IJAER/December - 2012/Volume-1/Issue-4 ISSN: 2278-9677

International Journal of Arts & Education Research

DETECTION SYSTEMS OF CLOUD ENVIRONMENT USING PARALLEL AND MULTISTAGE SECURITY MECHANISM

Kapil Dev
Research Scholar
CMJ University Shillong

Dr. Amal Kumar Deka
Professor
Guwahati University Assam

Abstract

The technology of cloud computing is developing at a breakneck speed as a result of the fast growing demand for services required by a variety of businesses, institutions, and people. Despite this, the data stored in the cloud environment is not entirely safe against intrusions and assaults coming from both the outside and the inside of the system. An improved method for securing data in a cloud computing environment using a parallel and multistage security mechanism (PMSSM) is proposed in this article. The goal of this method is to provide simultaneous security checks and procedural multistage security by employing authentication methods, intrusion detection, and encryption. The parallelism in the verification process and the multistage security will increase the probability of identifying the intrusion or attack that is being carried out by the attacker if this strategy is taken into consideration. This will allow for a greater chance of identifying the attack as it is being carried out. Additionally, taking into consideration the dynamic nature of the intrusion, employing parallel and multistage security can assist in preventing the occurrence of such an event. Following the debate of the proposed mechanism, it became clear that this model has the potential to be applied in the service of giving cloud customers increased data protection.

Keywords: *Detection Systems, multistage, mechanism, Cloud Environment*

Introduction

People are increasingly turning to the cloud computing environment for their professional as well as their personal computer needs. It is essentially a pool of computers that are shared in order to be used across the network as a means of avoiding the expenditures or administration efforts that would otherwise be required. Therefore, rather than having the data stored locally on the PC of each user, the data are uploaded to a shared or hosted server. Datacenters are typically thought of as the entities that are in charge of delivering services of this nature. The majority of people who utilise cloud computing do so in an effort to cut down on the expenses associated with purchasing computer hardware and software. Despite the fact that cloud services can be accessed anywhere in the world through the use of the internet, not all cloud services are the same or suitable for all users. The cloud environment makes available a variety of alternative models and services to its users. In general, the deployment methods for the cloud may be broken down into four distinct categories: public, private, community, and hybrid models. The cloud computing environment may be leveraged to deliver a variety of services. Software as a Service (SaaS), Performance as a Service (PaaS), and Infrastructure as a Service are some examples of these (IaaS). These may be put together to make everything into a service (EaaS). Both the cloud deployment models and the cloud service models are depicted in Figures 1 and 2, respectively. As was discussed in the preceding paragraph, there is a wide variety of cloud deployment options and cloud services available. Nevertheless, the level of security presented by any of these approaches may be a significant concern. [1] Therefore, in order to solve this issue, there ought to be some procedures that can give security to any and all of these models, whatever the kind of model being considered. The most important thing that has to be done is to come up with a generic security model that can be included into any kind of cloud architecture. This is necessary in order to protect the information and data that cloud users save. To this end, this discussion will cover the many security concerns as well as the various security measures.

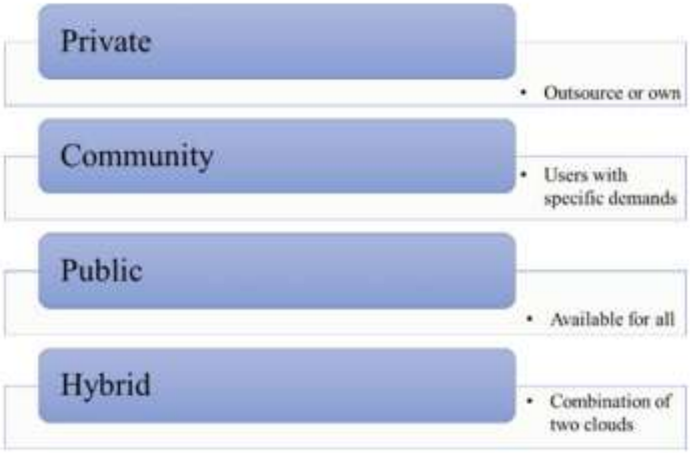


Fig. 1 Cloud deployment models

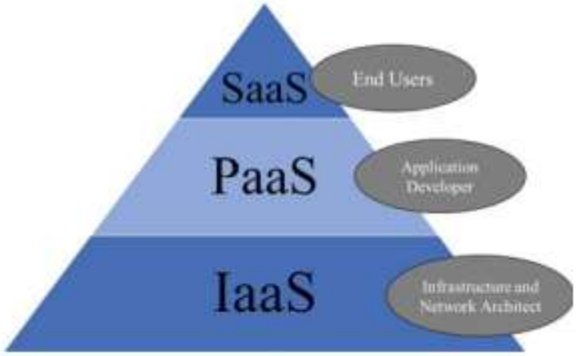


Fig. 2 Cloud service models19

Cloud Computing Security

The concept of cyber security is the assurance of safety from the activity of multiple entities (human and not), both internal and external, physically and in the cyberspace domain. Cyber security is classically characterized by the CIA triad:

1. Confidentiality: This is the assurance that user information is kept private from unauthorized agents to access.

2. Integrity: This is the assurance of data remaining accurate and unmodified from the original state.
3. Availability: This assurance of data reliability is readily accessible to the authorized personnel upon request.

Cybersecurity must be taken into consideration and used in order to safeguard the information of the users who are participating in the implementation of cloud computing technology in a secure manner. Keeping cyber security at the forefront of cloud-based settings contributes to a reduction in the risks associated with cyber threats as well as an assurance of compliance with the laws and regulations that have been established to protect information security. Cloud computing is a topic that is familiar to a sizeable portion of individuals working in the field of information technology. As a result, they have to invest a considerable level of time and effort into comprehending the security features exhibited by cloud computing as well as the dangers that are associated with it. The growing number of people using computers and the increased demand for their services both has the potential to result in enhancements to service quality and user needs. Web development has resulted in a multitude of challenges, one of the most notable of which is the availability of massive amounts of data on the internet. As a result of this, there has been an increase in the number of servers that have substantial storage capacity, which has made it possible to store a huge amount of data in the cloud across vast geographical areas all over the world. Cloud computing is defined as a model that realises the on-demand network accessibility, convenience, and ubiquity of computing resource configuration. This includes networks, storage, services, servers, and applications. This definition comes from the National Institute of Standards and Technology (NIST). [2]They are swiftly delivered and released, and they do not involve a large amount of contact from either management or service providers. A broad network access, a measured service, on-demand self-service, resource pooling, and the capability to have quick flexibility are the five essential aspects that are covered by the technology that is integrated in cloud computing. It is difficult to build a standard security model that can be implemented by end-users of cloud computing since service delivery models have varied implementations. This makes it more difficult to develop a standard security model. Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service are the three different types of service models (PaaS). There are four deployment models for cloud computing, which may be categorised as three fundamental and extensively used deployment models: public, private, and hybrid clouds, as well as a fourth form that is used far less frequently and is known as the community cloud.[3]

1. A private cloud is deployed and managed within a single organization.
2. A public cloud is deployed and managed in a third-party organization.
3. A hybrid cloud consists of private and public cloud technologies.
4. A community cloud consists of sharing computing resources within multiple organizations and has the management operations completed by an in-house IT department or third party.

Classification of Detection Mechanisms to Secure Cloud Computing Against DDoS Attack

Several groups of academics have come up with various ideas for defences against DDoS attacks on CC. Recent studies have highlighted the threat that a DDoS assault poses to cloud computing. According to the findings of research by [4], cloud blocking attacks have a negative impact on the target server, as well as network resources and service providers. In addition, research conducted by [5] demonstrates that DDoS attacks and the subsequent interruption of client services are contributing to the precipitous decline in the price of cloud services, which in turn has a detrimental impact on service providers. In addition, research [6] shed light on how distributed denial of service attacks occurred on cellular networks and shown that these attacks led to disruptions in service.

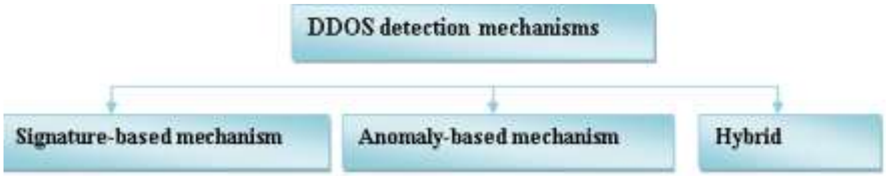


Fig. 3. DDoS-based Detection Mechanisms Classification

DDoS-based Detection Mechanism

These techniques are only able to notice the assault and cannot stop it from happening. Instead, they use a variety of approaches, including monitoring, categorization, and trackback. The following is a discussion of the most recently proposed strategies for detecting distributed denial of service attacks against cloud computing:

Signature-based Mechanism

In the databases, a set of attack rules and patterns are utilised. The traffic in those databases is watched for patterns, and those patterns are compared to the ability to identify an attack. Because of the precision with which it can identify assaults even in the face of ongoing maintenance to its databases, this method is among the most essential of those that are available. However, one of its drawbacks is that it is unable to identify assaults that have not yet occurred. Research was out by [7] prevails VM-based intrusion detection systems (IDS) with graphical user interfaces, well-organized databases of MySQL data, and the ability to monitor signals generated by cloud fusion units located within the front-end of Eucalyptus cloud designs. They come to the conclusion that the Barnyard tool will be used to identify assaults, while a stamped-based SNORT will be arranged with pre-determined DDoS rubrics to guard against well-known DDoS attacks. Barnyard stores the intercepted assault packets in a binary unified file, which is subsequently sent through a secure channel to central MySQL information on the front-end. The Stacheldraht is a DDoS incursion instrument that performs an infrastructure resource reduction attack. This attack consists of ICMP flooding, UDP flooding, and transmission control protocol SYN. DDoS intrusions were imitated with the help of the Stacheldraht. Even though the system had a higher discovery proportion due to the occasional false positive, the key weakness of this method is in its inability to spot unidentified attacks. This is an intrinsic weakness of the signature-based method. Even though the system had an increased discovery proportion due to an occasional false positive. According to a study by [8], it is advised to make use of the filter tree approach to retain information rather than using the application layer flooding.

The five (5) components that make up the projected method have been recreated in order to find and fix XML and hypertext transfer protocol-based DDoS incursions that take place in requisitions for resources victimisation, Straightforward Object Access Protocol (SOAP), and electronic communication. These incursions take place in requisitions for resources to be used. At the edge router, the scientific discipline marking module makes use of the Versatile Settled Packet Marking (VSPM) theme to identify SOAP messages. On the other hand, scientific discipline employs the VSPM theme to identify SOAP messages. There is a possibility that the "Trace back" file is a logical one that maintains an inventory of a "blacklist" of addresses related to scientific disciplines that are given by Cloud Defender. We have come to the conclusion that the Cloud Defender screens for potential threats by employing a five-stage process, which includes the following filters: detector filter, hop count filter, scientific discipline frequency divergence filter. These assures a genuine user scientific discipline filter and double signature filter. First and foremost, four phases are utilised to locate hypertext transfer protocol distributed denial of service attacks, however an XML distributed denial of service attack is discovered throughout all five stages. In addition, research projects carried out by [9] predicted the utilisation of attack detection techniques that were enabled by the VM profile optimization. When there was an intrusion of TCP SYN flooding as a result of the threshold for rule pattern at the beginning of the rule formation stage, the rule-based recognition approach was used to match packets. This was done in order to prevent further damage. In addition, [10] provided a model for the detection of invasions that would allow for the management of the enormous flow of packets by inspecting as well as acquiring information on these packets. The output of the IDS may be increased with the help of the proposed prototype by using multi-threading technologies. The Network Intrusion Detection System (NIDS) is capable of not only detecting network traffic but also monitoring it in order to search for malicious packets. An alarm is delivered to an arbitrator observing system if a malicious packet is identified; this system then alerts the CC management system. The NIDS prototype consisted of three different units: the unit for capture and queuing, the unit for processing and analysis, and the unit for reports. The.NET framework found in Windows was utilised for this prototype's development environment.

According to the findings of the investigation that was carried out by the investigators, using many thread preparation styles can save more money than using a single thread preparation style. In addition, research carried out by [11] employed IDS in VMs to defend against DDoS intrusions. IDS sensing element makes use of SNORT, which is a sign-based building approach that is placed on the virtual interface of a VMware virtual ESX machine to study both incoming and outgoing traffic in real time. This type of protection is intended to prevent Distributed Denial of Service (DDoS) attacks within the network and transport layers. It identifies the IP addresses that were used in these attacks by automatically creating an admission management log, which causes complete packets to be dropped if they come from a proscribed IP address. This solution will be intended to halt these sorts of traffic and transfer the targeted application to a virtual machine (VM) that is stored in a different data centre when the intrusions occur from units that are classed as zombie computers. In addition, [12] offered an IDS-primarily based technique that was spread throughout the cloud setting. Once an association invasion has been identified, the alerts are modified through the IDS nodes that are dispersed across the cloud setting. The IDS system is comprised of four components: the attack discovery, the reaction and block, the threshold check and alarm cluster, and the cooperative operation. Every IDS that is put into use has a supplementary agent embedded inside it to determine whether or not it will acknowledge the alert that has been directed at it by various IDS nodes. These related approaches will lead to a reduction in the number of intrusions that are discovered and reported by the various IDS nodes.

Attacks and Security Issues

The cloud environment is still susceptible to a number of security flaws and threats, which makes it unsafe for the outsourcing of data [13]. The distributed denial of service (DDoS) is the most common type of cyberattack . In reality, it is based on a denial of service attack (also known as DoS). A denial of service attack, often known as a DoS attack, is a sort of cyberattack in which the attacker sends a huge number of useless packets or requests in an effort to halt the services running on the victim's computer. The victim system becomes preoccupied with processing these requests once it has received them, and as a result, it is unable to attend to the requirements of the genuine user. In most cases, this occurs when the number of requests made to the system is more than the number of requests that the system is able to process.

These things are what people usually refer to as "bandwidth depletion," and they are responsible for wasting the system's bandwidth. Another method of assault is known as a man-in-the-middle attack (MITM) . There are many other kinds of assaults, but they are all connected to one another and to the MITM attack in some manner. This is because all of these attacks attempt to steal information by playing the role of a middle man in some way.

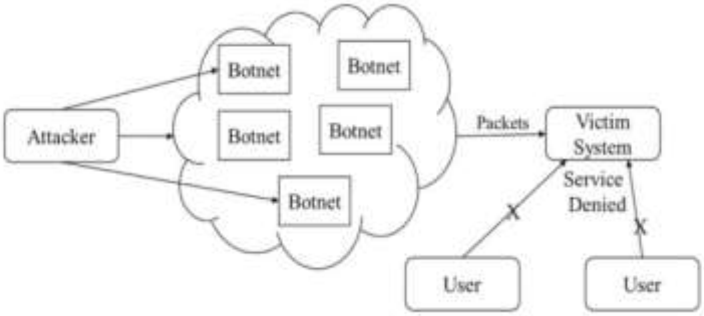


Fig. 4 DDoS attack on victim system

The denial of service assault may appear to be sufficient to finish the job, but in reality, this approach is not effective in finishing the job in a timely manner. As a result, this kind of assault is typically carried out on a system by a number of different systems. These computers, which have been hacked in order to carry out the assault, are referred to as zombies or botnets. A machine that has been compromised and is configured to carry out some type of harmful activity in order to carry out a task without the awareness of its real user is referred to as a botnet or a zombie. In most cases, the attacker will operate these botnets remotely from a separate location. Malware may be used to create these, and an attacker can introduce it into a system through a variety of entry points, including the Internet, a piece of software, or a USB drive, for example. Because of this, distributed denial of service attacks are carried out with the assistance of botnets by bombarding the victim's system with useless packets or requests in an effort to render the victim's system inaccessible to legitimate users. The Distributed Denial of Service attack (DDoS) that was carried out against the target by deploying botnets is shown in Figure 4.

Proposed Model

In this part, a proposed security model for cloud computing is presented, taking into account the assaults and security challenges that were covered in the previous section (Section 2). The suggested cloud security paradigm, also known as PMSSM, may be shown in Figure 5. At first, the client is required to supply the data, such as user id and password, which will be used to check for client account. These details will be used to check for client account. If the customer information is accurate, then you should accept it and go on to the next step of the verification process. It is important to note that the PAP use plain text while transmitting the information. Nevertheless, an upgrade may be made by encrypting the sensitive information, such as the password, in order to avoid the likelihood of an MITM attack. The Challenge Handshake Authentication Protocol, or CHAP, will be carried out in the background as soon as the user is prompted to supply the necessary information for the PAP. The CHAP protocol will begin by delivering a challenge string to the client, and it will then wait for the client to respond to the challenge string. The server will check the answer that has been sent by the client as soon as it arrives and decide whether to accept or reject it. In the event that the proposal is accepted, the mechanism will proceed to the subsequent stage of the verification process. The next thing to do is look for any signs of an invasion. It's possible that the invasion came from the inside or the outside. The CHAP is designed to prevent an entrance from the inside, therefore at this moment, only an incursion from the outside is feasible. Therefore, this is the stage where the user's login activities and patterns, such as DNS and location, will be matched. If the user is successful in passing this stage of verification, then access to the data, such as the ability to upload or download the data from the cloud storage, will be granted to the user. In the event that an intrusion is discovered, the request for access will be denied, and the information, including the IP address, DNS server, and date, will be logged. The data that is stored in the cloud has been encrypted using AES 256 bit, and as a result, even if an MITM attack occurs, the data cannot be understood by the attacker even if the attacker has access to the data. Despite the fact that it is a very remote possibility that the attacker would be able to access the data despite the security measures that have been put in place. In spite of this, and taking into account the chance that the data may be accessed by the adversary, the data are encrypted before being saved in the database. This is done in order to improve and optimise the user's level of safety. The algorithm for the proposed PMSSM is presented in Table 1.

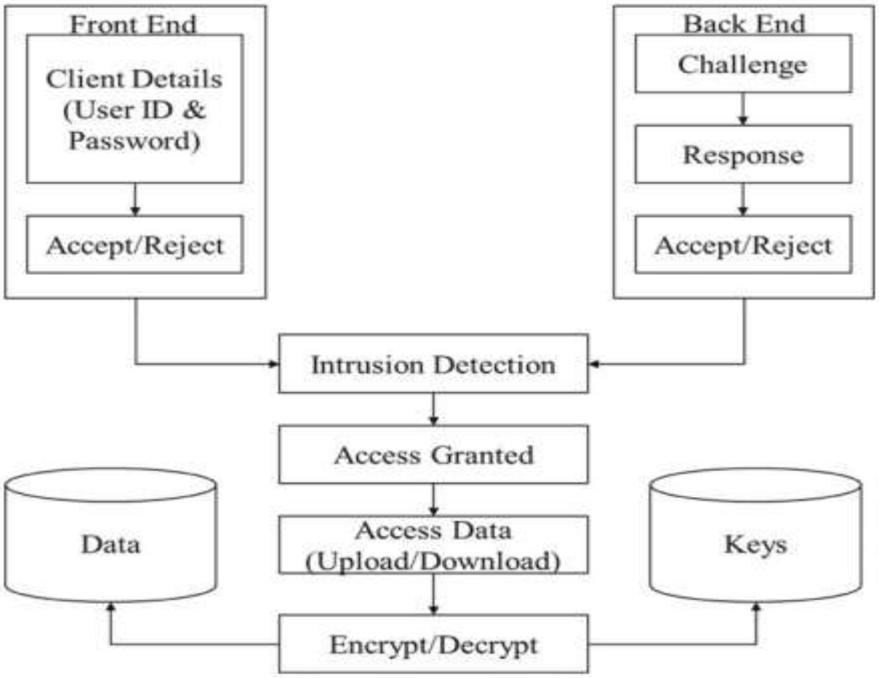
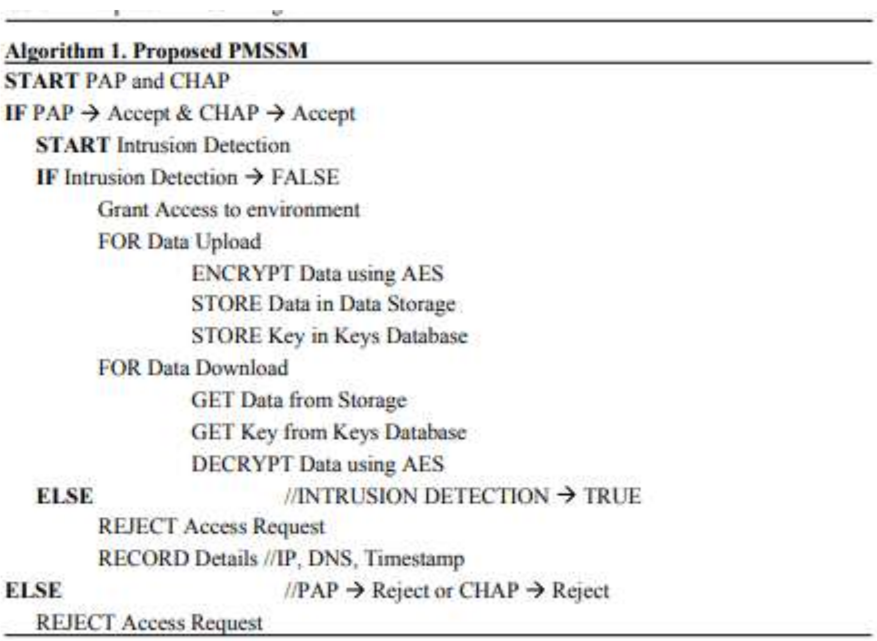


Fig. 5 Proposed PMSSM model

Analyses and Discussion

In this section, a discussion is offered to assess the suggested model based on the potential attack scenarios and its protection mechanism. Specifically, this section examines the proposed model. Consider first the distributed denial of service (DDoS) assault scenario. In the instance of a distributed denial of service attack, the attacker will try to overwhelm the server with a huge number of requests in an effort to prevent the legitimate user from accessing the system.

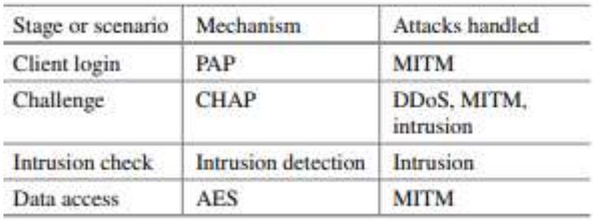
Table 1 Proposed PMSSM algorithm



```
Algorithm 1. Proposed PMSSM
START PAP and CHAP
IF PAP → Accept & CHAP → Accept
    START Intrusion Detection
    IF Intrusion Detection → FALSE
            Grant Access to environment
            FOR Data Upload
                        ENCRYPT Data using AES
                        STORE Data in Data Storage
                        STORE Key in Keys Database
            FOR Data Download
                        GET Data from Storage
                        GET Key from Keys Database
                        DECRYPT Data using AES
    ELSE                        //INTRUSION DETECTION → TRUE
            REJECT Access Request
            RECORD Details //IP, DNS, Timestamp
ELSE                            //PAP → Reject or CHAP → Reject
    REJECT Access Request
```

If an attacker tries to submit such requests, the server will reject them thanks to the incorporation of the CHAP mechanism. After the limit is reached, the server will remove any requests that have been rejected. As a result, the model is not vulnerable to DDoS attacks. Think about the many attack scenarios that include different types of MITM attacks. In this scenario, the attacker may try to extract the information through either the PAP mechanism or the CHAP method, and they might even be able to circumvent one or more of these mechanisms. However, because it is difficult to design for the attacker a strategy that may serve in bypassing both of the mechanisms at the same time, it is difficult to circumvent both of the mechanisms at the same time. One of the reasons for this is that there is a maximum permitted number of times that you may try to have your password authentication authorised. Because the password is encrypted, even if the attacker succeeds in obtaining it, it will be difficult for them to decode it at the same time as authenticating the CHAP method. This is due to the fact that the password is encrypted. Despite this, even if the attacker is successful in circumventing the technique, there is a good chance that the attacker will still set off the intrusion detection mechanism as a result of some change in behaviour or activity. In addition, even if the attacker is successful in gaining direct access to the cloud database that stores the user's data, they will not be able to extract the information from the database since the data is encrypted with AES encryption. As a result, there won't be any problems with the system caused by an MITM attack of any type. The assaults that were countered at each level of the planned PMSSM are outlined in Table 2.

Table 2 Attacks handled at various stages in PMSSM



Stage or scenario	Mechanism	Attacks handled
Client login	PAP	MITM
Challenge	CHAP	DDoS, MITM, intrusion
Intrusion check	Intrusion detection	Intrusion
Data access	AES	MITM

Conclusion

The conclusion that can be drawn from the discussion on the potential attack scenarios is that the proposed model can be used for the purpose of providing high security to the users of the cloud. This is because the model protects the cloud from the most significant attacks, such as DDoS and MITM attacks. We may also draw the conclusion that, now that this model has been introduced, the model can be incorporated into any kind of cloud model, including public, private, community, and hybrid models. This is due to the fact that the model is created for general application. This architecture can be easily integrated into the public cloud by storing the public cloud's data in a data cloud and the public cloud's keys in a private cloud. Only private databases will be accessible using the private cloud. Both the community and the hybrid will make use of the databases in a manner that is analogous to the former. The actual performance of this model will serve as the basis for further development in the future. The model is capable of receiving additional improvements based on the parallelism in the security mechanism, taking into account the amount of time necessary for the system to carry out each individual mechanism.

References

[1] Pandith, M.Y.: Data security and privacy concerns in cloud computing. Internet Things Cloud Comput. 2(2), 6–11 (2009)

[2] Singh, N., Kumar, N.: Information security in cloud computing using encryption techniques. Int. J. Sci. Eng. Res. 5(4), 1111–1113 (2010)

[3] Hassan, N., Khalid, A.: A survey of cloud computing security challenges and solutions. Int. J. Comput. Sci. Inf. Secur. 14(1), 52–56 (2011)

[4] Jaafar, G.A., Abdullah, S.M., Ismail, S.: Review of recent detection methods for HTTP DDoS attack. J. Comput. Netw. Commun. 2019, 1–10 (2010)

[5] Prabu, S., Ganapathy, G., Goyal, R.: Enhanced data security for public cloud environment with secured hybrid encryption authentication mechanisms. Scalable Comput.: Pract. Exp. 19(4), 351–360 (2008)

[6] D. Parwani, A. Dutta, P. K. Shukla, and M. Tahiliyani, "Various Techniques of DDoS Attacks Detection and Prevention at Cloud : A Survey," Orient. J. Comput. Sci. Technol., vol. 8, no. 2, pp. 110–120, 2012.

[7] K. S. Sri and P. Lakshmi, "DDoS Attacks , Detection Parameters and Mitigation in Cloud Environment," vol. 3, no. 01. pp. 1–4, 2011.

[8] P. Kaur, M. Kumar, and A. Bhandari, "A review of detection approaches for distributed denial of service attacks," Syst. Sci. Control Eng., vol. 5, no. 1, pp. 301–320, 2011.

[9] A. M. Lonea, D. E. Popescu, O. Prostean, and H. Tianfield, “Evaluation of experiments on detecting distributed denial of service (DDoS) attacks in eucalyptus private cloud,” Adv. Intell. Syst. Comput., vol. 195 AISC, pp. 367–379, 2012.

[10] G. A. Karnwal, Tarun, “A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack,” 2012.

[11] P. Negi, A. Mishra, and B. B. Gupta, “Enhanced CBF packet filtering method to detect DDoS attack in Cloud computing environment,” Arxiv, pp. 2–6, 2012.

[12] Gul and M. Hussain, “Distributed Cloud Intrusion Detection Model,” Int. J. Adv. Sci. Technol., vol. 34, pp. 71–82, 2011.

[13] Bakshi and B. Yogesh, “Securing cloud from DDOS attacks using intrusion detection system in virtual machine,” 2nd Int. Conf. Commun. Softw. Networks, ICCSN 2010, pp. 260–264, 2010.

[14] C. Lo, C. C. Huang, and J. Ku, “A cooperative intrusion detection system framework for cloud computing networks,” Proc. Int. Conf. Parallel Process. Work., pp. 280–284, 2010.