YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.gov.tr/ybs

Yayın Geliş Tarihi: 30.04.2020 Cilt:6, Sayı:2, Yıl:2020, Sayfa:1-28
Yayına Kabul Tarihi: 14.05.2020 e-ISSN: 2630-550X
Online Yayın Tarihi: 27.12.2020

BULUT BİLİŞİM ORTAMINDAKİ YBS İÇİN SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ ÜZERİNDE BİR DEĞERLENDİRME

Ahmet EFE [1*]

[1,*] Internal Auditing, PhD, CISA, CRISC, PMP, Ankara Development Agency, Ankara Turkey

Sameer ABBAS [2]

Hakam SAMEER [3]

[2, 3] PhD Students, Department of Computer Science, Yıldırım Beyazıt University, Ankara, Turkey

Öz: Bulut bilişim (BB), talep üzerine kaynakları paylaşmak için ağ erişimine izin veren ve Yönetim Bilgi Sistemleri (YBS) tarafından uzaktan kullanılan çeşitli veri ve bilgilerin hesaplanması ve depolanması için kolaylık sağlayan bir hizmet modelidir. Bununla birlikte, güvenlik ve mahremiyet ile ilgili endişeler, kuruluşlar tarafından yaygın olarak benimsenmesinin önündeki başlıca engellerdir. Saldırı Tespit Sistemleri (STS) ve Saldırı Önleme Sistemleri (SÖS), genel olarak BT ve YBS güvenlik ve uyumluluk alıştırması için çeşitli tür tehditlerden veya saldırılardan elde edilebilen bulut kaynaklarını ve hizmetlerini kurtarabilen önemli araçlardır. Türkiye'de, TC Cumhurbaşkanlığı Dijital Ofisi tarafından devlet daireleri için bulut altyapısının kullanılması, doğrulanmış ulusal çözümler hariç olmak üzere 2019 yılından itibaren yasaklanmıştır. Bu araştırmanın amacı, en son bulut bilişim sistemlerinde teknolojik yenilik bakış açısını sunmak ve STS'nin BB ortamında güvenlik fonksiyonları açısından performansının değerlendirilmesini sağlamaktır. Ayrıca, BB ortamında yer alan işletmeler, kurumlar ve BT şirketleri için önemli güvenlik risklerine karşı makul önlemler geliştirmeye çalışıyoruz.

Anahtar Kelimeler: IDS, IPS, IDPS, WAF, Hibrit bulut, MIS Güvenliği.

AN ASSESSMENT OVER THE INTRUSION DETECTION AND PREVENTION SYSTEMS FOR MIS IN THE CLOUD COMPUTING ENVIRONMENT

Abstract: Cloud computing (CC) is a model that allows on demand into a network access to share resources and provides availability for computing and storing various data and information which are being used by Management Information Systems (MIS) remotely. Nonetheless, security and privacy are the main barriers to ease of success and widespread adoption by organizations. In addition, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have become better known in general terms for IT and MIS security and compliance exercise that can save attainable cloud resources and services from various kind of threats or attacks. In Turkey the usage of cloud infrastructure for government departments is prohibited by Digital Office of TR Presidency in 2019 except for verified national solutions. The aim of this research is to present technological innovation point of view in the latest cloud computing systems and provide an assessment of the performance of IDS in terms of security functions within the CC environment from the latest literature. We also try to recommend best actions of mitigation plans against major security risks for business and IT companies that are involved in the CC environment.

Keywords : IDS, IPS, IDPS, WAF, Hybrid cloud, MIS Security.

[*] Contact Author: icsiacag@gmail.com

1. INTRODUCTION

Cloud computing or, more commonly, online and remote distribution of information; is the general name of the services that enables sharing of information between information devices with remote intervention. Cloud computing is the system, storage and utilization of information and data in the store of phone-tablet-computer and similar devices on the internet and access can be provided if requested by third part cloud service providers. Cloud Computing service is offered in three ways: Infrastructure as a Service (IaaS), Platform as a Service (**PaaS**), Software as a Service (**SaaS**).

SaaS provides programs such as CRM, ERP, finance and accounting software that users need in the cloud. For companies operating in different locations, SaaS does not create extra software costs and provides a serious economic advantage. The best example for SaaS is Gmail. With this service from Google, you can send mail, edit your documents and back up your files. You can perform all your transactions even if you do not have software knowledge.

PaaS, enables application developers to develop their projects by offering hardware and software layers. This service offers platforms like system management, operating system, programming language environment, database etc. Since the system management is performed by the service provider, you only manage your applications and data. For example, you coded a software with PHP. You don't have to deal with the SQL and web server infrastructure of the software you encode. PaaS provides only the platforms on which your software should work.

IaaS, is the most basic service of CC. A virtual server is created with IaaS and users are provided with cloud server service. With the cloud infrastructure, virtual server resources are allocated for you. With IaaS, you have a flexible infrastructure. For example, web sites that organize holidays increase the need for server resources close to the start of the holiday seasons. The resources used can be increased / decreased at any time by making use of the flexible structure of Cloud Computing.

The events that make MIS in business the most remarkable subject are the continuous change of technology, the use of technology in management and its impact on business success. New businesses and sectors are emerging, old ones are decreasing, and businesses that learn how to use these technologies are becoming successful in the competition. In today's technology, Cloud computing platforms are emerging as an important innovation used in businesses. In this way, a flexible collection created from computers on the internet has started to do the work traditionally on corporate computers. Today, businesses represent developing cloud computer platforms based on new hardware and software technologies. Every day, more and more business software is moving from PC or desktop computers to mobile devices and remotely managed cloud platforms including corporate MIS solutions.

Cloud technology, in which all institutions and private organizations are in some way connected, can be considered as the services delivered and given when evaluated from different perspectives. Services can be obtained from the cloud technologies that are faster, safer and more flexible to the IT resources you need in an institutional sense including the functionalities of MIS software. This opportunity will save you from many costs as well as reduce your management costs. On the other hand, when it comes to data centers served, some of the most important parameters for network management will be continuity and security. It is very important that the advantages of cloud computing such as high processor power, capacity and bandwidth can be managed correctly. Again, considering the network management, it is important that the data has a dynamic structure such as capacity and service adjustments that are appropriate for the need.

Today, security is no longer an individual activity of IT departments. The types and objectives of the attacks have also been quite different, thus gaining an institutional dimension with business perspectives. Highly professional attackers and hacktivists are especially interested in resources and services used in cloud computing technologies. Therefore, the management and continuity of virtual resources used within data centers has also become important. Again, in countries like Turkey, attacks such as "*Stopping/disrupting access to information and services*" (Ddos etc.) and privacy violations (bank and credit card fraud) aimed at providing financial interests and hostile state sponsored cyber actions can be counted among popular attacks. Over time, the types of attacks and their goals may

vary. Energy, defense, education, health, corporate MIS etc. are now managed through cloud based digital systems. It should be noted that there may be international attacks such as information stealing or denial of service. Network management technologies need to consider these elements.

In spite of advantages of the internet, such as web service, sharing data, business and government electronic applications for efficient services there are also several disadvantages of security weaknesses in the internet and the hackers can make use of the internet to run several models of attack, for example Distributed Denial of System Attack (DDOS) (Kolahi, 2015). It is an arranged attempt targeting networks and services to make computer resources unavailable to its users. The aim of (DDoS) attack is to weaken bandwidth, processing capability of a targeted network (Stephen, 2014).

DDoS attacks have begun first at the beginning of the millennium. February 9, 2000 prime DDoS attacks were waged against E-Trade, Amazon, Yahoo.com, Buy.com Federal Bureau of Investigation (FBI) and often other websites fell as a victim to Distributed Denial of System Attack (DDoS) attacks resulting insubstantial damage and inconvenience (Peng, 2006) furthermore, the WikiLeaks site (WikiLeaks) has suffered from DDoS Attacks as well (Robinson , 2015).

The transition to cloud computing is in full swing. According to the latest data, at least one application of 73% of corporate companies or part of the IT infrastructure is in the cloud. But it seems that this is not enough. The findings show that IT departments are fewer than 100% pressure on the cloud. It is obvious that we are in a rapid change, but this brings with it risks. Meeting with more than 250 IT security leaders, Kaspersky Lab revealed that the uncontrolled transition to cloud computing was the biggest security issue for more than half of the Chief Security Officers (CISO) (58%). Using multiple cloud platforms within a hybrid cloud infrastructure, companies can offer their products and services faster, maximize their performance, and increase the reliability of their services. However, in spite of the advantages it offers, cloud computing can bring additional challenges to cyber security, especially when a third party provides the cloud infrastructure. The average cost of data leakage from open cloud services to corporate companies is around $ 2 million. Therefore, when an organization's overall IT infrastructure is used in conjunction with the cloud, CISOs face more challenges to ensure data security and maintain the company's material structure (Kaspersky, 2018).

Managing complex IT environments is becoming more and more difficult due to the lack of experts. This is another problem in corporate cyber security. For the transition to the hybrid cloud, it is necessary to have the ability to create and manage security in every part of the IT infrastructure. For CISOs this means a shortage of staff. 38% of CISOs say they find it hard to find experts to cope with this 'cloud farm'. In this environment, CISOs need not only a high level of security, but also a single solution that enables the company to manage and manage the cyber security layer across the entire cloud infrastructure with a limited cloud security team (Kaspersky, 2018).

It is very important to support the cloud platform's own security features while protecting data and workloads in the cloud environment. In protection layers; they have to have the ability to monitor application behaviors, stop suspicious activities, prevent exploits using the latest threat intelligence, find vulnerabilities and automatically install patches to protect data and workloads from threats in the cloud infrastructure. The best solutions also can offer management capabilities. This way, IT teams can control which workloads are accessed and which are used.

There are basic risks and difficulties in cloud computing, which threatens data security. To help mitigate threats, cloud industry leaders should invest heavily in risk assessment to ensure that the system encrypts data for protection, and industry leaders should establish a reliable organization to secure the platform and infrastructure and provide high assurance in the assessment. İn this study we aimed to work on security issues of cloud computing that must be addressed for a reliable cloud computing technology.

If we provide the general structure and definition of IDS systems; they are real-time detection of potential threats or attacks that may affect the operability of reliable and protected systems. In the system content, all packets passing through the network are examined and related details are kept in the log records. The important point here is that the system is only monitored and no precautions are taken by the IDS system; threats are only detected and information is provided to the personnel concerned in a correctly configured structure. IPS systems are an improved version of IDS systems.

With the development of technology day by day, we know that the use of computerized systems has become a necessity. Parallel to this, we observe that computerized systems have emerged due to security weaknesses and a different vulnerability has been detected in each new day. At this point, we can say that the process of detecting and taking measures against the weaknesses that have arisen with the use of IPS systems has decreased to minimum levels. Since IPS systems are structures that we consider as the advanced version of IDS, the harmful situations detected by IDS are detected both by IPS and in parallel, they take the necessary precautions against the detected vulnerability in software.

2. THE CLOUD COMPUTING SYSTEM CHALLENGES

The main goal of CC is to know that they only use what they want and pay only for what they use. Below Fig. 1 shows different aspects of the CC (Madhavi, 2012).

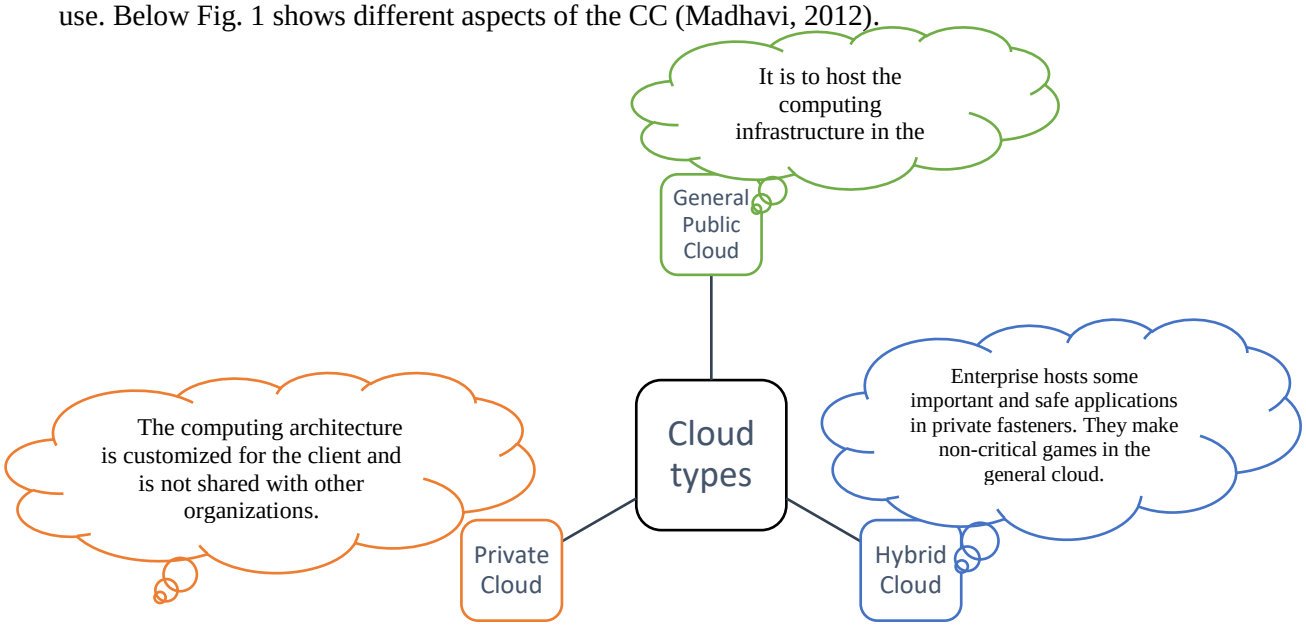


Figure 1. Depiction of main types of clouds

One of the biggest problems of IT sector, which is a constantly developing, comes from qualified workforce and cost effectiveness. Especially the companies that do not have primary working area informatics are more difficult to solve these problems than other firms. Providers of cloud computing services are a very good solution partners for companies within this scope. Due to the difficulties encountered in Cloud Computing, the companies that think about the transition to the cloud systems continuously postpone this process. This may also lead to the difficulty of predicting the problems that may arise after the transition.

2.1. Originality in applications:

With the increasing importance of information and the spread of information systems, information technologies have been of great importance for all companies. In the past, information technologies, which have helped the functioning of institutions, have been transformed into environments where all processes are carried out. Companies with in-house culture and business models that vary in many different sectors and different service areas benefit from information technologies effectively in order to reach their goals. These differences often make it difficult to form a common model. In Cloud Computing, especially for cost advantage, you create once than many times (built once use many) method. In particular, the fact that critical business applications are unique is the problem of firms' inability to adapt their business processes to common models.

2.2. Information Security

While it is difficult for companies to secure the security of their vital information, it is a serious problem that this information is stored in environments belonging to a third company. With the increasing financial value of the information with each passing day, the risk of industrial espionage is a fact that cannot be ignored in terms of firms. However, despite the advance of Information Security Technologies today, the security problems arising from software vulnerabilities are still a serious and important challenge for the institutions. For example, credit card information held in the records of a firm may be granted by third parties. In spite of all these risks, Cloud IT service providers do not accept a sanction specifically for information security violations (Kene, 2015).

Service Provider's Competence: Moving information technologies to cloud environments for companies is a process that needs to be analyzed very seriously. Here, it is very important to know how much the service provider can understand the needs and to what extent it is capable of addressing these needs. In addition, the possibility of the cloud service provider not being able to provide the desired service level or because it cannot sustain its financial existence for a long time creates problems for companies as much as the transition to the cloud environment.

2.3. Auditing Challenges

Corporate audit is an important business item for large scale companies. As CC is a newly developing model, the existing law and control mechanisms have not been fully updated to cover this model. However, the fact that data are physically located in the cloud environment is another difficulty in terms of control.

2.4. Challenges in Billing and Accounting

One of the most important reasons why cloud computing model seems attractive to companies is the investment model applied. The firms are more efficient in terms of taxing and accounting, instead of making investments for information technology needs. However, “the other pay as you go” logic in Cloud Computing is another point to consider when considering the idle processing power. A standard and efficient billing method has still not been developed for cloud service providers in the payment system by resource utilization rate. Existing methods are to reflect the initial investment costs to the users on a monthly basis rather than pay as you go. Cloud Informatics is a technology that we actually use in most of daily lives through services such as Dropbox, GoogleDrive and iCloud. Cloud technology, which is widely used in different fields, meets the current needs in the corporate sector with innovative solutions (Modi, 2013).

The world giants such as Microsoft, Amazon and IBM are expected to reach $ 20 billion in 2018, while cloud investments in 2017 are around $ 16 billion. With the CC services like Infrastructure, Platform and Services (IaaS, PaaS and SaaS), it seems to be moving the cloud technology to another place. Nowadays, many big manufacturers such as VMware, Microsoft Hyper-V, Citrix, IBM Power VM, Oracle VM are competing with each other and pushing technology forward. Virtualization and cloud computing are considered today's and future technology.

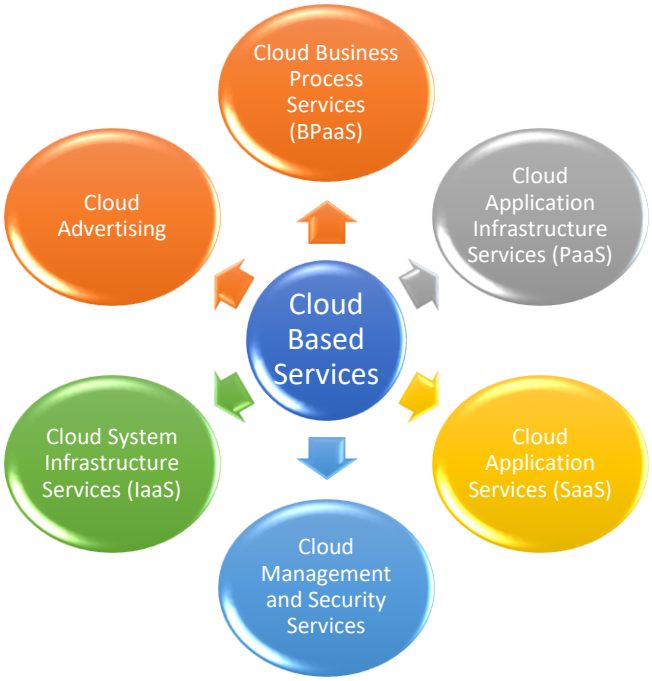


Figure 2. Demonstration of kinds of different cloud systems

As is depicted in the Fig 2., there are many types of cloud-based services. In 2018, it is predicted that factors such as delay times, connection speed and bandwidth will be determinant in the increase of cloud-based applications. According to Gartner's "2018 Planning Guide for Cloud Computing" report, specify whether to hire any cloud solution over 71% of SMEs in Turkey increased in 2018 show that this trend. The total volume of cloud computing investments and cloud services is projected to be over $ 530 billion, according to the IDC report.

If we look at the trends of cloud technology for 2019:

- Software Service (SaaS), infrastructure and platform spending will increase.
- Storage capacity in data centers will increase: According to surveys, total storage capacity around the world is expected to be 1.1 ZB, which is twice as high as 2018.
- The Internet of Things (IoT) and AI (AI) will trigger the use of real-time data and cloud computing.
- More content will be used in the distribution network.
- Machine learning will continue to expand: according to IDC data, in 2021, 75% of enterprise commercial applications will have machine learning that needs high performance.

Nowadays we are talking about Industry 4.0 and digital transformation, new technologies are transforming our way of doing business while changing our daily lives. All individuals and all companies are experiencing digital transformation by knowing or not knowing. Think about how fast we've been in the past decade; Facebook, Uber, WhatsApp. These apps did not exist in our lives. According to Gartner's research (2007), companies investing in innovation by 2019 will spend an additional $ 7 billion on their operational activities in order to adapt their digital transformation to business processes for every $ 1 they spend. 25% of the world economy is expected to return to digital platforms by 2020. The investment of companies in technology will be very valuable. Table 1 demonstrates the advancements in the types of cloud services by years.

Table 1. Types of CC Services (Gartner 2017)

CC Service Type	**2016**	**2017**	**2018**	**2019**	**2020**
Cloud Business Process Services (BPaaS)	39.6	42.2	45,8	49,5	53.6
Cloud Application Infrastructure Services (PaaS)	9.0	11.4	14.2	17.3	20.8
Cloud Application Services (SaaS)	48.2	58.6	71.2	84,8	99.7
Cloud Management and Security Services	7.1	8.7	10.3	12.0	13.9
Cloud System Infrastructure Services (IaaS)	25.4	34,7	45,8	58.4	72.4
Cloud Advertising	90.3	104,5	118.5	133.6	151.1
Total Market	**219,6**	**260.2**	**305,8**	**355.6**	**411.4**

As can be seen in the report published by Gartner in 2017, the importance of cloud computing in our lives is increasing day by day. According to Turkish secondary law, it is forbidden to keep the accounting data of government institutions in the cloud. Confidence in Cloud companies has been shaken by providing personal information to the internet as a result of various cyber-attacks. In addition to the data sent to the cloud environment by encrypting the cloud company can access the data through a variety of methods, Cloud companies to copy unauthorized data due to reasons such as the transition to the cloud slows down. In 2011, a few companies with Cloud service experienced technical problems. Amazon facilities in Ireland, a lightning strike because of Microsoft's services for nearly two days could not be reached. Another problem experienced in the same period due to the cloud service on the cloud of the Blackberry Company for 62 hours internet, e-mail, and blackberry messenger services could not reach. (In 2011, there were 55 million Blackberry users) Although such big companies can solve the technical problem, it may take a few days for the systems to recover. The availability of services is threatened by DDoS attacks that cause denial of service.

3. POSSIBLE WAYS FOR DDOS ATTACK ON CC.

DoS and DDoS attacks, which are the fearful dreams of almost every organization, are quite a headache. Although negative-popular, most people don't yet know what these attacks mean and how to protect them. Just before DoS (Denial of Service). In other words, this kind of attack, which has emerged as the attack towards a target from a single source, has been transformed from a large number of sources to a single target in order to increase its intensity in time. DoS attacks are a form of attack to prevent accessibility of systems. Each system is installed; certain values are envisaged for such elements as number of users, line capacity, number of instant requests, and design so that they can lift the load slightly above these values (Madhavi, 2012).

a) DDoS assaults are designed to goal any facet of an industry and its assets and can with difficulty

b) Disable a distinct computer, provider or complete network

c) DDoS attack are more a vulnerable to targeted alarm, printer, telephones or laptops

d) Hit approach assets like bandwidth space, CPU time or routing knowledge

e) Execution malicious code that effects processors and triggers mistakes in PC microcode

f) Make the most operating system liability to drain method resource

g) Disrupt the operating system.

In the case of DoS / DDoS attacks, the system becomes tired and unable to respond with instant request, instant number of users far above the load that the system can handle. In addition, it is

possible to target the accessibility of the system by filling the line instead of directly exhausting the system itself. The cyber world is also changing the way they arm. Now, with a simple operation, security systems may be down, and even if the time is too short, you may lose serious figures on the monetary scale. According to the survey done by the International cyber security organization Arbor Networks*, the biggest attack to block online access in 2018 (DDoS) reached 1.200 Gb per second, 60 percent above the figure recorded in 2017. In 2019, the situation is as follows; attacks on network and endpoints, DDoS and the risk of involuntary data loss raise more concern than attacks on mobile, cloud, social media, and the supply chain. The need for qualified personnel to manage the complex security environment is another concern. As DDoS attacks grew, it also became more frequent and complex (Ambikavathi, 2015).

4. EFFECTIVENESS OF INTRUSION DETECTION SYSTEM

It is a type of a security programming prepared to consequently alarm a specialist when a man or something enters the data system or premises through vindictive exercises or during a security chance arrangement. Fig 3 below demonstrates different IDS functions and pertinent applications.

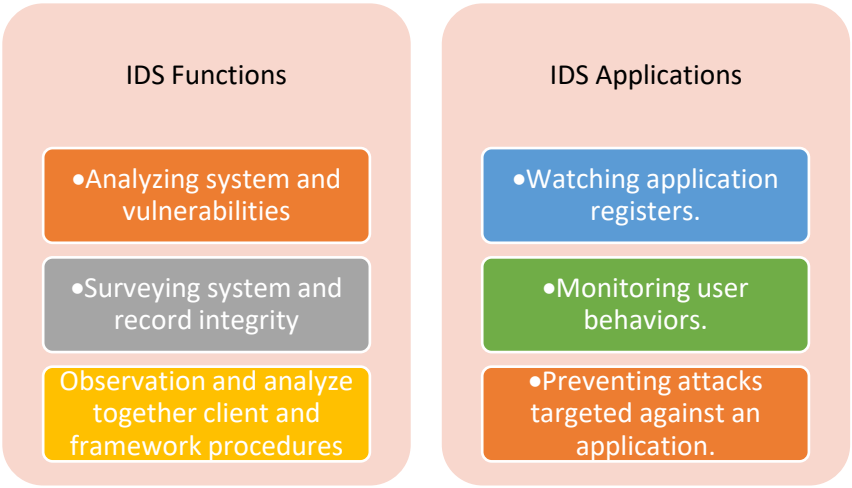


Figure 3. Depiction of IDS funcionality and applications

Advantages IDS is that the encrypted data can be read. But as a problem of IDS, it is positioned too high in the attack chain (the attacks reach the application). Fig 4 demonstrates the positioning of IDS system in a standard network topography.

* More more information see: https://www.netscout.com/arbor-ddos?lang=en (last accessed on 11th May, 2020)

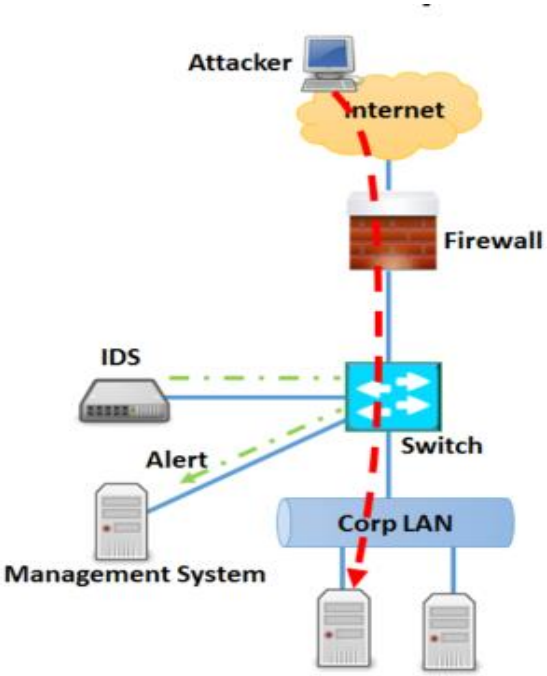


Figure 4. IDS system (Ghosh, 2015)

4.1. Host IDS (HIDS) and HIPS (Host-Based Intrusion Prevention System)

This takes a "photo" of the entire arrangement of framework records and analyzes them first. There are extensive contrasts, for example, missing logs and records that the manager will be given alerts (Madhavi, 2012). A host-based unauthorized intrusion detection system continuously monitors the events on a computer system's network and the traffic around the system. This type of intrusion detection system works by looking at the data in the computer system that the administrator tries to protect in his / her files. This review should include both the application files and the configuration files.

A HIDS must back up the configuration files in the system for a possible adverse situation. Maintaining root access on Unix-like platforms or registry modifications on Windows systems is another important issue. HIDS cannot prevent such changes because it works on the role of a detective, but should give warnings when such illegal access is concerned. To have a complete control, some sort of software must be installed on each HIDS monitor. It is possible to install HIDS to monitor a computer system. However, HIDS setup may be more typical in every device in the network environment. The reason for this is that the configuration changes of any piece of equipment should not be ignored. Naturally, if you have more than one HIDS host in a network, you do not need to log in to each one to get feedback. For this reason, a distributed HIDS system should include a central control module and be a system that encrypts communications between the hosts and the central monitor. a present mechanism is a necessity.

Host-based IPS system is a single server (Physical Host or VM Host) in a system, products such as computers against viruses, over the Internet traffic creates a defense mechanism against threats. It provides you with a security mechanism from Layer 3 to Layer 7 on the host, from the network layer to the Application layer. HIPS regularly controls the host on which it is installed, data transfer, services of the applications running on it and the characteristics of the host. HIPS analyzes the database where system events, application logs, and changes to the file system are kept, and provides control over changes and unauthorized entries. HIPS uses object attributes when making comparisons for each object in the database, and checks for changes in content over a period of time to create its own awareness and take action. HIPS also checks the memory partitions for any changes made to the memory.

If we talk about the advantages of HIPS, it increases the level of security with the security policy it provides on outsourced systems such as corporate and public institutions. By working on the

host, it also provides an important measure against the possible attacks and threats that may come over the local network.

With the development of Virtualization technology, we can see that different vendors offer different platforms. On the HIPS side, developers can also be positioned in the VM network with virtual sensor structures. Because these platforms actually had a traffic in itself and the traffic inside turns inside itself. Here you can transfer data between each other via virtual switches located in your traffic network without the need of your IPS device or Firewall device. The reason for opening this point can be many web applications, outsourcing services or internal network services in virtual platforms hosting server systems in general. At this point, there may be malicious personnel or users who may use weaknesses that may occur inside. In this case, you can take your security to the upper levels with the measures that can be taken with IPS systems. With HIPS, you can provide anti-malware, web reputation, integrity monitoring, IPS-signature-base, log inspection or application control.

IPS positioning methods can be examined under 4 different headings:

- SPAN Mode (Pasif Sniffer Mode): IPS SPAN ports can be connected to one or more network switches to connect to BDU (Defense Unit) detection ports. Thus, return actions, such as resetting the TCP connection, can be injected by the BDU using the same port.

- TAP Configuration: In this mode, incoming and outgoing traffic can be monitored and analyzed in the IPS device and if there is an integrated solution used inside, action can be taken with the information to be received from it. There is full traffic capturing here. It allows deep analysis against threats.

- Inline Mod (Active Gateway Mode): In fact, this is the mode most of us actively use. Sensors can be used to prevent attacks by taking IPS measures and actions. Usually UTM Firewall and IPS only devices are operated in this mode to increase the security level.

- Virtual IPS: The sensors support the innovative and powerful concept of Virtual IPS (Virtual). It reveals the ability to divide a sensor into a plurality of virtual sensors that can be fully customized by security principle. This includes individualized attack selection and associated response actions. The virtual IPS may be defined by an IP address block, one or more VLAN tags or specific ports or ports on a sensor

4.2. Network Based IDS (NIDS)

This technique will do examination for activity on an entire subnet and will make a match to the movement going by to the assaults definitely known in a library of known violation. The network intrusion detection function, also known as network intrusion detection system, can perform all traffic on your network without resting. In this way, a typical NIDS also includes deep packet checks to collect data for analysis (Sing, 2016).

A NIDS analysis engine usually runs on a rule-based basis and adds new rules the set of rules can be changed in parallel with the desired policies. Once you have learned the NIDS rule scenario with any choice, new rules will be easier to create. NIDS normally cannot analyze all of the data. Hence, the rules governing analysis in a NIDS must use selective data capture techniques for the event. For example, if there is a rule for some kind of abnormal HTTP traffic, NIDS can only receive and store HTTP packets pointing to these properties. Typically, a NIDS work is built on a special piece of hardware. Comprehensive and low-cost enterprise solutions can exist as part of a network kit that includes pre-installed software. A NIDS requires a sensor module to receive traffic, so it is possible to load it into a LAN analyzer or to assign a special computer to carry out such tasks. However, it must be ensured that the piece of equipment selected for the task has sufficient speed to slow down the network. (Patel, 2013)

Normally, a NIDS has much more tracking power than a HIDS. It is possible to detect attacks with a NIDS, but HIDS cannot predict what kind of attack it is when only one thing is wrong when a setting on a file or device already changes. However, the fact that HIDS is not as active as NIDS does

not mean that they are less important. Not only are the detection systems preferred to avoid interruptions due to false positives. NIDS usually depends on independent equipment, which means that it will not force server processors. However, HIDS activity is not as aggressive as that of NIDS. A HIDS function can be performed by an open background in the computer, but more CPUs may be required for the normal computer to operate in parallel with the timing of the network traffic. For this reason, existing hardware capabilities should also be considered.

4.3. DIDS (Distributed Intrusion Detection System)

A DIDS involves numerous IDSs (for instance NIDS, HIDS) that are conveyed over a major system to surveillance and examine the activity in order to nosy identification conduct the member IDSs can talk with each other or with a Central server. Each one of these individual IDSs has its own practical segments: part discovery and connection director. Uncover. The part inspects the conduct of the framework and moves the gathered data in a standard organization to the connection. Network Behavior Analysis Intrusion Detection is an interruption identification approach which is giving to choose if the system activity is suspicious or not (Alharkan, 2012).

5. IDS METHODOLOGY

It is no doubt that the increasing use of DDoS in attack vectors with increasing complexity as a vehicle system used with technical infrastructure radically changes the security environment in organizations. As institutions continue to regulate security architecture based on availability, access and performance, it can be said that distributed tools can always take the necessary measures to combat the attack. Firewalls, IDS and IPS continue to play an important role in protecting networks against service denial attacks. However, today's threats require a holistic solution that can effectively distinguish between legitimate and illegitimate traffic in order to maintain layers of network and application and keep institutions in working order. Because of the precaution, legitimate traffic is often negatively affected. At this point we have developed our research question. How effectively any threat to the system is perceived by attackers using DDoS technology? This question raises an important problem as most institutions are busy with. For the answer to the question, there are a multiple ways detection is performed by IDS. There are two major (IDS) techniques which used by Intrusion detection system for example;

1. Anomaly detection (in light of conduct of clients).
2. Recognition (rely upon signing up of known assaults).
3. Hybrid detection its utilized to inherit the execution of IDS, it is improve to utilize addition from ones methods Fig.6. Below show kind of Detection methods used by intrusion detection system (Kene, 2015) .

All IDSs normally use two different modes of operation to detect anomalies or unauthorized access. Some can only use one or the other, but in most cases, they can use both modes.

- Signature based
- Abnormal base
- Hybrid

The signature-based detection method queries from a previously updated database to ensure authentication. This method is applicable by NIDS as it is by HIDS. A HIDS looks at the registration and configuration files for unexpected repetitive signals, while a NIDS will look at the total integrity of the packages and the authentication integrity of systems such as SHA1 (Pandeeswari, 2015).

Intrusion Prevention Systems (IPS) software and IDSs are considered different branches of the same technology to combat the attack. Since an IPS cannot provide protection without attack or unauthorized access detection, an IPS must also include IDS functionality at the same time. Another way of expressing the difference of the security tools against the attack vectors between these two branches is to classify them as passive or active. The direct attack monitoring and alerting system is sometimes referred to as "passive" IDS, which is known as "reactive" IDS or IPS, which when activated, attempts to stop any damage and further attack activity from a detected source.

IPSs do not usually apply a fixed packet solution directly, and therefore are not "one size fits all" type solutions. Instead, they can interact with firewalls and applications by adjusting the required behavior. For this reason, reactive HIDS would prefer to adapt to the security environment interacting with a range of network support devices to restore settings on a device such as SNMP or an installed configuration manager. It can be an effective and efficient solution and only through this kind of virtual interaction and cooperation.

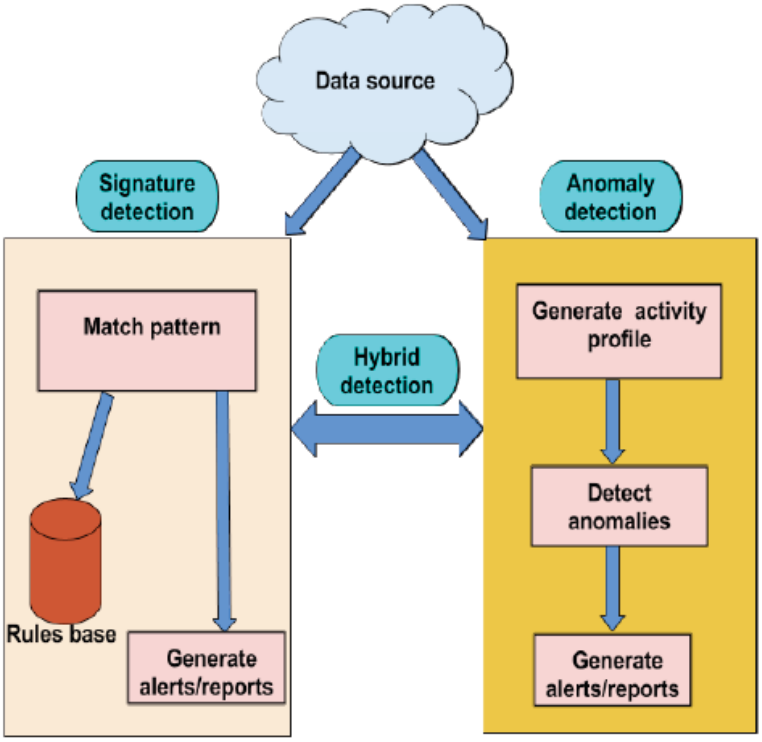


Figure 5. Detection methods utilized by intrusion detection system (Madhavi, 2015)

5.1. Signature based detection technique.

Fortunately, hackers often do not manually attempt to write passwords directly to their computers in order to break a password or gain access to coarse-grained users using brute-force techniques. Instead, expert hackers try to hide themselves and their bad behavior from IDS and IPS systems using automated procedures provided by the specific tools they use. These vehicles tend to produce the same traffic signatures each time. Because computer programs constantly repeat the same instructions much more than they offer random variations (Muthukumar, 2015).

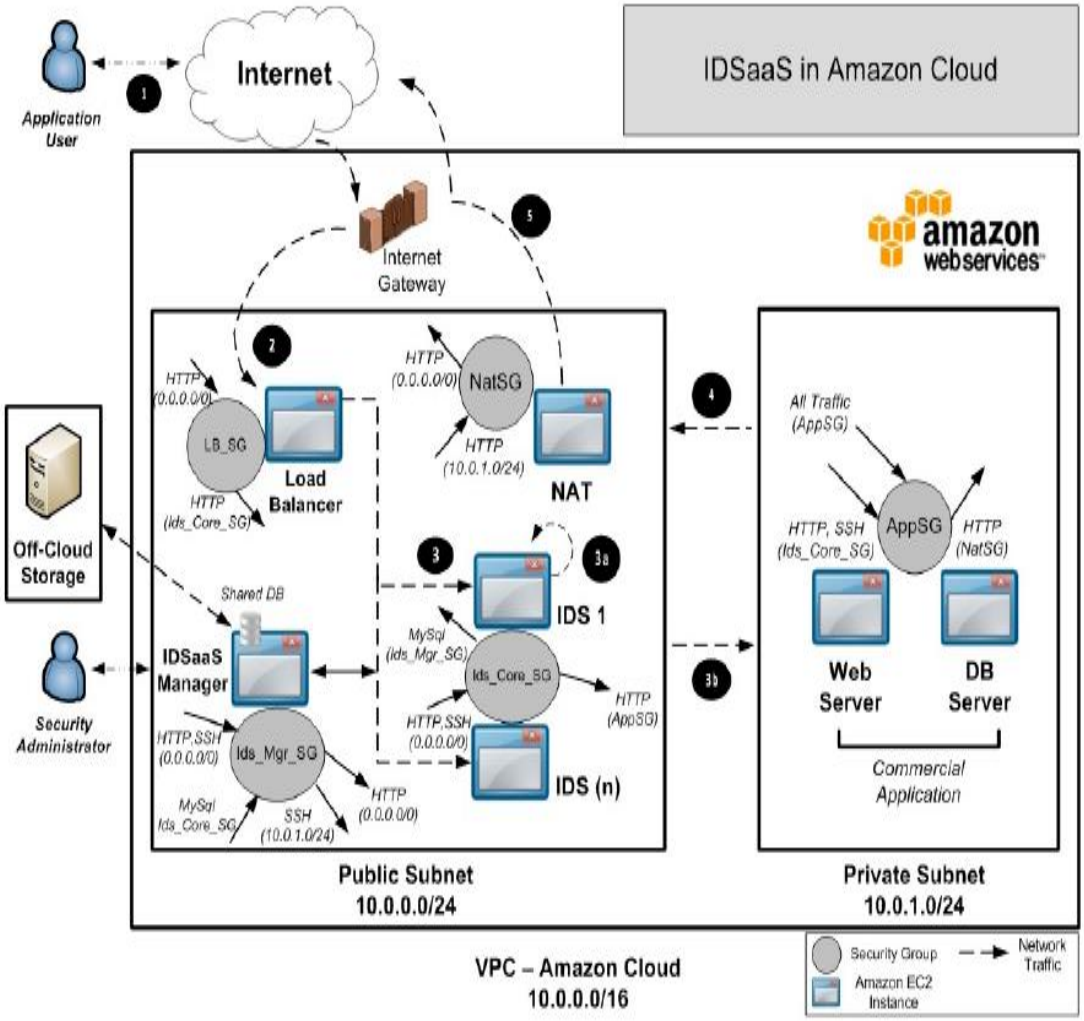
The IDSaaS structure was actualized in Amazon web administrations utilizing the EC2 cloud. The IDSaaS uses the VPC benefit from Amazon. it was made both private and open subnets. The private subnet keeps up the ensured business application VMs. People in general subnet have different IDSaaS VMs (Sangeetha, 2015).

As is shown in Fig. 6 explaining the usual planning of the Intrusion Detection System as a Service in the Amazon VPC.

1) *IDS Core* is the gatekeeper to the business application

2) *IDSaaS Director* is the security manager get to point where different supervision assignments can be performed by manager. Connection supervisor joins information from various IDS and produces abnormal state alerts that keep up a correspondence to an assault. Examination stage makes utilization of mark based and irregularity-based identification methods so DIDS can distinguish referred to and also obscures assaults.

3) *Load Balancer* growing the accessibility of the Intrusion Detection System as a Service in Cloud. It is in charge of balancing the movement loading between various IDS Center VMs. The downsides are:



-

Figure 6. Cloud based IDS (Madhavi, 2015)

5.2. Anomaly Detection Technique and Neural Security

It is an IDS for distinguishing both grid and PC intrusions and wrong use by observing framework action and ordering it as either ordinary or bizarre. The grouping depends on heuristics or standards, instead of examples or marks, and endeavors to distinguish any kind of abuse that drops out of typical framework activity (Khatri, 2014)**.**

Anomaly-based detection systems are based on the logic and reasoning behind the definition of unexpected or unusual activity patterns. This is a new but very important functionality and technique that can be implemented by both host and network-based intrusion detection systems. In the case of HIDS, an abnormality can repeatedly alert failed entry attempts or an unusual network activity at the port of a device scanning port. NIDS case, an anomaly detection approach is ongoing standards to establish a standard for comparison of situations where traffic patterns and the identification of unusual behavior and requires an initial establishment. The traffic in this context is considered normal and is triggered by an abnormality warning when the current traffic goes out of that range.

Advanced NIDS can over time create a shift in standard behavior and automatically adjust these limits via machine learning (ML) as their service life advances and event patterns compared. Signature-based methods work much faster than perception based on anomalies, as they use direct

comparison techniques from a table. A comprehensive deflection-based sensing engine uses artificial intelligence (AI) methodologies that can be costly to develop by businesses. In the case of signature-based detection in case of HIDS, mapping of file versions and models is a very simple process that can be performed using normal command line utilities. For this reason, they are not costly to develop and are more likely to be implemented in free intrusion detection systems. A comprehensive intrusion detection system, known as hybrid systems, requires both signature-based methods and anomalous-based procedures, but is known to be an expensive solution compared to conventional ones.

5.3. Hybrid Detection Technique

The activity of Intrusion Detection System can be essentially enhanced by collecting anomaly setup with signature-based techniques which result new technique is called Hybrid detection method. The thought behind the execution of hybrid detection discovery is to find both known and known assaults rely on mark and peculiarity recognition procedures (Kene, 2012).

Today, it is understood that IT attacks will be based on artificial intelligence and therefore defense systems and methods should be supported with artificial intelligence. In the following period, digital money theft, ransom attacks, attacks on critical infrastructures will increase, internet-connected devices will be targeted, spam e-mails will continue, cloud-based storage platforms will be more exposed to threats and mobile threats will increase. Cyber attackers who develop malware will focus more on individuals, organizations and computer networks. In fact, cyber attackers will perform vital attacks through fitness bands, wearable heart monitors, biometric motion sensors and pacemakers. In active networks, cyber-attacks can destroy infrastructure, the most powerful systems. It is difficult to develop software with traditional fixed algorithms for defense against emerging attacks. In the virtual world of health, banks, populations, family-controlled computer systems such as all our vital information, unauthorized, secretly entered through the internet virtual enemies are not seen, still, inaccessible, unknown and incomprehensible. Therefore, software flexibility, early detection methods and artificial intelligence applications with learning ability are needed in cyber defense. Artificial intelligence is a technique consisting of algorithms that enable machines to produce solutions to complex problems such as humans, and includes techniques such as reasoning, inference, generalization, and learning from past experiences. Here, the most appropriate example of artificial intelligence; DeepBlue, who defeated the Russian chess champion Kasparov (Kaliyamurthie , 2012).

What distinguishes DeepBlue from other software is that it has a knowledge base that includes all possible chess information, and that it generates information from this base, merges, analyzes, concludes, and links these results to causes. These are the features that make artificial intelligence attractive in cyber defense. Defense against smart cyber-attacks can only be achieved with smart software. Cyber defense methods require state awareness, artificial intelligence software that can respond quickly to attacks, analyze and make the necessary decisions. All these processes are too complex to be solved with traditional algorithms. Intelligent approaches such as artificial neural networks, genetic algorithms, expert systems, fuzzy logic, machine learning, which are used in the solution of problems that are difficult to solve with traditional methods, are within the sub-branches of artificial intelligence (Khalimonenko, 2017).

Artificial neural networks are the systems that model the working principle of cells in the human brain, formed by the combination of artificial neural cells (neurons). In this system, the information is represented by the connection weights of the network. To the extent that the weight values of the network are correct, the performance of the network is high. For these reasons; operations are fast, providing a large number of parallel learning and decision-making functions. Can be used in cyber defense, DDoS detection, virus, spam, malware detection. Due to their high speed, they are widely used in graphics processors and hardware.

Genetic algorithms, an artificial intelligence technique used in solving complex problems, are based on the principle of generating new sequences of chromosomes and biological evolution. The goal is to achieve the best chromosome. In cyber defense, it distinguishes between abnormal data in inter-computer traffic and normal data using traffic sniffers. Fuzzy logic, which acts according to complete and unclear information and tries to make the right decisions from them, provides solutions

with fuzzy if-then rules in cyber defense. The system, which has a fuzzy rules base, is used for decision making in detecting abnormalities in cyber defense (Gupta, 2015).

Expert systems, which are also a subfield of artificial intelligence, use the knowledge and logical inference mechanism of the expert or persons to solve the problems. The most important feature of an expert system is that it has a large knowledge base obtained by the traditional data processing mechanism. The expert system determines the way the system decides by processing its data. To decide; all rules in the knowledge base are provided by forward chaining on the if-then basis or reverse chaining, which is the opposite decision-making unit. These systems have the ability to respond quickly to attacks, high performance, reliability, and to base the results on statistical data.

Gains the ability to learn machines using statistical techniques such as machine learning, inference and probability, which are separated according to supervised, unsupervised, reinforced learning styles. Algorithms include classification, regression and clustering which are data mining methods. In cyber-attack area; activities such as fishing, captcha, malicious software, intelligent botnets, human voice imitation; in the field of cyber defense; studies such as malware analysis, network intrusion detection, malicious code detection, malicious URL detection, botnet detection, spam filtering, user authentication, detection of phishing attacks are performed.

While the first known cyber-attack was the Morris worm produced by Robert Morris in 1988, cyber weapons, which we now call APT (Advanced Persistent Threats) are differentiated from classical viruses and cyber weapons with many features, are actively used in cyber wars and target especially critical infrastructures. Stuxnet, which targeted Iran's nuclear program in 2010, and Duqu and Flame, which were thought to have been developed with similar codes, are among the best examples of the APT attacks (Patel , 2013).

Attacks and types to critical energy infrastructures in the past are as such; 1982 -Siberia Pipeline Explosion-Trojan, 2000 -Russia Gazprom -trogen, 2010-Iran Bushehr nuclear reactor-stuxnet, 2012-Iran's oil refinery on Kharg Island-viper, 2012-Saudi Arabia's national oil company Saudi Aramco- Shamoon, 2014-Western energy companies-dragonfly, 2015 oilPoland Air company LOT - power failure, hard disk failure, failure of security software, 2015-New York Bowman Dam-infiltration with cellular modem, 2016-Ukrainian electrical system-malware (BlackEnergy) -phishing-is written in Python as GCat back door opening screen capture and keylogger (Patel , 2013).

According to research reports in the field of cyber defense, ransomware attacks have increased; institutions improved their processes and prevented 87 percent of targeted attacks in 2018. 87% success is due to network, system-hardware, data communication security, up-to-date and secure software development, public and legal security policies in line with the needs, awareness and ultimately secure corporate quality information systems that comply with quality standards. It is provided (Khalimonenko, 2018)

In short; It is understood that simple and traditional algorithms are not sufficient for cyber defense software to perform its duties and it is more appropriate to use artificial intelligence algorithms. Artificial neural networks are used more technically in cyber defense but there is a need for faster and performance expert system algorithms in decision support, awareness and information management. Thus, faster and more efficient decisions can be made against cyber-attacks with artificial intelligence techniques.

WAF and IDPS Collaboration

IDS and IPS systems are vulnerable to DDOS attacks and cause swelling. Unlike the protection drop network traffic. IDS and IPS systems have to be used with firewalls, thus avoiding performance problems. The most important aspect of IPS is that it does not slow down the system through hardware ASIC technology.

IDPS consists of a combination of IDS and IPS systems, where both systems work in a coordinated way. WAF (Web Application Firewall) are used for protection of web applications. Web applications are meant to protect from attacks..WAF is a fairly sheltered systems against attacks such as SQL Injection, OS Command and XSS. WAF checks requests made by users, monitors URLs for unusual behavior. Firewalls usually use two types of blocking methods, such as “Drop” and “Reject”.

For example, suppose that a website and our users' information is stored in the database and should be kept confidential. There are basically 4 settlement scenarios for WAF, where and how to use them according to the settlement scenarios.

1-Bridge: In this mode, WAF acts as a bridge and passes the flow over itself. This method is similar to IPS.

2-Offline: It works in a similar way to IDS, receives a copy of the requests, generates malicious requests and answers, which are TCP RST packets.

3-Integrated: This is the simplest placement mode, operating according to the operating system.

4-Reverse Proxy: This layout model works with proxy logic. The way for those who want to reach the page goes through the WAF first, if the WAF system finds it suitable to pass, then it reaches the server. In case of infiltration attempts, a package wafer is sent to the system, the system responds with it various packages. Let's show a Nmap as an attempt using Kali Linux tools:

nmap -p 21 –script http-waf-detect.nse (IP)

It takes us to WAF, and there is another way to understand it, so our help is to run the wafw00f tool. We can easily identify WAF as such:

Wafw00f.py ' www.abc.com '

We've identified the WAF and now it's time to get rid of the WAF. Now let's experiment with how to bypass the WAF. SQL injection attacks is realized in this system. For an average firewall a variety of methods can be used as such:

*http://www.abc.com/index.php?page_id=-15 / *! UNIOn * / / *! SelECt * / 1,2,3,4….*

If you use this method, the system will understand the query so let's try it in a different way:

*http://www.abc.com/index.php?page_id=-15 /*UNunionION*/ /*SEselectLECT*/ 1,2,3,4…*

Action is okey and now you can use the SqlMap tool, the SqlMap's "tamper" file contains a number of scripts and these scripts are used to bypass firewalls such as WAF.

"sqlmap.py -u abc.com/catalogs.php?id=453 –tamper 'tamper/randomcase.py' –dbs"

If there is an IPS or IDPS then you can not go further easily.

6. TOP IDS TOOLS

There are many products on the market that can serve as IDS for different platforms. While IDS software vendors are more focused on Unix-like operating systems, others produce codes based on the POSIX standard for the IDS product. In all of these cases, it may mean that Windows is excluded from IDS technologies. Mac OS X and Mac OS operating systems are Unix-based.

Snort is the leader in open source NIDS solutions. Snort uses both signature-based intrusion detection and anomaly-based detection methods and can rely on user-generated rules or update signatures from the database as emerging threats. Suricata is a direct opponent of Snort. It applies a security and abnormality-based approach based on signature-based detection methodology to detect attacks. Snort is an open source network-based IDS. It is the most preferred intrusion detection system with more than 4,000,000 downloads and around 500,000 registered users. Real-time network traffic analysis and packet logging can do. It detects attacks by analyzing protocols and content in the packages it listens from the network. Buffer overflow, port scanning, CGI can detect movements such as attacks.

Snort consists of different components that work together to detect attacks and produce output. Snort-based IDS systems consist of the following components:

- *Packet Decoder*: The network receives various types of packets from the interface and prepares them for the next snort component.

- *preprocessors:* Before the Detection Engine, it prepares the packages for it and tries to detect attacks according to the abnormalities in the package headers. Preprocessor usually works piece by piece to bring together large pieces of data.
- *Detection Engine*: It is one of the most important components of Snort. It is responsible for identifying the types of attacks in the package. It uses snort rules to detect these attacks. An attack flag specified in the snort rules is compared with the contents of the packet from the preprocessor component and, if there is a dangerous situation, the next module is passed to perform the action in the rule header.
- *Logging and Alerting System*: After detecting the rule that the package content overlaps; the Detection engine component performs operations such as logging and warning according to the action specified in the rule header. Logs can be saved to a simple text file in tcpdump or other file format. The command to run snort can also be specified with the -l parameter to log.
- *Output Modules*: It allows us to redirect or otherwise use the output of the detection engine component. Initially, the output is usually saved in / var / log / snort. Output using this module can be sent to another destination.

Output or 'Logging and alerting system' components can be used in the following ways. We can keep snort logs systematically in the database. For example, we will keep snort outputs in a MySQL database. The name of the database should be snort, the user name should be 'snort' and the password should be 'test' and the database should be located on the local machine. In this case, the snort.conf file should contain a declaration like the one below.

output database: log, mysql, user = snort password = test dbname = snort host = localhost

Sending SMB pop-ups to Windows:

output alert_smb: workstation.list

Both SMB send to Windows and save to database is also another choice. Sometimes it may be necessary to report the results to more than one location. In this case, we can determine our action with the keyword ruletype. For example, in snort.conf, an action type that we set as * *'smb_db_alert'* * will both register to the database and issue an SMB pop-up warning.

Bro IDS uses an anomaly-based intrusion detection method. The language of Bro IDS is a specific language specific to network applications. It is very effective in traffic analysis. Used in forensic medicine and related use cases. OpenWIPS-NG is a popular open source project for wireless security, offering tens of thousands of dollars of solutions free of charge, even without logo and documentation. Signature-based intrusion detection technology includes sensors for capturing wireless traffic, a server that analyzes attacks, and a graphical user interface for easy management. Security Onion is an Ubuntu-based Linux distribution for IDS and network security monitoring (NMS). Platform, Snort, Suricata, Bro as well as the best tools, such as Sguil, Squert, ELSA, Xplico combined with many tools such as comprehensive intrusion detection, network security monitoring and daily management provides the opportunity.

The following table shows which IDSs are connected to the networked mainframe and which operating systems can be installed on which platforms:

Table 2 Basic Properties of Top IDS Tools (Cooper, 2019)

IDS	HIDS/NIDS	Unix	Linux	Windows	Mac OS
OSSEC	HIDS	Yes	Yes	Yes	Yes
Snort	NIDS	Yes	Yes	Yes	No
Bro	NIDS	Yes	Yes	No	Yes
Suricata	NIDS	Yes	Yes	Yes	Yes
Sagan	Both	Yes	Yes	No	Yes
Security Onion	Both	No	Yes	No	No

AIDE	HIDS	Yes	Yes	No	Yes
Open WIPS-NG	NIDS	No	Yes	No	No
Samhain	HIDS	Yes	Yes	No	Yes
Fail2Ban	HIDS	Yes	Yes	No	Yes

7. EFFECTIVENESS OF IDS FOR DDOS ATTACKS

There are DDOS attacks on different types. An easy example is the SYN flood attack. In this attack, the attacker sends a TCP connection request (a packet with the SYN flag set). The server normally allocates and responds to the connection. The aggressive response is ignored and the server tries to send ongoing requests until an expiration time has passed. If there is sufficient demand for a while, the server resources become exhausted and become unresponsive. If the server is a public server (for an e-commerce site or an e-government system), then it has to wait for connection requests from any computer in the world. Diagnosing connection requests as legitimate customers and reducing malicious connection requests is a prerequisite.

Intelligent attack attempts to hide itself by abusing the dynamic system by corrupting the source IP addresses. For this reason, IDS will not know that it is just an attack instead of too much normal traffic. If the system attempts to reduce the number of connections by rejecting some requests, it may also reject legitimate customer requests. An attacker can use a botnet consisting of zombie IoT devices to surprise over different IP sources. These mechanisms can be placed in the gateway routers. Another type of attack is SYN mirroring. An attacker sets an IP address and sends a request to a server. The server responds with the SYN / ACK message to the rogue IP address. The fake address is the victim machine and all responses must be processed as if they were the original requests of the senders. To summarize, successful attacks appear to be legitimate requests from a number of machines and cannot be easily distinguished from normal traffic (Khaldi, 2014).

The idea that device exploit or an unknown attack can be correctly identified via IDS is a significant development in terms of strong enough and distributed identity systems. Variety of dynamic and proactive mechanisms that are easily implemented by sophisticated advanced warning systems such as automatic traffic filtering on firewalls and rejection of service countermeasures should be considered. These are very promising and encouraging steps for DDoS prevention (Messier, 2014).

It is now a well-known fact that DDoS attacks cannot be fully identified with signature-based detection mechanisms, but nevertheless problems related to these mechanisms should be considered. The signature-based detection mechanism basically requires the creation of a profile or signature associated with a specific type of attack that is stored in the database when encountered during an attack. However, the number of DDoS attacks can vary in quantity and quality, starting with typical TCP flooding, UDP flooding, ICMP flooding, SYN flooding, and specific resource-based and target-based bandwidth and scanning attacks. With the development of new generation networks and systems, a new generation of attacks can be developed that are difficult to catch when trying to pair against some signature schemes that are quite hybrid in nature and developed in parallel by new generation attacks. In addition, it becomes even more problematic to distinguish DDoS attacks from legitimate traffic volumes called Flash Crowds. Now the real solution is to create the right profiles based on deep anomaly analysis and machine learning that can change like the kinds of attacks that need real time and develop at the same time.

Table 3. Example of Zero Day Exploits of IDS Systems

Date	D	A	V	Title	Type	Platform	Author
2019-07-24	⬇		✗	Trend Micro Deep Discovery Inspector IDS - Security Bypass	Remote	Multiple	hyp3rlinx
2018-03-05	⬇		✗	Suricata < 4.0.4 - IDS Detection Bypass	DoS	Multiple	Positive Technologies
2018-01-01	⬇		✓	Apple macOS - IOHIDSystem Kernel Read/Write	DoS	macOS	Siguza
2017-12-08	⬇		✓	FS Quibids Clone 1.0 - SQL Injection	WebApps	PHP	Ihsan Sencan
2016-04-20	⬇		✓	Hyper-V - 'vmswitch.sys' VmsMpCommonPvtHandleMulticastOids Guest to Host Kernel-Pool Overflow	DoS	Windows	Google Security Research
2016-02-20	⬇		✗	SOLIDserver < 5.0.4 - Local File Inclusion	WebApps	PHP	Saeed reza Zamanian
2013-12-06	⬇		✓	NeoBill - '/install/include/solidstate.php' Multiple SQL Injections	WebApps	PHP	KedAns-Dz
2011-09-27	⬇		✓	Vanira CMS - 'vtpidshow' SQL Injection	WebApps	PHP	kurdish hackers team
2009-07-08	⬇		✓	Rapidsendit Clone Script - 'admin.php' Insecure Cookie Authentication Bypass	WebApps	PHP	NoGe
2010-08-31	⬇		✓	HP Insight Diagnostics Online Edition 8.4 - 'idstatusframe.php' Multiple Cross-Site Scripting Vulnerabilities	WebApps	PHP	Mr Teatime
2009-01-15	⬇		✓	Active Bids - 'search' SQL Injection	WebApps	ASP	Pouya_Server
2009-01-15	⬇		✓	Active Bids - 'search' Cross-Site Scripting	WebApps	ASP	Pouya_Server
2014-03-26	⬇	◘	✓	Apache CouchDB 1.5.0 - 'uuids' Denial of Service	DoS	Multiple	Krusty Hack
2006-11-18	⬇		✓	Link CMS - 'prikazInformacije.php?IDStranicaPodaci' SQL Injection	WebApps	PHP	Ivan Markovic

As is seen in the Table 3 above, there are many vulnerabilities that are being published as zero-day exploits in the exploitdb* database. The most recent ones are taken into the table filtered from 42,086 total entries. Therefore, an effective IDS is not a standalone solution. They are also being bypassed by hackers. Just as an example we have explored the vulnerability data file of "*Suricata < 4.0.4 - IDS Detection Bypass*" for Surricata in the exploitdb database and have reached the information below:

Vulnerability Type: Detection Bypass

Affected Product: Suricata

Vulnerable version: <4.0.4

CVE number: CVE-2018-6794

Found: 25.01.2018

By: Kirill Shipulin (@kirill_wow), Positive Technologies

Severity: Medium

About Suricata:

Suricata is a high performance Network Threat Detection, IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community

Attack Description:

If as a server side you break a normal TCP 3 way handshake packets order and inject some response data before 3whs is complete then data still will be received by the a client but some IDS engines may skip content checks on that.

Attack scenario TCP flow scheme:

* For more information see https://www.exploit-db.com/

Client -> [SYN] [Seq=0 Ack= 0] -> Evil Server

Client <- [SYN, ACK] [Seq=0 Ack= 1] <- Evil Server

Client <- [PSH, ACK] [Seq=1 Ack= 1] <- Evil Server # Injection before the 3whs is completed

Client <- [FIN, ACK] [Seq=83 Ack= 1] <- Evil Server

Client -> [ACK] [Seq=1 Ack= 84] -> Evil Server

Client -> [PSH, ACK] [Seq=1 Ack= 84] -> Evil Server

IDS signature checks for TCP stream or Http response body will be skipped in the case of data injection. This attack technique requires all three packets from a malicious server to be received by a client side together before it completes 3whs. Proof of concept server was written in C to reproduce this and it works reliably in local networks. Since some network devices may affect packets transmission exploitation is not so reliable for the internet scenario.

This attack possibly may impact other network monitoring or intrusion detection systems because is not limited to Suricata IDS: an old Snort IDS version 2.9.4 is also affected.

Successful exploitation leads to a complete TCP-Stream response or HTTP response signatures bypass and may be used to prevent malicious payloads from network detection.

PoC:

A Working PoC server is available here: https://github.com/kirillwow/ids_bypass

There is also a traffic capture of this data injection technique.

Timeline Summary:

2018-01-25: Issue submitted to the bug tracker.

2018-01-30: Patch ready.

2018-02-14: Suricata 4.0.4 containing the fix has been released.

Intrusion detection systems are one of the most important security components for the detection of possible attacks, violations and threats, including methods for monitoring network activity and analyzing traffic. Intrusion prevention systems are network security systems that include detection and prevention of attacks. IDS / IPS systems have functions such as frequent monitoring of the network, identifying potential threats and logging related events, stopping attacks, and reporting to security administrators. In some cases, these systems can also be used to identify vulnerabilities in institutions' security policies. IDS / IPS can also detect attackers' network-gathering activities and stop attackers at this early stage. However, IDS are not capable to effectively and efficiently fight against DDoS attacks. IDPS hybrid systems are more effective. Furthermore, usage of WAF and UTM new generation firewalls are also required.

8. CLOUD COMPUTING STANDARD FOR SECURITY

The interest in cloud computing has increased rapidly in recent years due to the high flexibility and accessibility of low wages. On the other hand, security and privacy have some concerns for organizations while moving their practices and data to the cloud. Standardized studies are being conducted in many countries around the world to reduce these concerns. The increasing use of cloud computing in our country has raised the need for standardization in this field.

The European Commission considers that certification of standards for cloud computing by regulatory bodies is complied with and that supporting such implementation will add momentum to cloud computing. It is thought that the standards for cloud computing will affect the public sector, small and medium-sized enterprises and consumers, rather than the ICT industry. Since most users may not have in-depth knowledge of the standards offered by the service provider and the transition between operators, it is considered by the European Commission that certification can be useful. Cloud computing standards are established in the world and NIST (National Institute for Standards

and Technology) has issued widely accepted definitions. However, in the EU, a group has been formed in order to comply with the interoperability standards of the ETSI (European Telecommunications Standards Institute) and to monitor the cloud computing standardization needs, and the group has started work (EC, 2012).

The European Commission has decided to finalize the studies on cloud computing contracts by the end of 2013. In this context, it is aimed to develop the articles related to cloud computing including the transfer of personal data to third countries which will promote the development of cloud computing in the global sense. It is considered that the data transfer to be made outside the EU and the European Economic Area, together with new studies on personal data security, will be more secure with the elements to be included in the articles of the Convention, and will contribute to data security (EC, 2012).

In line with Council of Ministers Decision No. 2013/4890 in Turkey, dated 20.06.2013 published in Official Gazette numbered 28683 and entered into force in Turkey as the National Cyber Security Strategy and responsible action on the creation of standards in the field of security in the 2013-2014 Action Plan for Turkey, the Standards Institute has been appointed. The assignment is an important factor and basis for establishing this standard. The need to establish standards for cloud computing is not limited to security and is spread over a wide range of areas such as security, reliability, performance and prevention of firm dependence.

When studies within ISO are analyzed, it is seen that studies have started on ISO / IEC 27017[*], ISO / IEC 27018[†] and ISO / IEC 27036-4[‡] standards. The first of these standard works, ISO / IEC 27017 study, best practices for information security controls for cloud computing services based on the ISO / IEC 27001 Information Security Management System standard, ISO / IEC 27018 study is the best data protection controls in public cloud computing services. It aims to provide examples of implementation and ISO / IEC 27036-4 cloud computing security guide in terms of supplier services.

The "Cyber Security Special Committee", which was established in the first quarter of 2013 within the body of Turkish Standards Institute (TSE), has started efforts to set standards for the security of cloud computing infrastructures. Despite the fact that it has been a while, the work produced in 2014 as a draft still continues[§]. standards are necessary to determine the leading countries, especially America with international organizations in the cloud computing area under study for the investigation of particularly cloud computing and security for Turkey. For this reason, security standards for cloud computing are considered important and efforts should be made to complete the work in this area as soon as possible.

9. LATEST LEGISLATIVE CHANGES ON THE PUBLIC USAGE OF THE CLOUD SERVICES

The Turkish Presidential Circular dated 06.07.2019 with 30823 number are proposing quite shocking measurements for government organizations. About 14 months before this Circular has been issued, the Capital Market Board (CMB) published provisions on the Information Security practices of the following institutions and banned Cloud Services with Foreign Locations in its Communiqués published in the TR official newspaper dated January 5, 2018.

- Borsa İstanbul A.Ş.,
- Exchanges and other market places organized with market operators,
- Pension investment funds,
- Istanbul Clearing and Custody Bank Inc.,
- Central Registry Agency Inc.,
- Portfolio custodian organizations,
- Capital Markets Licensing Registry and Training Agency Inc.,

[*] For further details see: https://www.iso27001security.com/html/27017.html
[†] For further details see: https://www.iso.org/standard/76559.html
[‡] For further details see: https://www.iso.org/obp/ui/#iso:std:iso-iec:27036:-4:ed-1:v1:en
[§] For further details see: https://tse.org.tr/IcerikDetay?ID=939&ParentID=1202

- Capital market institutions,
- Public partnerships,
- Turkey Capital Market Association,
- Turkey Appraisers Association.

With this circular, foreign cloud services were banned for the public. There are many statements in the Circular articles that exclude domestic service providers. Of course, the circular is not limited to this; First of all, it starts with the words Privacy, Integrity and Accessibility, which form the basis of the ISO 27001 standard. Therefore, let us emphasize that the circular is not limited to KVKK and the need to record information assets other than personal data and personal data that pose a risk to the government institutions by method of asset inventory.

In the continuation of the circular, special emphasis was given to personal data and their safe storage at home. It is useful to remind the encryption obligation again with the Resolution of the Personal Data Protection Board (KVKK) dated 31/01/2018 and numbered 2018/10 regarding "Sufficient Measures to be Taken by Data Officers in Processing Special Qualified Personal Data". At the end of the day, there are foreign cloud restrictions on special personal data that we have to encrypt and keep the crypto key in a different environment.

The circular, which also emphasized the storage of critical data in the network in a secure environment that is closed to the internet, reminded me of the "*Communique and Principles on Control of The Public Network and Control of The Public Network"* published in the Official Gazette No. 30103. Because the fact that the communication of public institutions with each other is compulsory at many points, sometimes suggests that several institutions should act as a single institution in matters such as File Sharing and Communication. As a matter of fact, we have also mentioned that the word KAMUNET refers to the "*closed circuit, public virtual network infrastructure, which will be transmitted by public institutions and organizations, in a way that is isolated from the private environment and the internet environment, safer against physical and cyber-attacks*".

It is necessary to touch upon the log records that have been dealt with about this article and the protection of the log records against modification. These issues are also expressed in sub-articles of A.8, A.9 and A.12 of ISO 27001 articles. It is also inevitable to point out that the issue is not limited to the internet traffic logs mentioned in the Act 5651 numbered "*Law on The Regulation of The Publications Made In The Internet Environment And The Communication of The Crimes Through These Publications*", it is inevitable to refer to all transaction logs.

The statement enforces; "There will be no confidential data sharing and communication over mobile "apk" except authorized crypto mobile applications." In another article of the circular, "Emphasis is placed on the security of dissemination (TEMPEST) or similar security measures where confidential information is processed. "Users will not put the data or voice recorder (USB memory, Flash Disk, MP3, MP4, mobile phone, etc.) used for data transfer on the computer into a unit / headquarters / institution," which we recall from the 19th article of MY 114-4 Information Security Instruction. A statement similar to the statement is now valid for the whole public. As a matter of fact, it should take similar measures for critical environments and meetings subject to critical data, without making a public-private distinction.

The circular also emphasized software development security and security tests. Especially, ISO 27001 standard emphasizes the distinction between testing and live environment, but does not provide detailed guidance to the institutions that make their own software. Here again, it is useful to mention GSP (Good Security Practices), although it recommends a multidisciplinary approach. In this context, it may be recommended; "TSEK 322 Basic Rules for Safe Software Development" to software developers. It is especially important for institutions trying to develop a number of MIS modules from within.

Apart from the KamuNet Communiqué, it is useful to mention the SOMEs within the scope of "Communication And Principles On The Installation, Duties And Works Of Intervention Teams Of The Cyber Events" and the Corporate SOME Foundation & Management Guide published in the Turkish Official Gazette No. 28818. It can be said that the SOME process and USOM applications, which were initiated before the Telecommunications Communication Presidency (TIB) was abolished

and its powers were transferred to Information Technology Board (BTK), will soon be included in the business life again and effectively. The transition of USOM to the digital notification system is an important and positive development in this context. SOME units from now on can work more effectively for the security of MIS applications in the cloud environment in the future.

Apparently the Gsuit, Onedrive, DropBox, Yandex Disk, Gmail, Yandexmail, Outlookmail vs Turkey-based platforms and domestic legal personality have not carried out a restructuring. Considering the presence of a small number of domestic service providers, we can say that a nice area has been created for investors, and a channel has been created for young IT professionals.

10. REASONABLE PRECAUTIONS

Frameworks used (ITIL, COBIT, TOGAF) followed standards (ISO 9001, 27001-2, 27017, 27018, 27036-4 and BS 25999.) and the regulations GDPR and KVKK are important elements for effective security. Furthermore, enrolment of subject matter experts with professional credentials (CISSP, CEH, CISA, CRISC, etc.) and trained staff will also be important indicators in terms of quality of service. The following points should be considered:

10.1. Access and Authentication

Access to services received during a service company must secure connection method should be used. This access is only to ensure that is done by the service person or institution, the following access control (authentication) technology for (two factor - such as two-tier control- etc.) one or more must be one supported.

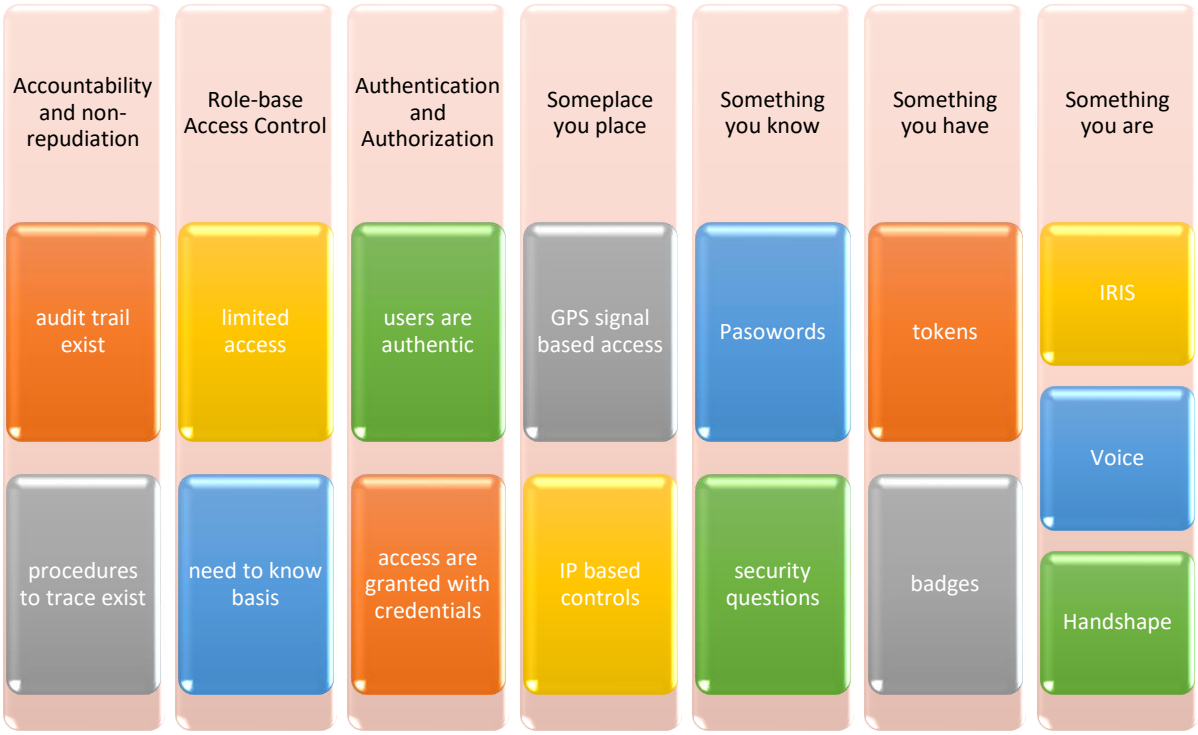


Figure 7. Depiction of possible security methods of access

10.2. Accessibility

For CC services received, SLA's (Service Level Agreement) should be used. For example, the survival of the services to be received 99.99% of the time server, etc. Particularly in projects involving high availability requirements, "Disaster Prevention" (Disaster Recovery) must be checked whether this kind of services are also delivered (Al-Shdaifat, 2015). Of course, the service provider will be decisive for the financial situation of the company and the quality of the service will be uninterrupted.

10.3. Physical Security

Cloud Computing provider of data center (Data Center) that they have physical security certificates (TIER 3-4, etc.) and security (biometric controls, fireproof walls and doors, 7x24 safety, physical barriers, flood-fire suppression systems, UPS systems, cooling systems, alarm mechanisms) should be examined, it should be investigated whether the cases should be controlled, as part of needed options.

10.4. Legal and Operational Security

The service received state licenses and legal obligations should be secured by contracts. In Turkey, CMB, BRSA and the guidelines of organizations such as legal obligations, also from the current 5651 law of Turkey etc. should be considered. The responsibilities of such regulations should be followed. Serving signed with the firm's personnel in operational service NDA etc. such contract staff should be investigations, if possible, on the resume information / commitment as it should be requested.

10.5. Data and Infrastructure Security

Especially PCI - DSS (Payment Card Industry - Data Security Standard) compliance with regulations such as the contractual obligations, the company received services data backup and delete / destroy forms should be questioned. Using bits of data, destruction methodologies should be investigated if possible, to be taken as a separate service. Company's intellectual knowledge or institutional importance of the data server that contains a strong encryption (encryption) algorithm stored, the service should be provided as to be retrieved when needed. The serving of the company's network infrastructure should be sure 7x24 proactively monitored. If possible, the proactive measures (DDOS protection, firewall system of IPS / IDS, Anti-Malware systems, anomaly detection systems, etc.) to be controlled by taking as a service, or should desirably be seen in regular reports.

11. CONCLUSION AND FUTURE WORK

Cloud Informatics, which has become increasingly popular in recent years, has been created and expanded by internet service providers such as TTNet, SkyAtlas, Amazon, Google, Microsoft, Aliyun, Intel etc. This service, provided by giant organizations, offers advantages such as data storage, infrastructure provisioning and online computing for MIS requirements. In addition, the transition to the online infrastructure raises concerns that unauthorized persons will be able to access personal information and will cause legal problems in the future. The main reason for possible privacy violations is that users' information is served on the same servers. Cloud Computing has not been able to address concerns about privacy violation; service providers can access the information stored in the cloud at any time. This also allows unauthorized users to change or delete data intentionally (intentionally) or unconsciously (accidentally). The main purpose of the continuity of online service received from the cloud systems, the integrity, availability and confidentiality of the data provided in the detection, audit and consulting services; protection of privacy and security. It is recommended that all persons and organizations using the Cloud System receive this service periodically from an expert team.

In this paper, we have introduced a few interruptions of Cloud assets and services. Firewalls alone may not be capable and adequate to protect the Cloud against those dangers. Denial-of-Service or Distributed Denial of System assaults are perplexing to recognize utilizing customary firewall. The Intrusion Detection System is a needed in part to distinguish digital attacks. At that point, we have introduced diverse interruption discovery methods utilized by Intrusion Detection System in an extensive and outlined path. The depiction of different kinds of Intrusion Detection System in cloud condition is given.

We have dissected some most recent research works that have been proposed to upgrade the cloud security utilizing Intrusion Detection System. The investigation demonstrates that albeit diverse Intrusion Detection System strategies help in recognitions of interruptions yet they don't give full security assurance. We prescribe to utilize the hybrid method to discover attacks and fulfill both

execution of distributed CC and security issues. We noticed that it is important to develop and update the hybrid working technique so as to enable it to detect most types of attacks and improve the security of the CC environment. Mathematical models and intelligent systems based on deep learning must be developed for the proposed identification strategies. Model-based analyzes should show that the proposed methods can increase the true alarms for DDoS attacks and differentiate the DDoS flood attacks from the flash crowds. Extensive experiments and simulations are needed to further study this area to confirm the effectiveness of the proposed detection strategies.

In order to decrease false positive and false negative alerts of IDS systems, additional security teams should be supported with threat intelligence systems. Cyber threat intelligence aims to raise awareness of potential threats. It is a necessary area to intervene before the undesired incidents occur. In this way, security solutions are maximized and necessary precautions are taken. Among the benefits of cyber threat intelligence; data loss prevention, detection of data breaches, incident response, threat analysis, data analysis and threat intelligence sharing can be improved significantly.

CC also poses a certain number of risks, since the storage of personal data in the cloud leads to the prevention of unlawful processing and access as well as the separation of the data officer, who is obliged to maintain the law EU General Data Protection Regulation (GDPR) and/or TR Personal Data Protection Law (KVKK), from his information technology network and the processing of personal data by cloud service providers. Therefore, it is necessary for the data officer to assess whether the security measures taken by the CC service provider are adequate and appropriate. In this context, it is recommended to Cyber Events Interference Teams (SOME) of government agencies that the personal data stored in the cloud be known in detail, backed up, synchronization is provided and at least two-step authentication control is applied for remote access if this personal data is processed. When storing and using personal data in these systems, it is necessary to encrypt them by cryptographic methods in cloud environments and to use encryption keys where possible for personal data, especially for each cloud solution that is serviced. When the cloud service relationship ends; all copies of the encryption keys that may be used to make personal data available must be destroyed.

REFERENCES

Alharkan T. and Martin P., (2012), "IDSaaS: Intrusion Detection System as a Service in Public Clouds," Proceedings of the 12th IEEE/ACM International Symposium on Cluster, *Cloud and Grid Computing* (CCGrid), pp. 686-687.

Al-Shdaifat B., Alsharafat W.S. and El-bashir M., (2015), "Applying Hopfield Artificial Network and Simulating Annealing for Cloud Intrusion Detection," *Journal of Information Security Research* ,vol. 6, pp.49-53.

Ambikavathi C. and Srivatsa S.K., (2015), "Improving virtual machine security through intelligent intrusion detection system," *Indian Journal of Computer Science and Engineering* (IJCSE), vol. 6, , pp.39.

CloudControls, Cloud Control Framework (Controls, Risks and Customer Questions), Cloud Controls Project, Netherlands, (online) (last accessed on 7th March, 2014).

Cooper S., (2019) "Best Intrusion Detection Systems (10+ IDS Tools Reviewed)" VPN News, [Online]. February 27, https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

CSA, Security Guidance, v3, Cloud Security Alliance, November 2011.

CSA, Cloud Controls Matrix, v1.4, Cloud Security Alliance, March 2013.

EC, European Commission, Report, (2012), "Unleashing the Potential of Cloud Computing in Europe" [Online]. 27 oct., https://www.pdpjournals.com/docs/88053.pdfGartner, (2017) "Strong SaaS and IaaS Performance Is Driving Growth in 2017", STAMFORD, Conn., October 12, https://www.gartner.com/en/newsroom/press-releases/2017-10-12-gartner-forecasts-worldwide-public-cloud-services-revenue-to-reach-260-billionin-2017 (last accessed on 11th May, 2020).

Ghosh P., Mandal A.K. and Kumar R., (2015), "An Efficient Network Intrusion Detection System," Chapter Information Systems Design and Intelligent Applications, vol. 339 of the series *Advances in Intelligent Systems and Computing*, pp91-99.

Gupta S. and Kumar P., (2015), "Immediate System Call Sequence Based Approach for Detecting Malicious Program Executions in Cloud Environment," *Wireless Personal Communications*, vol. 81, pp.405-425.

ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements

ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

ISO/IEC WD 27017 Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services

ISO/IEC WD 27036-4 Information technology -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud service

Kaliyamurthie K. P., Suresh R. M., (2012) "Artificial Intelligence Technique Applied to Intrusion Detection", *International Journal of Computer Science and Telecommunications*, Vol. 3, No. 4, pp. 20- 25.

Kaspersky (August 4, 2015) "DDoS Intelligence Report Q2 2015", By Kaspersky Lab [Online]. https://securelist.com/kaspersky-ddos-intelligence-report-q1& q2-2015/71663/

Kaspersky, (April 28, 2016), "DDoS Intelligence Report for Q1 2016", Kaspersky Lab [Online]. https://securelist.com/kaspersky-ddos-intelligence-report-for-q1-2016/74550/

Kaspersky, (November 3, 2015) "DDoS Intelligence Report Q3 2015", By Kaspersky Lab [Online]., https://securelist.com/kaspersky-ddos-intelligence-report-q3-2015/72560/

Kaspersky, (August 1, 2016), "DDoS Intelligence Report for Q2 2016", Kaspersky Lab [Online]. https://securelist.com/kaspersky-ddos-intelligence-report-for-q2-2016/75513/

Kaspersky, (January 28, 2016), "DDoS Intelligence Report for Q4 2015", By Kaspersky Lab [Online]. https://securelist.com/kaspersky-ddos-intelligence-report-for-q4-2015/73414/

Kene S.G., Theng D.P., (2015), "A review on intrusion detection techniques for cloud computing and security challenges*," IEEE 2nd International Conference on Electronics and Communication Systems* (ICECS), 2015, pp.227-323.

Khaldi A., Karoui K. and Ghezala H. B., (2014), "Framework to detect and repair distributed intrusions based on mobile agent in hybrid cloud," Inter. Conf. Par. and Dist. Proc. Tech. and Appl. (PDPTA'14), pp.471-476.

Khaldi A., Karoui K. and Ghezala H. Ben, (2014) "Framework to detect and repair distributed intrusions based on mobile agent in hybrid cloud," Inter. Conf. Par. and Dist. Proc. Tech. and Appl. (PDPTA'14), pp.471-476.

Khalimonenko A, Kupreev O, (2017), "DDOS attacks in Q1 2017" [Online]., https://securelist.com/ddos-attacks-in-q12017/78285/

Khalimonenko A, Kupreev O, Ilganaev K (2018) "DDoS attacks in Q4 2017" [Online]., Feb 6, https://securelist.com/ddos-attacks-in-q4-2017/83729

Khalimonenko A, Kupreev O, Ilganaev K (2017) "DDoS attacks in Q3 2017", [Online]. November 6,, , https://securelist.com/ddos-attacks-in-q3-2017/83041/

Khalimonenko A, Strohschneider J, Kupreev O, (2017), "DDoS attacks in Q4 2016" [Online]. February 2, https://securelist.com/ddos-attacks-in-q4-2016/77412/

Khatri J.K., Khilari G., (2015), "Advancement in Virtualization Based Intrusion Detection System in Cloud Environment," *International Journal of Science, Engineering and Technology Research* (IJSETR), vol. 4, pp.1510-1514.

Kolahi .S, K, Sarrafpour. B. (2015), "Analysis of UDP DDoS Flood Cyber Attack and Defense Machanics on Web Service with Linux Ubuntu 13". New Zealand, 978-1-4799-6532-8/15: Department of computing Unitec Institute of Technology. Auckland, IEEE.

Kupreev O, Strohschneider J, Khalimonenko A. Kaspersky, (2016) "DDOS intelligence report for Q3 2016" [Online]. October 31,,https://securelist.com/kaspersky-ddos-intelligence-report-for-q3-2016/76464/

Madhavi, M. (2012), "An Approach For Intrusion Detection System In Cloud Computing", International *Journal of Computer Science and Information Technologies*, 3(5), 5219–5222. 2012

Manthira S.M. and Rajeswari M., (2014), "Virtual Host based Intrusion Detection System for Cloud," *International Journal of Engineering and Technology* (IJET), vol. 5, pp. 5023- 5029.

Messier R., (2014) "Collaboration with cloud computing security, social Media, and Unified communications" *Elsevier.*

Modi C.N, D. Patel, (2013), "A novel Hybrid-Network Intrusion Detection System (H-NIDS) in Cloud Computing*," IEEE Symposium on Computational Intelligence in Cyber Security* (CICS), pp. 23-30.

Modi C.N. and Patel D., (2013), "A novel Hybrid-Network Intrusion Detection System (H-NIDS) in Cloud. Computing," *IEEE Symposium on Computational Intelligence in Cyber Security*(CICS), pp. 23-30.

Modi C.N., Patel D.R., Patel A. and Rajarajan M., (2012), "Integrating signature A priori based network intrusion detection system (NIDS) in cloud computing," *2nd International Conference on Communication, Computing and Security,* pp.905–912.

Muthukumar B. B. and Rajendran P.K., (2015), "Intelligent Intrusion Detection System for Private Cloud Environment," *Communications in Computer and Information Science* , vol. 536, pp.54-65.

NIST, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, Draft Special Publication 800-144, USA.

Pandeeswari N. and Kumar G., (2015), "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN," *Mobile Networks and Applications,* pp.1-12.

Patel A., Taghavi M., Bakhtiyari K., Junior J.C., (2013), "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview," *Journal of Network and Computer Applications,* vol. 36, pp.25–41.

Peng T, Leckie C, Ramamohanarao K. (2006), "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems." *ACM Transactions on Computational Logic* ,1-0.

Robinson T., (2015), "Series of DDoS Attacks plague linode data centers, infrastructure". *SC Magazine.*

Sangeetha S., Devi B.G., Ramya R., Dharani M.K. and Sathya P., (2015), "Signature Based Semantic Intrusion Detection System on Cloud," Chapter 66 of the book "*Information Systems Design and Intelligent Applications",* vol. 339 of the series Advances inIntelligent Systems and Computing, pp. 657 666

Singh D., Patel D., Borisaniya B., Modi C., (2016), "Collaborative IDS framework for cloud," *International Journal of Network Security*, vol.18, pp.699-709.

Stephen M. Specht, Ruby B. Lee. (2004), "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures". *International Workshop on Security in Parallel and Distributed Systems* pp. 543-550, September.