International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 6, No. 1 (Jan-2018)

http://dx-doi.org/10.12785/ijcnt/060104

Detection and Prevention Cyber-Attacks for Smart Buildings via Private Cloud Environment

Zaid A. Ali[1] and Siddeeq Y. Ameen[2]

[1] *Ministry of Higher Education, Baghdad, Iraq*
[2]*Department of Management Information Systems, Applied Science University, Bahrain*

Received: 2 Oct. 2017, Revised: 20 Dec. 2017, Accepted: 22 Dec. 2017, Published: (1 Jan. 2018)

Abstract: The paper investigate a major challenge of the protection of mutual and transmitted data that exchanged between smart buildings and data centers that works through private cloud computing environment. This challenge faces the operators and officials of private cloud computing and smart building. The paper highlighted a protection system to secure circulation data through a proposed intrusion detection and prevention system IDPS. The IDPS geared and routed to protect software and application on the private cloud. IDPS also provides protection to the private cloud platforms by using a rule set of agents and sensors. Data collected from these sensors are stored in complementary memory that helps to reduce detection time by avoiding the duplicate detection process by helping the IDPS to accept or ignore the alerts from sensors.
The proposed IDPS have been implemented and the results of simulation showed that active IDPS works efficiently in the open-source environment. Agents and sensors are working to monitor network events and analyze diverse network packets to detect attack signature. The system contributed to reduce the detection time and increases the service reliability in the private cloud.

Keywords: Intrusion Detection Prevention System, Sniffing Suspicious Packets, Data Incubator and Checking System, Private Cloud Computing, VLAN.

1. INTRODUCTION

As the use of Internet increase, the penetration of the Internet in the daily life has become more spread of information and access to it. The traditional methods used in data and network security considered, such as the mechanics of data and firewalls and other methods encoding is not sufficient on its own. IDPS was nominated and elected as the best mechanism for insurance computing systems and it became the first perfect choice to secure important IT projects [1]. By taking advantage of the many programs and computer systems enables us to monitor and identify scenarios used to attack the heavily for tidied computer networks and terminals associated to determine the fingerprint of the types of attacks on computer networks [2]. Normal and classical IDPS relies in its work on the cultivation of systems software in the form of agent sensors deployed in the network cultivated in a separate terminal to protect and monitor the specific networks and secure it from attack [3].

Humans generally become interested now broadly to achieve their business, especially after the emergence and spread of private cloud service. Private Cloud computing is an ideal way to codify and reduce expenditure and effort on building networks server rooms and software system. Private Cloud computing technology has enabled a lot of institution and companies that do not have their own data centers to take advantage of the timber in the private cloud computing.

In this paper we present a method of IDPS work within the cloud focuses its work on the protection of the software service in the cloud and protect the users of these services. The proposed system consists of two main parts; the first central station connected the second parts consisting of asset of sensors and agents planted in parts of the network. The IDPS is working to compile data received from agents and sensors distributed across multiple computer checks linked through electronic cloud. The proposed system adopts the mechanism of networking based on the virtual local area network (VLAN) to hold the collection of data from distributed network implicitly linked through electronic cloud.

E-mail: zaid.aaraji74@gmail.com, prof-siddeeq@ieee.org

2. RELATED LITERATURE

A. Intrusion Detection Prevention System

The IDPS are software and/or hardware acting independently or interconnected with each other manages and controls. The passage of the retina process information packages and events within the network, are analyzed to detect any suspicious events. This data and information are collected to prepare reports for interaction and manage the new events. From this an IDPS consists of the central part that collected and recorded information in a database. This information is used to activate the warning mechanism and stimulate alarm system [4]. The control unit is used to monitor and raise the warning and alarm system and sensors or agents that work to generate the information. IDPS can be divided into two parts Network NIDPS and Host Intrusion Detection System (HIDPS) [3], [5].

The main function of the NIDPS is mainly focused on the detecting unknown attacks by sniffing and capturing the data packet exchanged between networks and analyzes them. Sniffing information through sensors distributed in parts of the network. The sensors collect data and deliver it to a central unit for the study and evaluation of these data. The system focuses on the protection of the terminals on the sensors [4], [6]..

HIDPS emerged in the beginning prompt a software system for the protection of the mainframe computer and central computers in the network without attention to the terminal station. It is based in its work to monitor incoming and outgoing packets from computer system [5]. The system administration and management is very complex because it requires the data on all grouped computer to be analyzed. Therefore, the system software is existed in specific computer client within the system network. However this client is vulnerable to attack the others [7].

Methods of detecting and prevention intrusion system are divided into two main parts: misuse IDPS and anomaly IDPS.

Misuse IDPS which is the preferred type of intrusion, the most widely used. This type focuses in its work on the analysis of the expected attack patterns and works by relying on the analysis of events and activates and search for predefined patterns of attacks. This is done by placing the imprint attack specific signature for each predefined style scope. The overall shape of the system depends on the method of determining each style of patterns independently, it is determined by the signing of each style and the development of a central database of types of each style and development of a central database of types of attacks anticipated base. This database is updated automatically on cultural norms attack [5]. The system works in professional manner so that it does not give any false alarms, as well as the system automatically do not need any specific training.

Anomaly IDPS aimed at non-natural activates and distorted pattern of events. This type is used a narrow range of users with a specific style focuses on detecting abnormal events and actions especially at the level of the client and at the network level in general. The system prepares profile reports of normal action for all the system elements (users, client, and networks). The system relies on mentoring the system elements to identify and diagnosis abnormal behaviors that works in anomaly from normal operation. The system has weaknesses, such as the existence of many alerts and false alarms [5]. Working of the system needs a comprehensive training to be able to separate and isolate natural patterns from anomalies.

B. Electronic Cloud Computing Architecture

Private cloud computing and its contents of properties and services can be defined as a payment of specific amounts for the provision of limited computing services process by providing network access and get benefit from its resources for customizing services [7], [8]. In other words, we can say it access to computer services and software requirement in simple and effortless process. Cloud computing divided into three parts Infrastructure as service (Iaas), Platform as service (Paas) and Software as service (Saas). Any part of the three cloud computing do not contain any mention to the hardware parts (network parts and software) [9].

The first part paas is the the basic tier system for cloud computing. It contains the virtual clients and virtual. computing network and provides software services through this layer. It contribute seriously to reduce the infrastructure computing expenses and provides a new and effective concept to get into the published software applications [9].

The second part infrastructure as service (iaas) represents the middle class of the system and contains the varied virtual operating systems. It provide a suitable working environment programmers and systems integrators and operate the hardware resources and virtual resources [9].

The third part software as service (saas) provides the services delivery portal and access to the software through it. It represents the class that deals with the end users and acts as a services provider to provide incubated applications through network or Internet connection [9].

Private Cloud computing leadership of the process needs to be skilled in its main three parts. These skills are very important to connect the virtual parts of the cloud with the hardware parts. With all that has been mentioned, should not be overlooked update of the cloud and the development of services offered through it [10].

The benefits of the private cloud computing can be summed up in the following [3], [11]:

i. A safe and reliable usage of electronic communication network for government institution.

ii. Savings in the hardware and software purchase and operating systems consumption coordination.

iii. Reduction in the private expenses for training that required to manage resources effectively.

iv. Direct and immediate access to cloud computing services without human intervention (the user deal directly with the cloud system).

v. Dynamic services according to the need to reduce or increase the amount of resources at any time and without limitations.

vi. Massive scalability and the ability to absorb a huge amount of software, operating systems and strong space.

vii. More usages of virtual terminals and hardware resources.

viii. A genuine partnership between users and the system for providing protections and data.

C. E-Cloud Computing security and Smart Buildings

Cloud security is a shared responsibility between the cloud management and users, so the cloud security had become a penchant from both sides. All signs indicate that the concept of the cloud will be the closest option for all institutions and companies for providing access speed and ease of use at the reasonable cost. Thus the cloud and its services will be susceptible to multiple types of cyber–attacks [12]. The security challenge is a common concern among service providers and customers. Smart buildings are those that have into their design and build the possibilities of easy and direct access to various types of networking (wired and wireless). Providing networking requirements is a major and active for all government and commercial institutions [13]. Smart buildings are no longer confined to large companies and institutions, but the case has become pressing need, even in small companies and institutions. Quick access to Internet services and video conference and networking has become the object and purpose of each institution.

Security concerns and the protection of smart buildings is the biggest concern for officials and operators of smart buildings [14]. Furthermore, access to the E-cloud computing through network connection allows multiple security options for users, according to the nature of work [15]. In this aspects, it worth to mention that cyber-physical systems are used integrate computational and physical elements and manage the significant and intimate couplings between the two aspects. These complex systems increasingly operate in loosely supervised and complex environments, interact with the Internet and its services, operate with a high degree of autonomy, involve humans-in-the loop, and, often, are safety critical [16].

3. PROPOSED PRIVATE CLOUD COMPUTING IDPS

We proposed a mechanism for the adoption of intrusion prevention system to ensure the protection of the E-cloud computing, virtual network and users. This will provide protection from cyber-attacks. The protection system based in its work to protect software and deployed application via the cloud.

The proposed restructuring of the system includes four overlapping phases that provide the mechanism of detection and prevention system of E-cloud from diverse attacks. These four overlapping phases shown in Figure (2) are:

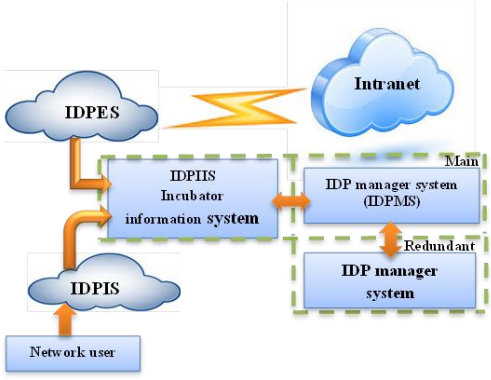

Figure 1. Represents the cloud computing IDPS mechanism.

i. Intrusion detection prevention internal sensors (IDPIS) that specially used to check the information and data packet that pass or access from external sensors, the IDPIS does not generate many of false alarm.

ii. Intrusion detection prevention external sensors (IDPES) that is an external sensor give us a good vision to detect the type of cyber-attack directed to virtual networks.

iii. Intrusion detection prevention incubator information system (IDPIIS) which is used to assemble the hyphen data from the sensors, analysis and expected the nomination of attacks.

iv. Intrusion detection prevention manager system (IDPMS) which is used to read the detected reports generated by the IDPIIS. It contains the decision making and matching system and has the ability to get access to the other parts of the system through remote controller.

A. Intrusion Detection Prevention Mechanism

Usually the security system (IDPS) is placed in a separated host in the network that is connected through the private cloud. Therefore, the IDPS will use some of the hardware and software resources of the private cloud to work optimally. The IDP deals with all the type of network packets at the same security level. Sensors planted in the networks and its hosts must have the ability to distinguish data packets and other type of packets, like connection establishment and FIN packets.

In general, using IDPS will reduce the network speed. Thus small light programs were used and planted in the network edge as a sensor. These sensors have the ability to distinguish between all the different types of the packets. Sensors are classified and divided into two main sections. The first section identifies the predefined cyber-attacks based on pre-built database of known attacks, whereas the second type is working on trying to uncover new abnormal behavior and then analyze and feed the database [17]. Sensors work as a reliable link especially external sensors between the internet and the private cloud computing on the one hand and between the private cloud computing and the VLAN, associated with it.

One of the major tasks of the security system is to provide and ensure the security of sensors system. Basically main targets to any cyber-attacks directed to stop the work of sensors system, so the IDPS trying to make them hidden.

B. Sniffing Suspicious Packets Procedure

Detection and screening process for packets is the solidarity of responsibility between the sensors and the (IDPIIS). Detection operation is done by the sensors help to reduce the burden on the protection system. Thus, it is no longer need to send packets that examined by the sensors to the (IDPIIS). Within intrusion detection and prevention system that work and operate in real-time action based sensors works to sniff and examine each data packet that sent and received (Rx and Tx). When use an intrusion detection and prevention system we must accept the idea of a delay in the transmission and receipt of the packets. In the aspect of sniffing and suspicious packets avoidance, the proposed system should be used for:-

- ✓ Simple packet sniffer.
- ✓ Packet logger and debugging.
- ✓ Network intrusion prevention system.

Therefore, the first phase in detection process is to examine the header of the data packets, where the main function of the sensors is depth examination and analysis with packets that showing suspicious signs [18]. Normal packets are not allowed to intercept there way access without delay. The flowchart shown in Figure 2, shows the screening and detection steps that exposed the network data packets into the proposed intrusion detection and prevention system.

C. Data Incubator and Checking System Procedure

The IDPS checked all incoming and outgoing data packets. Screening process carried out in cooperation between the internal and external sensors and between IDPIIS. Sensors are distributed in parts of the system in the form of work groups, group planted in the Cloud and other aggregates are distributed in virtual networks and terminals. The system works by receiving data packets, to ensure no loss of any data packet. The Memory stationed in IDPIIS. Memory usage helps to speed up the process of detection and disposal of cases of multiple and frequent disclosure. Therefore, a cash memory is equipped with the system.

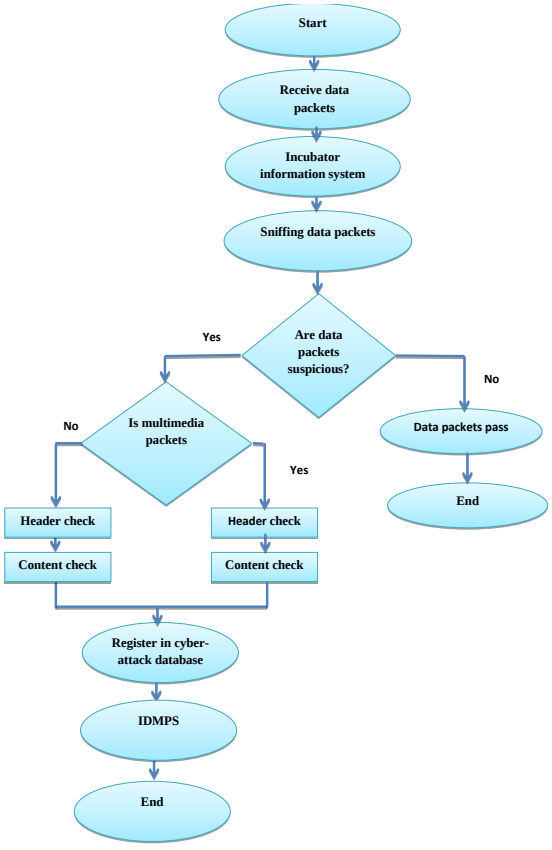

Figure 2. Represents the cloud computing IDPS mechanism.

The incubator absorbs all packets and assembled in order to be transferred later to sniff packets program such as Snort or any other program [19]. The main function of the program is to examine the packet header and data content. In addition to that, the sniffer program analyzes and identifies network protocols used. Data packet analysis helps to know the type of data contains a suspicious kind of cyber-attacks like (OS fingerprinting

attempts, buffer overflows, CGI attacks, stealth port scan, SMB probes and ext.) [19]. Normal packets should leave to proceed in its process. When data packets are suspected of having the cyber-attack, the system determines whether they a normal data or multimedia packets [17]. The processes of determining the content of the packets are necessary for the purpose of routing packets to their own sensors group.

The system contains a superset of some special sensors firmly normal data and other private firm multimedia, this process helps to avoid a repetition of the case in the examination of packages, in addition to control cash memory consumption. The sensors performed pre-testing of data packet. If there is any suspicion of a cyber-attack in the data packets, these packets will diverted into the (IDPMS) and then incorporated and registered in the database of the kinds of cyber-attack.

4. THE PROPOSED IMPLEMENTATION AND EVALUATION

The implementation and testing environment of the proposed (IDPS) is done in real and effective data center. The data center runs using open source operating system (Linux Squeeze) and contains 19 servers. Mainly the major part of the data center is the repository system, which contains (apache web server), database server (MySQL server), file server type (Fedora), search engine (Solar) and content management system (CMS) type (Drupal6). The repository system divided into three layers, user interface layer (UI layer), application layer, and storage data layer as shown in Figure 3.

The main objective of the proposed intrusion detection prevention system (IDPS) is to secure data center servers, secure data center from internal and external attacks based on the Integration work of both internal and external sensors. Therefore, the essential function of the IDPS is to protect the Intranet cloud computing that connected together with the data center which can be considered as the Intranet cloud computing with the data center as a secure Intranet network by using the proposed IDPS.

The main part in IDPS is internal and external sensors. External sensors collect information from VLANs that connected to the data center and then feeding the system protection database with the information. Internal sensors are present in all the computers and clients linked to the network. These sensors automatically loaded in the computers during the association computer or peripheral to the network, this process is done through three ways handshaking.

The main (IDPMS) are placed in the apache web server and the redundant (IDPMS) are placed in the file server (fedora server). Data are exchanged in real time between the main and redundant system, and working in (active: active) mode.

For each virtual network (VLAN) connected to the cloud computing we put a dedicated intrusion detection prevention incubator information system (IDPIIS). All the intrusion detection prevention incubator information system (IDPIIS) are assembled in specific server named (incubator information server), where internal and external sensors groups are associated with that server.

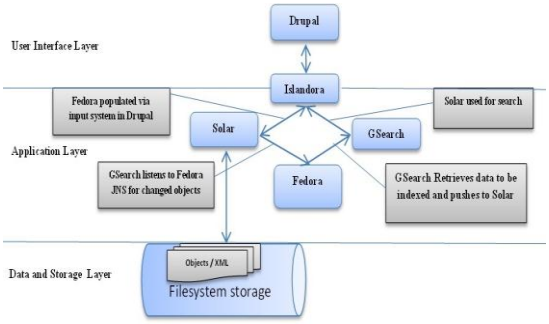

Figure 3. The Repository System Architecture

TABLE I. REPRESENTS THE NETWORK ADDRESSES (IP ADDRESSES) OF THE DATA CENTER SERVERS AND VIRTUAL NETWORKS (VLAN) BEING USED EFFECTIVELY IN THE PROPOSED IDPS

Servername	Specification	IP Details
Apache web server	Main (IDPMS)	IP: 172. 16. 0.5 Subnet: 255.255.255.0
Fedora File Server	Redundant (IDPMS)	IP: 172. 16. 0.7 Subnet: 255.255.255.0
Incubator Information Server	Collect VLANs Information	IP: 172. 16. 0.8 Subnet: 255.255.255.0
	VLAN 1	IP: 172. 16. 1.0 Subnet: 255.255.255.0
	VLAN 2	IP: 172. 16. 2.0 Subnet: 255.255.255.0
	VLAN 3	IP: 172. 16. 3.0 Subnet: 255.255.255.0
	VLAN 4	IP: 172. 16. 4.0 Subnet: 255.255.255.0
	VLAN 10	IP: 172. 16. 10.0 Subnet: 255.255.255.0

Testing the proposed system on the proposed environment shows that the proposed protection system detects and prevents most of the known types of attacks like brute force attack, DDOS, fingerprint attack, MIM (Man In middle) attacks and more than thirty other kinds

of attacks. This will preserve the availability of the private cloud, integrity and continuity of services.

Reliance on the protection system, the (IDPS) provides the private cloud operators a variety of mechanisms of inspection and verification which works constantly. They became able to protect the cloud by taking advantage of sniffing and fully analyze packets as shown in Figure 4.

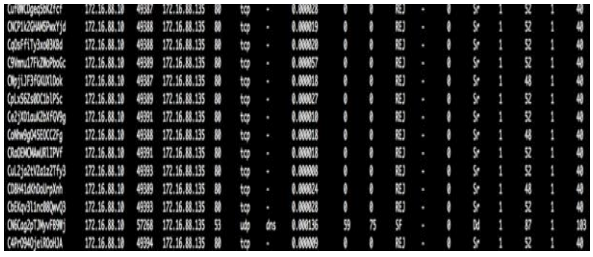

Figure 4. Summary of the full analysis and sniffer the network packets.

The results also show that the protection system provides a full description of all networking protocols that are exchanged between the networks IP. An example of this, the ability to listen and sniff the network packets of specific ports, or even listen to a specific port to focus surveillance and tracking operations like port (80) as shown in Figure 5.

```
172.16.88.10 49493 172.16.88.135 80 f52pwerp32iweqa57k37lwp22erl48g63m39n60ou.net /
172.16.88.10 49495 172.16.88.135 80 h54jtbqmuj56hwb48e41p42g33h34c29grbqfxm29.ru /
172.16.88.10 49511 172.16.88.135 80 iqcqmrn30iuoubuo11crfydvkylrbtmtev.info / -
172.16.88.10 49512 172.16.88.135 80 ezdsaqbulsgzh44m59p42eqmrkxa57n40brcq.com / -
172.16.88.10 49513 172.16.88.135 80 o41lwmqnqarmxiyi35iyftpzaye21osjyjq.ru / -
172.16.88.10 49516 172.16.88.135 80 n30arh24frisbslqmqoxgvpvk47o11pritev.biz / -
172.16.88.10 49517 172.16.88.135 80 jsa57n20hyisjxcre11fwl58gta37i65ovf32o51.info /
172.16.88.10 49518 172.16.88.135 80 j36lxf52hsj56itc49lqayoveymwfzosi15jw.org / -
172.16.88.10 49519 172.16.88.135 80 g53lvo61ayoucrm49kzgvm69irhwl58erjwfu.net / -
```

Figure 5. Listen and sniff to specific port

The results also show that the IDPS can detect stealth through ports which is known as the (SYN_ACK flags attack) and give us the ability to detect any attempts to spy on and sniff our network by using ARP scanner. Furthermore, the results show that the IDPS is capable to control and monitor the work of specific port or ports to see if the port request was rejected (rej) or the request had no replay(S0) or if the port don't have SYN_ACK(SH) as shown in Figure 6.

```
172.16.88.10 49508 172.16.88.135 80 tcp REJ
172.16.88.10 49510 172.16.88.135 80 tcp REJ
172.16.88.10 57852 172.16.88.135 53 udp SF
172.16.88.10 49509 172.16.88.135 80 tcp REJ
172.16.88.10 57399 172.16.88.135 53 udp SF
172.16.88.10 49510 172.16.88.135 80 tcp REJ
172.16.88.10 57456 172.16.88.135 53 udp SF
172.16.88.10 49511 172.16.88.135 80 tcp S0
172.16.88.10 62602 172.16.88.135 53 udp SF
172.16.88.10 54957 172.16.88.135 53 udp SF
172.16.88.10 49511 172.16.88.135 80 tcp SH
172.16.88.10 49512 172.16.88.135 80 tcp S0
```

Figure 6. Control and monitor specific port

From the above results, we found that:

i. The proposed system can handle any size of data exchanged via private cloud environment.

ii. Memory have been utilized effectively and increases the effectiveness of processor consumption as a result of ignoring the redundant packet since more than 50% of the network packets are duplicated.

iii. IDPS location within the private cloud environment is of high benefits in the implementation of the analysis, tracking and detection operations for network packets.

iv. Adoption distributed work scenario for system parts made it difficult to attack the infrastructure of the cloud.

v. The complementary memory usage within the protection system is working to update itself automatically to record all suspicious activities and incidents within the environment of the private cloud.

5. CONCLUSIONS

The proposed system was designed and applied to work within a limited Intranet networks connected with each other through electronic cloud computing. Results of observation and analysis of the data exchanged between virtual networks on one hand and between the data center on the other hand, show that the system security is well maintained. Furthermore, the system provides the efficiency and flexibility in the transmission of information between the cloud computing parts.

Using internal sensors and external sensors provide an acceptable level of protection and reliability of the data collected by these sensors. The collection of internal and external sensors into a single system process certainly provides an added security value. However, it causes an increase in the complexity of system administration, and make it respond to any act of additional burden with a a faster process speed. Finally, adding memory to the

working system accelerate the process of analysis and detection of potential violations.

Future research can be conducted in the improvement of the system security and applied on the Internet and in line with the rapid developments in the electronic cloud services via the Internet. Further research recommendation is to make the system able to examine and analyze the content of multimedia packets because they represent the most commonly used methods to penetrate and attack the Internet networks and find an efficient way to manage the data retrieval process from cloud computing.

REFERENCES

[1] J. Weng and G. Qin, "Network Intrusion Prevention Systems", JTB-Journal of Technology and Business, pp.37-49, October 2007.

[2] U. Thaker, "Honey Analyzer–Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot", the second International Conference on Innovations Information Technology, Dubai, UAE September, 2005 26-28.

[3] E. Amoroso and R. Kwapniewski, "A Selection Criteria for Intrusion Detection Systems," Proc.14th Ann. Computer Security Applications Conf., IEEE Computer Soc. Press, Los Alamitos, Calif., 1998, pp. 280–288.

[4] K. A. Scarfone and P. M. Mell. Guide to Intrusion Detection and Prevention Systems (IDPS).Computer Security Resource Center NIST Special Publication, January 2010.

[5] V. Marinova-Boncheva, "A Short Survey of Intrusion Detection Systems," Problems of Engineering Cybernetics and Robotics, vol. 58, pp. 23–30, 2007.

[6] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, vol. 31, no. 8, pp. 805–822, 1999.

[7] I. Mukhopadhyay, M. Chakraborty, S. Chakrabarti, A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems, Journal of Information Security, 2011, 2, 28-38.

[8] S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing. IEEE, 2009, pp. 729–734.

[9] K. Vieira, A. Schulter, C. Westphall, and C. Westphall,"Intrusion detection for grid and cloud computing," IT Professional, vol. 12, no. 4, pp. 38–43, 2010.

[10] 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, no. 1, pp. 1– 11, 2011.

[11] L. Youseff, M. Butrico, and D. Da Silva, "Toward a unified ontology of cloud computing," in Grid Computing Environments Workshop, 2008. GCE'08. IEEE, 2008, pp. 1– 10.

[12] X. JIANG and X. WANG, "Out-of-the-Box" monitoring of VM-based high-interaction honeypots. Proceedings of Recent Advances in Intrusion Detection. 2007, p. 198–218.

[13] J. Bruneau, C. Consel, M. O'Malley, W. Taha, and W.M. Hannourah. Virtual testing for smart buildings. 8th International Conference on Intelligent Environments (IE), 2012, pages 282–289.

[14] K. Khaund, "Cybersecurity in Smart Buildings inaction is not option any more", A Frost & Sullivan Collaborative Industry Perspective, Sep. 2015.

[15] J. A. Stankovic, J. W. Sturges, and J. Eisenberg, "A 21st Century CyberPhysical Systems Education", Computer Publication, IEEE Computer Society, Dec. 2017.

[16] W. Xin, H. Ting-lei, and L. Xiao-yu, "Research on the intrusion detection mechanism based on cloud computing," in Intelligent Computing and Integrated Systems (ICISS), 2010 International Conference on. IEEE, pp. 125–128.

[17] M. F. Umer, M. Sher and Y. Bi, "A two-stage flow-based intrusion detection model for next-generation networks", PLoS ONE 13(1), 2018.

[18] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network ids into an open source cloud computing environment," Sixth International Conference on Information Assurance and Security (IAS), 2010, 265-270.

[19] Brugger, S. & Chow, J. An assessment of the DARPA IDS Evaluation Data set using Snort, Technical report, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, 2007.

Zaid Ahmed Ali recived the B.Sc. degree in Electrical and Computer Engineering from Military Engineering College, Iraq, in 1997, and the M.Sc. degree in Computer Engineering from University of Technology, Iraq, in 2004.
He worked as a lecturer at AL-Rafidain University College in Iraq from 2004-presnt in addition to his work in the Ministry of Science and Technology(MOST), in Information Technology Directorate, as a deputy of the E-ministry project and the chief of the data center servers department. His researches interests are in the area of cloud computing services and administration of data centers. He has an experience in server's administration, information technology (IT), Web services and Service Oriented Architectures, and cloud computing.

Siddeeq Y. Ameen received BSc in Electrical and Electronics Engineering in 1983 from University of Technology, Baghdad. Next, he was awarded the MSc and PhD degree from Loughborough University, UK, From 1990- 2006, Professor Siddeeq worked with the University of Technology in Baghdad with participation in most of Baghdad's universities. From Feb. 2006 to July 2011 he was a Dean of Engineering College at the Gulf University in Bahrain. From Oct. 2011-Sep. 2015 he joined University of Mosul, College of Electronic Engineering a Professor of Data Communication. Finally, from Sep. 2015- Sep 2017, he was a Dean of Research and Graduate Studies at Applied Science University in Bahrain. Through his academic life he published over 100 papers and a patent in the field of data communication, computer networking and information security and supervised over 110 PhD and MSc research students. He won the first and second best research in Information Security by the Arab Universities Association in 2003.