuse of the cloud-based services. To this end, the information security challenges, which are associated to fraud, lead to restrictions and barriers concerning the operational as well as the financial activities performed by the Cloud Service Provider (CSP). To counterbalance these security challenges, a Cloud Information Security (InfoSec) Framework should be incorporated in the operation of the CSPs' infrastructure. The proposed framework imposes the implementation of a series of phases oriented towards the entanglement with fraud threats so as to mitigate them and therefore secure the provision of the end-services, as well as protect the collected data.**

***Keywords*—CC paradigm; fraudulent activities; fraud threats; surface of cloud attacks; information security challenges**

I. Introduction

At the present time, cloud-based services are characterized as high-risk due to the number of threats that exist against their underlying CC environments. Moreover, the majority of the attacks which target the CC environment can be associated with fraudulent activities and be enhanced by them. According to Cloud Security Alliance (CSA) [1], the CC environments are targeted by perpetrators performing fraudulent activities because of their weak authentication schemes, ineffective access control allowing anonymous access throughout the usage of CC resources and limited capabilities concerning fraud detection and prevention. Consequently, the CC environments are susceptible to fraudulent activities. To this end, it is vital that the CSPs shall develop and integrate a viable information security framework into their corporate plans. The proposed Cloud InfoSec Framework facilitates a unified methodology concerning the confrontation of fraud across the CSPs' distributed infrastructures. This framework addresses fraud related security issues and challenges both in the functional as well as the technical layer of the environment. Moreover, it defines the necessary cyberspace operations which shall be accomplished so as to achieve a high level of security prior to the adaptation of processes and activities aiming to mitigate fraud attempts. Further, the proposed framework evolves around sensitive data such as personal and governmental. Furthermore, the framework also facilitates analysis about regulatory compliance in conjunction with legal as well as the constrains which emerge in that aspect through the provision of the end-service.

Main elements of this Cloud InfoSec Framework concerning fraudulent activities are the risk management, the employment of operational specifications, the security assessment and procedures as well as techniques which aim to construct a tamper-proof CC environment. Moreover, the framework involves governance control over internal corporate actions which are performed on the collected data and any contextual information about individuals. These elements aim at extracting cyber security intelligence with regard to illegal activities in the context of the CSP's operations.

This framework is enabled by the CSP's information security sector and provides tactical support to its infrastructure continuously. The Service Level Agreement (SLA) consists of an entity, which shall interact with the proposed framework due to the fact that facilitates privacy and trust. Following this, the SLA or any other commercial contract, between the CSP and the clients, are profiled by legal jurisdictions, expected performance as well as the level of security.

The remainder of this paper is structured as follows. In Section II the related research literature is reviewed while Section III depicts the taxonomy of fraud threats neutralized by the Cloud InfoSec Framework. Section IV contains description of the Cloud InfoSec Framework's purpose and phases. In Section V the Cloud InfoSec Framework's phases are placed under scrutiny while the Framework's evaluation is carried it out in Section VI. Finally, the concluding remarks are drawn in section VII.

II. Related Work

According to [3], the European Network and Information Security Agency (ENISA) defines a risk assessment process in order to determine the impact of specific vulnerabilities and address the risks associated to CC penetration scenarios. Moreover, in this report, ENISA deals with legal, technical and policy considerations and implications by surveying use-cases concerning explicit legal issues which also consist objectives of the provisioned cloud-based services such as the confidentiality. In [4], ENISA examines Critical Information Infrastructure Protection (CIIP) issues by analyzing the effects of cyber-attacks at the end-service of different cloud computing scenarios. Apart from this, ENISA proposes in [5] a security framework which is modeled in four phases in order to facilitate the adoption of the CC paradigm by governments of the Member States of the European Union (EU). This framework is based on the Plan-Do-Check-Act (PDCA) cycle so as to organize and manage the security objectives of the governmental CC environments with flexibility and efficiency.

The National Institute of Standards and Technology proposes guidelines on security and privacy in public cloud computing in [6], which are required to address public cloud security and privacy concerns during the transitioning of applications and services. According to [7], the NIST fills the gap between the available security standards and the security categories which shall be addressed in the context of a protected CC environment. Further in [8], which is currently in draft form, the NIST presents the Cloud Computing Security Reference Architecture (NCC-SRA) which defines a predictive model in order to secure the NIST's Cloud Computing Architecture. Moreover, this report introduces a methodology for applying a Cloud-adapted Risk Management Framework divided in specific steps using a set of security components so as to engineer a protected CC environment. In respect to the NIST's Special Publication 800-53 [9], the security and privacy controls that are introduced in this report so as to construct resilient environments against cyber threats, cover the area of cloud-based services in the context of federal CC environments.

Hormozi et al. argue in [10] that the detection of fraudulent activities on CC environments shall be performed by an Artificial Immune System (AIS) based on the Negative Selection Algorithm (NSA). In a recent study [11], the AIS-based Fraud Detection Model (AFDM) is introduced as an enhanced fraud detection model in terms of precision and cost which is based on NSA along with Clonal Selection. AFDM utilizes a cloud computing solution for its training phase which leads to certain advantages due to the CC computational features. Huang et al., in [12] propose a hybrid model for online fraud detection of Video-on-Demand Systems which combines two artificial immune system algorithms with behavior based intrusion detection using Classification and Regression trees (CART).

This paper sheds new light on accomplishing fraud threats disclosure on CC infrastructures. The main idea upon which the entire Cloud InfoSec Framework is based, is that fraud threats are highly correlated to security challenges without consisting independent problem and their mitigation should be implemented in every abstraction layer across the distributed CC infrastructure. In contrast to recent research which aims at constructing independent mechanisms, systems and methodologies so as to achieve concealment against fraud or security threats, the proposed Framework focuses on implementing a set of phases geared towards the confrontation of security challenges leading to fraudulent activities. Thus, a secure environment exploiting CC security countermeasures, as well as fraud-related policies, practicies and procedures are molded against the total cloud attack surface.

III. Fraud Threats Taxonomy

CC applications are increasingly becoming an integral part of society's pillar sectors such as the health and the financial due to their benefits. Thus, these sector are threatened by the cloud attacks. The cloud attacks (i.e. DDoS, Hijacking, Wrapping) can be leveraged as the initial phase of a penetration which ultimately aims to succeed a fraud activity. The fraud attacks are classified into the following main categories [13, 14]: skimming, pharming, identity theft, botnets and triangulation schemes. Analyzing these attacks, *skimming* is a form of fraud attack in which criminals copy the information stored on a payment card by means of a small device attached to an Automatic Teller Machine (ATM). Furthermore, *pharming* occurs when the fraud perpetrators hijack a bank's Uniform Resource Locator (URL) and manage to divert traffic to a malicious website of their own that looks legitimate and similarly seeks to harvest banking credentials and other personal information. Apart from this, *identity theft* is a form of fraud attack in which a user receives an email stating to be from his bank and lures him into submitting his banking credentials and other sensitive information. Therefore the attacker has the means to impersonate the victim and withdraw money from his banking account as well as locate CC resources in order to use them maliciously. In addition, *botnets* consist of computers and devices with internet connection which are under the control of a perpetrator. The perpetrator, botmaster, has obtained unauthorized access by remotely executing malicious software on them and is in position to launch attacks without traces leading back to him. The *triangulation schemes* is a form of credit-card fraud in which the customers provide their personal information in the course of obtaining goods through an infected website. Then, the perpetrators by using the customers legitimate information such as the credit card numbers, purchase other goods.

Overall, following the initial stages of any attack, the attackers are in position to coordinate their penetration technique with respect to the detected vulnerabilities by the active and passive reconnaissance. Then, the attackers exploit the vulnerabilities and gain control over internal services and systems. Following this stage, the attackers focus on maintaining access to the CC environment though malware software, which creates covered backdoors. Having completed the penetration, the attackers acquire passwords and sensitive information such as the cardholder's data in order to initiate fraudulent activities.

IV. Framework Phases

The scope of the Cloud InfoSec Framework is mainly to support the architectural and operational decisions, which form the security and governance level that characterize the procedures and functions performed over the CSPs' distributed facilities. Inside a CC environment, the security responsibility with regards to the services and deployment model, is shared among the CSP, the clients and the Third-Party providers. Thus, the data that circulate the cyberspace of CSP, have different ownership and they are subjects to different privileges. This event leads to a confusing and foggy situation in which transparency and trust is hard to establish and therefore fraud-related challenges emerge. The proposed framework consists of a solution that exploits already developed methods and tactics in order to confront vulnerabilities which lead to fraudulent activities. The Cloud InfoSec Framework is composed of six distinct phases as depicted on Fig. 1.

V. Phases Analysis

A. Laws Breakdown

The major role of CSPs is to process data on behalf of data controllers such as companies, organizations and even governments. In view of the distributed nature of the CC environment, the CSPs are involved in economies of many countries with a significant positive result, a great number of potential customers. However, beyond this advantage, due careful attention must be focused on the challenges that surface by the diversity of laws and regulations that apply in every country in which the CSPs' facilities reside.

By analyzing the national laws in the context of which the CC environment establishes its procedures, the CSPs take into account the necessary provisions and implement the imposed constraints with scope to achieve legal compliance. In this phase, the legal challenges concerning the data collection process that emerge from the correlation of laws, are addressed. It can thus reasonably be assumed that in the case that the provided service is a SaaS with focus group any individual in a specific country, then the legislation concerning the processing of personal data is to be acknowledged. In the events that the individuals are Community citizens of a Member-State of the European Union (EU), then the legal instructions of the General Data Protection Directive (GDPR) 2016/679 [15] and the Directive on Security of Networks and Information Systems (NIS Directive) [16], should be implemented.

Since the proposed Framework aims to fraud threats disclosure, the CSP must apply the required functional and technical measures to ensure that its environment complies with the obligations laid down by fraud-related regulations. The principal Directives with regard to fraudulent activities which apply in the context of the CSPs' operations inside the EU and the European Economic Area (EEA) are namely: the Directive 2009/136/EC [17], the Directive 97/7/EC [18], the Directive 2005/29/EC (”Unfair Commercial Practices Directive”) [19], the Directive 93/13/EEC [20] on unfair terms in consumer contracts and the Directive 2000/31/EC (”E-Commerce Directive”) [21].

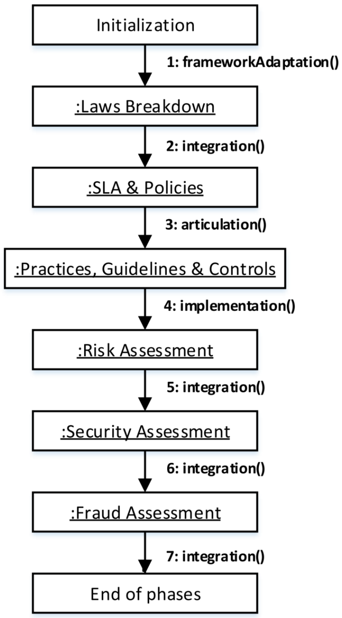

Fig. 1. Collaboration diagram of Cloud InfoSec Framework Phases.

B. SLA & Policies

The SLA consists of an entity of fundamental significance in the CSPs' operation due to its defining role to cover legislative gaps and misinterpretations. Through the SLA the CSPs are able to prove that they exhibit compliance to certain operational specifications and standards which are required in order to avoid the negative effects of fraud attacks. For example, the CSPs which acquire cardholders' data in order to dispose CC resources, should fulfil the Payment Card Industry Data Security Standard's (PCI-DSS) requirements and demonstrate compliance with it. Moreover, the SLA lays rights and responsibilities section which establishes the duties and rights of both parties in order to achieve security transparency. Cloud-based services offered in the critical sectors of society such as banking, government, military, health care necessitates strong SLAs around overall uptime, security, privacy and legal compliance. The SLA determines the objectives which should be met during the end-services' provision and sets the stage for privacy and trust among the agreeing parties through the orchestration of Service Level Objectives (SLOs). CSPs facilitating access to mission-critical services are expected to deliver in a constant basis, proof that the SLOs enforcement is performed effectively. On account of delivering reports to the clients, the CSPs should integrate into their operation specific metrics associated to the SLOs. In the light of mitigating fraud attacks, the metrics should be oriented to this purpose. Metrics which are collected with scope to prove the concealment against fraudulent activities are depicted on Fig. 2.

The policies are corporate documents defining the terms of services under which the CC environment should operate, apply requirements but also enforce the SLOs. Thus, they define the operational specifications concerning the CC environment's configuration but also the controls that would enable access to the clients. The policies' articulation should be implemented by following specific criterions when the CSP delivers mission-critical services. Thus, uniformity could be achieved concerning their approach on certain dimensions of CC environment such as the security and privacy measures with regard to fraudulent activities. Apart from this, the cloud architecture consists of many abstraction layers which comprise different data categories. To this end, the policies should address explicitly the emerging challenges of each layer with regard to the data and their importance. In view of fraud threats mitigation, an *anti-fraud team* should be established and operate by following the policy which determines the fraud risk management operations.

C. Practices, Guidelines & Controls

In this phase, the CSP should develop the appropriate provisions in order to implement the instructions issued by the policies and the employed standards (e.g. PCI-DSS). Part of this phase also consists of the guidelines' articulation which will fulfil the needs and objectives set down by the policies and imposed by the legislation. Apart from this, the controls are integral component of the CSPs' operation in order to achieve effective risk mitigation. Moreover, the controls implement the minimum measures so as to accomplish a balanced relation among the level of security and usability that mission-critical services require.

D. Risk Assessment

The risk level indicates the possibility of an attack to succeed and consists of a combination of threats and vulnerabilities. In order to accomplish effective risk assessment and address the risks thoroughly, a classification of risks in certain categories, should take place.

1) Organizational and Policy Risks: The most significant organizational risk consists of the SaaS lock-in. This particular risk blocks any transfer of collected data through a specific SaaS, to happen. Moreover, divergent termination or failure of the end-service as agreed in the SLA, leads to critical impact on the clients' ability to meet their duties and obligations. Furthermore, the CSPs' deviations from their obligations concerning the reporting of the SLOs' adequate enforcement consists of a significant risk which can potentially affect the clients' data.

2) Legislation Risks: The distributed nature of a CSP environment is based on multiple facilities located across many countries and in some occasions in high-risk countries. In high-risk countries, the national regulations do not define data protection guidelines as well as the privacy of data and the civil rights of natural people are not applicable [22]. Moreover, the national authorities in high-risk countries do not act according a predefined framework and their actions may endanger PII. In case the CSPs' environments collect and process PII, then they should be acting according specified data protection and fraud related directives and regulations depending on the country. The CSPs should follow changes in the national legislation framework concerning the process of personal data.

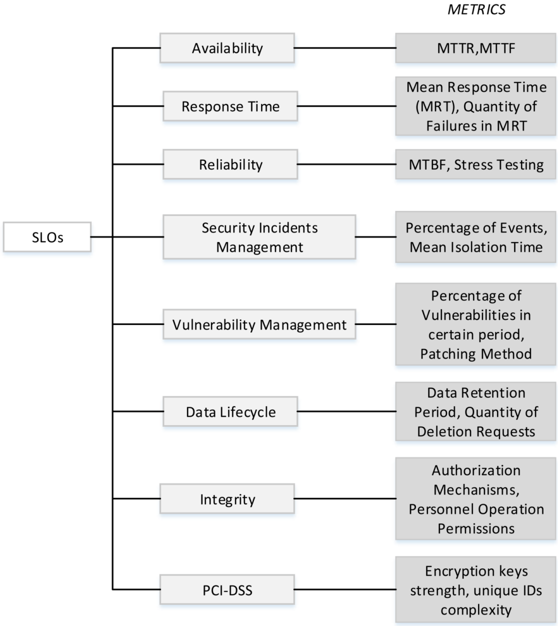
METRICS
SLOs
Availability
MTTR,MTTF
Response Time
Mean Response Time (MRT), Quantity of Failures in MRT
Reliability
MTBF, Stress Testing
Security Incidents Management
Percentage of Events, Mean Isolation Time
Vulnerability Management
Percentage of Vulnerabilities in certain period, Patching Method
Data Lifecycle
Data Retention Period, Quantity of Deletion Requests
Integrity
Authorization Mechanisms, Personnel Operation Permissions
PCI-DSS
Encryption keys strength, unique IDs complexity

Fig. 2. SLOs metrics.

3) Technical Risks: The CC environment is characterized by the scaling mechanisms which permit fast resource allocation according the demand. Due to the same mechanisms, the environment is susceptible to resource exhaustion, which can be leveraged by Distributed Denial-of-Service (DDoS) attacks. Data disclosure due to the actions of malicious insiders consist a critical risk as PII and data concerning the internal operation of this environment become available publicly. In distributed environments, data must be transferred in order to synchronize multiple distributed virtual machines, therefore large quantities of data are in transit over the intranets, creating attack vectors in multiple points.

Risk Management: In order to manage the described risks, the CC architecture should be divided into two distinct layers of risk namely, the *organizational layer* and the *business mission layer*. The definition of risk layers permits association between the attacks and the impact of them against the CC environment by identifying the type of data which are affected. The organizational layer is the high risk layer as data by every category are hosted there.

E. Security Assessment

The security assessment identifies PII and system information that can be leaked due to inadequate safeguards. This procedure consists of steps such as *active and passive reconnaissance*, *services' enumeration*, *networks mapping*, *services' exploitation*, *privileges escalation* and *trace deletion*. These steps contribute to the scope of the security assessment which is to define the minimum information the attacker could gain so as to exploit the cloud boundary. The cloud boundary is divided into the *outside* and *inside perimeter*.

1) Outside Perimeter: The Outside Perimeter extends among the computing entities that are visible to the clients.

The business mission risk layer belongs to this perimeter. Inside this perimeter also reside limited PII and information about specific CC systems and mechanisms.

2) Inside Perimeter: The Inside Perimeter extends among the intranets of the environment. The organizational risk layer belongs to this perimeter. This perimeter hosts PII and critical operational data.

In the CC environments, many computing entities with different characteristics interact and various technologies are combined (e.g. Software Defined Networks, Virtualization Technologies), creating a diversity of vulnerabilities. For the purpose of the security assessment, a wide spectrum of tools and techniques are orchestrated in order to identify the vulnerabilities and the attack vectors. The aggregation of the assessment's results leads to the vulnerabilities determination that can be leveraged for exploitation.

F. Fraud Assessment

The fraud assessment is a procedure performed by the fraud operator in the CC environment, the anti-fraud team. The anti-fraud teams consist of personnel with a variety of skills and knowledge in order to evaluate any fraud attempt by different perspective and implement a diversity of tasks. Firstly, the anti-fraud team identifies opportunities and vectors to commit fraud both in the outside and inside perimeter. Two main fraud risks for the CC environments are:

– The *misappropriation of assets* by interacting entities (e.g. clients, personnel) due to the distributed nature of assets. The CSP's threatened assets are all of them which, by the time they are breached have negative impact on the objectives set by the SLA concerning the end-service.

– The *corruption* is the process of exposure of confidentiality and misuse of cardholder data for private gain by the perpetrator.

For the purpose of confronting these risks and therefore mitigate the most dangerous fraud threats, the CSP should implement the steps depicted on the fraud assessment cycle of Fig. 3, in specified time periods as long as the end-service is available to the clients.

VI. Assessment & Gap Analysis

Notwithstanding the fact that the Cloud InfoSec Framework sets the stage for corporate governance and control over organizational and technical layers of an infrastructure against fraudulent activities, there are some areas and actions, which are disregarded and gaps emerge.

For the purpose of identifying the gaps, which are retained and allow fraudulent activities to come into existence despite the Framework's implementation, a cloud scenario that consist of many potential attack vectors for fraud perpetrators and bears a close resemblance to reality, is evaluated. In the context of this scenario, a bank integrates into its business plan a mobile cloud-based service in order to grant access to its clients' portfolio so as to enable management of digital credit cards, banking accounts and movements.

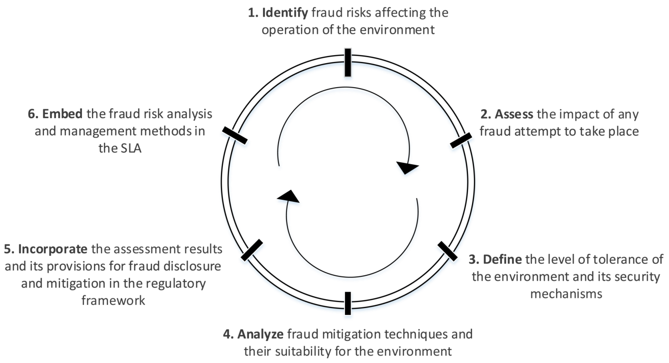
1. Identify fraud risks affecting the operation of the environment
2. Assess the impact of any fraud attempt to take place
3. Define the level of tolerance of the environment and its security mechanisms
4. Analyze fraud mitigation techniques and their suitability for the environment
5. Incorporate the assessment results and its provisions for fraud disclosure and mitigation in the regulatory framework
6. Embed the fraud risk analysis and management methods in the SLA

Fig. 3. Fraud assessment cycle.

The foremost gap of paramount importance, is the integration of fraud detection and prevention mechanisms beyond the measures orchestrated for the organizational layer in context of the second and the third phases. Detection mechanisms and preventive control procedures should be designed and implemented with regard to the end-service without confining its performance objectives across the CC distributed environment. For example, the mobile application may behave differently in the case that fraud detection mechanisms perform real-time analysis of data transactions in order to achieve rapid provision of countermeasures. Over and above this example, the majority of network protocols, CC security services, data encryption schemes coupled with fraud detection and prevention mechanisms impact throughput and delay the end-service's provision. To this end, these delays should be assessed against the nature of mobile applications attributes' such as any additional delays due to the coverage of Radio Access Networks (RANs) and the added overhead by the mobile network carrier, which will facilitate access to the backend CC infrastructure. Thus, following the mechanisms' implementation, they should be assessed periodically concerning their effectiveness and the assessment reports should be documented in order to revise and therefore improve the Framework.

Another absent key element, is that part of the anti-fraud teams' role should be the training of the CSP's personnel following professional standards. This gap lies on the side of the CSP's personnel while the perpetrators exploit their social enginneering skills as an intermediate stage in order to accomplish disclosure of confidential data such as banking credentials granting access to the mobile application, which can be then leveraged to facilitate fraudulent activities. By training the personnel, informing it about the potential threats, it will eventually possess adequate knowledge to support the Framework's implementation and report malicious activities to the anti-fraud team in order to deploy the appropriate countermeasures in time.

Additionally, a gap inheres on the fact that the Framework phases are implemented openly in the CC environment without concealment from the CSP's personnel. Thus, a substantial task to be applied, is that the instructions described by the Framework's phases, should remain confidential and the operation of fraud detection and prevention mechanisms should be concealed for the purpose of avoiding fraud threats relating to insider threats into the bank's corporate environment.

VII. Conclusion and Future Work

The proposed Cloud InfoSec Framework assembles a highly efficient security architecture across the abstraction layers of a CC environment through the implementation of specific phases. Each phase orchestrates a diversity of components and techniques aiming to integrate inside the CC infrastructure the concept of defense against fraud threats. Considerable insight has been gained with regard to the characteristics which should be taken into consideration on the CC paradigm considering mitigation of fraudulent activities.

Future work should concentrate on enhancing the CC defense mechanisms regarding the nefarious usage of CC resources or the abuse of *X-as-a-Service (XaaS)*. An important issue to resolve for future studies, is that work needs to be done on governmental or regional legislation to strengthen the cross-border guidelines with respect to fraud. On a wider level, it is recommended the standardization of a Fraud related Regulatory Framework in European level so as to serve as a basis for CSPs operating on Member-States of the EU.

Acknowledgment

The publication of this paper has been partly supported by the University of Piraeus Research Center (UPRC).

References

[1] Cloud Security Alliance (CSA), (2010). *Top Threats to Cloud Computing.* Version 1.0, March 2010.

[2] T. Mavroeidakos, A. Michalas and D. D. Vergados, *Security Architecture based on Defense in Depth for Cloud Computing Environment.* IEEE INFOCOM First International Workshop on Big Data Sciences, Technologies and Applications (BDSTA 2016), 10-15 April 2016, San Francisco, CA, USA, pp. 211-216.

[3] European Network and Information Security Agency (ENISA), (2009). *Cloud Computing: Benefits, risks and recommendations for information security.* November 2009, pp. 21-112.

[4] European Network and Information Security Agency (ENISA), (2012). *Critical Cloud Computing.* Version 1.0, December 2012, pp. 3-25.

[5] European Network and Information Security Agency (ENISA), (2015). *Security Framework for Governmental Clouds.* February 2015, pp. 5-22.

[6] J. Wayne, T. Grance, (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* National Institute of Standards and Technology (NIST), Special Publication (SP) 800-144, USA, December 2011.

[7] NIST Cloud Computing Standards Roadmap Working Group, (2013). *NIST Cloud Computing Standards Roadmap.* National Institute of Standards and Technology (NIST), Special Publication 500-291, Version 2, USA, July 2013.

[8] NIST Cloud Computing Security Working Group, (2013). *NIST Cloud Computing Security Reference Architecture.* National Institute of Standards and Technology (NIST), Special Publication 500-299, USA, May 2013.

[9] Joint Task Force Transformation Initiative, (2013). *Security and Privacy Controls for Federal Information Systems and Organizations.* National Institute of Standards and Technology (NIST), Special Publication 800-53 Revision 4, USA, April 2013.

[10] E. Hormozi, M.K. Akbari, M.S. Javan and H. Hormozi, (2013). *Performance Evaluation of a Fraud Detection System based Artificial Immune System on the Cloud.* 8th International Conference on Computer Science & Education (ICCSE 2013), 26-28 April 2013, Colombo, Sri Lanka, pp. 819-823.

[11] N.S. Halvaiee and M.K. Akbari, (2014). *A novel model for credit card fraud detection using Artificial Immune Systems.* Applied Soft Computing, 24, November 2014, pp. 4049.

[12] R. Huang, H. Tawfik and A. Nagar, (2010). *A novel hybrid artificial immune inspired approach for online break-in fraud detection.* Procedia Computer Science, 1(1), May 2010, pp. 27332742.

[13] Internet Crime Schemes, Federal Bureau of Investigation Internet Crime COmplaint Center (IC3). [Online]. Available: https://www.ic3.gov/crimeschemes.aspx.

[14] S. Anwar, J.B.M. Zain, M.F.B. Zulkipli and Z. Inayat, (2014). A review paper on botnet and botnet detection techniques in cloud computing. Proceedings of the ISCI, pp. 28-29.

[15] General Data Protection Regulation: officially Regulation 2016/679 on the protection of natural persons in regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Online]. Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX

[16] NIS Directive: officially Directive (EU) 2016/1148 concerning measures for a high common level of se- curity of network and information systems across the Union. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[17] Directive 2009/136/EC: amending Directive 2002/22/EC on universal service and users rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on co-operation between national authorities responsible for the enforcement of consumer protection laws. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

[18] Directive 97/7/EC on the protection of consumers in respect of distance contracts. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0007&from=EN

[19] Unfair Commercial Practices Directive: officially Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:en:PDF.

[20] Directive 93/13/EEC on unfair terms in consumer contracts. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0013&from=EN.

[21] Directive on electronic commerce: officially Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=en.

[22] Commission Delegated Regulation 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1675&from=EN.