**Chapter 1**

**INTRODUCTION**

**1.1 Background**

Revolutionary advances in hardware, networking, middleware, and virtual machine technologies have led to an emergence of new, globally distributed computing platforms, namely cloud computing, that provide computation facilities and storage as services accessible from anywhere via the Internet without significant investments in new infrastructure, training, or software licensing. Infograph reports that 63% of financial services, 62% of manufacturing, 59% of healthcare, and 51% of transportation industries are using cloud computing services (Meijer, 2012).

As a result, more than 50% of global thousand companies are projected to store sensitive detain public clouds by 2016 (Smith et al., 2011). However, a significant barrier to the adoption of cloud services is customer fear of data integrity and privacy loss in the cloud (Pearson et al., 2009). A survey by Fujitsu Research Institute reveals that 88% of prospective customers are worried about who has access to their data in the cloud and demand more trustworthiness (Fujitsu, 2010). Additionally, there are mission-critical clouds: for example, the NSA is using Map Reduce (Dean and Ghemawat, 2008) clouds for intelligence data mining (Iannotta, 2011), and the NIH is using AWS cloud (Amazon, 2013) for health data management (Cravedi and Randall, 2012). Therefore, cloud computing security has established its paramount importance. There are numerous security issues involved in clouds, some of which include:

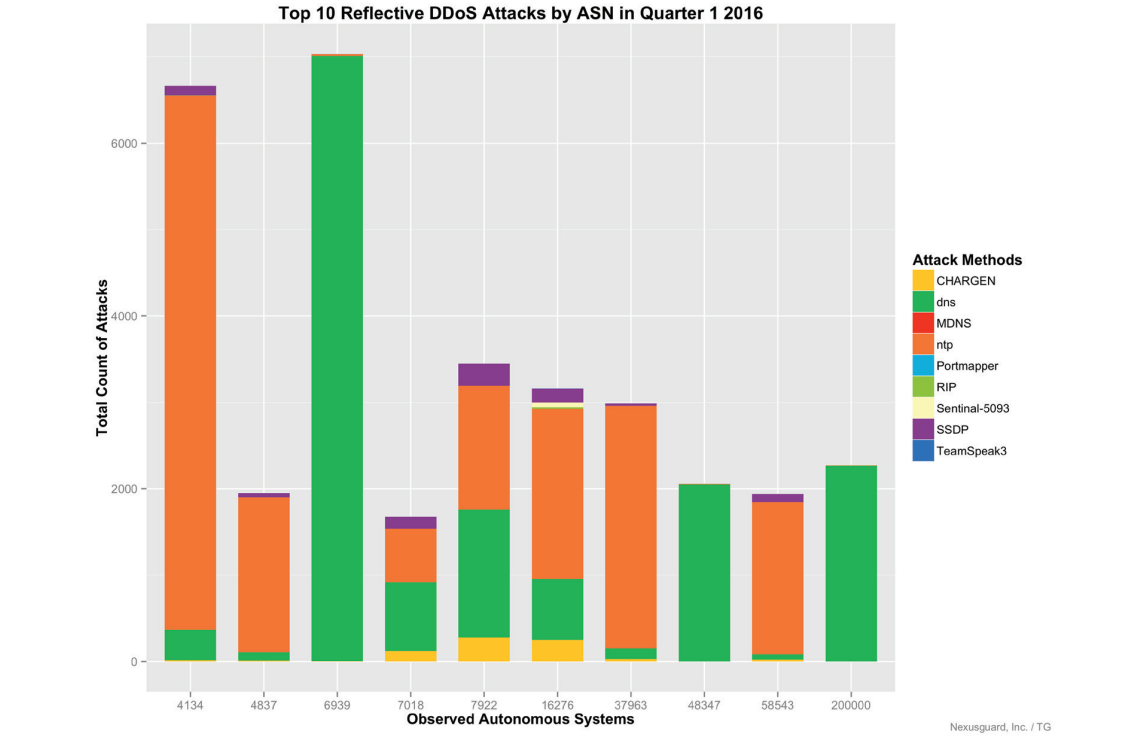
1. Privacy Preservation: preserving privacy of data and its own
2. Computation Integrity: ensuring computations are correct,
3. Secure Storage: storing data securely (e.g., via encryption),

As cloud computing services are becoming more practical and popular for the sake of its convenience and being more economical, its’ security vulnerability has been the continuous threat for both cloud service providers and clients. The more the financial benefits of these services became so attractive and the need for uninterrupted services grows, the distributed denial of services (DDoS) attacks that degrade and down its ‘service availability has been the major security concern. While researchers try to address this security threat and come up with lasting solutions for early detection of DDoS attacks, the degree of these attacks is getting higher and very sophisticated. The changing and aggressive nature of the attacks make it very severe threat and difficult to easily find remedy.

DDoS targeted web sites like Yahoo, Fifa, Amazon, Dell, E-TRADE, eBay, and CNN. The initial cost of the DDoS attack was estimated to be US$1.2 Billion, however, during an official trial that figure was downgraded to US$7.5 million by prosecutors. However, It is very hard to differentiate the real cost from actual cost due to the fact of potential revenue being lost or estimated to be lost while the victim site is under attack. In the other hand, the cost to launching an attack can be as low as a two digits figure, such a low cost was offered by a hacker who offered a six hours outage for only US$60 and the price can vary depending on the target victim (Golubev 2005). Some attacks can cost more to launch, for example it cost a US$100 to rent a botnet for one. Therefore, the reactive approach of cloud users into the following factors described by the large and increasing number of cloud connected computers.

* The ability to control large numbers of vulnerable cloud connected computers to launch wide scale attacks.
* The ability to control large numbers of vulnerable connected cloud DDoS based to launch wide scale attacks.
* New fully automated and complex cloud attacking technologies have been developed and implemented by attackers.
* With the complexity of the attacks the required time to detect and react is also increasing.
* High dependency on the Internet by users and online business mean that such attacks can be highly damaging.

It’s important to know how DDoS attack speared widely with it several attacks as shown in Figure 1.1.



**Figure 1.1:** Top 10 Reflective DDoS(Akamai, 2016)

For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism(Pradhan, Nayak, & Pradhan, 2016). IDSs are host-based, network-based and distributed IDSs. Host based IDS (HIDS) monitors specific host machines, network-based IDS (NIDS) identifies intrusions on key network points and distributed IDS (DIDS) operates both on host as well as network(Sanyal, Das, & Sarkar, 2015). IDSs produce alerts for the administrators which are based on true positives or true alarms when actually intrusion takes place and false positive or false alarms in case of a wrong detection by the system.

IDSs can detect intrusion patterns by critically inspecting the network packets, applying signatures (pre-defined rules) and generating alarms for system administrators. IDS uses two method of detection i.e. anomaly detection, that works on user behavior patterns and suspicious behavior(Bhuyan, Bhattacharyya, & Kalita, 2014). Other method is misuse detection that can detect through renowned attack patterns and matching a set of defined rules or attack against system vulnerabilities through port scanning.

Since Cloud infrastructure has enormous network traffic, the traditionalist are not efficient enough to handle such a large dataflow(Dinh, Lee, Niyato, & Wang, 2013). Most known IDSs are single threaded and due to rich dataset flow, there is a need of multi-threaded IDS in Cloud computing environment. In a traditional network, IDS monitors, detects and alert the administrative user for network traffic by deploying IDS on key network chokepoints on user site. But in Cloud network IDS has to be placed at Cloud server site and entirely administered and managed by the service provider(C. Modi et al., 2013).

In this case, if an attacker manages to penetrate and damage or steal user “data, the cloud user will not be notified directly. The intrusion data would only be communicated through the service provider and user has to rely on him. The cloud service provider may not like to inform the user about the loss and can hide the information for the sake of his image and repute. In such a case, a neutral third party monitoring service can ensure adequate monitoring and alerting for cloud user. In this report, we have proposed an efficient multi-threaded cloud IDS, administered and monitored by a third party ID monitoring service, who can provide alert reports to cloud user and expert advice for cloud service provider..

Despite the fact that intrusion detection systems are commercially developed and used for more than a decade, there still exist many issues around IDS (Iyengar & Ganapathy, 2015). Some of the shortcomings of the current IDS which handicap its effectiveness are discussed below:

- Only the known attacks are detected in signature based techniques which simply means no protection is offered against novel attacks or new variants of existing intrusions. A small variation in the attack pattern can invalidate a signature. By the time the new signatures/patches come up the intrusions might have done the intended damages.

- How well a signature captures the attacks in its string is again a matter of concern. There are quite a few such poorly written signature codes. So the actual attack pattern may stretch across multiple packets, easily evading the detection system.

* 1. **Problem Statement**
     1. **GENERAL PROBLEM STATEMENT**

DDoS are known to exhaust the victim’s resources like bandwidth, operating system resources and computing power(Somani, Gaur, Sanghi, & Conti, 2016). The DDoS attacks in cloud computing are very sophisticated and not easy to detect. Therefore, there are many issues and challenges regarding the detection, filtering, training, identification and implementation of defense and mitigation mechanisms in the environment of Cloud computing. Some of the issues and challenges are dis­cussed below:

1. **Leak of dataset performance metrics**

Selection and calculation of proper performance metrics is always a challenging task. It is important to make sure that suitability of a particular performance metric with dataset being used and environment in which they are executed. The conditions, in which the performance is evaluated, matters a lot, so that the results of the experiments can be used for comparing the results with other similar mecha­nisms for identifying better solution(C. N. Modi & Acha, 2016).

1. **Quality of datasets**

Creating the dataset with unbiased instances is a difficult and challenging task. Preparing normal traffic with some varia­tions in the information of the packets is a non-trivial pro­cess. Selection of dataset is a crucial task since it depends on correctness of the defense mechanism and other perfor­mance metrics. There are few less datasets available which are free and have enough information on attack traffic(Zuech, Khoshgoftaar, Seliya, Najafabadi, & Kemp, 2015).

1. **Location to place the defense mechanism**

There has always been a trade-off between safety of the system and correctness for finding the attack possibility based on the location of defense mechanism deployment. Nearer it is to the system, lesser is the safety and more is the correctness. But defense mechanism is deployed near the source of the traffic and farther to the system, it loses correctness, i.e., it may give false alarms more than the usual. But if the defense is earlier, better is the safety. Therefore, it is a challenging task to find out the location of the defense mechanism to be more investigation for the deployment(Zargar, Joshi, & Tipper, 2013).

1. **Dynamism of the defense system**

There are always limitations regarding runtime efficiency of the defense system. While detecting and filtering the runtime of the attack packets, system always should be able to capture and filter all the attack packets successfully without losing anything(Zargar et al., 2013). For most of the DDoS defense mechanism a normal behavior is calculated to compare it with the nature of incoming packets and this calculation must be done on line. Therefore, it is always challenging task to create such a system, which could process the packets and find out normal behavior in a very short time and requires minimum pro­cessing power. Since all this calculation has to be done at run-time, these can be repeated every time a packet enters. Therefore, it is important to keep it as efficient as possible.

1. **Environment of defense mechanism**

The environment, where the systems are working and where the defense mechanisms are deployed, may have critical effect on the result of defense mechanisms. It is challenging for the researchers to find out solution which works on every type of environment(Iyengar & Ganapathy, 2015). Ideally, defense mechanism must not depend on the environment. Also, the type of traffic plays a major role in the detection of the attack traffic. If traffic pattern consists of bursty traffic, then sometimes defense mechanism may give false alarms for that traffic(Cepheli, Büyükçorak, & Karabulut Kurt, 2016). Therefore, it is important for researchers to choose defense parameters that can deal with such excep­tional behaviour.

1. **Drawback of adaptability to new attacks**

DDoS attacks can be performed with wide range of dif­ferent types of attacks and every day attackers are finding new vulnerabilities in the system to perform with DDoS(Sieklik, Macfarlane, & Buchanan, 2016). It is itself challenging to construct a system that can deal with all these existing attacks. Therefore, it is difficult to design a system that can adapt with new type of attacks and give satisfactory solution to defend against them.

1. **RATE OF FALSE ALARMS**

The rate of false alarm must not be large in a defense mechanism. But, it cannot become zero. It is very chal­lenging for researchers to create a defense system, which detects the packets that are for attacks(Aggarwal & Dahiya, 2016).

1. **COMPLEXITY OF PRE-PROCESSING**

Pre-processing of the dataset or packets that are reaching to the system needs to be pre-processed. Sometimes infor­mation embedded in the packets may not be worth ana­lysing. Therefore, the traffic must be pre-processed to get relevant information from the packets. This may need powerful processors and sufficient memory to store inter­mediate results. Researchers have to keep the complexity of this processing lower to make the defense system faster(Hoffmann, Daily, Holland, & El Defrawy, 2016)

1. **SELECTION OF FEATURES AND CLASSIFIERS**

The most important task that has to be achieved by researchers is to select features or parameters between the system to be defended and connection to other party. By using these features, defense system must be able to identify the class to which that packet belongs to. The selection of this feature set is a very critical and chal­lenging task. Moreover, selection of fair classifiers from a group of classifiers is a challenging job(Aghdam & Kabiri, 2016).

**1.2.2 SPECIFIC PROBLEM STATEMENT**

One of the most common problems with an IDPS is the detection of false positives or false negatives, this occurs when the system blocks a activity on the network because it is out of the normal and so it assumes it is malicious, causing denial of service to a valid user, trying to do a valid procedure; or in the case of a false negative, allowing a malicious activity(Patel, Taghavi, Bakhtiyari, & JúNior, 2013).

Disadvantages of this prevention mechanism would be similar to that of the hardware version, false positives, but this would be to a greater degree in the sense that the user may not be computer savvy and if a procedure they are trying to perform comes up as a malicious activity in the IPS and they are cut off, it becomes time consuming for the IT department to have to check on every computer that has a false positive scenario. Nevertheless, there are several classical security methodologies so far that focus on trying to prevent these intrusions. However, it is impossible, or even infeasible, to guarantee perfect prevention.

Not all types of attacks are known, and new ones appear constantly. As a result, attackers can always find security holes to exploiting order to gain access in the sensor network. These intrusions will go unnoticed and they will likely lead to failures in the normal operation of the network, as Figure 1.2(a) suggests. The last resort is intrusion detection, which can act as a second line of defense: it can detect third party break-in attempts, even if this particular attack has not been experienced before. If the intruder is detected soon enough, one can take appropriate measures before any damage is done or any data is compromised.



**Figure 1.2:** Intrusion sequence. (a) Attackers may exploit a vulnerability and intrude into the network, causing a failure. (b) Intrusion detection functions as a second line of defense.

The main problem with IDPS has been that they have produced a tremendous number of alerts one IDS user reported having 1.8 million alerts monthly(El-Taj, 2015). This issue has been addressed, but it is very difficult to completely eliminate it. There will almost always be false positives; however it should be one of the main goals of the network administrators and the manufacturers of IPSs to minimize this as much as they can. False positives are typically generated by systems that rely on a single detection method, and by ones that cannot be configured at different levels to fit into the operational environment(Mudzingwa & Agrawal, 2012). If an IPS uses multiple techniques to detect malicious activities and inspect the incoming packets there is lesser chance of having false positives/negatives.

It is very important that DDoS attacks are detected early to remove any unwanted intrusions that could disrupt the end users or organizations resources. Intrusion detection systems are employed to detect these types of attacks. Furthermore, the intrusion detection system and prevention systems employed at the source can detect these attacks very early without any delay. So care should be taken to develop an intrusion detection system that detects these attacks with the least amount of time. However, the specific problem can be narrowed as followed points:

1. The drawback of the current available intrusion detection and prevention systems lies in their weakness of not detecting novel and sophisticated attacks. The present IDPS solutions used worldwide are not efficient in detecting newer attacks. The time these IDPS systems take to detect an anomalous behavior is very slow which indirectly results in the damage or deterioration of services. The downsides of these systems can be balanced by enhancing the overall performance of such systems. The performance of such systems can be enhanced if the algorithms converge faster, resulting in correct detection of anomaly.
2. Leak of few necessary features would result in a wrong IPDS If more number of unnecessary features are selected then the computation time also increases, which leads to a slower detection of intrusion or sometimes wrong detection too. It is very important that the necessary and notable features (optimized) are selected for a correct anomalous detection.
3. Till yet, there is no solution for the copious novel attacks. Because the available IDPS systems for anomaly approach uses two steps to find an intrusion. It employs training phase and a detection and prevention phase. The detection phase of every anomaly approach either uses supervised, semi-supervised or unsupervised methods to perceive anomaly. As the current IDPS solutions are inefficient in perceiving novel attacks, it is leading to a huge loss of resources and services to many.
   1. **Goal and Objectives**

The domain of this research is work is to develop solutions to DDoS attacks using Principal component analysis (PCA) and Linear discriminant analysis (LDA) with a hybrid Ant-Lion optimization for feature selection and Artificial Neural Networks for Classification and configure the hybrid cloud topology simulation through cloud server. Hence, the scope of this work is to design an intrusion detection and prevention model for DDoS –hybrid cloud computing system based on statistics and predict techniques. The training phase is assumed to be offline, and the detection- prevention phase online.

The scope of testing the developed concepts is confined to testing with standard datasets and limited number of real time datasets that will generated and validate with other scholar works. The work also aimed at reducing the number of features and utilizing search agents that produce global solutions. The goal of this research was to develop solutions that could detect the intrusions very quickly in addition to also being less computationally expensive.The work also aimed at reducing number of false alarms by characterizing the target network with appropriate network parameters and analyzing them with mathematical models.

The goals of this study is to illustrate the problems, explain why they exist, and highlight some of the implications of these problems in statically anomaly-based detection, but to highlight the challenges. Also, the challenges, organizational managers, users, program managers, and researchers of anomaly-based detection can more effectively communicate how a given techniques expected to operate in operational environments. But, most importantly this thesis aims to give an overview of DDoS attacks targeting public and private cloud computing attack.

This thesis also provides an in-depth knowledge about the different types of attacks and the solutions developed to counter the same. DDoS has seen a huge growth in size in the recent years with highly sophisticated implementations, novel attacks are immediately not prevented. This leads to a deterioration of the target’s resources. The main aim of this thesis is to find the intrusions faster and prevent it without any damage to the end user or target.

Due to the fact, the statistical hypothesis technique and statistical mean- variances model are also being used. The project is integrated with an open source signature based IDPS called SNORT so that it forms a complete package having both signature and anomaly techniques for effective defense against the Network attacks

* 1. **Research Scope**

The domain of this research is work is to develop solutions to DDoS attacks using PCA and LDA with a hybrid Ant-Lion optimization for feature selection and Artificial Neural Networks for Classification and configure the hybrid cloud topology simulation through cloud server. Hence, the scope of this work is to design an intrusion detection and prevention model for DDoS –hybrid cloud computing system based on statistics and predict techniques. The training phase is assumed to be offline, and the detection- prevention phase online.

The scope of testing the developed concepts is confined to testing with standard datasets and limited number of real time datasets that will generated and validate with other scholar works. The work also aimed at reducing the number of features and utilizing search agents that produce global solutions. The goal of this research was to develop solutions that could detect the intrusions very quickly in addition to also being less computationally expensive.

The work also aimed at reducing number of false alarms by characterizing the target network with appropriate network parameters and analyzing them with mathematical models.

The goals of this study is to illustrate the problems, explain why they exist, and highlight some of the implications of these problems in statically anomaly-based detection, but to highlight the challenges. Also, the challenges, organizational managers, users, program managers, and researchers of anomaly-based detection can more effectively communicate how a given techniques expected to operate in operational environments. But, most importantly this thesis aims to give an overview of DDoS attacks targeting public and private cloud computing attack.

This thesis also provides an indepth knowledge about the different types of attacks and the solutions developed to counter the same. DDoS has seen a huge growth in size in the recent years with highly sophisticated implementations, novel attacks are immediately not prevented. This leads to a deterioration of the target’s resources. The main aim of this thesis is to find the intrusions faster and prevent it without any damage to the end user or target.ue to the fact, the statistical hypothesis technique and statistical mean- variances model are also being used.

* 1. **Methodology**

The proposed model based on hybrid model for cloud with PCA, Linear discriminant analysis (LDA) and ant-lion optimization algorithms with a neural network based classifier that classifies whether the traffic received is normal or a DDoS attack via different dataset like UCLA dataset, Center for Applied Internet Data Analysis (CAIDA) .

In order to achieve the aforementioned objectives, the work was divided into seven distinct phases:

1. Thorough study of the security requirements and threats in hybrid cloud computing. This milestone is to be satisfied by contacting literature review.
2. A comprehensive literature review of the existing anomaly-based intrusion detection mechanisms and the corresponding user authentication approaches. This is done to examine the applicability of deploying anomaly detection methods on mobile devices as well as to assess the solutions proposed by other researcher’s sofa.
3. The design and implementation of a series of malicious case studies
4. An investigation of the applicability of new statistically advanced detection and prevention methods to be used as the core mechanisms for the deployment of IDPs schemes that are capable to run on the mobile device. The aim of these schemes is on the one hand to enable the Preventing the flooding attack that came from DDoS attack.
5. The collection and creation of proper datasets to support the experimental detection / prevention process. That is, the collection of a critical mass of user and/or system records to form a dataset. The dataset will be used to evaluate the activeness and accuracy of solutions - designed in milestone 4 and be implemented in 6 - to detect and prevent intrusions. It is stressed that this milestone is deemed necessary due to the complete lack of ready-to-use security-related datasets for smartphones in the literature.
6. The collection and creation of proper datasets to support the experimental detection process. That is, the collection of a critical mass of user and/or system records to form a dataset.
   1. **rESEARCH contribution**

Cloud computing provides an internet based environment which is capable of storing data in the cloud centers through networks. The data placed in cloud centers should be uploaded to the cloud server from a client’s system.

The vulnerability of internet, the distributive nature of cloud computing, various security issues related to cloud computing service models, and clouds main attributes contribute to its susceptibility of security threats associated with cloud service availability. One of the major sophisticated threats that happen to be very difficult and challenging to counter due to its distributed nature and resulted in cloud service disruption is DDoS attacks.

Even though there are number of intrusion detection / prevention solutions proposed by different research groups, and hybrid cloud currently using different only detection solutions by promising that their product is well secured, there is no such perfect solution that prevents the DDoS attack(Zuech, Khoshgoftaar, & Wald, 2015). The characteristics of DDoS attack, i.e., having different appearance with different scenarios, make it difficult to detect. Many DDoS attacks are carried out by botnets which produce undisruptive failures as they grow at an alarming speed. These harness the vulnerabilities present in user or the cloud systems and sift through the entire network by probing for any vulnerabilities on other systems.

This thesis will develop DDoS detecting and prevention model against different parameters, discussing their advantage and disadvantages, a combination technique for feature selection is implemented to reduce the computation time and thereby reduce the training time required by the classifier. A combination of PCA, LDA and a hybrid algorithm is used to obtain an optimized feature from the dataset. This removes the unnecessary data for further classification.

Ant-Lion optimization technique is used to choose the best (optimized) features from the reducts obtained by PCA and LDA. This process of feature selection becomes less expensive in terms of the computing time. This further speeds up the classification process of intrusion detection and prevention system. The classifier then classifies the incoming traffic either as normal or an attack.In this work, intrusion prevention systems are developed and the implementation is based on filtering methods that are combined with population based optimizers to verify the traffic for any anomaly and filter the same.

**1.7 Structure of the Thesis**

The thesis is organized in the following manner:

* **Chapter 2** discusses related work including approaches, drawbacks and challenges, and ends with a discussion on the history of the accomplished design.
* **Chapter 3** discusses the general requirements and considerations towards design of a practical DDoS detection and prevention system.
* **Chapters 4** and 5 discuss in detail the algorithms used for modelling TCP and UDP traffic with a note on their complexities for both the training phase and the deployment phase; and discusses experiments done on the system towards parameter tuning and performance estimation. The chapter ends with details of an effort to compare the system with existing methods.
* **Chapter 5** concludes on the thesis, and discusses the thesis conclusion for future work.

Aggarwal, P., & Dahiya, D. (2016). Contribution of Four Class Labeled Attributes of Kdd Dataset on Detection and False Alarm Rate for Intrusion Detection System. *Indian Journal of Science and Technology, 9*(5).

Aghdam, M. H., & Kabiri, P. (2016). Feature selection for intrusion detection system using ant colony optimization. *International Journal of Network Security, 18*(3), 420-432.

Akamai. (2016). Q1 2016 State of the Internet Security Report | Akamai.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: methods, systems and tools. *IEEE Communications Surveys & Tutorials, 16*(1), 303-336.

Cepheli, Ö., Büyükçorak, S., & Karabulut Kurt, G. (2016). Hybrid Intrusion Detection System for DDoS Attacks. *Journal of Electrical and Computer Engineering, 2016*.

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13*(18), 1587-1611.

El-Taj, H. R. (2015). Intrusion Detection and Prevention Systems (IDPS) State of Art: IDPS Challenges. *International Journal of Computer Science and Information Security, 13*(9), 28.

Hoffmann, H., Daily, M. J., Holland, G. D., & El Defrawy, K. (2016). System and method for deep packet inspection and intrusion detection: Google Patents.

Iyengar, N., & Ganapathy, G. (2015). Trilateral trust based defense mechanism against DDoS attacks in cloud computing environment. *Cybernetics and Information Technologies, 15*(2), 119-140.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications, 36*(1), 42-57.

Modi, C. N., & Acha, K. (2016). Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. *The Journal of Supercomputing*, 1-43.

Mudzingwa, D., & Agrawal, R. (2012). *A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS).* Paper presented at the Southeastcon, 2012 Proceedings of IEEE.

Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications, 36*(1), 25-41.

Pradhan, M., Nayak, C. K., & Pradhan, S. K. (2016). Intrusion Detection System (IDS) and Their Types. *Network Security Attacks and Countermeasures*, 228.

Sanyal, S., Das, N., & Sarkar, T. (2015). SURVEY ON HOST AND NETWORK BASED INTRUSION DETECTION SYSTEM. *Acta Technica Corviniensis-Bulletin of Engineering, 8*(1), 17.

Sieklik, B., Macfarlane, R., & Buchanan, W. J. (2016). Evaluation of TFTP DDoS amplification attack. *Computers & Security, 57*, 67-92.

Somani, G., Gaur, M. S., Sanghi, D., & Conti, M. (2016). DDoS attacks in Cloud Computing: Collateral Damage to Non-targets. *Computer Networks*.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046-2069.

Zuech, R., Khoshgoftaar, T. M., Seliya, N., Najafabadi, M. M., & Kemp, C. (2015). *A New Intrusion Detection Benchmarking System.* Paper presented at the FLAIRS Conference.

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: A survey. *Journal of Big Data, 2*(1), 1-41.