Attack Types and Intrusion Detection Systems in Cloud Computing

U. Oktay and O.K. Sahingoz

***Abstract*— In recent years, lots of organizations have adopted their systems for enabling cloud based computing to provide scalable, virtualized on-demand access to a shared pool of computing resources such as networks, servers, storage, applications and services. Mainly cloud computing technology enables users/enterprises to eliminate the requirements for setting up of expensive computing infrastructure and reduces systems' operating costs. As a result, this technology is used by an increasing number of end users. On the other hand, existing security deficiencies and vulnerabilities of underlying technologies can leave an open door for intrusions. Therefore, cloud computing providers need to protect their users' sensitive data from insider or outsider attacks by installing an intrusion detection and prevention system. In this paper, it is aimed to define different attack types, which affect the availability, confidentiality and integrity of resources and services in cloud computing environment. Additionally, the paper also introduces related intrusion detection models to identify and prevent these types of attacks.**

***Index Terms*— cloud computing, intrusion detection, intrusion prevention, security.**

I. Introduction

In recent years, cloud computing has rapidly emerged as a widely accepted paradigm in computing systems, in which an end-user can request some computing capabilities and services when he need it, and he can reach these resources across networks anytime, anywhere.

Pew Research Institute published a research about "the future of cloud computing", and depicted that about % 71 of technology stakeholders and critics believe that by the year 2020, most people will work in Internet-based applications, which can also be run from smartphones [22]. Therefore, it can be seen that the future of cloud computing technology is bright and will be widely used in the World.

While moving from traditional local computing paradigm to the cloud computing paradigm, new security and privacy challenges emerge because of the distributed nature of cloud computing. Some of these security vulnerabilities leave open doors, which stem from the existing computing models; and some of them, inherent from cloud-based models.

As a result, malicious users force these doors to attack the system, and they attack on end-users' private data; processing power, bandwidth or storage capacity of the cloud network. Cloud computing organizations have to provide a high quality service and protect the users' sensitive data. To prevent these attackers, firewall mechanism and/or Intrusion Detection System (IDS) are effective solutions to resist them. They can provide additional protection mechanisms on the cloud systems' distributed environments. IDS can identify suspicious activities by monitoring network traffic changes, configuration of the system, logs files, and actions of end-users. When such a suspicious event is detected, IDS sends an alert message to a person or monitoring console to trigger some actions for preventing these attacks.

In this paper, it is aimed to provide definitions and properties of different attack types in cloud computing and to introduce intrusion detection and prevention models to resist these types of attacks.

The rest of the paper is organized as follows: In the next section the cloud computing paradigm is introduced; In Section 3, security deficiencies and attack types of cloud computing are described; intrusion detection models and intrusion prevention models in cloud computing are detailed in Section 4 and Section 5 respectively, and finally conclusion and future works are depicted.

II. Cloud Computing

Ubiquitous computing is first defined conceptually as "accessibility of data with technological opportunities has to be realized with a continuous and an invisible way" by Mark Weiser who is a Xerox Palo Alto Research Center (PARC) Incorporated researcher with an inspiration from Philip K. Dick's Ubik novel [2, 3]. In Ubik, all objective entities are communicating each other as a smart entity. This communication occurs dependently with all factors in the environment. Communication networks allow data access perpetually independent from the environment. A real-time and location independent interactive communication environment was started to be used by inclusion of ubiquitous computing in daily life [4].

Cloud computing is an interactive communication model that is constituted in more than one place synchronously, easy to use, can be accessed whenever user needs, consist of configurable computing resources and needs minimal effort to achieve maintainability [5]. Nowadays cloud computing users are using services that they need from providers' computing resources and charged as they profited [6]. Cloud computing has many definitions in different resources, which are similar to each other. As a summary, cloud computing can be defined as today's computing technology that has time and location independent services, shaped with user's

Manuscript received July 15, 2013.

U. Oktay is with Turkish Air Force Academy (TuAFA), Yesilyurt, Istanbul, Turkey (e-mail: uoktay@hho.edu.tr).

O. K. Sahingoz is with Computer Engineering Department of Turkish Air Force Academy (TuAFA), Yesilyurt, Istanbul, Turkey (e-mail: sahingoz@hho.edu.tr).

needs, has a minimum effort to maintain and charged as the service usage.

A. *Specifications of Cloud Computing*

While there are many definitions of cloud computing, Mell and Grance highlight five essential characteristics [5]:

On-demand Service: A user can be provided by oneself with computing abilities such as server time and network storage whenever it is needed without any provider and human interaction.

Wide Network Accessibility: Cloud computing has to be held abilities, which are standardized on the network and can be accessed by different kinds of devices (mobile phones, tablets, laptops, workstations etc.).

Resource Pool: The provider's computing resources such as a storage area, processing power, network bandwidth and memory must be in a physical or virtualized pool, can be allocated dynamically or according to demand of the end-users and can be served multitenant at the same time. Users do not need to have any authority on the resources and do not know where the resources are.

Rapid Elasticity: Opportunities and abilities have to be provided, unserved and scaled interior or exterior in an elastic way. These services are introduced to end-users generally unlimited and provided as much as the requests.

Regular Service: Among to services, which are provided in cloud computing systems; resource usage can be monitored, controlled, reported; resource usage amounts can be determined and providers can serve these to users transparently.

B. *Structure of Cloud Computing Architecture*

Cloud computing architecture contains some types of actors, which can be either an individual or an organizational unit who attend cloud services/tasks. NIST defines five main actors [7]:

Consumer uses the cloud computing service and can be either an individual or an organizational unit. A consumer chooses the most appropriate service or services, which are provided by the cloud provider. Besides, the services are charged against to the agreement that is signed between the consumer and the provider.

Provider is an entity that is responsible for developing resources and services, which are used by individuals, organizations or consumers. Provider manages software, platform or infrastructure that is needed by consumers, and it builds obligatory technical infrastructure and provides specified service levels (mostly trust and security levels).

Auditor inspects whole information technology processes, performance and security issues independently within predefined criteria. Auditor must be a third party and can be either an individual or an organizational unit.

Broker: Manageability of cloud systems is very complicated because of its nature. Consumers can use cloud services not only get in contact with the provider directly but also broker. Broker organizes the connection between provider and consumer, and also manages performance and availability of the system.

Carrier realizes connection, communication and transfers between provider and consumer, and also it enables consumers can access to the services over communication infrastructure and other devices such as desktops, laptops or any mobile devices. Distribution of the cloud services can be realized via network and communication infrastructure or communication agents, which have high storage capacity opportunities.

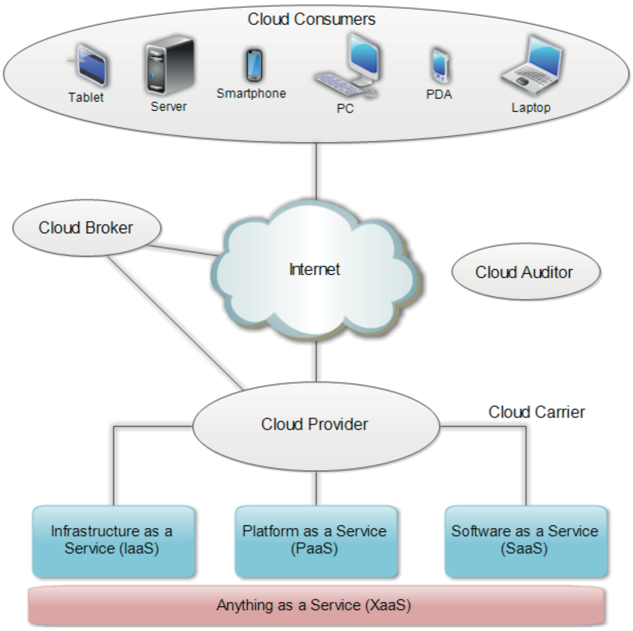
Cloud Consumers
Tablet
Server
Smartphone
PC
PDA
Laptop
Cloud Broker
Internet
Cloud Auditor
Cloud Provider
Cloud Carrier
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Anything as a Service (XaaS)

Fig. 1. Service models and actors in cloud computing.

C. *Service Models in Cloud Computing*

About the services, which are served over cloud computing systems there is a definition as *Anything as a Service* (XaaS). The word Anything defines the service, and it can take part as the type of the service like; *Communication as a Service* (CaaS), *Network as a Service* (NaaS) or *Monitoring as a Service* (MaaS). However, there are three fundamental service types to describe and define the service contents. They are *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) and *Software as a Service* (SaaS) [5]. These three main service models/actors of the cloud computing are shown in Figure 1 and detailed as follows.

Infrastructure as a Service (IaaS): With this ability, users can access processing power, storage area, network and other computing resources through opportunity and ability of the provider, also use every kind of software including operating system (OS) and applications. Users are not responsible for controlling and managing the cloud infrastructure, they only have authority on OS, storage, distributed software and network components which are going to be used.

Platform as a Service (PaaS): Users can develop and run software over cloud computing infrastructure via programming languages, libraries, services and with the tools that are supported by provider. Users are not responsible for controlling and managing network, server, OS and storage areas which are founded in cloud computing infrastructure, they can only interfere limited configuration changes.

Software as a Service (SaaS): All the infrastructure, platform and software utilities are supported and provided by the provider. Users can access to service based applications via different devices and interfaces as thin clients and network browsers. There are only some limited configuration authorities over the service based applications that can be made by users.

III. Security in Cloud Computing

While moving from traditional computing paradigm to cloud computing paradigm new security and privacy challenges has emerged. Security of the cloud computing system can be thought in two dimensions: physical security and cyber security.

Physical security concerns the physical properties of the system. For example, a data center, which is owned by provider infrastructure, has to realize security standards and hold security certifications globally, supervision and manageability on security preventions, incombustibility, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) are indispensable [8]. However twenty four hours and seven days monitoring for heat, humidity and air condition systems and also some biometric entrance systems may help for the business continuity.

On the other hand, *cyber security* defines the prevention of system from cyber world. There is a risk of cyber security attacks on services of cloud computing system. These attack can use huge amounts of computing resources, disables their usage by consumer efficiently. In this section mostly known attack types are detailed.

Insider Attack: Employee, entrepreneur and associates which are still or former attended who can or could access the whole information system with privileged authority are defined as *insider* [9]. Insider attacks are organized and run by these individuals to harm or temper knowledge about consumers or providers and include every kind of attacks which can be executed from inside [10, 11].

Flooding Attack: In this type of attack, attackers can send very large amounts of packets from exploited information resources, and they are called as zombie [11]. Packets can be either one of TCP, UDP, ICMP or a combination of these protocols. These kinds of attacks are mostly realized over unauthorized network connections. Because of cloud computing paradigms' nature, connections to the virtual machines are established over Internet. For this reason, exposition of cloud users with *Denial of Service (DoS)* and *Distributed Denial of Service (DDoS)* attacks are inevitable. Flooding attacks affect the availability of serviced for authorized users. An attack that is realized to a server which serves one kind of service can prevent a vast of scale accessibility to this served service. These kinds of attacks are called DoS attacks. If servers' resources are slogged after flooding attacks and it prevents the execution of other services, which run on the server, this kind of attacks are called indirect DoS attacks.

User to Root Attacks: In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system [11]. Buffer overflows are used for establish console connection for authorized processes. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines.

Port Scanning: An attack that identifies open, closed and filtered ports on a system [11]. In port scanning, intruders can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning are the most common scanning attacks. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

Attacks on Virtualization: After compromising hypervisor, control of the virtual machines in the virtual environment will be captured [11]. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates.

Multiple virtual machines use the same resource pool, especially hardware and with this kind of access side channel data has a chance to be captured, which flow one virtual machine to other [12].

Backdoor Channel Attacks: A passive attack type in which intruders compromise a node in the cloud and use this compromised node as a zombie resource to execute a DDoS attack. Trojans and similar structures on the system are help to compromise the system. After compromising system become a zombie and also data can be reachable on the system [11].

Storage allocation and multitenancy: There are some issues to be defined about the data that are processed on cloud [13]. Owner and control of the data, maintaining audit records, how and how much of the audit records will be shared with the consumer. To ensure consumers' data privacy, provider has to realize isolation of data and guarantee in service level agreement.

Authorization, Authentication, Encryption, Key and Identity Management: Different from conventional information technologies, in cloud computing deployment of virtual machines, IP addresses and resources are dynamic [13]. Authorization, authentication and identity management have to be configured with affectless from this dynamism in the way of synchronization. While achieving this configuration, data privacy is also indispensable. And the way of achieving data privacy a well-defined, well-configured and well-maintained key management.

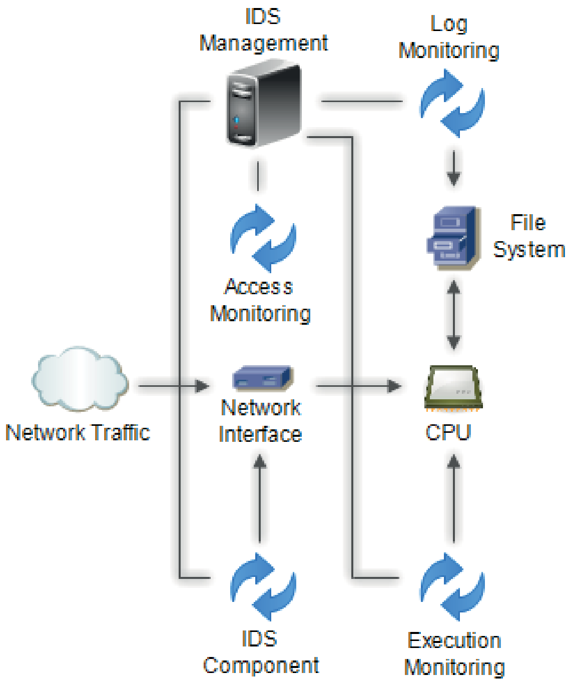

Fig. 2. Host-based Intrusion Detection System architecture.

Data Modification, Forgery and Integrity: Untrusted providers and system administrators can manipulate users' and consumers' data among to their own benefits [14]. Cloud users will be fall into a particularly bad position after such a manipulation or forgery occurs. With a combination of techniques like encryption and hash, this kind of integrity attacks can be prevented. AdjointVM and some improvement on AdjointVM are some solutions to prohibit tampering users' cloud data in the way of virtualization [15, 16].

IV. INTRUSION DETECTION IN CLOUD COMPUTING

As detailed in previous section, there are different types of attacks. *Intrusion Detection Systems (IDSs)* are one of the practical solutions to resist these attacks. IDSs are systems that realize intrusion detection, log detected information, alert or perform predefined procedures [17, 18]. They can be either hardware or software that includes whole observed computing entities. It does not mean every detected suspicious event is an intrusion. Some unexpected events can occur rarely, and it is a crucial point to decide if they are an intrusion or not. Mainly there are three types of IDS in cloud computing systems: *Host based IDS, Network based IDS, and Distributed IDS.*

A. Host-based Intrusion Detection Systems

Host Based IDSs analyze the suspicious activities like system call, processes or thread, asset and configuration access by observing the situation of host. It is especially used to protect valuable and private information on server systems. HIDSs are able to assign as NIDS if they are installed on a single host and configured to detect network activities. HIDS is composed of sensors located on servers or workstations which are made to prevent the attacks to a host. An HIDS is not just monitor network traffic, it can also trace more and settle with local settings of an OS and log records. The basic structure of a HIDS is shown in Figure 2 [18].

B. Network-based Intrusion Detection Systems

Network-based IDSs (NIDS) observe, monitor and analyses the specified and pre-identified network traffic. It can detect different situations based on specified points and generally located between the end point devices like routers, firewalls. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. Network traffic stacks on different layers and every layer delivers the data coming from a layer to another layer. OSI reference model and TCP/IP model define how these layers works and manages the traffic. An example for NIDS architecture and sensor placement is shown in Figure 3 [18].

C. Distributed Intrusion Detection Systems

Distributed Intrusion Detection System (DIDS) is the way of intrusion detection in a distributed environment such as grid and cloud computing [19]. All the components in the distributed area communicate each other with an agent-based approach. There are three fundamental components and assignments are similar to other types of IDSs' components. Main subject in DIDSs deal whole system like a traditional network or host [20]. DIDS components do not have a worldwide accepted standard, but there are network and host based sensor components, detection engine and management component. A systematic model of a DIDS is shown in Figure 4.

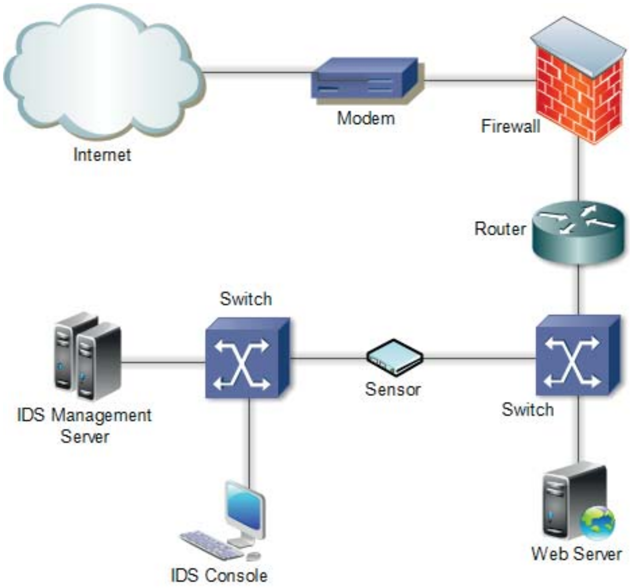

Fig. 3. Network-based Intrusion Detection System architecture.

D. Network Behavior Analysis Intrusion Detection

Network Behavior Analysis Intrusion Detection (NBAD) is an intrusion detection methodology which is providing to decide if the network traffic is suspicious or not by the statistical data and formal situation of network traffic. Sensors detect DoS attacks with the help of to be aware of

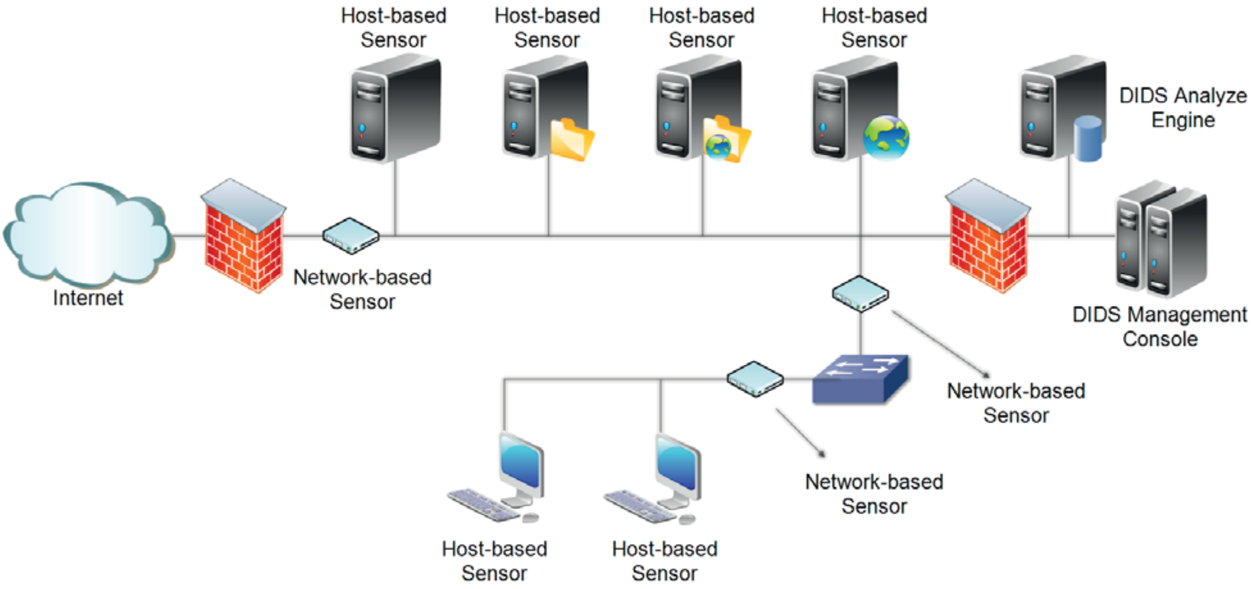

Fig. 4. A systematic view of Distributed Intrusion Detection System.

the network traffic and unexpected application services and rule violations by scanning the network. Traditional NIDSs and NBAD systems share some common components like sensors and management consoles, but NBAD systems generally do not have database servers, unlike the traditional NIDSs. NBAD systems work to decide in the case of unexpected data traffic. It is generally efficient to detect DoS attacks and worms.

V. INTRUSION PREVENTION SYSTEMS

An Intrusion Prevention System (IPS) holds all capabilities of IDSs and plus prevention characteristics [17]. IPSs can interfere most of the component in prevented environment. In a nutshell, security of a system has some traditional steps. There will be a firewall, IDS, IPS and guard system behind modem, router or switches where ever it is needed. IPSs can change configurations of manageable computing entities. If an intrusion detected by the mechanism, a firewall rule can be applied, a routing configuration can be changed, or a virtual machine can be isolated among security procedures.

In cloud computing, intrusion detection and prevention transactions and processes are a challenging issue because of many reasons. Fundamentally, because of the distributed nature of the cloud computing systems, all monitored and prevented resources are taken place in many different locations. Sometimes, they will be in different countries. So that, intrusion detection sensors placement, collecting intrusion data, analyzing by detection engines and interfering for prevention precautions are not easy to implement and apply. At the same time, load balancing, allocation of CPU and memory, deciding for positive and negative rates, bandwidth usage and so the whole price because of pay per usage model is the areas to be overcome.

Proxy Network Intrusion Detection System for Cloud Computing is introduced to minimize expenditures of hardware usage [21, 22]. The study based on locating a NIDS in a virtualization based cloud environment by putting on intrusion detection assignment on a different entity in the network. So the expenditures of hardware usage (CPU and memory) aimed to be reduced. Studies and models must study and concentrate for the most effective and proactive detection and prevention approaches.

VI. CONCLUSION

Cloud computing is a rapidly emerged technology and it is a widely accepted computing paradigm all around the world by its advantages on quick deployment, cost efficiency (on setting up and improvement), large storage space, and easy access to system anytime and anywhere. Apart from these advantages it has some disadvantages on security and privacy concerns, which are seen as the primary obstacles to wide adoption. At the same time, because of the distributed nature of the system, there is a risk of security attacks on services and resources in cloud computing. These attacks can be both outside and inside the cloud provider's network. In this paper, we have introduced the security issues of cloud computing and in terms of attack types and their defense mechanism by means of intrusion detection and prevention systems.

REFERENCES

[1] J.Q.Anderson, L. Rainie, "The Future of Cloud Computing", http://pewinternet.org/~/media//Files/Reports/2010/ PIP_Future_of_the_ Internet_cloud_computing.pdf

[2] M. Weiser, "The Computer for the 21st Century," Scientific American Special Issue on Communications, pp. 94-104, 1991.

[3] P. K. Dick, "Ubik," Doubleday, 1969.

[4] D. Amor, "Internet Future Strategies: How Pervasive Computing Services Will Change the World," New Jersey: Prentice Hall Computer Books, 2000.

[5] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, NIST Special Publication 800-145 (SP800-145)," National Institute of Standards and Technology, Gaithersburg, September 2011.

[6] U. Tupakula, V. Varadharajan and N. Akku, "Intrusion Detection Techniques for Infrastructure as a Service Cloud," *Proc. IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, Sydney, 2011, pp. 744–751.

[7] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291 (SP500-291)," Gaithersburg, July 2011.

[8] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," *Proc.* MIPRO, 2010 Proceedings of the 33rd International Convention, Opatija, 2010, pp. 344-349.

[9] D. M. Cappelli and R. F. Trzeciak, "Best practices for mitigating insider threat: Lessons learned from 250 cases," [Online]. July 2013, Available: http://www.cert.org/archive/pdf/RSA-CERT-InsiderThreat.pdf.

[10] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider Attacks in Cloud Computing," *Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, 2012, pp. 857–862.

[11] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, January 2013.

[12] J. C. Roberts II and W. Al-Hamdani, "Who Can You Trust in the Cloud ? A Review of Security Issues Within Cloud Computing," *Proc. Information Security Curriculum Development Conference,* Kennesaw, 2011, pp. 15-19.

[13] M. K. Srinivasan and P. Rodrigues, "State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud," *Proc. 2nd International Conference on Advances in Computing, Communications and Informatics,"* Mysore, 2012, pp. 470-476.

[14] S. Meena, E. Daniel and N. A. Vasanthi, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," *Proc. International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2013, pp. 1076-1081.

[15] J. Kong, "AdjointVM: a new intrusion detection model for cloud computing," Energy Procedia, vol. 13, pp. 7902-7911, 2011.

[16] U. Oktay, M. A. Aydin and O. K. Sahingoz, "Circular Chain VM Protection in AdjointVM", *Proc. The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE2013)*, Konya, 2013, pp. 94-98.

[17] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94 (SP800-94)," Gaithersburg, February 2007.

[18] G. Tyler, "Information Assurance Tools Report Intrusion Detection Systems," Information Assurance Technology Analysis Center (IATAC), September 2009.

[19] R. Robbins, "Distributed Intrusion Detection Systems: An Introduction and Review," SANS Institute Information Security Reading Room, GSEC Practical Assignment, version 1.4b, Option 1, January 2002.

[20] X. Qing, "The Structure Design of A New Distributed Intrusion Detection System," *Proc. 2nd International Conference on Computer Engineering and Technology (ICCET),* Chengdu, 2010, pp. 100-103.

[21] U. Oktay, and O. K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing", *Proc. The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE2013)*, Konya, 2013, pp. 99-105.

[22] U. Oktay, "Proxy Network Intrusion Detection System for Cloud Computing," MSc. Thesis, Department of Computer Engineering, Turkish Air Force Academy (TuAFA), Istanbul, 2013.

U. Oktay was born in Istanbul in 1984. He graduated from the Computer Engineering Department of Turkish Air Force Academy (TuAFA) in 2006. He received his M.Sc. degree from Computer Engineering Department of TuAFA Aeronautics and Space Technologies Institute (ASTIN), Istanbul, Turkey in 2013. His research interests include cloud computing, intrusion detection and cyber warfare and security.

O. K. Sahingoz is currently an assistant professor in the Department of Computer Engineering at Turkish Air Force Academy. He graduated from the Computer Engineering Department of Bogazici University in 1993. He received his M.Sc. and Ph.D. degree from Computer Engineering Department of Istanbul Technical University, in 1998 and 2006, respectively. His research interests lie in the areas of Wireless Sensor Networks, Artificial Intelligence, Parallel and Distributed Computing, Soft Computing, Information Systems, Intelligent Agents, Multi Agent Systems.