Asian Journal of Research in Computer Science

6(2): 46-56, 2020; Article no.AJRCOS.62109
ISSN: 2581-8260

Identifying and Isolating Zombie Attack in Cloud Computing

Peter Awon-natemi Agbedemnab[1*], Salifu Abdul-Mumin[1] and Zakaria Abdulrahim[1]

[1] *Department of Information Systems and Technology, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana.*

Authors' contributions:

This work was carried out in collaboration among all authors. Author ZA did the preliminary analysis and wrote the first draft of the manuscript. Authors PAA and SA re-organized the draft and did further analysis. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2020/v6i230157
Editor(s):
(1) Prof. M.A.Jayaram, Siddaganga institute of Technology, India.
Reviewers:
(1) A. Prasanth, PSNA College of Engineering and Technology, India.
(2) Gundu Srinivasa Rao, Dravidian University, India.
(3) Rajesh Thakare, Rashtrasant Tukadoji Maharaj Nagpur University, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/62109

Received 10 August 2020
Accepted 14 October 2020
Published 25 October 2020

Original Research Article

ABSTRACT

The cloud computing architecture is a berth in which third party, virtual machine and cloud service providers are involved in data uploading and downloading. A major challenge in this architecture, however, is the security of the data as there exist various forms of attacks from malicious people and devices. Among these security attacks, the zombie attack is the most advance type of attack. The zombie attack reduces network performance in terms of delay and bandwidth consumption. With zombie attack, some malicious users may join the network which, in turn takes off the data of legitimate users and at the same time enable zombie nodes to communicate with a virtual machine on behalf of the legitimate user. In this paper, a technique based on strong authentication which, is able to detect malicious users from a network and isolates them from the cloud architecture is proposed.

Keywords: Authentication; cloud computing; security; malicious user; virtual machine; zombie attack.

**Corresponding author: pagbedemnab@cktutas.edu.gh;*

1 INTRODUCTION

Cloud computing has become the order of the day as the world of businesses and other firms are moving from the local way of keeping records to cloud infrastructure format. Cloud computing companies have been estimated to grow at a rate of 20 percent compounded annually according to the technology consulting firm Gartner [1].

Cloud computing is a virtualized platform that offers a network only on-demand service and for smooth access to computing vital resources such as applications, storage, servers and network. It can be characterized into two forms: Deployment models and Service models. The deployment models include private cloud, public cloud, community cloud, and hybrid cloud. Service models on the other hand, include Software as a Service(SAAS), Infrastructure as a Service (IAAS), and Platform as a Service (PAAS).

Cloud computing has made it possible for users to use various digital gadgets such as Personal Computers, Laptops, Smartphones and other various machines to connect virtually. Since the user is the client, he or she is able to use and modify data stored on the cloud by him or her and pays for the services rented by the cloud owners. Due to this, users do not have to worry about the hardware cost for putting up cloud environment, hence it is very economical for the user. Because the cloud computing is internet based, it provides various resources such as shared, software and information to the various computers and devices on demand. Which means that the user pays for whatever he uses.

Cloud computing comes with it a lot of benefits and advantages but the challenges associated with it too are enormous especially, ill-minded users who can access any other user data at the blind side. Network security, information security and many other security types like the computer security together make the term Cloud Security. It gives the wide set of technologies, rules and controls that are used to provide the security to data and several applications that exist with the cloud computing environment [2]. Security is the most pressing need to any service. But security issues such as downtimes, data losses, botnets, spoofing, phishing, sniffing, and password cracking are eminent in cloud computing. Now, all these security issues need to be addressed in one way or the order to fully gain control of the cloud computing. It is in this light that this paper proposes an efficient technique to detect and isolate zombie attack thereby mitigating its attack in cloud computing. The rest of the paper is organised as follows: Section 2 reviews some existing works on the subject matter, Section 3 presents the proposed algorithm and the steps to identifying and isolating zombie attacks, with detail screens showing the workings of the technique. Section 4 presents an analysis of the workings of the proposed technique.The paper is concluded in Section 5.

2 LITERATURE REVIEW

A work by [3] posited that cloud computing is a technology where the computing resources are being provided by cloud services providers to host their data or perform their computing tasks based on demand and only pay as per usage. They used the exact methods such as anti-malware, anti-virus, honey pots and intrusion detection systems. Also, to create high time decisions on the virtual machines and storage of the data, they used the Cloud Controller (CLC) which is the main interface for the clients and it is the top level management for the cloud, Node Controller (NC) which is implemented on each physical server and it is responsible for managing the client virtual machine, Walrus Storage Container (WSC) which provides user data and storage for virtual machine images, Cluster Controller and finally Elastic Block Storage. They also elaborated on the design choices for securing customer virtual machines in the cloud and proposed techniques to deal with the attacks. Their model enables to differentiate traffic from each virtual machine even if multiple virtual machines on a VMM are sharing a single IP address, [3]

The categories of attacks were also highlighted by [2]; they stated that at the network layer, different types of attacks affect the cloud computing such as Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, Spoofing, Man in the Middle attacks, Routing information protocol (RIP),

DNS Poisoning attacks, Service Injection attacks, Phishing attack among others and that these categories of attacks can negate the confidentiality and the integrity of the cloud data or resources. The paper went further to use the Bayesian classifier for the anomaly detection and snort-based NIDS as detection based on signature. Based on performance and quality, they used eucalyptus and installed it on ubuntu OS, in order to monitor the traffic, they installed Wire-shark on front end and back-end of the cloud using scrappy tools in order to differentiate the base rates with various size of data. The problem with this proposed technique is that the cost of computation also increases.[4]

[5] used the pie chart for security issues; security issues with grouped categories, solutions citation and then went further to show the comparison between citations and grouped types. Using radar charts, security issues and solutions were made. In order to identify threats, security alliance was used. This paper was intractable due to the fact that proper definition of how to detect threats and provide security solutions were not addressed. [6] used another technique to identify and analyze current state and the most vital security issues for cloud computing and also providing counter-solutions for these risks. One of the countermeasures is hyper-safe. The main task of hyper safe to protect the hypervisors by using the technique is non bypass able memory lockdown and then evaluates the effectiveness of the hypersafe. They also use the Platform of cloud computing that is trusted. This Trusted Cloud Computing Platform (TCCP) [2] allows users to describe the environment before installing the virtual machine. It is concerned with the analysis of security issues for cloud computing. The Traditional security techniques is unable to perform well in cloud computing due to the complex structures and methods that is used to combine different technologies.

In the work by [7], 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 [8]. 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.

3 PROPOSED SCHEME

This proposed scheme was tested using DDos attack, Dos attack, impersonation attack, insider attack and man in the middle attack. These two methods are good for mitigating these attacks because it will be able to detect the attacks mentioned above and then prevent them completely from getting access to the information. The step by step representation of the technique is depicted in Fig. 1, which illustrates the flow from the beginning to the end of the algorithm.

3.1 Flowchart

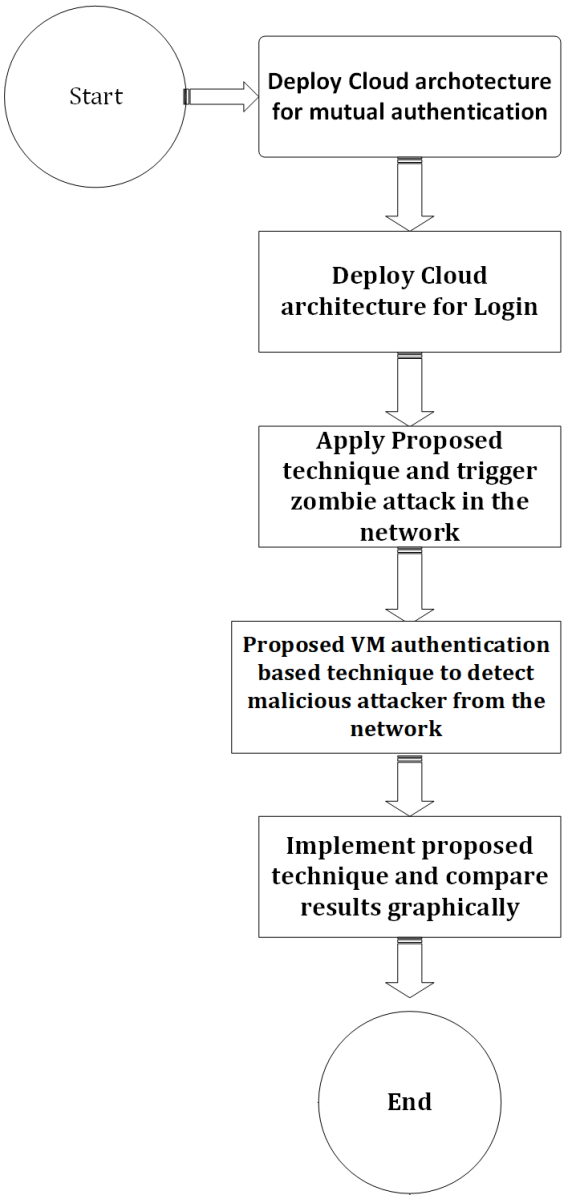

Fig. 1. Flowchart of the proposed scheme

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.

3.2 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.

3.3 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.

3.4 Algorithm for Authentication During Registration:

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 $H1 = a||P$.
2. VM computes primitive root for that instance.
3. User computes public key as $Ya = Q^a modP$.
4. User computes its Secrete key as $k1 = (yb)^a modP$

3.5 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 $Yb = Q^b modP$.
4. VM computes the its secret key as $k2 = (ya)^b modP$.
5. If k1 is equal to k2, then both the user and VM are genuine.
6. VM store s the k1 for future authentication.

3.5.1 Details processes involved during Login on one-sided authentication by the server.

ALGORITHM AT THE USERS END:

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 $h3 = hash(ID||password)$.

vi. User sends the encrypted value, random number and the hashed parameters to the server or VM verification.

ALGORITHM AT THE VIRTUAL MACHINE END TO AUTHENTICATE THE USER
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 $k2 = (ya)^b modP$.

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.

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.

4 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:

4.1 Mutual Authentication Stage

Fig. 2. is a screenshot of the mutual authentication page, where both the user and the virtual machine will have to authenticate each other.

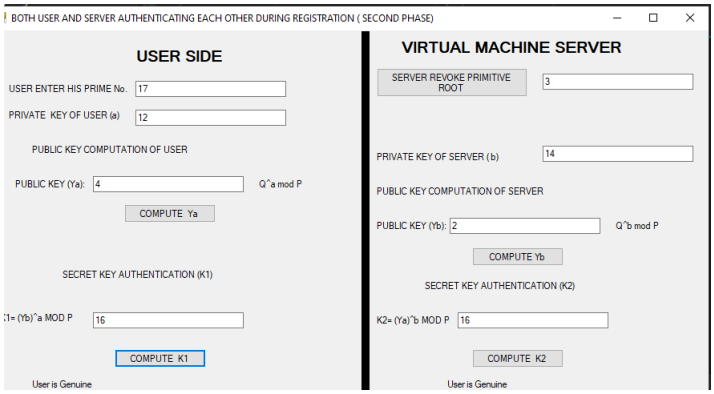

Fig. 2. Step one: Mutual authentication

4.2 User Sending Original Data Stage

Fig. 3. 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.

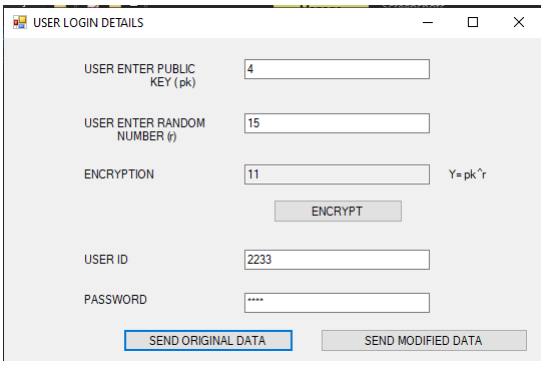

Fig. 3. Step two: User sending original data

4.3 Virtual Machine authentication Stage

Fig. 4. displays the processes at the back end of the virtual machine when it is authenticating the user during the login process.

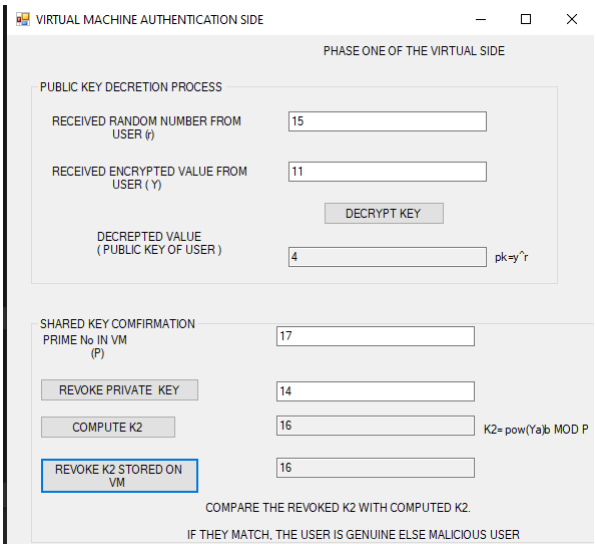

Fig. 4. Step three: VM authenticating user during login

4.4 Virtual Machine Verification Stage

Fig. 5. 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.

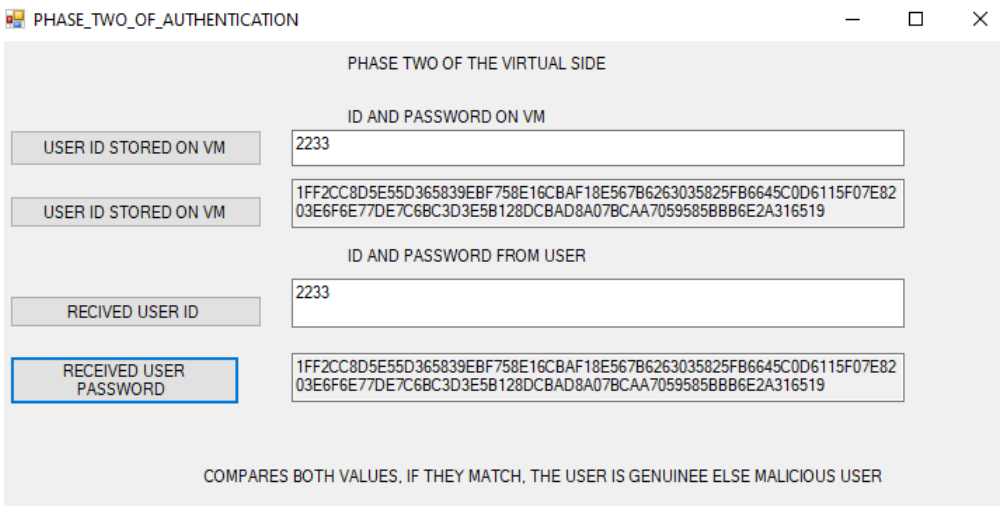

Fig. 5. Step four: VM verifying user details

4.5 Attacker capture and Modified Data Stage

Fig. 6. is a screenshot of the page where a malicious user is detected by a comparison of the login credentials.

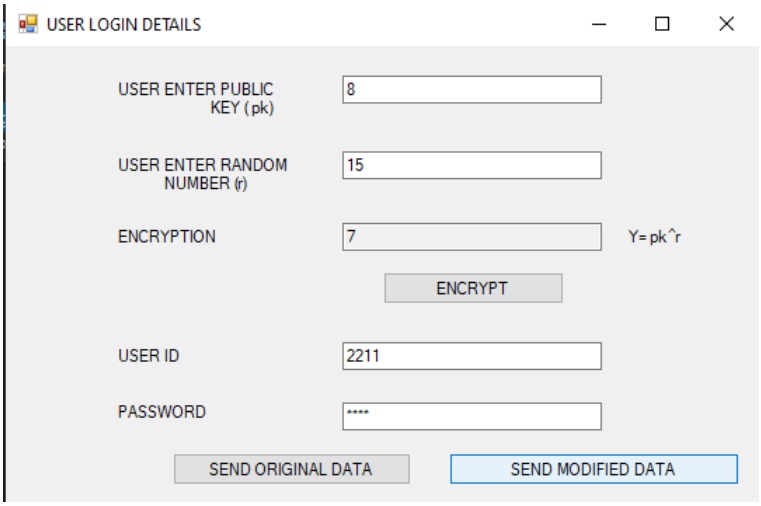

Fig. 6. Attacker sending modified data during login

4.6 Virtual Machine Authenticating Stage

Fig. 7. is also a screenshot of the stage where the VM will authenticate the modified data being received.

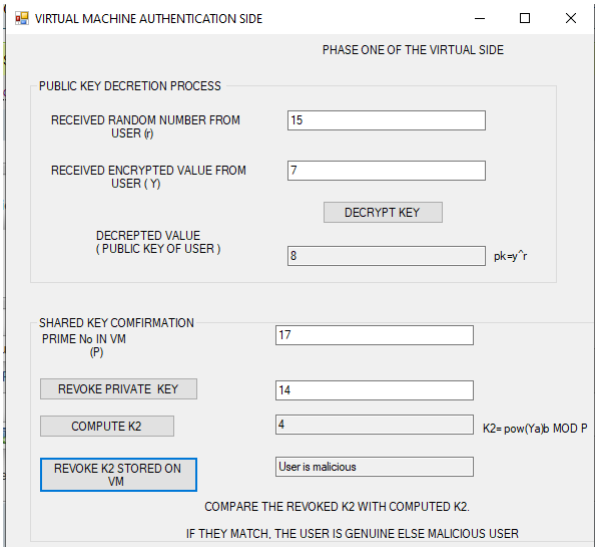

Fig. 7. VM modified authenticating user data

4.7 Virtual Machine Verification Stage

Fig. 8. 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. 7.

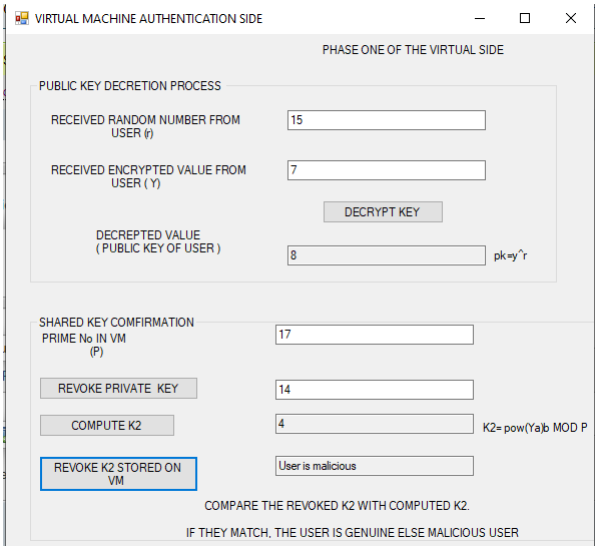

Fig. 8. VM modified verifying user data

4.8 Security Analysis

In this section, various security attacks will be tested using the above technique based on mutual authentication during registration and virtual machine authentication during login. It is as follows:

4.8.1 DoS and DDos attacks:

An attacker obtains public Key and encrypt it with r using XOR cypher and also computes ID and password. Virtual machine captures the encrypted value together with r and computes public key of user using XOR Decipher. The virtual then uses the public key plus some parameters computed during registration to calculate K2. If calculated k2 is not matched with k2 of the legal user, then it means user is illegal and it is not feasible to apply Dos attack.

Also, since there is registration and much computations during login from the user side, it is not possible for an attacker to apply DDos attacks on the Virtual Machine at the same time and so therefore not feasible to achieve.

4.8.2 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.

4.8.3 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.

4.8.4 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 is valid for only one session. So, this attack is infeasible.

4.8.5 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.

5 CONCLUSION

Cloud computing has become a major tool for development in the business world as well governmental and non-government organizations. But the possibility of a zombie attack is eminent in the cloud, which can lead to the reduction network performance in terms of bandwidth usage and delay in speed. This paper presented an efficient technique for the detection of malicious users from the network based on strong mutual authentication and server authentication without impeding the network performance. Man in the middle attack,insider attack,impersonation attack, DoS attacks were tested using the proposed technique. In future, this work will expanded to other optimal encryption techniques such as RSA and GARN in order to detect advance attacks.

COMPETING INTERESTS

The authors declare that they have no competing interests.

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] Udaya Tupakula, Vijay Varadharajan, Naveen Akku. Intrusion detection techniques for infrastructure as a service

cloud. Proceedings - IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC. 2011;744751.

[4] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan. A survey on security issues and solutions at different layers of cloud computing. Journal of Supercomputing. 2013;63(2):561592.

[5] Nelson Gonzalez, Charles Miers, Fernando Red, Marcos Simpl. Open access a quantitative analysis of current security concerns and solutions for cloud computing. 2012;118.

[6] Keiko Hashizume, David G. Rosado, Eduardo Fernandez-Medina, Eduardo B. Fernandez. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2013;4(1):113.

[7] 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.

[8] Tharam Dillon, Chen Wu, Elizabeth Chang. Cloud computing: Issues and challenges. Proceedings - International Conference on Advanced Information Networking and Applications, AINA. 2010;2733.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/62109