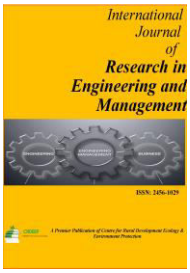
Content is available at: CRDEEP Journals
Journal homepage: http://www.crdeepjournal.org/category/journals/ijrem/

International Journal of Research in Engineering and Management (ISSN: 2456-1029)
A Peer Reviewed UGC Approved Journals



Full Length Research Paper

Identifying and Isolating Zombie Attack in Cloud Computing

S M Firdaus Zaki Rizvi[*] and Dr. Amar Nath Chatterjee[2]
[1]-Research Scholar in Computer Science Magadh University Bodh Gaya, India.
[2]-Assistant Professor, Department of Mathematics, K.L.S. College, Nawada, India.

ARTICLE DETAILS

Corresponding Author:
S M Firdaus Zaki Rizvi

Key words:
Cloud computing, safety malware, simulated machines, identification, and zombie attacks

ABSTRACT

The architecture of cloud computing involves the uploading and downloading of data from third parties, virtual machines, and cloud service providers. The security of the data, however, is a significant concern with this design since there are several ways that malevolent individuals and machines might attack. The zombie attack is the most sophisticated kind of security breach among all. Network performance is decreased by the zombie attack in terms of latency and bandwidth use. In a zombie attack, malevolent users might join the network, stealing the data of reputable users while also allowing zombie nodes to interact with a virtual machine on the reputable user's behalf. This study proposes a powerful authentication-based approach that can identify fraudulent users on a network and isolate them from the cloud architecture.

1. Introduction:

Cloud Computing is a rapidly emerging computer security sub-domain of network security, and, more generally, the security of information. It relates to a wide range of policies, techniques, and controls implemented to safeguard Cloud Computing information, applications, and related Cloud Computing infrastructure.Since corporations and other organisations are switching from local record-keeping methods to cloud infrastructure formats, cloud computing has become the norm. The technology consulting company Gartner [1] has forecast that cloud computing enterprises will expand at a compound annual growth rate of 20 percent.

Cloud computing is a virtualized platform that provides on-demand network access to applications, storage, servers, and other critical computer resources. It may be divided into two categories: service models and deployment models. There are four types of deployment models: societal, private, public, and hybrid clouds. In contrast, platform as a service (PAAS), infrastructure as a service (IAAS), and software as a service (SAAS) are examples of service models. Users may now connect virtually via a variety of digital devices, including smartphones, laptops, and personal computers, thanks to cloud computing. The user pays for the services that the cloud owners rent out and is able to utilise and alter data that they have stored in the cloud because they are the clients. Because of this, customers may set up a cloud environment without worrying about the expense of hardware, making it incredibly cost-effective for them.

While cloud computing is internet-based, it can instantly supply different computers and devices with resources like shared software and data. This implies that the consumer covers the cost of everything he consumes. Although cloud computing has many advantages, there are also significant drawbacks, particularly with regard to malicious users who may access other users' data without authorization. The phrase "cloud security" refers to a combination of network security, information

[*] Author can be contacted at: *Research Scholar in Computer Science Magadh University Bodh Gaya, India.*
Received: 15-6-2024; Sent for Review on: 19-06-2024; Draft sent to Author for corrections: 28-06-2024; Accepted on: 30-06-2024; Online Available from 11-07-2024

DOI : 10.13140/RG.2.2.32114.72646

security, and several other security measures, such as computer security. In order to secure data and various applications that are part of the cloud computing environment, it provides a broad range of technologies, guidelines, and controls [2]. For every service, security is the most important need. However, there are several security risks associated with cloud computing, including downtimes, data loss, botnets, spoofing, phishing, sniffer, and password cracking. It is now necessary to handle each of these security concerns in some manner in order to properly take control of cloud computing. In light of this, this research suggests an effective method for identifying and containing zombie attacks in order to lessen their impact on cloud computing. The remainder of the document is structured as follows: Section 3 contains the suggested algorithm and the procedures for locating and isolating zombie attacks, along with detail screens demonstrating the method's operation. Section 2 analyses some previous publications on the topic. An examination of the suggested technique's operation is provided in Section 4.Section 5 concludes the paper.

2. Zombie Attack

Zombie at tack is one of the advance at tacks in cloud comput ing environment which degrades the per formance of the network and throughput of the network. There are malicious nodes which act as a zombie of one of the connected users. A system that has been inser ted with a program that puts it under the cont rol of malicious users without the awareness of the system user . Zombie is used by malicious users to launch DoS or DDoS at tacks. Through an open communicat ion por t , the illegit imate user sends commands to the zombie.

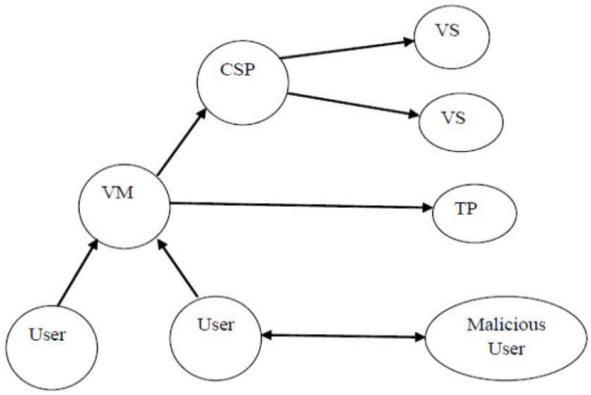


Fig 1: Zombie Attack

According to above figure, Virtual Machine (VM) is described. VM is connected with cloud service provider (CSP) which is further connected with virtual server (VS). Third Party (TP) is available, which is directly connected with virtual machine. There are number of users which are connected to virtual machines. There is also one malicious user which spoofs credentials of connected user and act as a user, the whole process comes under zombie attack.

3. Literature Review

Cloud environment is cost effective and flexible and the data security in a cloud is a challenging task. Cloud resources like infrastructure, platform and software are subject to theft, harm, abuse and unlawful distribution. Data leakage to a competitor is also a major threat in the cloud. Cloud security reduces unauthorized data access and storage. Though there are so many advantages with the cloud, the threat on security hinders towards the technology adoption. Once the technology gets used, the protection and data management of users need to be taken care of by the service providers [3].

Waseem et al. [4] discussed that secure computing environment can protect data manipulation and loss from an unknown source. It can be a system implementation for the use of data and storage. Secured computation minimizes physical computing device damage that may end up with malware. Secure environment drastically reduces the cost of cloud services. Security improves the performance [5] by reducing the data damage, software damage as well as hardware damage. According to Anurag Singh Tomar et al. (201), [6]cloud computing is a collection of different IT technologies. The security issues regarding the data in the cloud involve accessing the data from the cloud securely. Before accessing the service from the cloud, the user will exchange the key with the cloud service provider securely. Initially, the user will generate the key with the help of Primitive Roots 18, 19, and 20 of the group. After that, the user will send the information about key and the CSP can compute the key. In this way, the cloud service provider can perform authentication based on Image authentication. To authenticate the user in the cloud, they use the RSA algorithm. Finally, they encrypt the data with the help of symmetric algorithm. Chirag Modi et al. [7] have developed a methodology which considers security issues as an essential part of cloud systems to design and implement. This was meant for the implementation of secure cloud applications and service. A set of stereotypes was used to define a vocabulary for annotating Unified Modelling Language (UML) based models with information relevant for integrating the security specifications into cloud architectures. Several researchers have proposed cloud architectures like secure

virtualized architecture [8] architecture named CSAViD (Cloud Application SLA Violation Detection Architecture) [9] and architecture for insider threat security reference (ITSRA) for securing cloud environment where the organizations have to prepare adequate security controls. Obviously, decoying information technology was used to confuse the attacker. H. Monowar, et al. [10] have developed a detection component called VMWatcher which aims to support especially anti-malware software for outsider attacks only. However, no one has used SLA violation detection method for malicious insider detection. Likewise, artificial neural network has been used for the detection of malicious insiders in a cloud environment.

In the work by [11], it suggested that since there is high risk involved in cloud computing, it proposed a new mutual authentication scheme where the cloud server and the user can authenticate each other. In order to increase the level of security, they used the secret key that is shared between both the cloud user and the server and also used the steganography to cover image and data [12]. The previous mutual authentication such as plain password, and various existing schemes such as user authentication, time bound base scheme, mutual authentication scheme based on new ticket by using smart cards, reliable and strong user authentication where both the user and the server prove their identity. It states that these schemes have some security lapses, and for that, it proposed a new scheme using four phases: Registration Phase, Login Phase, Mutual Authentication Phase and Password Change Phase. In this scheme, various attacks were tested on and analyses were done to verify its resistivity. The attacks were masquerade attack, replay attack, DoS attack, insider attack.

With this scheme, both user and server shared the same session key, change the password if the need be and also allows mutual authentication. Out-of-band authentication provides human interaction which makes the protocol stronger as no additional hardware or software or training is required for the end user. it posited. Since this scheme did not show any comparison related to performance with other schemes that already exist, resource constrains were not given much priority. The problem with this scheme however, is that, it does not cover zombie attacks and does not detect zombie nodes from the cloud network.

4. Recommended Plan

DDoS, DoS, impersonation, insider, and man-in-the-middle attacks were used to test this suggested technique. These two techniques are effective in mitigating these assaults since they can identify the aforementioned attacks and then entirely stop them from accessing the data. Fig. 1 shows the flow of the algorithm from the start to the finish and provides a step-by-step depiction of the approach

Flowchart

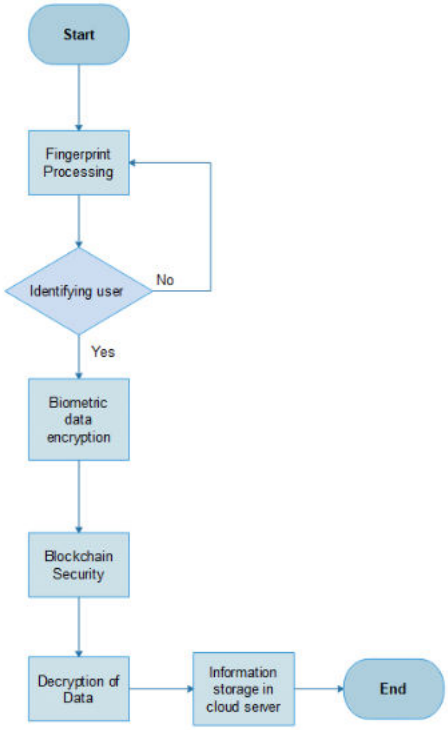


Fig. 2. Flowchart of the proposed scheme

The algorithm used is Diffie-Hellman Key Exchange because of its high anonymity and safe sharing of keys. The asymmetric cryptography for authentication and XOR decipher for encrypting the user public key during login. In order to achieve this, the scheme will be divided into two phases: registration phase and login phase.

4.1 Registration Phase:
1. Registration
2. Mutual authentication based on asymmetric algorithm during registration.
3. Secrete key exchange from both sides and stores on the virtual machine after registration.
4. User selects ID and password and submit to the VM in a hashed form.

4.2 Login Phase:
1. Authentication based on virtual machine side. That is, VM authenticating the user using public key sharing together with Xor cypher encryption technique.
2. VM compares the ID and Password to the one already on the VM.

4.3 The registration process's authentication algorithm
Let q be primitive root, p be prime number, r be random number from the user, pk be the public key, a be the private key. Private key, prime number, public key are the parameters employed by the user.
1. User enter H1 = ajjP.
2. VM computes primitive root for that instance.
3. User computes public key as Y a = QamodP.
4. User computes its Secrete key as k1 = (yb)amodP

4.4 Virtual Machine Side:
1. VM revokes Prime number of the user.
2. VM computes the primitive root of that number (P).
3. VM computes its public key as Y b = QbmodP.
4. VM computes the its secret key as k2 = (ya)bmodP.
5. If k1 is equal to k2, then both the user and VM are genuine.
6. VM store s the k1 for future authentication.
Details processes involved during Login on one-sided authentication by the server.

4.5 At The User's End Algorithm:
i. User enter first parameter which is its public key.
ii. User enter any random number that will be used to generate the session for that particular instance.
iii. User encrypt the public key using the random number generated.
iv. User encrypt the public key using the random number generated.
v. User enter second and third parameters in a hashed form. That is h3 = hash(IDjjpassword).
vi. User sends the encrypted value, random number and the hashed parameters to the server or VM verification.

4.6 Algorithm to Authenticate the User at the End of the Virtual Machine First Phase
i. VM receives encrypted value plus the random number.
ii. VM decrypt the encrypted value using the random number to find the user the user public key using XOR encryption method.
iii. VM revokes its private key used during registration.
iv. VM computes secret key using the public key of the user its private key as k2 = (ya)bmodP.
v. VM compares the k2 computed with k1 stored in the system.
vi. If they are equal, the user is genuine else the user is malicious.

4.7 Second Phase
VM receives the ID and Password of the user and compares it with the one in the server,if it match the user is genuine else the user is malicious. Private key, prime number, public key are the parameters using by the user.

5. Results and Discussion
This section displays the results of the various steps as followed in in the previous Section graphically after successful testing and debugging. Implementation has been done based on three ways; firstly both user and virtual machine authenticating each other, secondly, when user sends the original data to the virtual machine and thirdly, when an attacker captures the original data and send a modified data to the virtual machine. These two scenarios have been implemented as follows:

5.1 Mutual Authentication Stage

Fig. 3. is a screenshot of the mutual authentication page, where both the user and the virtual machine will have to authenticate each other.

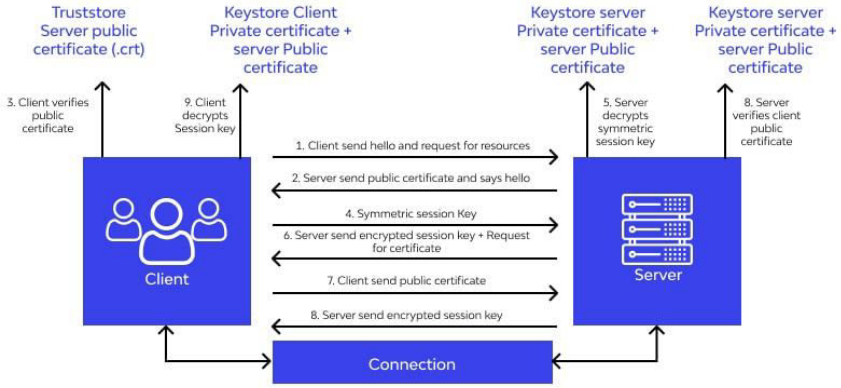


Fig. 3. Step one: Mutual authentication

5.2 User Sending Original Data Stage

Fig. 4. is a screenshot of the user login credentials page, this is where the user will have to send the original data to the virtual machine.

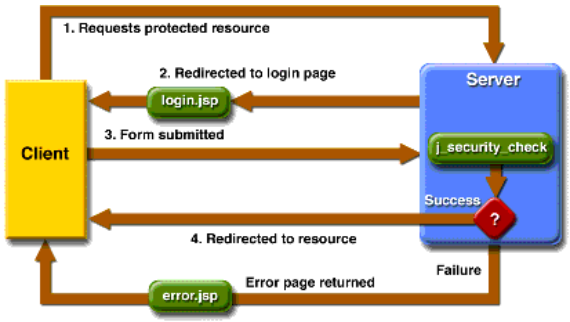


Fig. 4. Step two: User sending original data

5.3 Virtual Machine authentication Stage

Fig. 5 displays the processes at the back end of the virtual machine when it is authenticating the user during the login process.

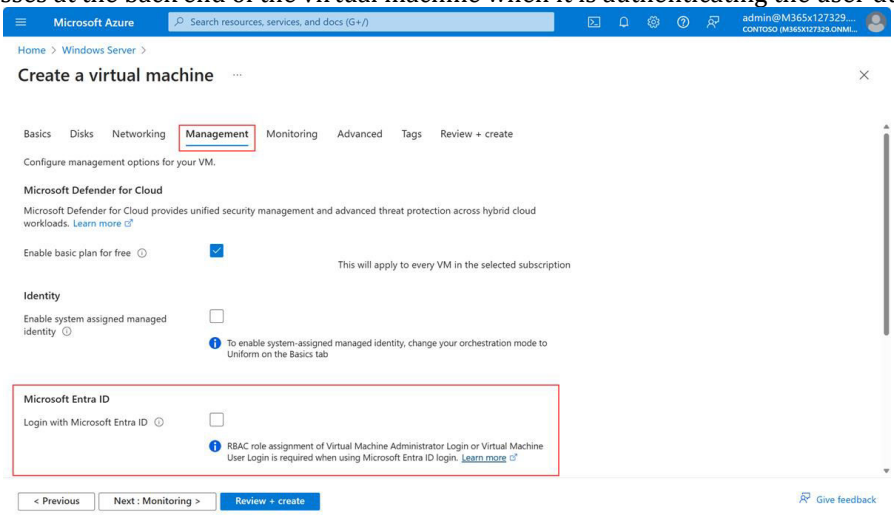


Fig. 5. Step three: VM authenticating user during login

5.4 Virtual Machine Verification Stage

Fig. 6. is a screenshot of the second stage of authentication, that is, the verification page, where either a valid user and a malicious user is identified.

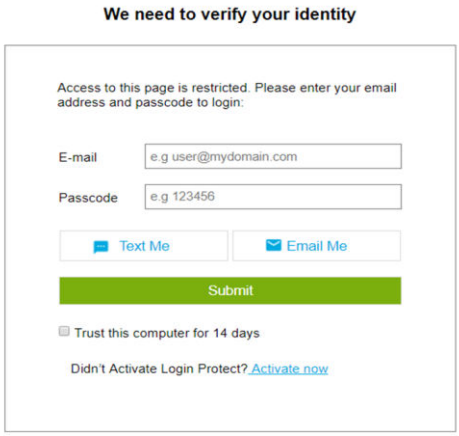


Fig. 6. Step four: VM verifying user details

5.5 Attacker capture and Modified Data Stage

Fig. 7. is a screenshot of the page where a malicious user is detected by a comparison of the login credentials.

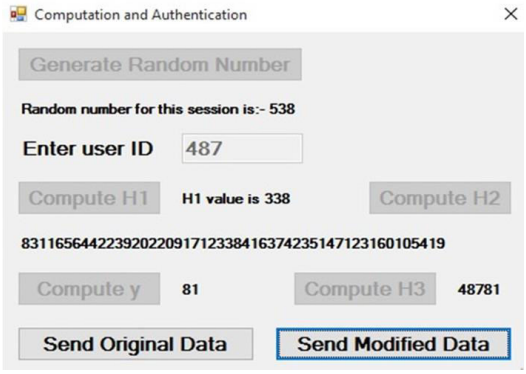


Fig. 7. Attacker sending modified data during login

5.6 Virtual Machine Authenticating Stage

Fig. 8. is also a screenshot of the stage where the VM will authenticate the modified data being received.

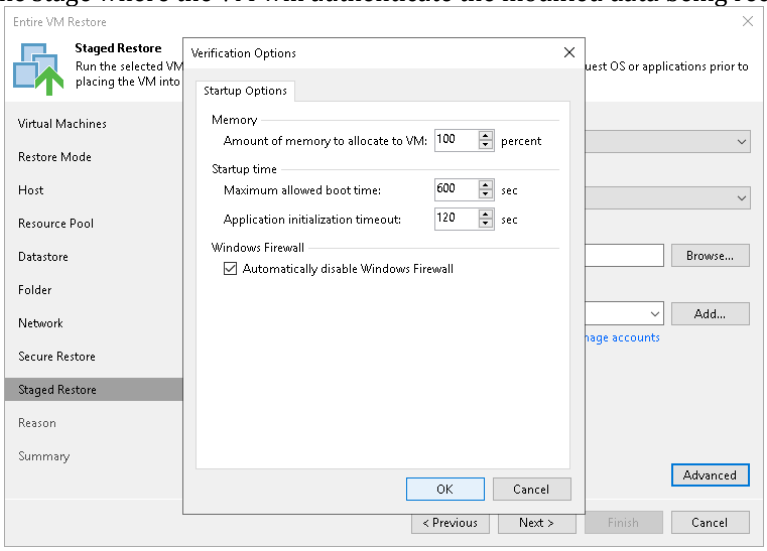


Fig. 8. VM modified authenticating user data

5.7 Virtual Machine Verification Stage

Fig. 9. is a screenshot of a verification process of the data that has been modified by the user by the VM after it has authenticated in Fig. 8.

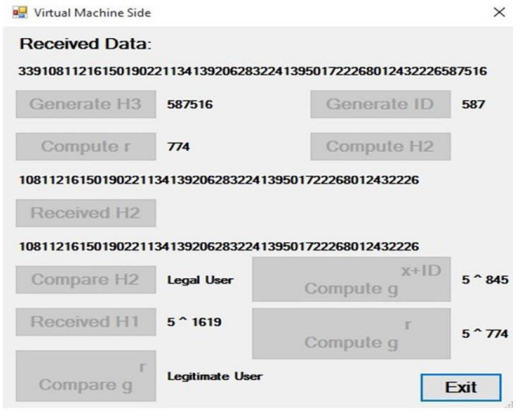


Fig. 9. VM modified verifying user data

5.8 Integrity Evaluation

This section will evaluate the aforementioned method of mutual authentication during registration and virtual machine authentication during login against a variety of security vulnerabilities. It looks like this:

5.9 DoS and DDos attacks:

An attacker acquires the public key, computes the ID and password, and encrypts it using the XOR cypher. The virtual machine uses the XOR Decipher to calculate the user's public key after capturing the encrypted value together with r. The virtual then calculates K2 using the public key and a few parameters calculated during registration. It indicates that the user is unlawful and that a DoS attack is not possible if the computed k2 does not match the k2 of the legitimate user. Additionally, because logging in requires registration and a lot of processing on the part of the user, it is not viable for an attacker to execute DDos assaults on the virtual machine at the same time.

5.10 Man In The Middle Attack

If an attacker obtains pk and r and changes either one of them and sends to Virtual machine. Virtual machine computes k2 and matches it with the legal user k2, and if computed k2 is not matched with legitimate k2, It means the user is not legal and attack is not feasible.

5.11 Insider Attack

An insider attacker needs user pk and Password before it can gain full control of the user data and exposes it. But since these parameters cannot be gotten at the virtual machine side, it is not feasible to apply this attack.

5.12 Impersonation Attack

An Attacker obtain an ID of the User, But an attacker does not know k2 and r because k2 is shared between the user and the virtual machine during registration, and r is random number that infeasible.

5.13 Replay Attack

Even if the attacker manages to get most of the parameters of the legal user right such as pk,ID and password, it is not feasible applying it because of r, and when r changes during replay, everything about the authentication goes to ruination.

6. Conclusion

Cloud computing has emerged as one of the most important development tools for businesses, governments, and non-governmental organisations. However, there is a high likelihood of a zombie attack in the cloud, which might result in decreased network performance in terms of bandwidth utilisation and speed delays. The effective method for identifying malevolent users on a network using robust server and mutual authentication was provided in this study, all without affecting network throughput. The suggested method was used to test DoS attacks, impersonation attacks, insider assaults, and man-in-the-middle attacks. To identify advanced assaults, this approach will be extended in the future to additional optimum encryption schemes like RSA and GARN.

7.References

[1] Frederick R. Carlson. Security analysis of cloud computing; 2014.
[2] Anurag Singh Tomar. Energy studies, and Shashi Kant Shankar. to detect and isolate zombie attack in cloud computing; 2017.
[3] Ahmed. M., Pal, R.,Hossain, H.M., Bikas, M. , Hasan, M.K., "NIDS: A Network Based Approach to Intrusion Detection and Prevention", Computer Science and Information Technology—Spring Conference; pp.141–144,2009.
[4] Waseem, M., Lakhan, A., and Jamali, I.A., "Data Security of Mobile Cloud Computing on Cloud Server," Open Access Libr. J., 3, 2016.
[5] Khorshed, M.T., Ali, M.S., and Wasimi, S.A., "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Futur. Gener. Comput. Syst., 28 (6), pp. 833–851, June 2012.
[6]Anurag Singh Tomar. Energy studies and Shashi Kant Shankar. to detect and isolate zombie attack in cloud computing; 2017.
[7] Chirag Modi, Dhiren Patel, Bhavesh B orisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan, (2013), "A survey of intrusion detection techniques in cloud", Journal of Network and Computer Applications, 36(1), pp. 42–57.
[8] WU, H., DING, Y., WINER, C., and YAO, L., "Network security for virtual machine in cloud computing", In Proceedings of IEEE 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), pp.18-21, 2010.
[9] ALZAIN, M., PARDEDE, E., SOH, B. and THOM, J, "Cloud computing security: from single to multi clouds, In Proceedings of IEEE 45th Hawaii International Conference on System Science (HICSS), pp.5490-5499,2012.
[10] Monowar, H., Bhuyan, D., Bhattacharyya, K., and Kalita, JK, (2014), "Network Anomaly Detection: Methods, Systems and Tools", IEEE Communications Surveys and Tutorials, 16(1), pp.303-335.
[11] Nimmy K, Sethumadhavan M. Novel mutual authentication protocol for cloud computing using secret sharing and steganography. 5th International Conference on the Applications of Digital Information and Web Technologies, ICADIWT 2014, 2014;5(2):101106.
[12] Tharam Dillon, Chen Wu, Elizabeth Chang. Cloud computing: Issues and challenges. Proceedings- International Conference on Advanced Information Networking and Applications, AINA. 2010;2733.