The Comprehensive Analysis of Intrusion Detection Systems in Cloud Computing Security

R. Renugadevi[1], M.Umamaheswari[2]
[1]*Assistant Professor, Department of Computer Science,*
Vels Institute of Science and Technology Advanced Studies (VISTAS), Chennai.
[2]*Research Scholar, Department of Computerscience*
Vels Institute of Science and Technology Advanced Studies (VISTAS),Chennai.

Abstract- Cloud computing is the modern model of the technology that is, reliable, on-demand network access to shared configurable computing resources that are quickly provisioned and free with minimal structural management effort. These cloud resources, information and applications square measure vulnerable for attacks. Intrusion Detection Systems (IDS) square measure utilized within the cloud to find malicious behavior within the networks and conjointly within the hosts and The Network Intrusion Detection Systems (NIDS) which analyzes all packets which transferred through network by capturing every network communications. Intrusion Detection Systems for Cloud computing were increased in several biases, but cloud computing still has several problems regarding securities, like privacy problems, loss of information and purloined of information.Furthermore, securing the new advanced technologies has become more challenging. Cloud computing and containers are among those emerging technologies that have introduced security challenges, and it is necessary that they be addressed. One of the main features of both cloud and container technologies is the sharing of resources of both hardware and software. Some Authors Discussion and Some security problems over cloud services as well as confidentiality, integrity, convenience, privacy and attacks square measure involved by the users. Following this paper we have a tendency to reviews a number of problems and their current solutions.
Keywords: Cloud computing, security, IDS, NIDS, CIDS

I. INTRODUCTION

Cloud computing stepped in the information Technology (IT), security problems faced by cloud suppliers and customers became a very important issue. The present reasonable technologies that are quite capable of handling securities, like Cisco, Cloudflare., some developers still couldn't provide the most effective of security in their services. This creates the cloud services as vulnerable as it will simply be attacked by attackers. Firewalls and Intrusion detection systems play major roles in maintaining the network firmly. Network Intrusion Detection is an associate attack defense reaction during which intruders are known support varied characteristics of their request within the network. Thus, cloud suppliers guarantee a secure infrastructure and shieldthe client's information and applications.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processed.

Integrity: The property of accuracy and completeness.

Availability: The property of being accessible and usable upon demand by an authorized entity. What is Intrusion Detection? Heady etal. [1]defined intrusion as "any set of actions or process that invoked to compromise the integrity, confidentially, and availability of a resource and services " Stephen Smaha[2] classified the intrusions by the following types:

Attempted breach-ins by un-authorized users which can be detected by typical behavior profiles or predefined alert patterns of security.

Masquerade attacks which occur when intruders try to convince the system that they are authorized to access. It also can be detected by typical behavior profiles or predefined violations of security patterns.

Penetration of the security control system which happens when an intruder attempts to modify system characteristics. It can be detected by using privileged logins.

Leakage, that causes moving information out of the system. It can be detected by atypical usage of I/O resources.

Denial of service that makes resources and services become unavailable and accessible tothe admin and legitimate users. It can be detected by a typical usage of the resources.

Malicious use, such as deleting files and exhausting resources can also be detected by atypical behavior profiles, violations of security constraints, or usage of special privileges.
Intrusion detection systems are available in several types. Some have small, and one set of appliances that fit perfectly into your server while other modules, like IDSM[3], that are implemented directly into an active network's components. IDS are simple software applications that can run on servers and workstations. Their main purpose is to monitor sessions on cloud systems and networks and is will notify to security administrators of event that sensor was determined as a worthy of alert, When the network traffic or flood matches the known exploit signature, they trigger an alert and detects the intrusion. These IDS were known as the Signature-based IDS. Other IDS which collect a baseline of "default
"Network operations over time. They will continue to monitor a network for every situation which doesn't match what they have already determined as default. And, theytrigger thealert. These type of IDS are called anomaly-based IDS. Some IDS can perform automated actions beyond simply sending alerts, such as resetting malicious connections by using a technique called TCP Reset, blocking offending source addresses, or shunning the IP address.Some of the more advanced IDS sensors can even reconfigure ACLs on routers and firewalls dynamically.

II. LITERATURE REVIEW

All cloud services have their own service providers, service providers are ISP companies that gives internet support to cloud computing. Cloud computing is build up by three different layered. Since cloud computing has numerous technologies like virtualizations, databases, transactions, networks, load equalization, operative systems, resource planning, memory management and concurrency management, there square measure plenteous of security considerations in cloud computing [4]. These technologies and systems have several security problems that square measure related to cloud computing. As an example, quite few numbers of security considerations were resulted in cloud computing regarding virtualization, and networks should be unbroken secured so as to interconnect the systems within the cloud. In addition, mapping of the corporeal machines and therefore the virtual machines should be carried out during a secure matter. Besides, knowledge security emphases on encoding and additionally the acceptable policies area unit ensured to be enforced for knowledge sharing. In addition, memory management and allocation of resources algorithms should be during a secured condition, and therefore the detections of malware in clouds should be applicable in techniques of information mining. Cloud computing components consist of client, data center and distributed server. Client is divided into three types which are mobile device, thin client and thick client. Thin client is that the most well-liked because it is cheaper, less security problems and low failure and knowledge lost chance. Data center consists of a collection of servers that stores data and software. Distributed server gives options and security flexibility to cloud providers. There are two types of categories in security threats model which external and internal threats. External threats include Dos, DDoS, port scanning, IP spoofing, DNS poisoning, phishing and packet sniffing. Internal attacks involve an attacker as an insider to access user's resources. There are many types of cloud service threats that can lead intrude to client model, and misuse of cloud data, insecure in API interfaces,and the insider payload or maliciousinsider, data theft, session and service hijacking, risk in identity theft. Changes to providing IT services can be secured by high level end-to-end encryption and trust management policies. Proper validation/verification and stronger authentication can be implemented to handle misuse of cloud computing. Proper security model and access control mechanism can be implemented to settle insecure API interfaces. Malicious insider, management transparency are should be avoided to avoid the risk. Patching in SLA will help in shared technology security issues on IaaS. Loss of control to data should be mitigated by security of API, data integrity, data backup.
In Cloud security the security architecture only can effectively secure the cloud services from threat only if the correct defensive steps were carried out. Cloud security control as a safety guard on the weakness of the cloud and reduce the loss of the attack. When we survey about the data security, few security requirements need to consider for preventing every attack on cloud computing service. Security requirement such as data availability, data confidentiality, data privacy and data integrity control over data accessing by different parties and policies to reduce the issues in riskof many abuse or misuse of data in cloud computing. Availability is defined to ensure that users can use the infrastructure, software and data anytime at anywhere [5]. Data redundancy is a technique to provide the availability in cloud which can stores a multiple copies or cache of similar data [6]. This increases the speed of searching and reaches the availability of the system. Next, confidentiality and privacy is important [7]. The data of user should not be disclosure to any other unauthorized third party. Only the authorized user can access to the system for retrieving data. In order to enhance the confidentiality, encryption of the data should be implemented.

Homomorphic Cryptography performed on an encrypted text [8]. When storing the cloud data, the data can be stored at any location in the world and it has to follow the privacy and confidentiality laws of the country that the server is located. In order to improve the security, Two-Factor authentication solution should be implemented in order to avoid the breach in privacy. Integrity is not only related to edit or modification of stored data but also the data lost or stolen. It is a key aspect of security in cloud computing system.

III. SECURITY CONCERNS IN COLUD

The security issues is always to be concerned in a cloud computing as nowadays people always storing their important data inside the cloud because of easy to access at anywhere and anytime[9]. Hence, cloud service provider must make sure that user's information is secure and without confronting any issues such as information loss. All servers should be kept safe from any external risks and it should be made assured by service providers, There are nine threats should be concerned in order to prevent the threat issues happened which including data breaches, information loss, accounts stealing, un-certain APIs, Denial of Service (DOS), intruders and malicious insiders, vulnerability of cloud service, unhandled network traffic and shared technologies issue. The foremost reason that caused the data loss is hardware malfunction and the software vulnerability and second is insider attackers.

According to [10], some security issues include confidentiality, integrity, availability, privacy and attacks. Data security remains a big issue as sensitive data may become untrusted after transferring to cloud. Unexpected incidents like controllost on IT services and insider threats or attacks may occur. A few key parts of security problems in SaaS, PaaS and IaaS thought of that square measure in data security, data confidentiality, authentication, authorization and integration then on. Cloud service provides cowl the scope of security below the application level of PaaS. Hackers could attack the cloud infrastructure and perform extensive black box testing. IaaS store applications and sensitive data in cloud environment by using virtual machines. There are many possible security attacks include Denial of Service (DoS) attacks, side channel attacks, authentication attacks, man-inthemiddle cryptographic attacks and network security.

There are seven types of cyber-attacks which include metamorphic attacks, SQL injection attack, service and virtualization attacks, MITM (man-in-the-middle) attacks, meta-data sealing and spoofing attack, phishing attack and backdoor payload attacks and zombie attacks. Zombie attack intrudes and interrupts availability and response of cloud. Better authentication, authorization and IDS/IPS can be used to solve this. Service injection attack will be defended by performing service integrity checking and robust isolation between VMs. Virtualization attacks perform by VM Escape and rootkit in hypervisor. IDS, IPS and firewall will be accustomed handle virtualization. Manin-the-middle attack access the information exchange between two parties. SSL configuration and electronic communication tests are suggested to defend the attack. Spoofing attack typically modifies or changes the service's net Services Description Language (WSDL) file. Customers ought to keep associate degree encrypted sort of information to beat it. Phishing and backdoor attack will be eased by robust authentication. Prevention controls that reduce the vulnerability through strengthen the system against the incident that might happen if the control cannot completely eliminate the vulnerability. One of the methods is having strong authentication to reduce the vulnerability for attacker to have unauthorized access to important sensitive data.

The aim of data confidentiality is to make sure the data is only available to the authorized user especially the sensitive data and disclosed to illegal users. The only owner of the data can fully access the data in cloud computing without the leakage of the data content to other parties or clients. [14] Only the services allowed by data owner can access the data through well-defined access control over outsourced data. This control ensures each service who allowed to access to the outsourced data using different access privileges with regard to different data pieces. The owner must take over the control of the data especially in untrusted cloud computing environment to prevent any possible loss. Data integrity protects the data from any modify, delete, fabricate or illegally encapsulation by other services. This requirement allows the accuracy and completeness of the data and having correct and trustworthy of the data stored in the cloud system. If there have any incident happen to data either deleted or corrupt, data owner able to detect it and get back the lost data. Many security threats like vulnerability in virtualization, cross channel attack, misuse of cloud services and the others threat can be prevented by limit the stored data in cloud systems.

IV. INTRUSION DETECTION SYSTEM

Intrusion Detection System (IDS) which is based on the type of data that is used for detection mechanism in cloud. Host based intrusion detection System (HIDS) and network based intrusion detection System (NIDS) are two major types in this category of intrusion detection System.

HIDS that is rely on the information available from various sources like host systems, that includes the contents of operating systems, system and application files. NIDS analyzes the packets that travel across the network by capturing from network communications.

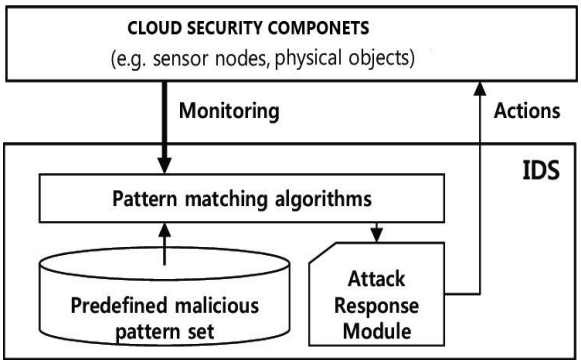

Figure 1: IDS Module

Intrusion detection systems are based on the mechanism applied to detect the intruders. Misuse Signature-Based Detection and

Anomaly Statistical-Based Detection these are two types are fall in this classification. The misuse detection mechanism identifies the legitimate users by comparing the available request data with well-known patterns of attacks.

The limitation of this mechanism is that it can identify only the signatures attacks i.e., known vulnerabilities. Anomaly/Statistical Detection: In anomaly-based detection system, an observation is made to identify an unusual activity of a network request.

V. INTRUSION DETECTION TECHNIQUESIN CLOUD

Cloud computing provides various services like application and storage to its clients on remote servers. This makes the client of the cloud to free from maintenance. A hypervisor server in cloud data center will host the client services on physical machines and for the clients it visualizes the resources. Flooding attacks like ICMP flooding, ARP flooding, Economical Denial of Sustainability attack (EDoS), Root attack, Scanning port Attack (very common attack), Backdoor attack, attacking Virtual Machines and Hypervisors etc., are some of the attacks on Cloud systems.

Deploying Cloud Based Intrusion Detection System (CIDS) in hypervisor machine would allow the admin to monitor the virtual machines on that hypervisor. But with the rapid flooding of high data as in cloud service, there will be lacking issues in performance like overloading of VM hosts IDS and data packets. Also if the host system is compromised by an offender attack. In such case, a network based IDS would be more suitable and reliable for deployment in cloud computing infrastructure. Various techniques as shown below is used to detect attacks in cloud systems:

5.1. Machine Learning Algorithms for CIDS

In this part, a detailed explanation of several machine learning algorithms which can be applied on CIDS

- A request packet in Network is considered as a new request and the related data of the request packet is captured.
- The captured packet from Network is transformed same as the data samples in the available sample patterns which is known as a knowledge base.
- Now the transformed data that supply's an input for CIDS.
- The algorithm’s is to find whether the newly arrived packet is a legitimate request or not.
- CIDS perform many pattern recognition algorithm to check the arrived packet.
- If CIDS mapped the request to a standard (legitimate) pattern then the system can permits the request into the cloud surroundings and map it as a legitimate one.
- Otherwise the defense mechanisms were considered the packet as illegal request and the packet will be discarded or declined.

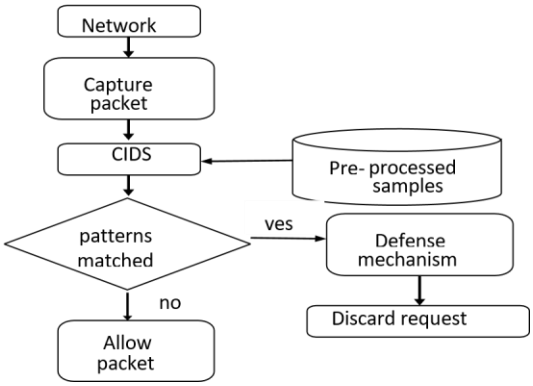

Figure 2: Workflow of CID

5.2. Classification algorithms

Classifications algorithm are supervised learning algorithms that is based on the class label in the data set. In this part of learning technique the available samples were categorized as training set and test set. The trained and predefined samples are used to build the machine and now the test is applied on that machine to find the accuracy of the machine. If the required accuracy is met and the trained machine is ready to find unknown (new) requests. Decision tree primarily based strategies, Rule primarily based strategies, and Memory primarily based reasoning, neural networks, with the assistance of matrix
Accuracy.

5.3. Clustering algorithms

This is an unsupervised algorithm. This type of algorithm is applied when lack of prior knowledge in class labels. The unlabeled data sample were grouped in clustering algorithm by maximized similarities in inter clusters and minimized similarities in intra clusters. These groups are known as clusters. When unknown (new) request is marked to a specific cluster based on its nearnestness to that cluster. The nearestness can be measured using the distances, grids. Root mean square error is the one of the measures in the clustering accuracy. This algorithm tries to minimize the mean square error rate to increase the performance of clustering algorithms.

5.4. Signature Based Intrusion Detection

This type of IDS uses the database rules of the signatures in different attacks found in prior scenarios. The signature is also known as predetermined attack patterns. These signatures were used to compare the network patterns which is incoming, only if the incoming network pattern matches the signature, and the intrusion is detected. This type of detection policies has an advantage, by knowing the network behavior the signatures are easy to Create and understand. In alternative words, we tend to might use a signature that appears for a specific strings inside an exploit payload to notice the attacks that try to take advantage in specific bufferoverflow of vulnerability. It has very high accuracy in detection of per-determined attacks and a minimum number of false positive results. The new signatures can be added directly into the database without modifying the existing ones. One of the big drawback in this Signature based IDS is, it can't able to detect the intrusion of undefined attacks patterns or new breach; even a small variation in the signature pattern can fool the intrusion detection.

5.5. Anomaly Based Intrusion Detection

Anomaly based IDS mostly uses behavior based approach. It identifies the event that seems to be malicious as compared to the standard system behavior. It checks the deviation between the standard behavior and current user's behavior. It collects the information of legitimate user's action or behavior over a quantity of some time. This knowledge is utilized to educate the system. Then a mathematics take a glance at is performed to examine whether or not or not this behavior belongs to legitimate user's behavior. Anomaly based totally IDS can observe unknown or zero dayattacks [13] despite the very fact that system is not updated. As associate degree example, suppose that a portable computer becomes infected with a replacement variety of malware. The malware might perform such

variety of behavior like inflicting large numbers of e-mails and consumption of the computer's method resources that will be considerably and completely different from the standard system user's behavior.

VI. RESULTS AND DISCUSSIONS

Cloud computing permits user to decide on what info they need access to inside the cloud. It provides cloud storage for user to store info and use the pc resources. This successively helps entrepreneurs and firms to chop price in getting hardware or different devices. Cloud computing provides flexibility for the asking over the network. Its location and hardware independence and resources square measure occupied by several users at a time. It more provides dependability, security and maintenance to users. A way to select cloud providers? SaaS provides convenience for users to accumulate identical software system on all of your devices promptly. There are many solutions and practices are mentioned so as to increase the security in cloud computing. Firstly, cloud service supplier ought to take a glance at the vulnerability of their cloud service often and should incessantly sustain and update the cloud to limit the gettable get to purpose and should be diminish the hazard which will provide the chance for hacker to attack your service. Secondly, sure cloud service supplier ought to be continuously chosen by user like Google, Microsoft and IBM. User ought to suppose properly before chosen the cloud as distinctive service supplier have numerous approaches on manage info} information within the cloud. Besides that, all of the knowledge store at intervals the cloud ought to be encrypted well so as to increase the safety of the information. Nobody will get to the knowledge on cloud while not permission, service supplier should be certify that user access is that the one World Health Organization storing the information. Apart from that, user ought to perceive clearly concerning the safety condition of knowledge on cloud, user is accountable to contact the service supplier before mistreatment it. Cloud service supplier should backup the user's knowledge so as to create that if knowledge loss accidently occur, they will directly recovery the information of the users. Users access to their knowledge on cloud not solely attest by username and positive identification however additionally digital knowledge. Single Sign-on allows user to access multiple applications and services through one login and sturdy authentication. Security defense may be put in that embrace virtual personal networks (VPNs), virtual native space network (VLAN) segmentation, authentication, Intrusion hindrance Systems (IPS) and intrusion detection systems (IDS). Cloud accessibility may be done by active/active bunch, dynamic server load balanced and ISP load equalization at intervals the network infrastructure. Knowledge loss hindrance (DLP) tools may be wont to increase knowledge privacy and CSP (cloud service provider) may be used for knowledge integrity. Virtual Machine Protection functions by uninflected and inspecting different network segments. Another answer for security problems may be a bedded framework of cloud security is planned to assure that the protection in cloud computing may be created higher. The primary layer is stacked at rock bottom that is that the secure of virtual machine layer. The second layer is the cloud storage layer, to construct a vast of computer storage, this layer provides an infrastructure that may mix resources from multiple of cloud services. The fourth layer, cloud knowledge layer, handles the issues for example key lumberjack XEN[4] to assist mix along software system and hardware solutions in virtual machines (VM). The potency of cloud computing may be live through security and performance in a very security system. Security is a component to guard the system from threats whereas performance indicates the speed of process the info to and fro from totally different nodes. Security of the cloud computing can have an effect on the amount of performance as a result of threats can have an effect on the practicality of bound a part of the cloud system and low practicality can have low performance. Security is one in all the system potency issue and potency is that the main thought in performance. Thus, each performance and security depend upon one another in the development of the system. In SLA, the service supplier ought to build security offered to user however user are a security breach if he failed to follow the protection policy. During this case, user ends up in low security of the system that may directly have an effect on the performance of the system. In different hands, security have an effect ons the performance of the cloud system whereas performance have an effect on by the user and repair supplier and therefore the part of the services affects the protection. Many authors like[11] Khamis A. Zidan, Abdullatif Ali Hussain were researched on implementation of dynamic key structure (DKG-CS) which is to generated dynamic session keys in cryptographic platform which may reduce the attackers to sniff the session but in this case many attackers using web session sniff with ACK and SYN flag redirection. And another author [12]Sunghyuck Hong who researched in secure protocol for IOT , by using nodes which the Nodes A, B, C Communication are nodes. Node A's identification which is assigned before deployment in the field now Node A's forward message functionto node A's neighbor nodes , Node A's secret key , IV is an initial vector for helping decryption which is not encrypted and at last sink node Decrypt

the encrypted message. If we implemented this type of node encryption in cloud architecture this encryptions give improved security in client to server connection sessions, while using secure protocol.

6.1 Responsibilities in Cloud Security

Cloud Service Provider

Responsibilities of a cloud ISP include meetingthe following security controls:-

- Web Application Firewall (WAF).
- Real Traffic Grabber (RTG)
- Firewall
- Data Loss Prevention (DLP)
- Intrusion Prevention Systems
- Secure Web Gateway (SWG)
- Application Security (App Sec)
- Virtual Private Network (VPN)
- Load Balancer
- CoS/QoS •Trusted Platform Module
- Netflow and others.

Cloud Service Consumer

Responsibilities of a cloud service consumer include to meet the following security controls:-

- Public Key Infrastructure (PKI).
- Security Development Life Cycle (SDLC).
- Web Application Firewall (WAF).
- Firewall •Encryption.
- Intrusion Prevention Systems •Secure Web Gateway
- Application Security.

Security Attributes	Requirements
Integrity	Workload State Integrity
	Guest OS Integrity
Availability	Zombie Protection
	Denial of Service Attacks
	Malicious Resource Exhaustion
	Platform Attacks
Confidentiality	Backdoor Protection

Table 1: Security Requirements

VII. CONCLUSIONS

Cloud computing is changing into in style during this technology world. People are probably to store their information on the cloud as a result of it's convenient for them to access their information anyplace and anytime over the web. However, security problems are getting the challenges for service supplier. so as to possess a resilient and joint understanding between the cloud service supplier and therefore the client, each of those users ought to certify that the cloud they use is secure enough from any outside threats and no alternative parties will be access while not permission. It's necessary for service supplier to seek out a lot of defense approach to scale back the safety problems arise.

Cloud security contains a giant gap between its observe and analysis that is that the assumptions within the analysis that overlook some terribly crucial variations between virtual machine security and therefore the actual cloud security. Analysis ought to be the bridge of those gaps. One layer in the framework would be possibly facilitate in beginning with an answer to watch the management of the cloud software system and another layer would possibly facilitate in solving the secluded process for a specific client's application. So as to deliver the integrated security,

the mixing and combination with alternative security controls at totally different layers ought to be supported. Cloud computing security ought to be ready to amendment the atmosphere by following the strain of stakeholders. Multi occupancy protection ought to be enforced that solely permit the user to look at his own security configurations.
We can also use Proxy chaining method which automatically changes the proxy each time when increase in incoming connections (floods) so the attacker will have response while sending attacks and the attack will be suspended because of proxy changing, so this will prevent the hacker or attacker while sending floods like ARP Flooding and ICMP Flooding.
Cloud computing may be a new innovation generally processed in further years. Currently there are several security risks and limits expose in utilizing these technologies. during this paper, we've bestowed the projected algorithmic rule has been designed and enforced for generating dynamic keys in cloud computing supported varied techniques. These techniques are improved the protection of the cloud thanks to, the keys generators have the flexibility to get random keys with totally different lengths. Additionally, to, the employment of logic circuits and AI techniques will increase complexions.

VIII. REFERENCES

[1] Richard Heady, George F Luger, Arthur Maccabe, and Mark Servilla. The architecture of a network level intrusion detection system. University of New Mexico.
[2] Stephen E Smaha. Haystack: An intrusion detection system. In Aerospace Computer Security Applications Conference. IEEE.
[3] C.TateBaumrucker, James D. Burton, Scott Dentler , Michael Sweeney “Cisco Secure Intrusion Detection System” , SYNGRESS.
[4] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security Issues for Cloud Computing." International Journal of Information Security and Privacy 4, no. 2 (2010): 36-48.
[5] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and MuttukrishnanRajarajan. "A survey on security issues and solutions at different layers of Cloud computing." The journal of supercomputing 63, no. 2 (2013): 561-592.
[6] Singh, Saurabh, Young-SikJeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." Journal of Network and Computer Applications 75 (2016): 200-222.
[7] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem."arXiv preprint arXiv:1609.01107 (2016).
[8] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3, no. 4 (2013
[9] An, Y. Z., Z. F. Zaaba, and N. F. Samsudin. "Reviews on security issues and challenges in cloud computing." In IOP Conference Series: Materials Science and Engineering, vol. 160, no. 1, p. 012106. IOP Publishing, 2016.
[10] Basishtha, S., Boruah, S. “Cloud computing and its security aspects.” International Journal of Research in Engineering and Technology. (2013): vol 2(2), 62-67.
[11] Khamis A. Zidan, Abdullatif Ali Hussain “Improved Cloud Computing Security” Conference Paper · November 2018.
[12] Sungghyuck Hong “Secure and Light IOT Protocol for aniti-hacking”20 March 2017 J ComputVirol Hack Tech DOI 10.1007/s11416-017-0295-5
[13] Dotan Cohen, What is a Zero-Day Exploit? http://what.com/what_is/zero_day_exploit.html,
[14] Mudzingwa, D.; Agrawal, R, A study of methodologies used in intrusion detection and prevention systems (IDPS), Proceedings of IEEE Southeastcon, pp. 1-6, 2012.