International Journal of Cloud Applications and Computing
Volume 13 • Issue 1

A Secure Framework to Prevent Three-Tier Cloud Architecture From Malicious Malware Injection Attacks

B. V. Subba Rao, PVP Siddhartha Institute of Technology, India
Vivek Sharma, Sharda University, India
Neeraj Rathore, University of Petroleum and Energy Studies, Dehradun, India*
Devendra Prasad, Amity University, Patna, India
Harishchander Anandaram, Amrita Vishwa Vidyapeetham, India

https://orcid.org/0000-0003-2993-5304
Gaurav Soni, VIT Bhopal University, India

ABSTRACT

The concept of cloud computing makes it possible to have a shared pool of reconfigurable computing resources that can be deployed and released with little involvement from administration work or service providers. Cloud computing makes this possible. The communication among the nodes is possible with the help of internet. All users are able to use the services of cloud. The small-scale industries are really happy to use the cloud services. The attackers are degrading the performance of services, and also the users are not receiving the response. This paper presents the imprint of cloud computing. Flooding attacks or the DoS attack is one attack that reserves the communication resources in network, and the rest of the attacks, like Sybil attack, misguide the users, and also it is not easy to identify the exact identification of the sender. The security schemes are able to remove attacker infection, and on the basis of that, it is possible to design better schemes against attackers in the cloud.

KEYWORDS

Admin, Attacks, Cloud, Data, Routing, Security, Users

1. INTRODUCTION

Cloud The term “cloud computing” refers to the aggregation of data and the availability of computing resources that are made available via the internet. On your personal computer, there is no data that is saved. The provisioning, on demand, of computing resources such as servers, data storage, networking, and databases, amongst other such resources. The ability to provide multiple users with

DOI: 10.4018/IJCAC.317220
*Corresponding Author

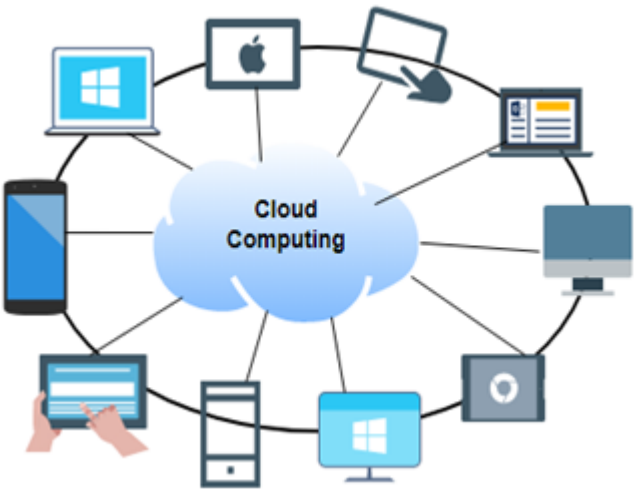
access to data centres is one of the primary goals of cloud computing (P. Mell et. al. 2009, Zhao G et. al. 2009). Users also have the option to view data stored on a remote server. The potential for financial savings is the primary driver behind the adoption of cloud computing by a large number of companies and organizations. Figure 1 shows how many different kinds of devices and applications are able to satisfy their needs with the help of cloud computing. Cloud computing gives you the freedom to access resources whenever you need them and the flexibility to pay for only what you consume. The infrastructure of the cloud has made it easier to manage IT tasks as an outsourced unit without having to hire a lot of personals.

A cutting-edge technology that now allows for the provision of varied computing resources to developers is cloud computing. Through the cloud computing area, resources are offered as Software as a Service, Platform as a Service, and Infrastructure as a Service (P. Mell et. al. 2009).

Cloud computing environments can be broken down into two distinct categories of actors: cloud providers and cloud users (P. Mell et. al. 2009). On the one hand, providers keep massive amounts of computing resources in large data centers and then rent them out to customers on a pay-per-use basis. On the other hand, some users have apps that can handle a variety of loads, and they rent resources from providers in order to run those apps. The relationship that exists between providers of a service and the people who make use of that service typically takes the form shown in Figure 1.1. The process begins with a user sending a request for a resource to a provider. When the request is received by the provider, the provider searches for resources that can satisfy the request and then allocates those resources to the user who made the request, typically in the form of virtual machines (VMs). The user will then run the programmed on the allocated resources, at which point they will be required to pay for the resources that they have used. After the user is finished making use of the resources, they are handed back over to the person who provided them.

One of the most interesting aspects of the ecosystem that cloud computing exists within is the fact that its participants are typically separate parties with different interests. The majority of service providers have set their sights on maximising their profits while minimizing the amount of capital they put into their operations. To achieve this goal, they might want to maximize the use of their computer resources by, for example, hosting as many virtual machines on a single system as is technically possible (Peshraw Ahmed Abdalla et. al. 2019). To put it another way, providers want to maximize the use of the resources at their disposal. However, running an excessive number of virtual machines on a single physical computer increases the risk of those machines interacting with one

Figure1. Example of Cloud Computing



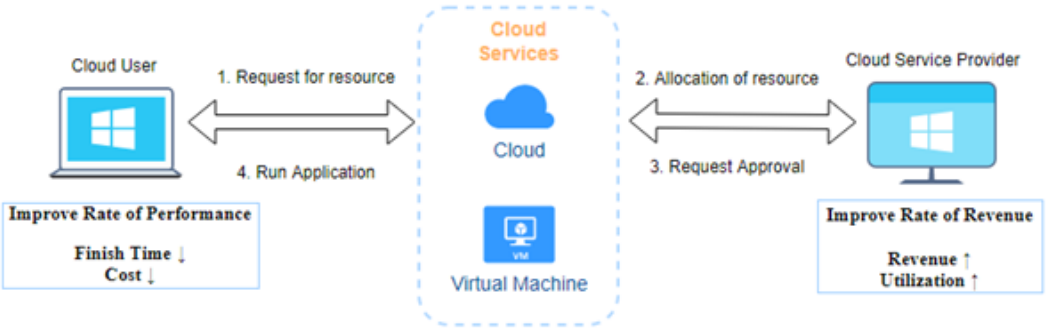
another, which can result in performance that is unreliable and/or frustrating for users. On the other hand, users want their tasks completed for the least amount of money possible, or, to put it another way, they want to maximize the cost performance of their systems. In order to keep the service quality high, providers may delete existing virtual machines (VMs) or refuse requests for resources. However, this could make the environment even more unpredictable. This requires having adequate resources that are tailored to the workload characteristics of the apps that users are running, as well as apps that make effective use of the resources that are available. When they look for resources and schedule applications, they have to remember to account for unforeseen resources as well.

However, due to the fact that these two parties do not wish to share information with one another, it is more difficult to distribute resources in the most effective manner. For instance, providers might not want to disclose the number of devices they have, the types of devices they have, or the manner in which they are connected because such information is critical to the operation of their business. Users will not divulge the specifics of their task to third parties, including service providers, and this includes both source codes and data sets. Because users are not aware of what resources are available to them, they are unable to express their resource requirements in a manner that will result in those resources being provided to them in a manner that is optimal for the applications. In a similar way, service providers don't have the knowledge they need to understand how their customers' apps are used, so they can't give those apps the resources they need in the best way possible.

The exponential growth of mobile devices, the increase in demand for storage brought on by the widespread use of cloud computing, the newly emerging problems faced by data centers, and the proliferation of digital content are all factors that contribute to the daily production of a massive amount of data. There is a need for research not only on the newest computer technology but also on the issues that are associated with it, such as climate change, increased fuel consumption, and rising energy prices. When it comes to the ongoing competition to find ways to process information more quickly, the advent of cloud computing represents a significant advance. The issue of the level of security of a newly introduced computing system immediately becomes one of the primary concerns of academicians and researchers as soon as the system is made available to the public. It is now absolutely necessary for the success of an information processing system to ensure the safety of the information processing that occurs across all information systems. The processing of information is made much quicker and less dependent on location with cloud computing. Because of this, trust is one of the primary concerns among users of cloud computing when it comes to making use of the cloud's resources (Zhao G et. al. 2009).

As a result, cloud security has become absolutely necessary for the effective deployment of cloud services. A built-in security mechanism is preferable to an externally provided security service in terms of convenience and cost. It is possible that the firewall is one of the solutions that can prevent attacks and threats to data security in the cloud. The infrastructure of the cloud is completely virtualized,

Figure 2. Cloud Usage Scenario



and it is capable of supporting a wide variety of hardware architectures. Consequently, ensuring the safety of cloud storage is a pressing concern in the modern era. The papers (S. Yu et. al. 2012) and (J. Francois et. al. 2012) provide a clear picture of the security concerns associated with cloud computing environments and we can use cloud in sensor network with 6G (G. Soni et. al. 2021). The cloud is vulnerable to a wide variety of attacks, including flooding attack, Malware Injection Attacks (MIA), spoofing attacks, Denial of Service (DoS) attacks of varying intensities, and distributed denial of service attacks. The detection of attack packets and the subsequent filtering of those packets security from attacker is the challenging task for cloud users. There are four distinct cloud models available, and you can subscribe to whichever one best suit the requirements of your business. The following is a list of the various types of clouds (D. Soni et. al. 2017):

1. **Private Cloud -** This is where computer services are deployed by a single entity, where computing services can be managed, controlled and run by the same company.
2. **Community Cloud -** The community and organizations are equipped with computational services.
3. **Public Cloud -** Public cloud is typically used for B2C (Business to Consumer) applications, this sort of cloud has a computation resource that is owned, managed, and controlled by a business, academic institution, or the government.
4. **Hybrid Cloud –** For all types of interactions in cloud environment hybrid cloud can be used. This implementation approach is called the Hybrid Cloud since computing services are joined together by various clouds.

1.1 Features of Cloud Computing

It provides a range of appealing features for both companies and customers. Some of the features mentioned below are (P. Mell et. al. 2009, Zhao G et. al. 2009):-

1. **Device and Location Independence -** Users can connect to the cloud network from any location and device,
2. **Pay per-use -** Users need to pay only for the tools they have used out of the pool of software and facilities available and do not need to pay for the entire infrastructure.
3. **Multi-Tenancy -** Provides the sharing of resources, software applications, networks and their costs by large users.
4. **Stability -** The reliability of the infrastructure is enhanced with the use of several redundant servers for databases and data storage, so that data can be recovered quickly in case of failure.
5. **Efficiency and Performance -** The productivity of projects using cloud networks with applications running improves as many users operate on the same database and program concurrently, it will provide better performance.

Cloud Computing Advantages - The cloud computing is really important for accessing information and resources. The some of the advantages (P. Mell et. al. 2009, S. Yu et. al. 2012) are as follows:-

1. **Cost-Effective -** The usage of cloud technology in networking and storage can minimize the total cost of buying and maintaining hardware and technological resources for the organization's mission.
2. **Accessibility -** The usage of cloud computing technology can offer simplicity and mobility for end-users to extract, store and exchange data from anywhere, at any moment, only by providing an Internet connection.

3. **Simple Data and Program Management -** All data is stored on a single server such that it is easier to monitor the data and track who is accessing whatever form of data at that location through the management.
4. **Platform Flexibility -** In cloud computing, the same data and software can be downloaded on multiple platforms such as tablets, tablets, desktop PCs and iPads.
5. **Increased Storage Space -** The capacity of servers to store data is much greater than the storage capacity of the user computer.
6. **Automation of Software Upgrade -** Cloud infrastructure can deliver automated updates to all systems and software programmers operating on its network on a timely basis.

Disadvantages in cloud computing - The some of the drawbacks (P. Mell et. al. 2009, S. Yu et. al. 2012) of Cloud computing are as follows: -

1. **Need for Reliable and Highspeed Internet Access -** The entire definition of cloud infrastructure relies on the provision of a permanent Internet connection.
2. **Protection Issues -** Since more than one company share the same computer space on public cloud networks to store and access their data and applications.
3. **Relocation Issue -** It is very difficult for customers to transfer a massive data and application device to another cloud network. It would exhaust a lot of time and resources.
4. **Issue of Security in Cloud -** Wireless data transmission and storage over the Cloud is an option for user. The multimedia data transmitted over a wireless network can be secured using content-level methods like digital watermarking or streaming level methods like media authentication code (MAC).

Applications of Cloud Computing - Every program on a cloud service has the same functionality and can be run on a cloud service (D. Soni et. al. 2019). The expansion to many fields could offer us a multitude of solutions at no cost.

1. **Sharing File online -** The main benefit of cloud computing is that it makes storing and accessing software from anywhere an issue because it relies on an internet connection.
2. **Editing software or editing videos -** With this app, you can both assemble and alter the videos. we can still see and search for videos in the cloud, so they do not need to be stored on our devices.
3. **File Converters -** A number of different programs exist to alter the file format in the HTML to the given example, among which are available include programs which apply HTML to PDF.
4. **Comparable Antivirus Software -** All of the viruses and malware are located and scanned for by the program, and the problem is then resolved. and installing the program has an extra feature that enables them to improve the OS on the device.
5. **Online marketing and e-commerce app -** Another great feature of Responsive Analytics is the capability to take advantage of new business opportunities and respond to new issues. Time is just money when you are poor; business magnates put profit above all else when they use the cloud.
6. **Business Process -** In the majority of business applications, the cloud provider's cloud is relied upon as a commodity. the organization places all of value that it possesses in the cloud, including the requisite data and valuable knowledge.
7. **Backup and Recovery -** This data will be secured and the great deal of protection will be given when the data is lost, the user will be able to retrieve the data he or she has saved in the cloud.

It is possible for a large amount of information to be stolen or lost at the terminal, as well as for the network to become unstable or even crash as a result of the large amount of information being

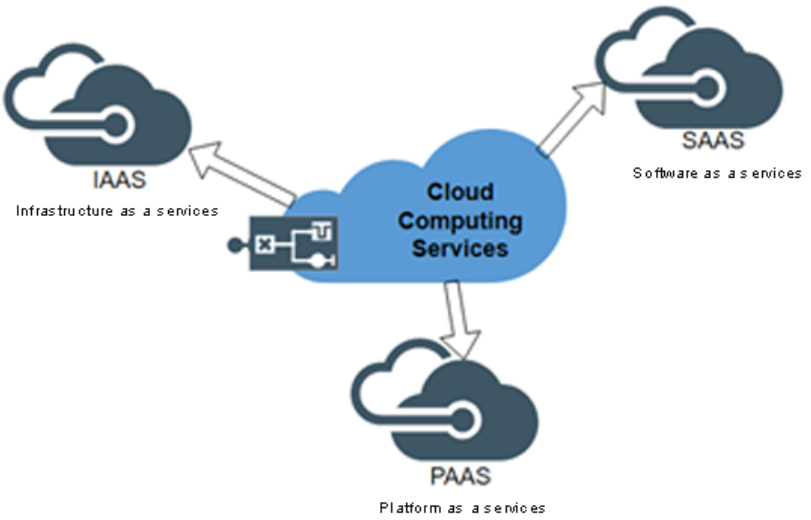
transmitted. The use of new technologies is growing at an ever-increasing rate, and new application domains have surfaced across the board. The wireless communication technology, Internet of Things (IoT), virtualization, artificial intelligence and cloud computing technology are some examples of recent technological advancements. Because of this circumstance, the potential threats to safety will significantly increase. The demand for intelligent terminals as well as the requirements of businesses have significantly increased in recent years, which may result in information being misplaced or exploited in an unethical manner. The number of people looking for intelligent terminals has significantly increased.

1.2 Cloud Service Model

Cloud computing involves gathering a significant quantity of data that has been highly virtualized to produce a sizable pool of resources. Users have the ability to analyze and obtain solutions that are beneficial to their own requirements by making use of the resources that are contained within the resource pool (D. Soni et. al. 2022). This technology is simpler to operate and more productive than its predecessors. There are three primary service models that are utilised by cloud computing. The following is a list of different models of cloud service (Michael Armbrust et. al. 2010): -

1. **Software as a Service**, also known as SaaS, gives users the ability to access and make use of applications owned and operated by a third-party provider while they are hosted in the cloud. Through either a thin client or a thick client interface, the applications can be accessed from a variety of client devices. The user does not have any management or control over the cloud infrastructure that is being used.
2. **Platform as a Service,** it is also known as PaaS, is a model of cloud computing that enables end users to independently deploy software and applications. It is to have authority over the applications that are being deployed rather than to manage or control the underlying cloud infrastructure such as the network, servers, operating systems, or storage.
3. **Infrastructure as a Service,** the ability to provision processing, storage, networks, and other fundamental computing resources is referred to as Infrastructure as a Service, or IaaS for short. This capability is provided to the consumer. Within these settings, the user is able to install and utilize any kind of software, including various kinds of operating systems as well as applications.

Figure 3. Services of Cloud



1.3 Motivation of Research

The consumers of cloud services, also known as clients, can be either thick clients or thin clients, depending on the type of cloud service that they want to use. It is possible that they will be billed on a per-use basis, but this will depend on the services that they receive. It's possible that these resources are a pool of virtual and physical resources that are accessible on demand and from any location via the cloud. In a cloud environment, there is no dependable entity that can be relied on to coordinate the functioning of the network. As a result, centralized networks present a greater number of security challenges compared to distributed networks. Although a great number of protocols have been developed and put into use in order to ensure the safety of data routing and transfer, this is the first time that a DoS attack has been recognized and neutralized in the cloud. Because the wireless medium is what it is, it is possible for malicious nodes or trusted nodes that have been infected by attackers to disrupt the operations of networks by injecting incorrect routing information or forging data packets.

The objective of the attacker is to deplete the resources of the cloud, such as bandwidth, and to consume the resources of a server, or to interrupt the routing operation in order to reduce the performance of the network. The attacker will also discard all of the data packets after the connection has been established. Everyone has access to the wireless channels, whether they are legitimate users of the network or attackers with nefarious intentions. The ability of traditional server-based solutions to provide security is hindered by the absence of a central agency that can be relied upon. The dynamic request gave the impression that any user on the network, whether they were being honest or not, could stop cooperative communication at any time by breaking the rules that are usually associated with communication.

An attacker attempting a DoS will try to disrupt the network by flooding it with unnecessary information and destroying the data that is being exchanged. This will prevent the network from operating normally. The goal of the attacker is not just to hinder the performance of a single sender or receiver; rather, they want to cause significant problems with the performance of the cloud. It is a virtual environment that is efficient in terms of cost and can serve as an alternative to expensive computing infrastructures for a variety of information technology solutions. Due to the fact that it is scalable, it is a flexible option that can either reduce the number of services it provides or increase the number of services it provides, depending on the needs of the end user.

The primary purpose of this investigation is to pinpoint the perpetrators of the flooding attack and devise countermeasures that can put an end to their nefarious activities. Keeping the local connectivity going strong is a very important task. In the network, there are some servers or nodes that are behaving improperly and continuously flooding the hello packet without maintaining the hello interval. It gets in the way of how the network is supposed to work, and it takes people's attention away from the real nodes in the network. Some of the attackers are forwarded, flooded unwanted packets and consumed data packets that affected the secure route establishment to sender and if the sender sends the data packets, then misbehavior is present cloud computing. The reliable security scheme shows the secure hello flooding, dropping and consumption of data in the network. Then our security scheme is:

1. To provide an efficient algorithm for the detection of DoS misbehavior.
2. To provide an efficient routing mechanism to detect DoS misbehavior.
3. To provide an efficient method of healing of flooding of unwanted packets in Cloud.
4. To provide the efficient communication algorithm along with the misbehavior prevention

2. LITERATURE SURVEY

In this section, the previous work that has been done in the field of cloud computing with security is mentioned. The work was completed by a variety of different people, and they were successful in achieving the goal that was decided upon.

Ranjan and colleagues (Iva Ranjan et. al. 2019) developed a strategy to protect against malware injection attacks. It is described here how it can be attacked, as well as what the impact of those attacks will be. If the cloud is under attack, the speed at which users can access it will vary. The research result that was proposed shows how it affects the speed at which one can access the cloud after it has been protected from users who use malware. When a user opens the cloud-based registry, the service provider shows the user's virtual machine as part of an image displayed by the cloud.

They proposed using a cloud-based central authentication system for a number of reasons, according to (Anika Anwar et. al. 2019). Because the computation and data are being handled by a remote server, control boards for computerized vehicles can be made smaller. This allows for a reduction in the overall cost of these types of vehicles. As a result of the majority of the computation being able to be performed on a cloud-based platform, the computational load in vehicles will be significantly reduced. Also, IT procurement takes almost no time, so cloud computing can help developers focus more on their goals and activities.

Using symmetric key encryption and decryption of a data set, the new method known as the Light Weight Data Sharing Scheme (LDSS) that was proposed by (Sunanda Nalajala et. al. 2019) was developed. Our research in this area demonstrates that lightweight devices can perform tasks in a straightforward and uncomplicated manner. This can be applied to algorithms and the inner codes of modules. We need to identify a weakness in the system that is currently in place. The fundamental performance is sluggish, and the limited mobile resources are unable to satisfy the prerequisites.

In this article (B. Thirumaleshwari Devi et. al. 2020), we take a look at some of the most significant attacks that are currently posing a risk to modern-day security. In low-interaction honeypots, it is acceptable for malicious software or attackers to have limited interactions. Honeypots with a low level of user interaction cannot be compromised by users who exploit the mirror vulnerability. In High Interaction Honeypots, the target software or service is one that is known to have security flaws. When compared to honeypots with a low level of interaction, those with a medium level of interaction require attackers to interact with more capability but lower performance than honeypots with a high level of interaction.

In this particular piece of research (Farhaan Noor Hamdani et. al. 2019), the authors propose a detection model that makes use of machine learning algorithms like artificial neural networks. The model is initially educated using some kind of data set in order for it to be able to differentiate between normal data traffic and attack data traffic. In this way, we make it possible for legitimate traffic to get where it needs to go. The model that is being used in this situation is based on characteristics such as accuracy, sensitivity, and precision. Techniques known as feed forward and back propagation are the foundations upon which artificial neural networks are built. In this scenario, the network traffic is constantly analyzed in accordance with the trained artificial neural network (ANN) in order to look for any abnormal patterns of behaviour. However, retrieving large amounts of data in a connection system with engaged routes can be both time-consuming and expensive. In light of this fact, the solution that has been suggested is to implement a different threshold for each protocol. If the number of packets in a network is higher than the threshold set by the protocol, the extra packets are collected and stored so they can be looked at later.

In this paper (Meenal Jain et. al. 2021), we begin by selecting the essential attributes using an optimal feature selection algorithm that was given the name Information Gain. Next, we label the unlabeled dataset using a clustering-based technique that was given the name K-Means. The information obtained was put to use when selecting the essential characteristics. These clusters were used as an input in two different classification techniques, namely decision tree and random forest, and positive results were obtained from both of these approaches. Random forest was found to be more accurate than decision tree. The proposed methodology was shown to be effective after it was applied to a real-time benchmark anomaly detection dataset known as ISCX 2012. In order to evaluate the efficacy of the algorithms, matrices of metrics such as accuracy, precision, recall, f1-score, and false positive rate have been applied.

Alan Saied and his colleagues (A. Saied et. al. 2015) have developed and described an Artificial Neural Network (ANN) algorithm in order to enhance the functional capabilities of IDS. Their work was primarily focused on identifying not only known attacks but also zero-day attacks, which was the primary purpose of their paper and the primary focus of their work. They provided a defence mechanism that allowed the genuine packets to pass through but prevented the faulty packets from in any way reaching the victim. When conducting the analysis of the findings of the study, the researchers utilised the criteria of accuracy, sensitivity, specificity, and precision as their guiding lights. They discovered that the ANN method was one of the most effective approaches for identifying anomalies when they compared their findings to those obtained from other methodologies, such as the signature-based solution (Snort), Chi-square, and support vector machine. This was the case when they compared their findings to those obtained from other methodologies.

The Naive Bayes algorithm was utilised by (N. A. Singh et. al. 2016) in order to identify potential attacks. The Information Gain technique was applied in order to select the features. Validation of the proposed structure was accomplished through the utilization of a real-time benchmark anomaly detection CAIDA dataset. They demonstrated that utilising both approaches together led to an increase in accuracy and was successful in detecting the attacks. Clustering is an effective unsupervised method for locating patterns and irregularities in unlabeled data that can be performed by anyone. But the unsupervised techniques that are available now have a high rate of false positives and only look at single data instances to find intrusions.

A study on distributed denial of service (DDoS) attacks, their detection, and various defence strategies against such attacks was carried out by (Bhandari, Nisha H., et al. 2013). DDoS attacks have evolved into a significant danger for users of cloud computing and other cutting-edge technologies in today's world. An attack known as a distributed denial-of-service, or DDoS, poses a significant challenge because it is difficult to identify this type of attack, there is no all-encompassing solution to this problem, and it has the potential to cut an organization's business off from the Internet. The primary objective of an attack is to prevent a victim from gaining access to a specified resource. The authors have conducted a comprehensive analysis of the existing DoS and DDoS detection and defence mechanisms.

Attributes-based DDoS Detection or Traffic Volume-based DDoS Detection was a method that was proposed by S.S. Chopade and colleagues (S.S. Chopade et. al. 2013). The first ones use things like IP protocol-type and packet size, source IP prefix and TTL values, as well as server port number and protocol-type, etc., to figure out what is considered to be anomalous behaviour. The later ones, on the other hand, make use of a multi-level tree that maintains packet rate statistics for subnet prefixes at a variety of aggregate levels. The rate of normal traffic to or from hosts and subnets is typically proportional to one another. As a result, an attack will be identified whenever there is a 526 proportional deviation in the rate of traffic that is observed. One more method that falls under the category of distance estimation techniques can be used to detect DDoS attacks. The authors of this paper used a DDoS detection technique that was based on average distance estimation.

The model and algorithm for detecting the most recent APT attacks were proposed in this paper (Jisang Kim et. al. 2013), which can be found here. To reduce the detection range to an acceptable level, distinguish between the patterns that the organization member normally uses and the abnormal patterns. In order to accomplish this goal, all types of outbound traffic that occurred during a given time period must be investigated, and the organization's acceptance of the traffic that was investigated must be manually judged. In a typical office setting, the proposed model and algorithm were tested to see how well they worked, and they were found to work well overall.

The purpose of this paper (Igor Nai Fovinoa et. al. 2009) was to investigate the effects that traditional forms of malware used in information and communications technologies (ICT) have on supervisory control and data acquisition (SCADA) systems. In addition to this, it provides examples of computer malware that is designed to attack a typical SCADA system and discusses the potentially harmful effects that these examples could have. Malware presents a significant danger to SCADA

systems as well as the industrial facilities that those systems control. The use of a simulation framework that is capable of mimicking the behaviour of malware is the most appropriate strategy for analyzing the effects of malware because it is risky to infect a real SCADA system with malicious software.

FireEye threat (Vrushali D Mendhule et. al. 2015) prevention platforms are typically installed in a position of secondary importance behind traditional network defences such as firewalls, next-generation firewalls, intrusion prevention systems (IPS), and anti-virus (AV) software. Actors using advanced persistent threats targeted a large number of countries around the world in their search for data related to research and development, national security secrets, and a great deal more. In order to detect and prevent malicious activity, the FireEye appliances run the suspected malware in a simulated setting. In most cases, they investigate malicious activities that have been successful in evading existing network defences and being discovered. As a consequence of this, they typically have an exceptionally low rate of false-positive alerts. Nevertheless, the scope of this report is limited to describing only those cyberattacks that occurred in 2013 and were detected by FireEye. In other words, this research data only includes assaults that meet the following two requirements:

1. Customers of FireEye were affected by this attack.
2. These particular FireEye customers have given their consent for FireEye to access their attack metrics.

(G. Soni et. al. 2020), proposed a L-IDS algorithm for WSN-assisted IoT black hole attack. Data is routed and packets are exchanged between sensor nodes connected by wireless links. RPL is IPv6's routing protocol. The proposed IDS confirmed the blackhole attacker's presence and stopped his malicious actions. The work done on packet dropping attacks and infection of attackers was not evaluated.

This paper (ByungHak Song et. al. 2007) proposes an efficient DDoS defence system that makes use of a collaborative scheme among distributed IDRSs that are located in close proximity to the network that is either the source of the attack or the victim of it. Within the framework that has been proposed, the victim IDRS and the source-end IDRS collaborate in order to identify the attack and reduce the number of false alarms to a significant degree. In addition, we propose the duplicate detection window scheme as a method for detecting multiple attack dynamics. This method gradually raises the detection threshold in the early stages, making it easier to spot attacks. The proposed system can find and stop many different kinds of DDoS attacks.

This paper (Bajaj, S. et. al. 2000) discussed about ns which help in finding challenges in operating new protocol and algorithms in internet. NS is multiprotocol network simulator which help networking researcher to find the needs of algorithm and protocol design, address the issue regarding it. It is an essential tool for quickly and affordably examining how these new protocols behave over a variety of topologies, cross-traffic, and interactions that could take place on the Internet. IT offers a number of abstraction levels to enable emulation, where real-world packets can enter the simulator, and simulations to span a wide range of scales.

This paper (D. Soni et. al. 2021) suggests the secure framework communication in cloud environment while sharing data. Key is automatically applied on the basis of sensitivity of data. If data is highly sensitive then combination of 3 keys generated by AES, RSA, RC6 is applied otherwise single key or combination of two keys are used. Classification is done through SAW and FCM algorithm. They also provide alert mechanism to detect and unauthorized access of data in communication.

3. PROPOSED CLOUD SECURITY MALWARE PREVENTION (CSMP) SCHEME

It has been observed that even though there is ongoing research being conducted in this field, the previously proposed solutions do not provide adequate protection in terms of the effectiveness

and efficiency of the routing process. Every solution has its share of flaws and restrictions. In the future, we will try to propose solutions that take into account their potentially high computational or communication overhead. Cloud Security Malware Prevention (CSMP) has the ability to collect and investigate audit data across the entire network. Therefore, based on that definition, we can draw the conclusion that the data stored in the cloud is of a distributed nature and that we cannot trust any of the mobile or stationary devices. This is due to the fact that we are unable to manage every time the topology of the network changes. This presents a very significant obstacle. Therefore, at that particular point, we set up the trust-based route in order to protect the cloud storage from malicious attack. Malware that causes damage can be spread using widely used communication tools, such as worms that are sent through email and instant messages. In this section define the algorithm in step-by-step process.

Algorithm Step for multi attack intrusion Prevention System
CSMP Algorithm
Step 1
Input:
N_i, which stands for the set of mobile nodes// N_0, N_1, N_2, N_3,…..
N_{i-1},
S_x: set of Sender Nodes // S_0, S_1, S_2, S_3,….. S_{x-1}
I_m: a collection of nodes located in between S and R// I_1, I_2, I_2, I_3,….. I_m,
R_x: stands for the set of receiver nodes. // R_0, R_1, R_2, R_3,….. R_{x-1},
$P_n \in N_i$ ¬ set of preventer node
ATr: suspected node//ATr ϵ N is the set of attacker nodes whose infection is being spread.
Output: PDR, data loss and delay
Step 2
S_x¬ execute-route(S_x, R_x, I_x,CSMP)
While (N_i <=Range) **do**
I_m receives of routing packets forward to next I_{m+1}
CSMP will monitor each individual I_m in the range and adjust ATr accordingly.
Call_ CSMP (I_m, packet)
While I_m [1] Rx **do**
Evalauate the PDR of I: (forwards and receives) / Attacker PDR is always decreasing in the network
If I_m and R_x are equal, **then**
forward ACK to the S_x node //Acknowledgement (ACK)
After received ACK S_x sends data packets
Else
R_x not in zone
End if
End do
End do
Step 3 CSMP (N_i, packets) / Packets may contain data or unwanted packets that have been injected by small malicious programmes.
If (I_m update data of S_x node) **then**
Check the latest data updates using I_m
If (update is True && R_x_ID is modified) **then**
$I_m \in$ ATr _ID // Check attacker presence
Capture information (infected_data, ATr,

```
symptoms)
                End if
End if
Step 4
          While (ATr_Behaviour == flooding) do //it does not
appear to be related to actual data,
        if (ATr_infection == high) then
        ATr Captured information are not consistent with normal.
        Capture node number
        Check the status of the heavy flooding.
        Analyze behavior
        Trace time of data update
        Else
        Send data packets to the destination or the next node.
        End if
End do
Step 5
P_n nodes match ¬ (attacker_infection, abnormal-table)
        Analyze the ATr using the abnormal table.
        Send a normal treat message to a recipient
if (flooding=true && Attacker (ATr) profile! = normal-profile)
then
        Attacker (ATr) is an ATr profile node.
        Communication with cloud blocked by P_n .
        Block the all ATr nodes after found attacker symptoms.
CSMP Sends information about the attacking node
Forward symptoms to all N_i that is connected directly.
        A fresh route of communication has been developed.
        Examine the functioning of the newly added link.
        Perform performance calculations on the network by step
4. //
Else
        Nodes are normal or not malicious
End if
```

Malware will also seek to exploit existing vulnerabilities in systems in order to make their entry quiet and easy. The proposed security scheme is based on the flooding because of the protect network from malware injection. The functioning of Malware to slow down the normal traffic and CSMP against providing security to stop their malicious activities. The strength of the work is to not degrade the performance and limitations is to at the beginning is very difficult to identify the malicious actions of attackers.

The block diagram of the Cloud Security Malware Prevention (CSMP) shows attacker infection detection and prevention on cloud mentioned in figure 5. Now, if the routing is normal, there is no need to identify the attacker in the network. However, if actual attackers are infecting the usual activity of the network, then it is absolutely necessary to apply an CSMP approach to protect the network from attackers. The flooding in presence of attacker is more than the normal routing, means it shows abnormal behavior.

The normal users and malicious users are access the same cloud for data storing and data fetching. In presence of attacker/s overload on server is also enhanced. The flooding attacker and CSMP scheme is depicted here using a flow chart.

Figure 4. Flow Chart of CSMP

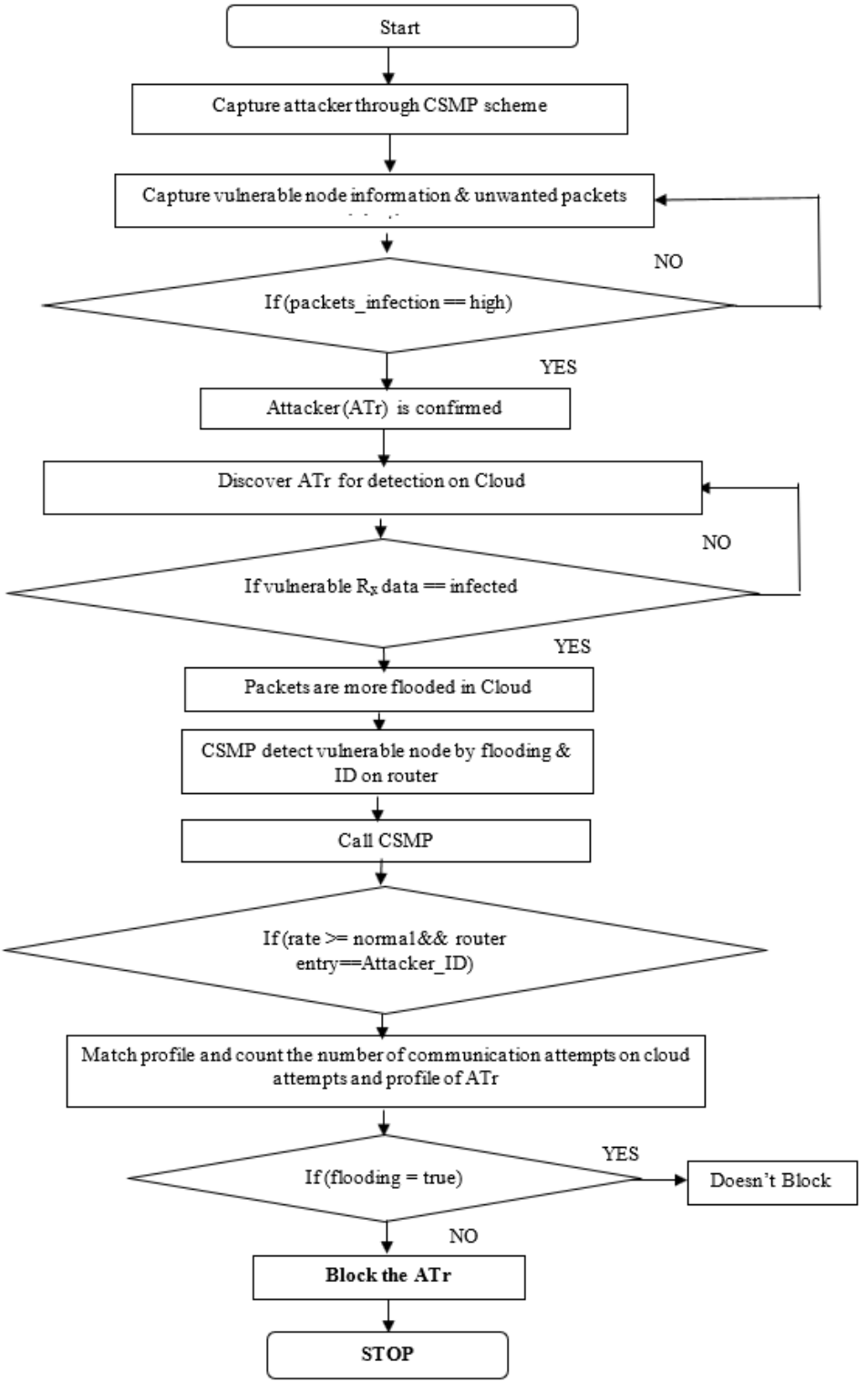
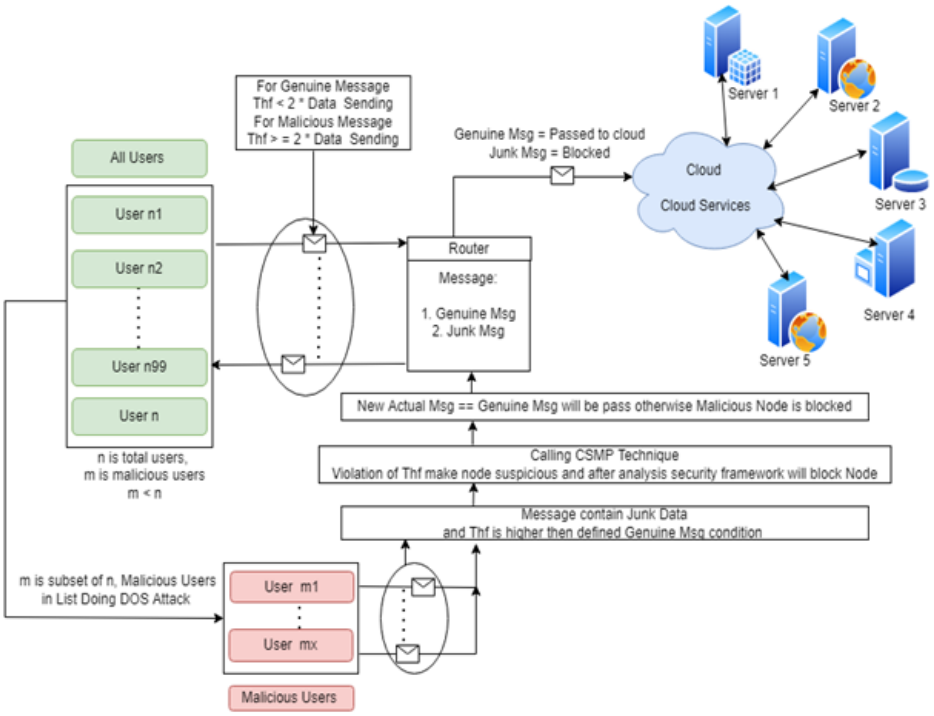


Figure 5. Block diagram of CSMP working



1. Identified the attacker using the proposed CSMP scheme by tally the number of attempts for communication to inject malicious code and presence of the attacker on the router while it was hosted in the cloud.
2. Record information about vulnerable nodes and calculate their infection rate in the event that an attacker infects vulnerable nodes in the cloud network
3. Control the data (It is attacker or normal packets) and rate in order to validate the existence of an ATr attacker.
4. The behavior of the attacker (ATr) is to detect the flooding on route or connected nodes, and susceptible receiver nodes are simply affected by the attack because of this.
5. After that, contact CSMP to determine who the attacker is in the cloud.
6. The CSMP protector is performing a check on the attacker by exceeding the capacity of the network's data transmission rate in order to send more data.
7. Block MIA activity through CSMP by sending rate control messages at different Inter Arrival Times.

4. SIMULATION AND RESULT

4.1 Simulator Overview

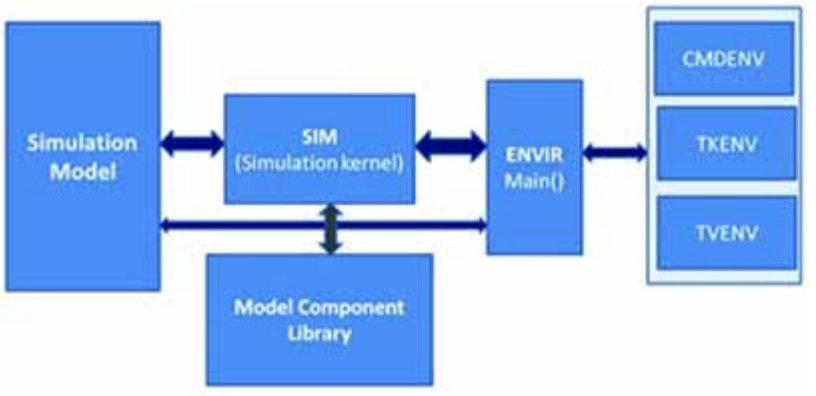
During a simulation, a model is developed to perform a numerical evaluation of a system over the course of some period of time. Estimating the system's characteristics allows for the selection of the option that is likely to yield the best results from a set of potential options that are being considered. Continuous simulation systems monitor the system at every point in time when there is a change in the state of the system. Discrete simulation systems are used to track the changes that take place in

a system's state at discrete points in time. The use of a computer programmer is essential in order to successfully simulate the vast majority of practical issues (OMNeT++ 2000). The study of the internal interaction of a subsystem with a complex system is made possible through simulation. It is possible to simulate and investigate the effects of changes in the informational, data collection and environmental settings ((OMNeT++ 2021).

1. A The use of a simulation model enables us to acquire knowledge regarding the enhancement of a system.
2. Determining the most important input parameters while the simulation inputs are being changed.
3. Before putting new designs and policies into effect, simulation can be used to test them.
4. The simulation of a machine's many different capabilities can be helpful in establishing its requirements.
5. The use of simulation models created specifically for training makes learning possible without incurring any additional costs.
6. Through the use of animated simulation, a plan can be visualized.
7. A The use of a simulation model enables us to acquire knowledge regarding the enhancement of a system.
8. Determining the most important input parameters while the simulation inputs are being changed.
9. Before putting new designs and policies into effect, simulation can be used to test them.
10. The simulation of a machine's many different capabilities can be helpful in establishing its requirements.
11. The use of simulation models created specifically for training makes learning possible without incurring any additional costs.
12. Through the use of animated simulation, a plan can be visualized.

The OMNET++ simulator is a discrete event simulator based on C++ that models, multiprocessors, distributed or parallel systems and communication networks. OMNeT++ (OMNeT++ 2000) was developed for this purpose. OMNeT++ is open-source and can be utilised under the Academic Public License, which allows for the software to be used without cost for charitable or educational purposes. OMNeT++ is an attempt to bridge the gap between research-oriented open-source simulation software like Network Simulator -2 (NS-2) and expensive commercial alternatives like OPNET (OMNeT++ 2021). OMNeT++ can be installed on all of the most popular operating systems, such as Windows, Linux, and Mac OS X, by utilising either the GCC tool chain or the Microsoft Visual C++ compiler. OMNeT++ is an example of an approach that uses a framework.

Figure 6. OMNET++ Architecture



NED Language - The user is responsible for defining the structure of the model in OMNeT++'s topology description language, NED. This includes the modules and how they are connected to one another. Simple module declarations, compound module definitions, and network definitions are the standard components that make up a NED description. The gates and parameters that make up the module's interface can be described using simple module declarations. Despite the fact that the NED language was developed with scalability in mind, the recent increase in the number and complexity of OMNeT++ based simulation models and model frameworks necessitated the need to make additional enhancements to the NED language.

Graphical Editor - The OMNeT++ package comes with an Integrated Development Environment (IDE), which includes a graphical editor that uses NED as its native file format. In addition, the editor is able to work with arbitrary NED code, including code that was written by hand. The decisions made during the design process of the NED language itself have made this possible. If arbitrary programming constructs were allowed, it would be practically impossible to write two-way graphical editors that would be able to work directly with generated as well as hand-made NED files. These editors would be rendered useless. NED has an advantage in many simulation scenarios due to its parametric topologies, both in comparison to OPNET, which only allows for the design of fixed model topologies, and in comparison, to NS-2, in which the building of model topology is programmed in TCL and is frequently intermixed with simulation logic.

4.2 Simulation Parameter

The following simulation parameters are represented in Table 1, which will be used to make a scenario involving routing protocols. The evaluation makes use of the detailed simulation model, which was developed using OMNET++ (OMNeT++ 2021). The topology structure of the network as well as the motion mode of the nodes can be defined with the help of the OMNET++ instructions, which can also be used to configure the service source and the receiver, among other things.

Performance Indicator - The following various performance indicators have been taken into account when conducting a simulation-based comparison analysis of these routing protocols.

1. **Packet Receiving Percentage -** The PDR is actually the number of data packets that were sent and truly acknowledged between the sender and the recipient. The PDR performance is showing the receiving percentage w.r.t sending.
2. **Packet Drop Percentage -** This metric describes how many data packets drop in network or packets not receive at destination. Higher data drop shows degradation in performance.
3. **Delay Analysis -** This analysis describes the unnecessary overhead of time or the extra time taken by senders for successful data transmission.

Table 1. Parameters used as Input for Network

Constraints	Outline Value
Environment	Cloud
No of Server	5
Server CPU	64 bit, 3GHz, Multi-Core
Number of User	N Users
Attack Type	Malware Injector
Secure Protocol	CSMI, CSMP
Network Router	On
Simulation Time (Sec)	100Sec

4. **Attacker Flooding Analysis -** It is the amount of unwanted data flooded by attacker in network. The number of packets is flooded by attacker and these packets quantity is very high.

4.3 Result Analysis

The performance of earlier protocols is discussed in this section, and it is shown that the proposed Cloud Security Malware Prevention (CSMP) protocol has superior results.

Network Scenario-:

The simulation that was tested in this paper was run on a test-bed that enables users to create arbitrary network topologies. This paper describes the network scenario. Users of OMNET++ are able to run tests in the servers without having to physically move the nodes in the network by altering the logical topology of the network. The router will forward any packets that are sent to it by the malware injector, which will result in an unnecessary flood of unwanted packets. While the servers communicate with one another using a wireless interface and store information in the cloud, the simulator uses an interface to control the test scenarios it generates.

Analysis of Packet Receives in Percentage - The proper data receiving in network is shows the network is able to handle the load efficiently. This graph shows the performance of the data packets receiving by servers. The CSMI protocol is not efficient for cloud communication due to the less carry out of the data packets in link because of malware injection attack. In this form of communication, assurance from reception does not give the confirmation of the successful transmission of the data is not certain. The CSMP is able to receive minimum 15% more on each server. The rest of the scenarios are also successfully receiving more packets as compare to the previous scheme. This means that, in the case of the CSMP approach is more effective than CSMI protocol.

Analysis of Loss Percentage of Data - The data dropping in network is definitely degrades the performance of network. The packet transmission efficiency is entirely based on network conditions like heavy loaded or lightly load. This graph reflects packet loss analysis in the case of proposed CSMP and previous CSMI. The loss of packets in the proposed scheme is only around 4% maximum on server 3 but in the case of the CSMI about 7122 packets are delivered throughout the network, which means that the efficiency of the CSMP protocol should accommodate the risk of congestion. Effective routing has been achieved in the proposed scheme to improve network capacity and balance load in network.

Figure 7. Simulation Environment in OMNET++

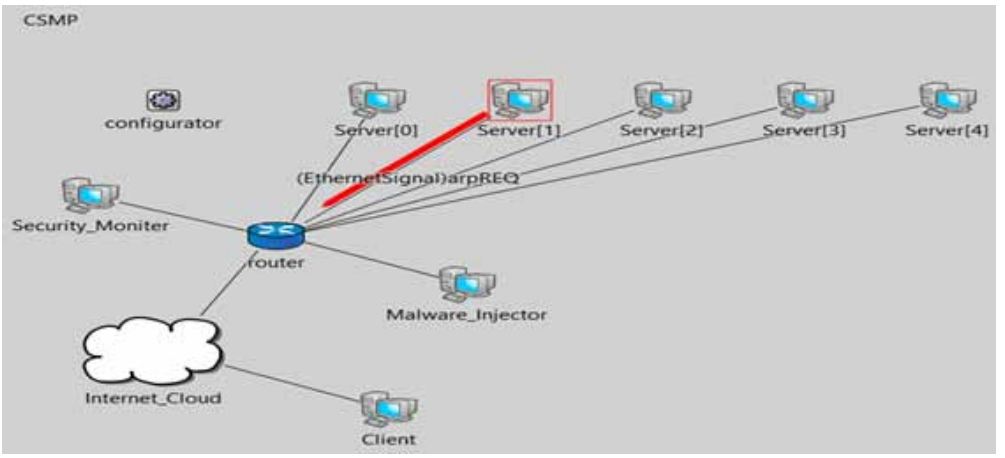


Figure 8. Packet Receive Percentage

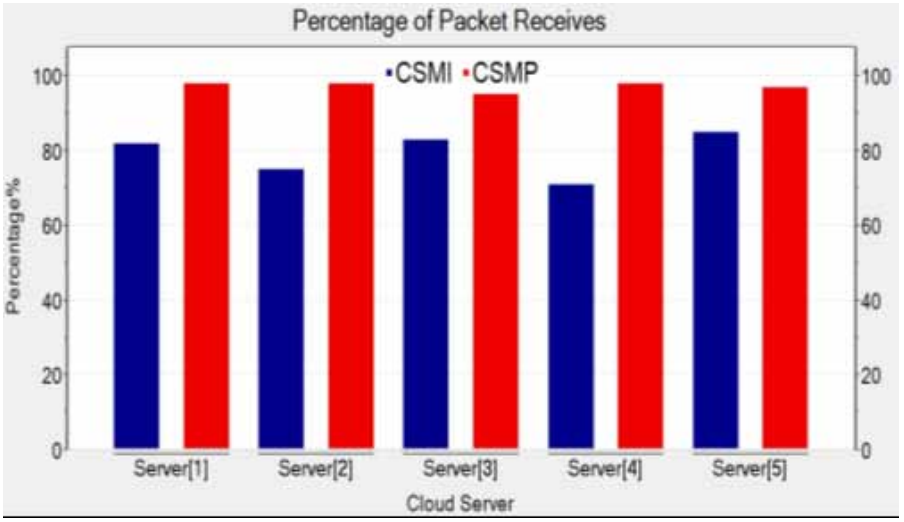
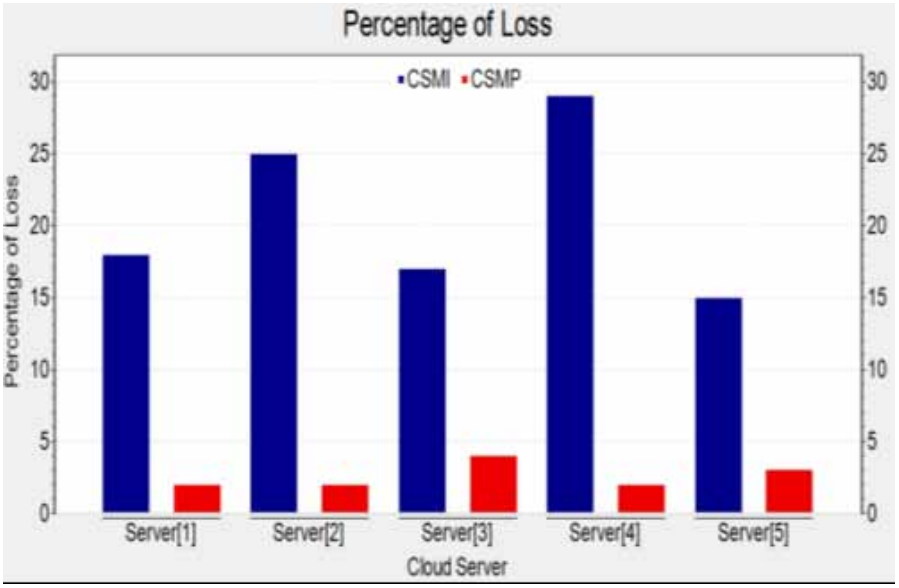


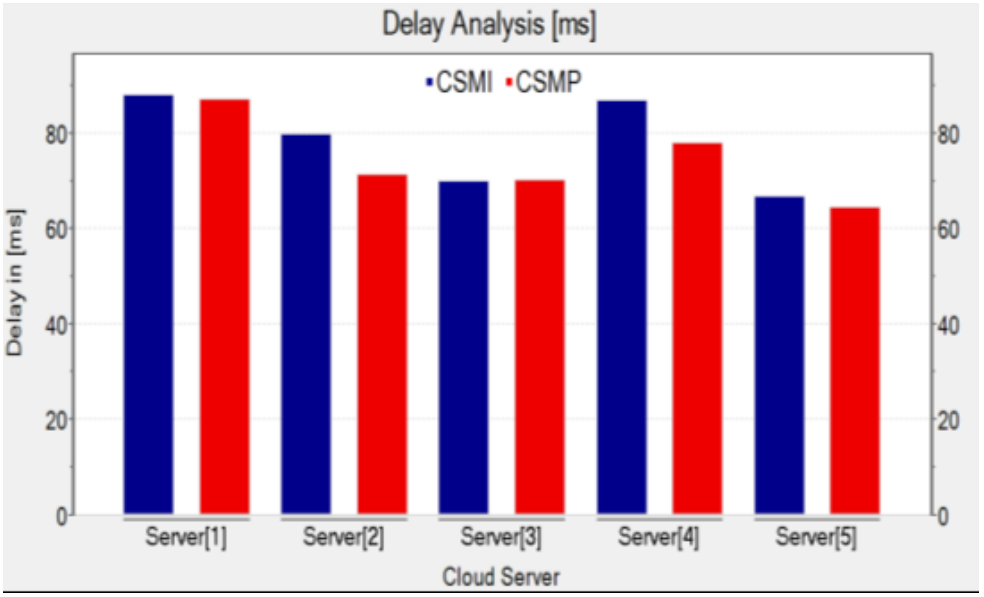
Figure 9. Percentage of Loss Packet



Delay Analysis (ms) - The delay is specified in terms of the amount of time extra required for receiving data in network. In this graph, the average latency for the CSMP scheme is lower than for the earlier CSMI scheme, and the network's performance is enhanced by the shorter delay. Here, in the case of the proposed scheme delay on server 1 is 805ms maximum but delay in the case of the previous scheme is also 805ms maximum but on two servers. The first is server 1 and server 4. The delay-based rate control scheme is definitely provides the strong link and because of that within time data is received at destination.

Summarized Analysis of Existing System - The amount of received data packets, loss data packet and other system measurement like delay measure against malware injection attack are calculated up

Figure 10. Network Delay in (ms)



to the termination of simulation stint. The fewer data reception on servers also shows the degradation in cloud storage. The presence of attacker in network is also enhance the load in network that is affect the data receiving and also affect the spectrum availability.

Summarized Analysis of Proposed System - The number of packets receiving, loss delay in malware injection attacks is calculated at the last of simulation when simulation is going to be end. The better data reception increases the use of the cloud space that is accessible through server. The presence of a trustworthy security system in a network also helps to reduce network load, which has an impact on data receiving and spectrum availability.

5. CONCLUSION AND FUTURE WORK

Implementation of cloud computing services by reviewing all the big security problems in cloud computing is required now a days. Lots of malicious users and attacker are also trying to capture the packet in the cloud. DDoS is one of the attacks which effect the processing capabilities of cloud

Table 2. Existing Cloud Security Analysis (CSMI)

		Server 1	Server 2	Server 3	Server 4	Server 5
Percentage of Received		82	75	83	71	85
Percentage of Loss		18	25	17	29	15
Round-Trip	**Min**	242.07	284.952	299.892	289.362	381.454
	Avg	462.238	496.848	474.835	474.808	520.863
	Max	655.22	640.509	669.262	673.565	697.359
Delay (ms):		88.0138	79.6923	70.0104	86.8314	66.7428
Variance		0.00775	0.00635086	0.0049	0.00754	0.00445

Table 3. Proposed Cloud Security Analysis (CSMP)

Proposed CSMP						
		Server 1	**Server 2**	**Server 3**	**Server 4**	**Server 5**
Percentage of Received		98	98	96	98	97
Percentage of Loss		2	2	4	2	3
Round-Trip (in ms)	**Min**	226.664	338.153	268.315	300.126	351.152
	Avg	448.227	494.884	485.99	476.342	524.898
	Max	664.579	694.25	663.836	630.504	684.346
Delay (ms)		87.1298	71.4012	70.1669	77.9575	64.3667
Variance		0.00759	0.00509813	0.00492	0.00608	0.00414

by flooding data continuously. With the CSMP method we can find the abnormal behavior of node who is trying to dangle the processing capabilities of cloud. Comparison of existing method CSMI with CSMP has been shown in table 2 and 3. Analysis has done in 5 different servers under different paraments. It is observed that avg. data receiving in servers are approx. 98%, avg. loss of data is 2.3%. Round trip (sending and receiving) is categorized in three types, MIN., MAX, AVG. Average data round trip time (ms) in MIN is 226.66, MAX is 630, AVG is 448, average delay (ms) and variance is 70.16 and 0.0049 respectively, which is better in comparison to existing method.

If an attacker uses all available resources, others user cannot use those resources and it affect the availability of cloud services. So, the reliable security scheme is definitely improving the performance and stop malicious activities in the network. This current methodology is effective in text and image data only, in future we can develop new approach for audio and video data with some new & more affective parameter. This framework is applicable in SAAS layer of cloud, in future we can implement it for PAAS layer. We can also incorporate AI & ML, FUZZY techniques as well to develop more secure framework for implementation in SAAS layer.

REFERENCES

Abdalla, P. A., & Varol, A. (2019). Advantages to Disadvantages of Cloud Computing for Small-Sized Business. *7th International Symposium on Digital Forensics and Security (ISDFS)*. doi:10.1109/ISDFS.2019.8757549

Anwar, A., Halabi, T., & Zulkernine, M. (2019). Cloud-based Sybil Attack Detection Scheme for Connected Vehicles. *3rd Cyber Security in Networking Conference (CSNet)*. doi:10.1109/CSNet47905.2019.9108923

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A View of Cloud Computing. *ACM Communication*, *53*(4), 50–58. doi:10.1145/1721654.1721672

Bajaj, Breslau, Estrin, Fall, Floyd, Haldar, Handley, Helmy, Heidemann, Huang, Kumar, McCanne, Rejaie, Sharma, Varadhan, Xu, Yu, & Zappala. (2000). Improving simulation for network research. *IEEE Computer*.

Bhandari, N. H. (2013). Survey on DDoS Attacks and its Detection & Defence Approaches. *International Journal of Science and Modern Engineering, 2*(7).

Chopade, S. S., Pandey, K. U., & Bhade, D. S. (2013). Securing Cloud Servers against Flooding Based DDOS Attacks. *International Conference on Communication Systems and Network Technologies*. doi:10.1109/CSNT.2013.114

Fovinoa. (2009). *An Experimental Investigation of Malware Attacks on SCADA Systems. International Journal of Critical Infrastructure Protection, 2*.

Francois, J., Aib, I., & Boutaba, R. (2012, December). Firecol, a Collaborative Protection Network for the Detection of Flooding ddos Attacks. *IEEE/ACM Transactions on Networking*, *20*(6), 1828–1841. doi:10.1109/TNET.2012.2194508

Hamdani, & Siddiqui. (2019). Detection of DDOS Attacks in Cloud Computing Environment. *Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2019)*.

Kim, Lee, Kim, & Park. (2013). Detection of Advanced Persistent Threat by Analyzing the Big Data Log. Advanced Science and Technology Letters, 29, 30–36.

Meenal, J. G. K. (2021). A Novel Distributed Semi-Supervised Approach for Detection of Network Based Attacks. *9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*.

Mell & Grance. (2009). *The NIST definition of Cloud Computing, Version 15*. National Institute of Standards and Technology.

Nalajala, Akhil, Sai, Shekhar, & Tumuluru. (2019). Light Weight Secure Data Sharing Scheme For Mobile Cloud Computing. *Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*.

OMNeT++ Home Page. (n.d.). http://www.omnetpp.org

Ranjan, I., & Agnihotri, R. B. (2019). Ambiguity in Cloud Security with Malware-Injection Attack. *Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology (ICECA)*. doi:10.1109/ICECA.2019.8821844

Saied, A., Overill, R. E., & Radzik, T. (2015). Detection of known and unknown DDoS Attacks using Artificial Neural Networks. *Neurocomputing*.

Singh, N. A., Singh, K. J., & De, T. (2016). Distributed Denial of Service Attack Detection using Naive Bayes Classifier Through info Gain Feature Selection. In *Proceedings of the International Conference on Informatics and Analytics, ser. ICIA-16*. ACM. doi:10.1145/2980258.2980379

Song, Heo, & Hong. (2007). Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks. *IEICE Transaction Fundamentals/Communication/Electronics/Information & System, E 85-A/B/C/D*(1), 1-10.

Soni & Sudhakar. (2020). A L-IDS against Dropping Attack to Secure and Improve RPL Performance in WSN Aided IoT. *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN),* 377-383.

Soni, D., & Kumar, M. (2017). Secure data communication in client-cloud environment: A survey. *2017 7th International Conference on Communication Systems and Network Technologies (CSNT),* 246-252. doi:10.1109/CSNT.2017.8418546

Soni, D., Sharma, V., & Srivastava, D. (2019). Optimization of security issues in adoption of cloud ecosystem. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU),* 1-5. doi:10.1109/IoT-SIU.2019.8777670

Soni, D., Tiwari, V., Kaur, B., & Kumar, M. (2021). Cloud computing security analysis based on RC6, AES and RSA algorithms in user-cloud environment. *2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT)*, 269-273. doi:10.1109/ICACFCT53978.2021.9837360

Soni, G., & Chandravanshi, K. (2021). Security Scheme to Identify Malicious Maneuver of Flooding Attack for WSN in 6G. *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, 124-129. doi:10.1109/SPIN52536.2021.9566066

Thirumaleshwari Devi, B., Shitharth, S., & Jabbar, M. A. (2020). An Appraisal over Intrusion Detection Systems in Cloud Computing Security Attacks. *Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020).* doi:10.1109/ICIMIA48430.2020.9074924

Vrushali, D. (2015). Interactive image segmentation using combined MRF and ant colony optimization. International Journal of Engineering and Computer Science.

Yu, S., Guo, S., & Stojmenovic, I. (2012). Can We Beat Legitimate Cyber Behavior Mimicking Attacks from Botnets? *Proc. INFOCOM*, 2851-2855. doi:10.1109/INFCOM.2012.6195714

Zhao, , Liu, Tang, Sun, Zhang, Ye, & Tang. (2009). Cloud Computing: A statistics aspect of users. In *First International Conference on Cloud Computing (CloudCom)*. Springer.

Neeraj Rathore is currently working as an Assistant Professor (Senior Scale) at UPES, Dehradun. He is also a research scholar (Part Time) with the Department of Computer Science and Engineering, NIT Uttarakhand, India. His research interest's domain is Machine (Deep) Learning, Computer Vision and its applications in the emerging trends, especially Salient Object detection. He has overall 14+ years of teaching experience in well know engineering colleges and universities in North India. Devendra Prasad is a Ph.D. scholar with the Department of Computer Science and Engineering, NIT Uttarakhand, India. His research interest's domain is machine (deep) learning and its applications in the emerging trends, especially biometric authentication, the health sector, and algorithm design for optimization problems. He has 15+ years of experience in total with 5 years being in the s/w industry. Around 10 years exposure with academics in well known engineering colleges and universities.

Harishchander Anandaram completed a PhD in bioengineering, an M. Tech, and a B. Tech in bioinformatics from the Sathyabama Institute of Science and Technology, Chennai, in 2020, 2011, and 2009. His bachelor's and master's theses, he worked on analyzing resistance in HIV protease inhibitors based on molecular mechanics and machine learning studies, a collaborative project with IIT Madras. In his PhD thesis, he worked on pharmacogenomics and miRNA regulated networks in psoriasis, a collaborative project with Georgetown University, USA, JIPMER, INDIA, CIBA, INDIA, and ILS, INDIA. His thesis illustrated a multi-disciplinary approach by combining computational biophysics and molecular biology machine learning. While doing a PhD, He had the opportunity to collaborate with international researchers and have publications in reputed international journals in bioinformatics and systems biology. He has received the prestigious "Young Scientist Award" from "The Melinda Gates Foundation" for his research abstract on "The Implications of miRNA Dynamics in Infectious Diseases". To date, he has reviewed more than 200 manuscripts in systems biology. He is currently working on predicting novel lead molecules and biomarkers using computational techniques to target inflammatory pathways associated with infectious and autoimmune disorders.