e-ISSN: 2455-7013
Asian Journal of Management, Engineering & Computer Sciences (AJMECS)
Vol. 3(4), October 2018: 1-16
URL: http://www.crsdindia.com/ajmecs.html
Email: crsdindia@gmail.com

RESEARCH PAPER

Review of Computer Systems Security: A Study

Gabriel Kabanda
Atlantic International University, 900 Fort Street Mall 40, Honolulu, Hawaii 96813, USA
Email: gabrielkabanda@gmail.com, profgkabanda@hotmail.com

ABSTRACT

The paper reviews the content, style and merit of the developments in Computer Systems Security. Information systems security comprises computer security and communications security. This can be strengthened by providing VPN support. Information Systems Security (ISS) is the the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. The normal requirement for network security is an Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Network intrusion detection systems were developed for network attack detection. The overall security in Cybersecurity is only as strong as the weakest link. Organizational policies should spell out the procedures for handling information security, with some legal assistance. It is of primordial importance that the company objectives clearly reflect access controls and security mechanisms. Common practice shows that employees are given access to only what they need, the internet is segregated into separate networks that compartmentalize security and access privileges are limited to minimise any security breaches. Separation of duties is one of the key principles of information security which can be supported by authentication and authorization systems that give access only to those business resources needed to perform one's duties. Practical examples of the application of IDS and IPS are given, including the ship communication network intrusion signal identification based on Hidden Markov model, collaborative intrusion detection method for marine distributed network, etc. An IPS is an IDS that also prevents the detected attack from taking place.

Key words: *Compute, Security, Review*

Received: 18th June 2018, Revised: 12th July 2018, Accepted: 16th July 2018

How to cite this article:
Kabanda G. (2018): Review of Computer Systems Security: A Study. AJMECS, Vol. 3[4]: Oct., 2018: 1-16.

ANALYTICAL EXPOSITION

The essay or review below describes or analyses the content, style and merit of the developments in Computer Systems Security. Information Systems Security (ISS) is the the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information systems security comprises computer security and communications security. The overall security in Cybersecurity is only as strong as the weakest link (Nielsen, R., 2015, p.8). It is of primordial importance that the company objectives clearly reflect access controls and security mechanisms. Common practice shows that employees are given access to only what they need, the internet is segregated into separate networks that compartmentalize security and access privileges are limited to minimise any security breaches (Nielsen, R., 2015, p.11). Nielsen (2015, p.12) argues that Virtual Private Networks or VPNs are known to provide secure access to internal company internet by employees on the Internet working from elsewhere outside the

company premises. The recommended network structure that provides a secure internet environment is shown on Figure 1 below (Neilsen, R., 2015, p.14).

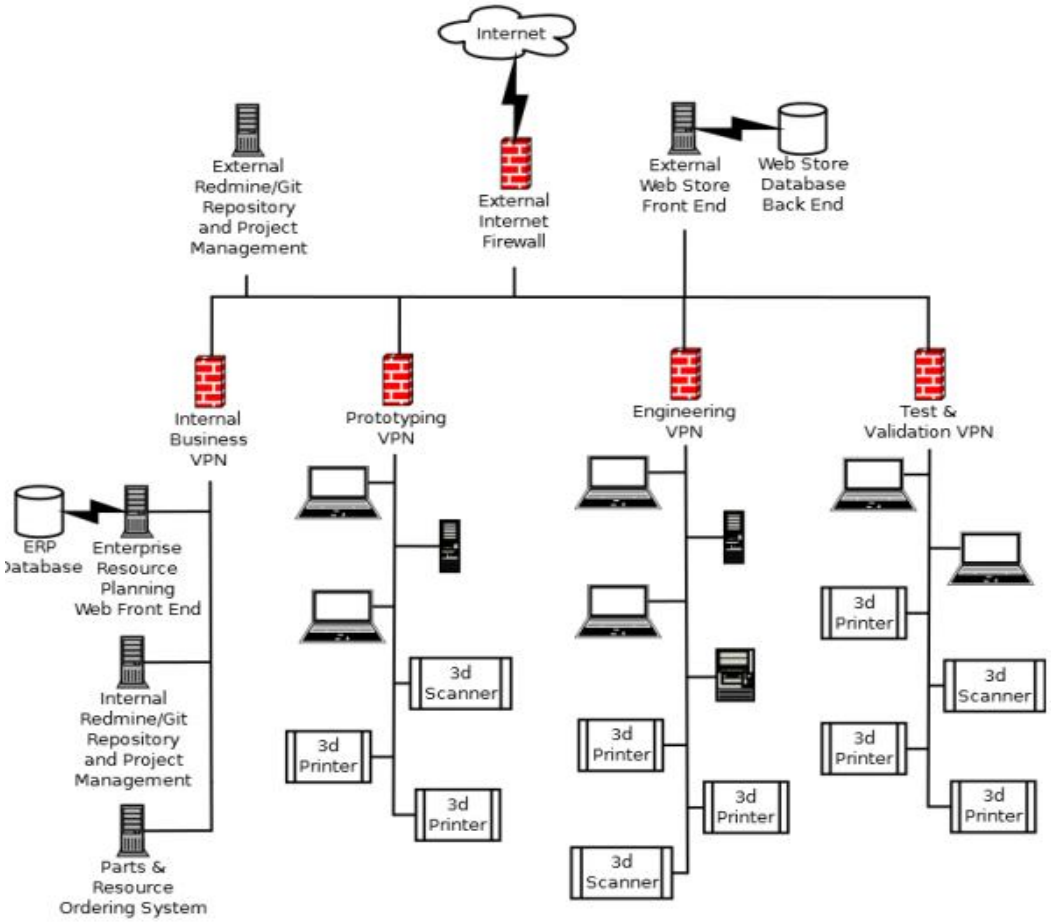

Fig. 1: Recommended Network Structure (Source: Nielsen, R., 2015, p.14)

A network can be defined as a group of computers and other devices connected in some ways so as to be able to exchange data. Each of the devices on the network can be thought of as a node; each node has a unique address.The first step in Network Security is redirect all network traffic through a single point and only open the ports on the firewall necessary for business traffic. This can be strengthened by providing VPN support (Nielsen, R., 2015, p.18). The normal requirement for network security is an Intrusion Detection Systems(IDS) and Intrusion Prevention Systems (IPS). Separation of duties is one of the key principles of information security which can be supported by authentication and authorization systems that give access only to those business resources needed to perform one's duties. As shown on Figure, this separation can be achieved through VPNs. A VPN provides mobility to the users to work on-site or off-site. However, in this separation of duties, there is need for an Intrusion Detection Systems(IDS) and Intrusion Prevention Systems (IPS) to protect the network (Nielsen, R., 2015, p.19). An IPS is an IDS that also prevents the detected attack from taking place. Organizational policies should spell out the procedures for handling information security, with some legal assistance. The policies should cover the following areas (Nielsen, R., 2015, p.14):

1. **Personal Electronic Devices (PED):**
   This defines the company handles company data on personal devices, such as cell phones, tablets, laptops, computers, other embedded devices, including 3D printers.
2. **Acceptable Use:**
   This policy specifies rules for use of company computing devices, rules for use of company network and company resources off-site, handling customer data, and rules for data in transit and data at rest.
3. **Records Retention:**
   The policy provides direction on retention of customer data, the business financial data, email, customer support transactions, and server and service logs.
4. **Identity Protection:**
   This policy is for the protection and preservation of customer identity and employee identity information.
5. **Server, Service and Project Computing Security:**
   This policy covers all server, service and project computing resources, including the computing security plan.
6. **Data Encryption:**
   The Data Encryption Policy provides the Framework and procedures for the encryption of customer data at transit, customer data at rest, business sensitive data in transit, and business sensitive data at rest.

System access threats fall into two general categories:

a. Intruders
b. Malicious software

With regard to intrusion, we take note of the following definitions (Stallings, W., 2015, p.3):

- *Masquerader:* an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
- *Misfeasor:* a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
- *Clandestine user:* an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection
- *Malicious Software:* these are programs that exploit vulnerabilities in computing systems, also referred to as malware. These can be divided into two categories:
  - **a.** Parasitic: fragments of programs that cannot exist independently of some actual application program, utility, or system program. Viruses, logic bombs, and backdoors are examples.
  - **b.** Independent: self-contained programs that can be scheduled and run by the operating system. Worms and bot programs are examples.

The Intrusion Detection System (IDS) often operates with sensors, analyzers and a user interface, as shown Figure 2 below. Intrusion detection in this case monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. The IDSs can either be host-based (monitors the characteristics of a single host and the events occurring within that host for suspicious activity) or network-based (monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity).

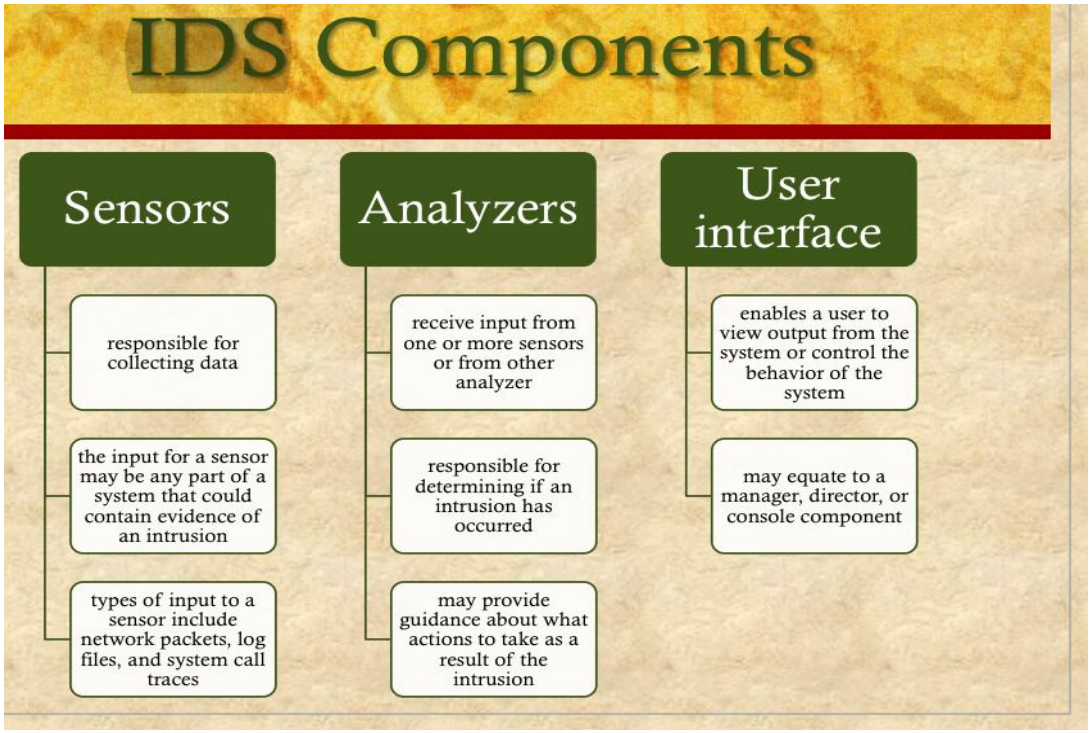

Fig. 2: The IDS Components (Source: Stallings, W., 2015, p.6)

A firewall provides network security against external threats and can simply be a dedicated computer that interfaces with computers outside a network with special security precautions built into it in order to protect sensitive files on computers within the network (Stallings, W., 2015, p.10). According to Stalllings (2015), the firewall is designed for these purposes:

1. The firewall acts as a choke point, so that all incoming traffic and all outgoing traffic must pass through the firewall
2. The firewall enforces the local security policy, which defines the traffic that is authorized to pass
3. The firewall is secure against attacks..

File System Access Control identifies a user to the system. Associated with each user there can be a profile that specifies permissible operations and file accesses, where the operating system can then enforce rules based on the user profile and the database management system then controls access to specific records or even portions of records (Stallings, W., 2015, p.19). However, the database management system decision for access depends not only on the user's identity but also on the specific parts of the data being accessed and even on the information already divulged to the user. Operating Systems Hardening is about the basic steps to secure an operating system (Stallings, W., 2015, p.28). This involves installing and patching the operation system, and then hardening and/or configuring the operating system to adequately address the identified security needs of the system by:

- removing unnecessary services, applications, and protocols
- configuring users, groups and permissions
- configuring resource controls
- installing and configuring additional security controls, such as antivirus, host-based firewalls, and intrusion detection systems (IDS), if needed.

Stallings (2015, p.31-38) recommends the following security control measures:

1. **Remove Unnecessary Services, Applications and Protocols:**
   The system planning process should identify what is actually required for a given system so that a suitable level of functionality is provided, while eliminating software that is not required to improve security. When performing the initial installation the supplied defaults should not be used, but rather the installation should be customized so that only the required packages are installed. It is better for security if unwanted software is not installed, and thus not available for use at all.

2. **Configure Users, Groups, and Authentication:**
   One should restrict elevated privileges to only those users that require them, but any default accounts included as part of the system installation should be secured. Those accounts which are not required should be either removed or at least disabled. Any passwords installed by default should be changed to new values with appropriate security.

3. **Configure Resource Controls:**
   Once the users and their associated groups are defined, appropriate permissions can be set on data and resources to match the specified policy. This may be to limit which users can execute some programs or to limit which users can read or write data in certain directory trees.

4. **Install Additional Security Controls**:
   It's possible to install and configure additional security tools such as antivirus software, host-based firewall, IDS or IPS software, or application white-listing. Some of these may be supplied as part of the operating systems installation, but not configured and enabled by default. IDS and IPS software may include additional mechanisms such as traffic monitoring or file integrity checking to identify and even respond to some types of attack

5. **Test the System Security:**
   Security testing is the final step in the process of initially securing the base operating system. The goal is to ensure that the previous security configuration steps are correctly implemented and to identify any possible vulnerabilities that must be corrected or managed.

6. **Security Maintenance:**
   The process of security maintenance includes monitoring and analyzing logging information, performing regular backups, recovering from security compromises, and regularly testing system security.

7. **Logging:**
   Since logging can generate significant volumes of information, it is important that sufficient space is allocated for them. A suitable automatic log rotation and archive system should be configured to assist in managing the overall size of the logging information. It is advisable to do some form of automated analysis as it is more likely to identify abnormal activity.

8. **Data Backup and Archive:**
   Performing regular backups of data on a system is another critical control that assists with maintaining the integrity of the system and user data. However, the needs and policy relating to backup and archive should be determined during the system planning stage, and key decisions may include whether the copies should be kept online or offline and whether copies should be stored locally or transported to a remote site.

9. Access Control Scheme:

When a user logs on to a Windows system a name/password scheme is used to authenticate the user. If the logon is accepted a process is created for the user and an access token is associated with that process object. The access token includes a security ID (SID) which is the identifier by which this user is known to the the system for purposes of security. The token also contains SIDs for the security groups to which the user belongs. The access token all necessary security information together to speed access validation, and allows each process to modify its security characteristics in limited ways without affecting other processes running on behalf of the user. The Windows Security Structure is shown on Figure 3 below.

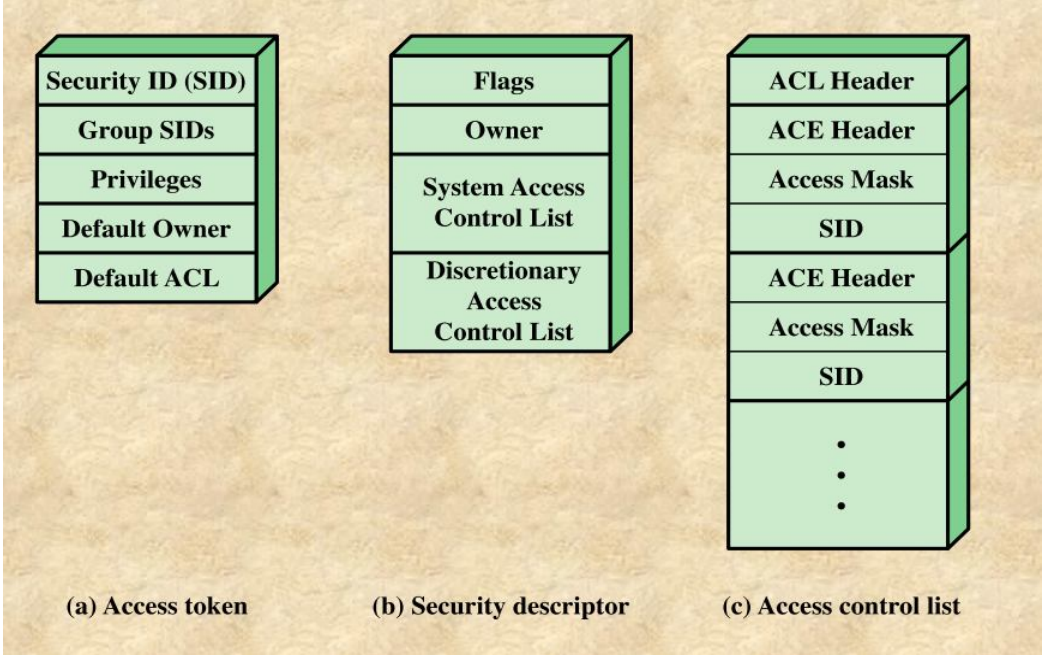

Fig. 3: Windows Security Structures (Source: Stallings, W., 2015, p.39)

CRITICAL CONTEXT:

The current intrusion signal recognition method cannot effectively suppress the noise signal interference in the ship communication network environment, and is sensitive to the initial parameters, which results in low recognition accuracy (Wu, W., 2018, p.1). Wu (2018) observed that because network attacks are widely spread in stages, it is very important to predict attacks and to warn of attacks in advance. Probability model can reflect the possibility of network intrusion, and enable system administrators to obtain the degree of risk. To address this problem, Wu (2018) proposed an identification method based on hidden Markov model for ship communication network intrusion signal, where the eigenvalue of the collected network signal CSI (channel state information) is denoised and classified. In the probability modeling methods, Markov chain model has been widely used in the field of intrusion detection.

There are many intrusion identification methods and these include a semi-supervised fuzzy clustering algorithm based on isomeric distance and sample density for network intrusion detection (Kylili *et al.*, 2018), but this method is constrained by the data sample dimension, and it is difficult to effectively deal with the problem of large scale network intrusion signal recognition. Geng, Li, and Ye (2017) proposed an intrusion detection method with rough weighted mean mono-dependent estimation based on rough set

theory and Bayesian theory. However, this method is based on rough set theory to reduce the attribute of network data and the recognition accuracy needs to be improved (Wang *et al*., 2010; Wu *et al*., 2010). To address the above problems, based on deep research of hidden Markov model intrusion detection method, combined with the characteristics of global optimization of genetic algorithm, Wu (2018) used the genetic algorithm to optimize the model for the sensitive problem of hidden Markov model to initial parameters, and proposed an identification method based on hidden Markov model for ship communication network intrusion signal. The proposed method can improve the accuracy of the model and the accuracy of intrusion signal identification, and effectively reduce the false alarm rate.

The channel state signal of the ship communication network is weak and is easily covered by the noise. To avoid the problem of denoising methods involving the use of low (high) pass filter, principal component analysis (PCA) method is applied to preprocess the network signal (Wei and Liu, 2016). By the orthogonalized linear transformation, the network signal is transformed into a new coordinate system, making the first variance of the data projected at the first coordinate (called the first principal component) and the second variance of the data projected at the second coordinate (called the second principal component), and so on, that is, sorting variance in descending order and dimensionality reduction (Wu, 2018, p.2). According to Wu (2018, p.2), there are two main advantages to the preprocessing of the network signal by the principal component analysis method:

1. PCA can reduce the dimension of the network signal collected on the receiving device, that is, extract the fluctuation signal related to the network activity, reduce the amount of calculation and improve the recognition accuracy.
2. As the background noise of the network environment is random and irregular, PCA can use the relative change rate to eliminate the noise in the background environment.

Wu (2018) proposed a hidden Markov model-based intrusion signal recognition method for ship communication network for the problem of low recognition accuracy and initial parameter sensitivity in the current network intrusion recognition method, where the principal component analysis method was used to denoise and classify the network continuous signals by selecting appropriate k value. In the process of building and training hidden Markov model, an improved genetic algorithm was used to optimize the initial parameters of the hidden Markov model. Under the condition of randomly selecting a set of output parameters, the result of genetic algorithm optimization was used as the initial parameter of hidden Markov model, which solves the problem that hidden Markov models are sensitive to initial parameters (Wu, 2018, p.4). Experimental results showed that the highest recognition accuracy of the proposed method was up to 97.58% and the prediction effect was achieved.

The current detection technologies for airport perimeter security usually include vibration cables, infrared detection, microwave detection, underground cables, tension fencing, video surveillance, and other technologies, but it is rare that laser detection technology is used (Wu *et al*, 2016, p.1). Compared with those detection technologies, laser technology has many advantages which include high density of transmitted power, small divergence angle, concentrated light beam, and adaptability to poor weather and environmental conditions. Under the same conditions, the power density is hundreds to thousands of times that of infrared light-emitting diodes, the detection range is up to several hundred meters or several kilometers, the transmission attenuation is much smaller than other similar detectors, and it has a strong ability to penetrate rain and fog so it can greatly reduce false alarms due to the impact of climate and environment (Wu *et al*, 2016, p.1). In consideration of the airport surroundings, Wu *et al* (2016) divided the

laser anti intrusion security system intro three parts: the decision-making system, the monitoring system, and the front-end laser detection system, as shown on Figure 4.

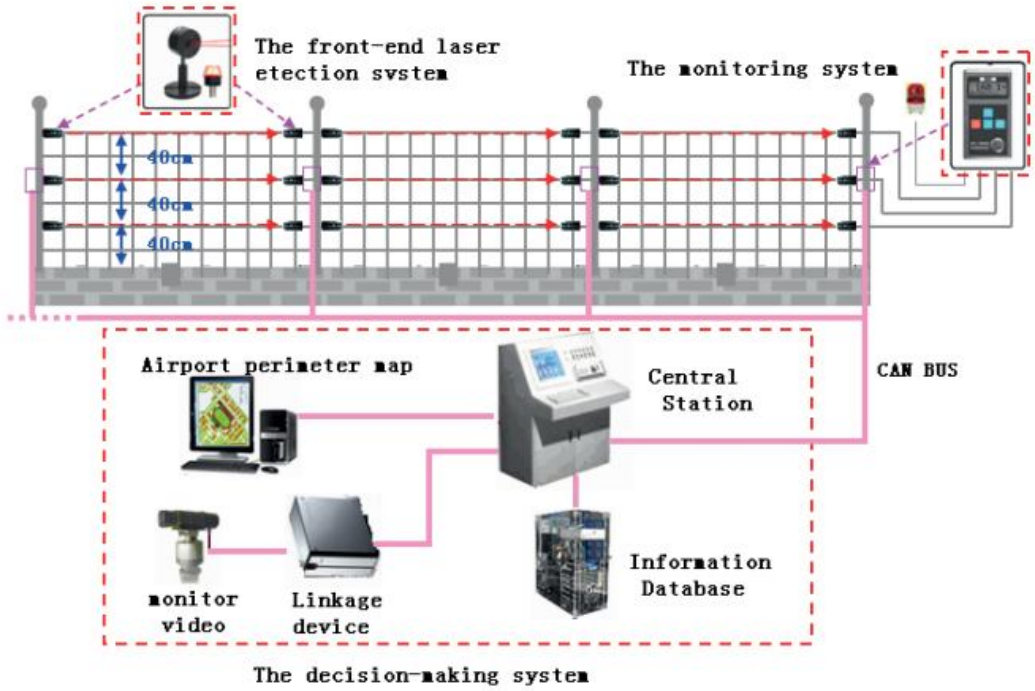

Fig. 4: The antiintrusion laser alarm system (Source: Wu *et al* 2016, p.2)

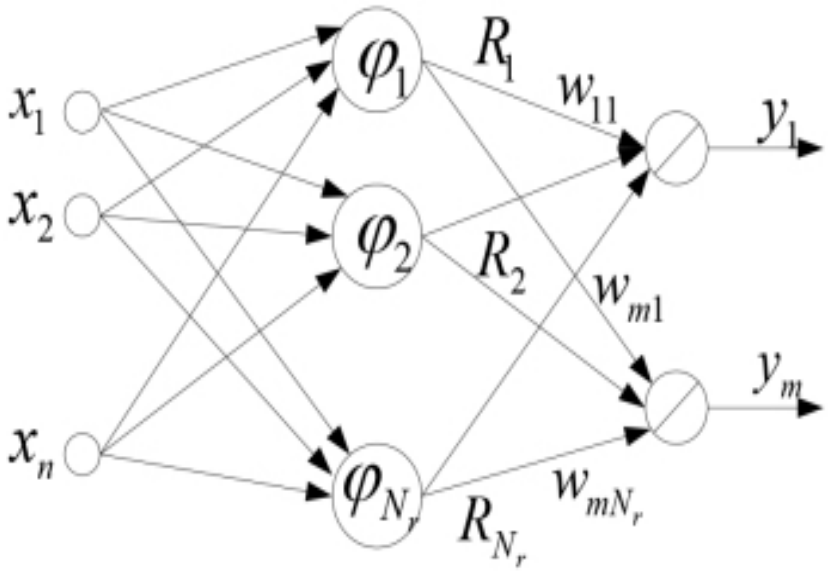

Fig. 5: The structure of the Radial Basis Function (RBF) neural network (Source: Wu *et al,* 2016, p.6)

Intrusion incidents at airport perimeters can be divided into six categories. The classification of incidents is a process of pattern recognition: correct classification and description by the cognition of things. Current pattern recognition methods have tended to use artificial intelligence, including expert systems, fuzzy theory, genetic algorithms, neural networks, and other methods. Among these methods, artificial neural networks have the unique capability of processing nonlinear information and distributed storage ways for information (Wu *et al,* 2016, p.6). The radial basis function (RBF) neural network is a two-forward type neural network, where the intermediate layer node's output is the value of the RBF, as shown on the network model on Figure 6.

X = {x1, x2, . . . , xn } are n-dimensional input vectors and the output of the hidden layer nodes are the RBF values. The hidden layer unit performs a nonlinear transformation, which is the input mapping to a new space. RBF is commonly a Gaussian function and its expression is as follows (Wu *et al*, 2016, p.6).

$$R_j = \varphi_j(X) = e^{-\|X-C_j\|^2/(2\sigma_j^2)}, j = 1, 2, \ldots, N_r$$

If the input vector X and the center point are farther away, the output value is closer to 0. The output of the RBF neural network is a linear combination of the output of the hidden units.

$$y_i = \sum_j w_{ij} R_j, i = 1, 2, \ldots, p$$

The RBF network converts the M-dimensional original space to P-dimensional output space by this nonlinear mapping.

Network intrusion detection systems were developed for network attack detection. From an analysis of packet contents of the network, one can find the attacks or malicious behavior. However, the packet inspection is a complicated and resource-consuming process that is usually impossible. One of the most effective methods used is by flow-based intrusion detection. In this approach, the common properties of network packets are analyzed instead of the packet contents, where only a fraction of network data is analyzed to detect the attacks. Karimpour *et al* (2016, p.1) employed the combination of flow-based and graph-based procedures to reveal attacks. In the project, network packets were collected to create the flows and which were then clustered using a graph-clustering algorithm that is based on a genetic algorithm. The average weight of clusters was calculated in a time series, and some threshold points and time intervals were investigated to achieve the most accurate detection rate of the attack. Security threats and related incidents in the Internet cause several problems for its users, and so the introduction of new intrusion detection methods is of the utmost concern. Internet traffic grows as line speeds increase which makes network monitoring a resource-consuming process when a huge volume of network traffic is found in today's networks. Concerning the the data communications in the network, one takes note of the relational behavior of the network, which is only obtained by using the flow and graph concepts.

Karimpour *et al* (2016, p.2) provided a general overview of intrusion detection approaches is provided, which are categorized in 4 parts as follows:

1. *Feature-based approaches:* the key idea of these approaches is based on the concept that similar graphs probably share common attributes such as diameter, eigenvalues, and a distribution of degree. Moreover, these methods can be used for checking the structure of a graph in order to find patterns and explore anomalies.
2. *Decomposition-based approaches:* in these approaches, tensor decomposition and graph structure are used as an interpretation of eigenvectors and convergence of graph attributes to find the patterns, respectively.

3. *Community-based approaches:* in these approaches, the main action is graph clustering. Clustering algorithms are employed to create cluster parameters of data, and the anomalies are recognized based on their values.
4. *Window-based approaches:* in this category, the evolutionary behavior of the anomalies in time intervals reveals the patterns. Many recent research studies have also employed these methods in order to detect the behavior of the network and whether it is a normal or malicious case.

A general view of these intrusion detection methods according to the above 4 categories are shown on Table 1 below.

Table 1: Anomaly detection methods (Source: Karimpour *et al* (2016, p.3)

Method	Data type	Attack	Proposed system	Accuracy
Graph in time series	Flow-based	DDoS	Graph-based	94.2%
Dispersion graph	Flow-based	DDoS	Graph-based	100%
Using flow concept	Flow-based	Dictionary	Flow-based	99%
Graph clustering and local deviation coefficient	Packet-based	DoS, Scan	Graph-based	95.3%
Graph clustering and local deviation factor	Packet-based	DoS, Scan	Graph-based	97.2%
Packet heard analyzing	Packet-based	DoS, Scan	Packet-based	95.4%

The flow and graph-clustering concepts were used by Karimpour *et al* (2016, p.3) to detect an attack in the network such that the nodes, the edges, and the weight of edges indicate the IPs, the flows, and the number of flows in the graph, respectively. Based on the average weight of clusters that are reached from the graph-clustering algorithm and comparing it in several time intervals and threshold points, the anomaly points can be detected. The corresponding steps used in the intrusion detection experiment by Karimpour *et al* (2016, p.3) are shown on Figure 6 below.

1. Collecting packets of network traffic
2. Extracting packet header
3. Creating flows based on common properties of the packets
4. Creating graphs and performing clustering algorithm on graphs in several time intervals
5. Calculating number and weight of clusters in normal and anomaly state
6. Detecting attack based on the above parameters
7. Creating Markov model based on average weight of clusters
8. Calculating detection rate of intrusion detection and accuracy of model

Fig. 6: Steps of the intrusion detection approach (Source: Karimpour *et al,* 2016, p.3)

The outcome of the research by Karimpour *et al* (2016, p.4) involved 7 weeks of network traffic and 5 types of attacks: DoS, scan, local access, user to root, and data, which are shown on Table 2 below, indicating the number and types of attacks in each categorized attack.

Table 2: Various attack descriptions (Source: Karimpour *et al,* 2016, p.4)

Attack type	Description
DoS	Denial of service; an attempt to make a network resource unavailable to its intended users: temporarily interrupt services of a host connected to the Internet
Scan	A process that sends client requests to a range of server port addresses on a host to find an active port
Local access	The attacker has an account on the system in question and can use that account to attempt unauthorized tasks
User to root	Attackers access a user account on the system and are able to exploit some vulnerability to gain root access to the system
Data	Attackers involve someone performing an action that they may be able to do on a given computer system, but that they are not allowed to do according to policy

$$AveW = \frac{\sum_{i=1}^{N}(W_i) - (\sum_{i=1}^{N} ExtW_i)/N}{N}$$

From the above illustration, the final model of attack detection can be created where the cluster-based data are given as input to the model, and then the proposed criterion is calculated in the time series so that the normal and anomaly points are detected based on defined threshold points. Different threshold points are investigated in the time series to identify the best one, and the best threshold point is extracted from the detection rates of the suggested way during several time intervals (Karimpour *et al,* 2016, p.5).

Li (2018) worked on a collaborative intrusion detection method of marine distributed network based on clustering with the aim to reduce the long delay in the current marine distributed network which had an intrusion detection method based on support vector machine. The research used correlation analysis method for mining data in marine distributed network, and clustered the marine distributed network data through the decision tree algorithm based on the relative decision entropy and the difference degree algorithm. A marine distributed network intrusion model was built on this basis, which not only occupies less memory space, but also its detection rate is above 92%, which improves the accuracy of intrusion detection. The marine distributed network is an important component of ship navigation system, and its stability and reliability directly affect the safety of ship navigation. The collaborative intrusion detection carries out the detection by the intrusion means and provides the monitoring information in time, which becomes an important means to ensure the security of marine distributed network (Li, X., 2018, p.1). The collaborative intrusion detection for distributed network guarantees the normal sailing of a ship. An experiment was conducted to verify the application effect of the proposed collaborative intrusion detection method of marine distributed network based on clustering. Li (2018) concluded on the following:

Advances in the area of machine learning provide opportunities to researchers to detect network intrusion without using a signature database. Demir and Dalkilic (2017) studied and analyzed the performance of a stacking technique, which is an ensemble method that is used to combine different classification models to create a better classifier, on the KDD'99 dataset. In this study, the stacking method was improved by modifying the model generation and selection techniques and by using different classifications algorithms as a combiner method. Model generation was performed using subsets of the dataset with

randomly selected features. Various metrics were used in model selection and only selected models were used as input for the combiner method.The stacking technique provided higher accuracy results all the time compared to pure machine learning techniques. The second important result was obtaining the highest detection rate for user-to-root attacks compared to other studies.

Ensemble learning is a machine learning approach where more than one learner (classification models or regression models) is used to solve the same classification or regression problem. In contrast to the conventional machine learning approaches that try to construct a model from training data, ensemble methods construct a set of models (learners) and combine them. Demir and Dalkilic (2017) proved that weak learners could be boosted to strong learners. There are three common and widely known types of ensemble techniques: bootstrap aggregating, boosting, and stacking (Demir, N., and Dalkilic, G., 2017, p.1). Bootstrap aggregating, known as bagging, trains each model by drawing random subsets of the training set. The random forest algorithm uses bagging and combines random decision trees. Boosting incrementally builds an ensemble model by training each new model using the misclassified training instances that previous models misclassified. Stacking, also known as stacked generalization, is a method where an algorithm is used to combine the outputs of other models' predictions. Stacking is the generalization of other ensemble methods.

Generally the base classification algorithm(s) and training data are accepted as inputs during the training phase. Model generation is used to train the algorithm with data and generate models. If the stacking implementation accepts only one algorithm, usually the "model generation" phase generates n models by using the algorithm with randomly drawn sub-datasets. If the implementation accepts multiple algorithms, usually the training set is trained with each algorithm. When the models are generated, these models then generate the predicted labels. (Demir, N., and Dalkilic, G., 2017, p.2). This constitutes the first layer of the two-layered training phase. The predicted labels of each model are given as input to the second layer. In the second layer, a classification algorithm (also called the combiner method) is used to generate a final model while the original labels are still used for labeling the new training data.The training phase of the stacking approach is shown on Figure 7 below.

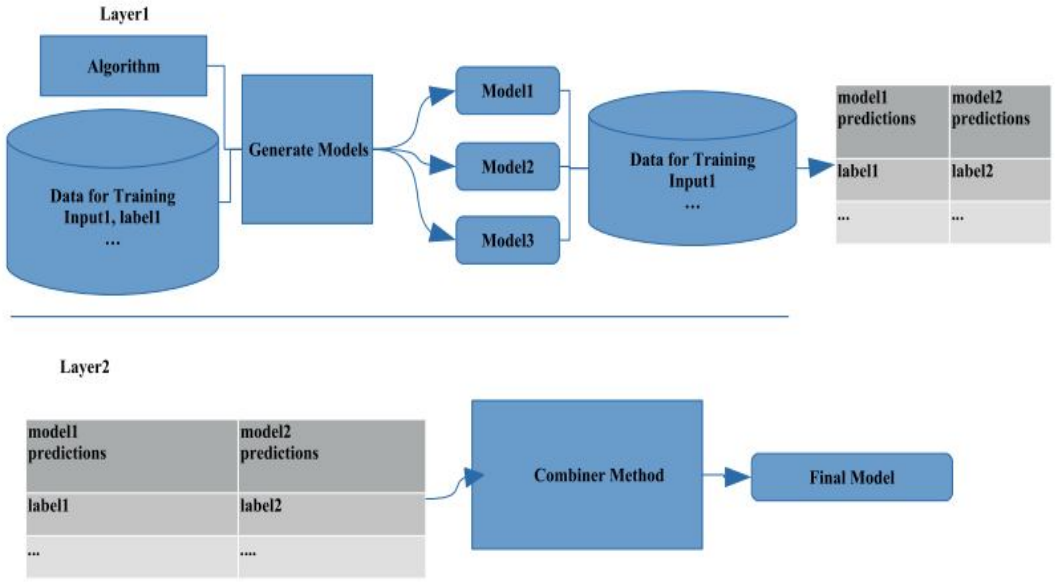

Fig. 7: Training phase of tracking approach (Source: Demir, N., and Dalkilic, G., 2017, p.4)

The prediction phase of the stacking also contains two layers. The first layer uses the input data and previously generated models and makes a prediction, and the second layer uses the model previously generated in the second layer of the training phase. The prediction phase of stacking approach is shown on Figure 8.

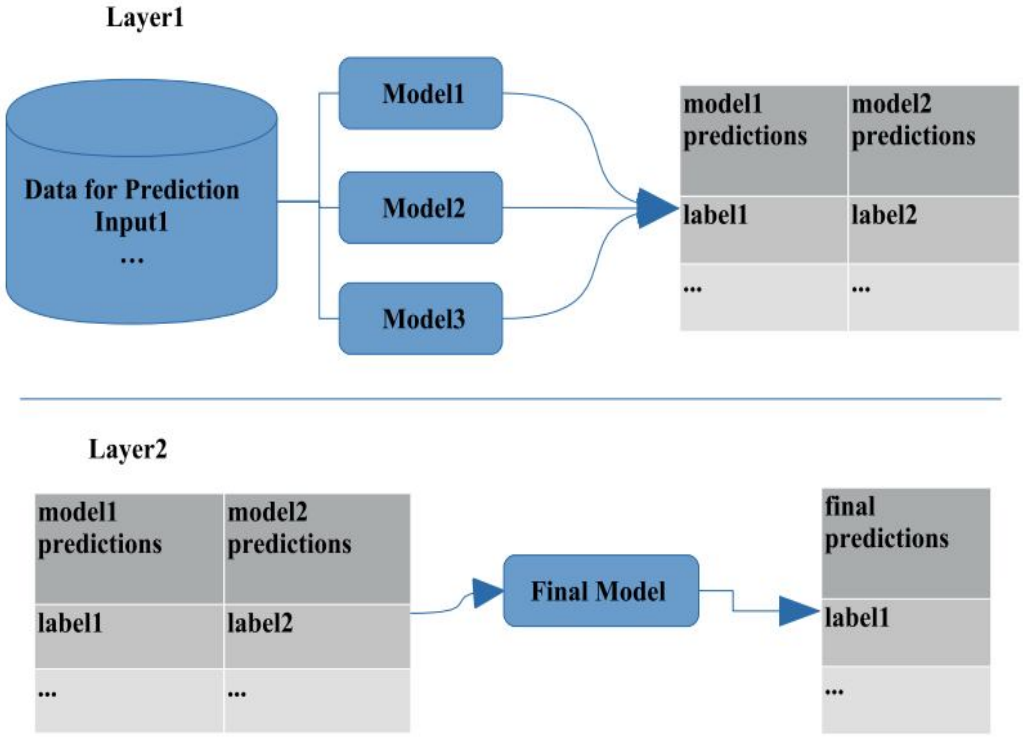

Fig. 8: Prediction phase of tracking approach (Source: Demir, N., and Dalkilic, G., 2017)

Demir and Dalkilic (2017, p.4) evaluated each experiment with six metrics, which led to 78 results. The evaluation metrics are listed below:

- tp normal: True positive percentage of normal labeled data,
- tp probe: True positive percentage of probe labeled data,
- tp dos: True positive percentage of DoS labeled data,
- tp u2r: True positive percentage of U2R labeled data,
- tp r2l: True positive percentage of R2L labeled data,
- accuracy: Accuracy of the experiment.

The results of the experiments are shown on Figure 9 below.

The research article by Demir and Dalkilic (2017) came out with a threat model which assumed that there is a monitoring system that collects information on the packet level. However, these assumptions may not always hold water. It also assumed that the attacker can do four types of attack:

- The attacker is able to gain a user right on the target host by exploiting various vulnerabilities of the applications running on the target host,
- The attacker already has a user account in the target host and can gain root access by exploiting various vulnerabilities of the applications running on the target host,
- The attacker is able to launch a denial of service (DoS) attack by exploiting the vulnerabilities of the applications running on the target host, and
- The attacker probes the target host with various techniques to gain information.

Combiner/stacking algorithm	Model selection method	Exp. #	tp_normal %	tp_probe %	tp_dos %	tp_u2r %	tp_r2l %	Accuracy %
Logistic regression (no stacking)	-	1	98.1	68.7	82.8	8.6	5.6	81.53
Logistic regression	all	2	98.3	83.5	97.3	12.9	5.2	92.43
	accuracy_score	3	98.4	72.9	97.3	8.6	5.6	92.33
	information_gain	4	98.4	73.7	97.3	7.1	5.6	92.36
	recall_mean	5	98.2	72.3	97.3	8.6	5.6	92.31
Decision tree	all	6	99.4	77.0	97.3	14.3	2.5	92.47
	accuracy_score	7	99.0	73.7	97.3	7.1	5.6	92.46
	information_gain	8	99.0	78.3	97.3	8.6	5.7	92.55
	recall_mean	9	99.0	75.2	97.3	18.6	5.5	92.46
Naïve Bayes	all	10	97.3	78.9	93.2	47.1	6.0	89.19
	accuracy_score	11	97.9	80.2	97.2	30.0	5.7	92.29
	information_gain	12	97.9	79.9	97.2	30.0	7.6	92.39
	recall_mean	13	98.0	79.0	96.7	35.7	5.6	91.90

Fig. 9: The results of the experiments (Source: Demir, N., and Dalkilic, G., 2017, p.11)

Cloud computing provides access to programs, storage, and development platforms through the Internet through any device such as PCs, smartphones, laptops or PDAs. The major benefits of cloud computing are cost savings, availability and scalability (Umamaheswari, K., and Sujatha, S., 2017, p.1). Intrusion detection system (IDS) is one of the tools for alerting any sign of intrusion activities at the virtual machine level of virtualised cloud. Intrusion detection and prevention systems (IDPS) include all protective actions or identification of possible incidents, analysing log information of such incidents, how to block them in the beginning itself and generate reports for the concern of security personnel (Umamaheswari, K., and Sujatha, S., 2017, p.1). The IDPS components must first and foremost be secure since it is the primary target of attackers who try to prevent the IDPSs functioning of detecting attacks or to access the sensitive data on IDPSs like host configuration and known vulnerabilities. According to Umamaheswari and Sujatha (2017), the components in IDPSs can be sensors or agents, management and database servers, user and administrator consoles for interaction and management networks. There is need for protection of the software-based IDPS components such that their operating systems and applications are kept fully up-to-date. Umamaheswari and Sujatha (2017) proposed a model of defence framework which arranges intrusion detection components in a maze-like structure so as to capture and dynamically correlate unknown attacks as early as possible. The model made two significant contributions for impregnable protection, one is to reduce alert generation delay by dynamic correlation and the second is to support the supervised learning of malware detection through system call analysis. The defence formation facilitates malware detection with linear support vector machine- stochastic gradient descent (SVM-SGD) statistical algorithm. It requires little computational effort to counter the distributed, co-ordinated attacks efficiently. The framework design, then, takes distributed port scan attack as an example for assessing the efficiency in terms of reduction in alert generation delay, the number of false positives and learning time through comparison with existing techniques (Umamaheswari, K., and Sujatha, S., 2017, p.1).

Encryption is one of the fundamental keys to cybersecurity for Government and private sector. However, encryption is expensive to obtain and time-consuming to certify.

INTEGRATIVE CONCLUSION

The overall security in Cybersecurity is only as strong as the weakest link (Nielsen, R., 2015, p.8). The essay or review described or analysed the content, style and merit of the developments in Computer Systems Security. Information systems security comprises computer security and communications security. Information Systems Security (ISS) is the the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. The normal requirement for network security is an Intrusion Detection Systems(IDS) and Intrusion Prevention Systems (IPS). This can be strengthened by providing VPN support (Nielsen, R., 2015, p.18). Nielsen (2015, p.12) argues that Virtual Private Networks or VPNs are known to provide secure access to internal company internet by employees on the Internet working from elsewhere outside the company premises. Common practice shows that employees are given access to only what they need, the internet is segregated into separate networks that compartmentalize security and access privileges are limited to minimise any security breaches (Nielsen, R., 2015, p.11).

Organizational policies should spell out the procedures for handling information security, with some legal assistance. Supportive computer security policies are required in any modern organization to mitigate against the risk of cyber attack. It is of primordial importance that the company objectives clearly reflect access controls and security mechanisms. The policies should cover the following areas:

1. Personal Electronic Devices (PED)
2. Acceptable Use
3. Records Retention
4. Identity Protection
5. Server, Service and Project Computing Security
6. Data Encryption

Each of the devices on the network can be thought of as a node; each node has a unique address.The first step in Network Security is redirect all network traffic through a single point and only open the ports on the firewall necessary for business traffic. Intrusion detection and prevention systems (IDPS) include all protective actions or identification of possible incidents, analysing log information of such incidents, how to block them in the beginning itself and generate reports for the concern of security personnel (Umamaheswari, K., and Sujatha, S., 2017, p.1). The IDPS components must first and foremost be secure since it is the primary target of attackers who try to prevent the IDPSs functioning of detecting attacks or to access the sensitive data on IDPSs like host configuration and known vulnerabilities. Stallings (2015, p.31-38) recommends the following security control measures:

1. Remove Unnecessary Services, Applications and Protocols
2. Configure Users, Groups, and Authentication
3. Configure Resource Controls
4. Install Additional Security Controls
5. Test the System Security
7. Security Maintenance
8. Logging
9. Data Backup and Archive
10. Access Control Scheme

REFERENCES

1. Demir N. and Dalkilic G. (2017): Modified stacking ensemble approach to detect network intrusion, Turkish Journal of Electrical Engineering & Computer Sciences, Accepted/Published Online: 15.11.2017, http://journals.tubitak.gov.tr/elektrik/

2. Geng X.C., Li Q.M. and Ye D.Z. (2017): Intrusion detection algorithm based on rough weightily averaged one-dependence estimators, Journal of Nanjing University of Science and Technology, 41(4): 420-427.
3. Karimpour J., Lotfi S. and Siahmarzkooh A.T. (2016): Intrusion detection in network flows based on an optimized clustering criterion, Turkish Journal of Electrical Engineering & Computer Sciences, Accepted/Published Online: 17.07.2016, http://journals.tubitak.gov.tr/elektrik/
4. Kylili A., Fokaides P.A., Ioannides A. and Kalogirou S. (2018): Environmental assessment of solar thermal systems for the industrial sector, Journal of Cleaner Production, 176: 99-109.
5. Li X. (2018): Collaborative intrusion detection method for marine distributed network, In: Liu, Z.L. and Mi, C. (eds.), Advances in Sustainable Port and Ocean Engineering, Journal of Coastal Research, Special Issue No. 83, pp. 57–61, Coconut Creek (Florida), ISSN 0749-0208.
6. Nielsen R. (2015): CS651 Computer Systems Security Foundations 3d Imagination Cyber Security Management Plan, Technical Report January 2015, Los Alamos National Laboratory, USA.
7. Stallings W. (2015): Operating System Stability. Accessed on 27th March, 2019. https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH15-OS8e.pdf
8. Umamaheshwari K. and Sujatha S. (2017): Impregnable Defence Architecture using Dynamic Correlation-based Graded Intrusion Detection System for Cloud, Defence Science Journal, 67(6): 645-653.
9. Wang C., Xiang H., Xu Y., Hu D., Zhang W., Lu J., Sun L. and Nie S. (2010): Improving emergency preparedness capability of rural public health personnel in China, Public Health, 124(6): 339-344.
10. Wang H.Z. (2016): Research and application of network intrusion detection algorithm in internet environment, Modern Electronics Technique, 39(21): 107-111.
11. Wei Z.W. and Liu F. (2016): Research of network intrusion detection based on particle swarm optimization and support vector data description, Microelectronics and Computer, 33(8): 144-148.
12. Wu H., Wang Z. and Wang C. (2016): Study on the recognition method of airport perimeter intrusion incidents based on laser detection technology, Turkish Journal of Electrical Engineering & Computer Sciences, Accepted/Published Online: 20.10.2016, http://journals.tubitak.gov.tr/elektrik/
13. Wu L.Y., Li S.L. and Gan X.S. (2017): Network anomaly intrusion detection CVM model based on PLS feature extraction, Control and Decision, 32(4): 755-758.
14. Wu S., Zhu W., Li H., Yu I.T., Lin S., Wang X. and Yang S. (2010): Quality of life and its influencing factors among medical professionals in China, International Archives of Occupational and Environmental Health, 83(7): 753-761.
15. Wu W. (2018): Ship communication network intrusion signal identification based on Hidden Markov model, In: Liu, Z.L. and Mi, C. (eds.), Advances in Sustainable Port and Ocean Engineering, Journal of Coastal Research, Special Issue No. 83, pp. 868–871. Coconut Creek (Florida), ISSN 0749-0208.