International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 45 • 2016

To Detect and Isolate Zombie Attack in Cloud Computing

Simanjot Kaur[a] Anurag Singh Tomar[a] Shashi Kant Shankar[a] and Manmohan Sharma[a]

[a]*Department of Computer Science and Engineering, Lovely Professional University, Jalandhar, Punjab, India.*

E-mail: simanshahi658@gmail.com

Abstract : The cloud computing architecture in which third party, virtual machine and cloud service provider are involved for data uploading and downloading. Security is the main issue for cloud computing architecture. Among security attacks zombie attack is the most advance type of attack. This attack reduces network performance in terms of delay and bandwidth consumption. In the zombie attack, some malicious user may join the network which spoof data of the legitimate user and zombie nodes start communicate with virtual machine on the behalf of legitimate user. In this proposed work, the technique based on the strong authentication which has been detect malicious user from the network and isolates them from the cloud architecture.

Keywords : *Cloud Computing, Security, Malicious User, ID, Server Authentication.*

1. INTRODUCTION

Cloud computing is the recently evolved computing terminology based on the utility and the consumption of computing resources. Cloud Computing is an environment which offers the network only on-demand and for convenient access to computing resources like applications, storage, networks, servers and the another services which are effective. Cloud is a centralized data in which a user, who is actually the client in cloud, can retrieve and modifies the stored data. It means that the user or the client who is using the service of cloud has to pay for whatever he/she is using or being used and served. It is a technique which gives a huge amount of applications under different topologies and these topologies provide some new specialized services. Cloud computing provides shared resources, software[10] and the information to the various computers and devices on demand because cloud computing is an internet based.

E.g. Drop box are a service of cloud and any user using their cloud either with premium account (account with some extra features) or free account. The problem of cloud computing is that any user can access the data of other user without the knowledge of that user.

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. Security is the most concerning point to any service. Only security ensures the privacy and integrity the cloud data. There are many types of security issues exist:

1. Data Loss
2. Downtimes
3. Phishing
4. Password Cracking
5. Botnets
6. Sniffing
7. Spoofing
8. and Other Malware

2. LITERATURE REVIEW

In 2011, Udaya Tupakula et.al[1] Cloud computing is the one important technology where all the people can use the resources of cloud provided by cloud service provider to complete their tasks and only pay as per usage. They use the exact techniques such as intrusion detection system, anti-malware, honey pots, as etc. They used the host based tools to detect the attacks and use the virtual machine monitor to permits to run multiple operating systems. They also use the Cloud Controller (CLC), Cluster Controller (CC), Node Controller (NC), Walrus Storage Controller (WSC) for create high decisions on the virtual machines. They use the different victor components are:

1. Packet differentiator.
2. Detection or prevention engine.
3. Shared packet buffer.
4. Operating system and repository.
5. Analyzer

In this, they show the performance based on unmarked packets and the marked packets. They use the two virtual machine monitor on hardware layer to detect the attack. To enable different traffic from every virtual machine even if many virtual machine on Virtual machine monitor have a single ip address that is sharing.

In 2012, Chirag Modi et.al[2] includes the survey on various security issues and solutions at different layers of cloud Computing. In this paper, they discuss the various threats to cloud computing are:

1. Changes to business model.
2. Insecure application program interface.
3. Malicious insiders.
4. Data loss.
5. Data leakage.
6. Service hijacking.
7. Identity theft
8. Risk Profile

These types of threats are affecting different types of services of cloud like Software as a Service, Platform as a Service and Infrastructure as a Service. They define the different types of attacks on cloud computing such as zombie attack, Man in the middle attack[12], spoofing attack, service injection attack, phishing Attack and backdoor channel attack as etc by exploit flaws in the system. They detect these attacks by using Intrusion detection system, Intrusion prevention system, using secure hypervisors, by proper configuration of secure socket layer and detect the mails that are spam and providing better authorization and authentication. It provides robust separation among different virtual machines to detect these attacks. They show the issues of the security at the dissimilar layers in cloud. Different layers are cloud user layer, cloud service provider layer, cloud virtualization layer and data storage and internal network layer. One solution of this to use the XML (Extensible Mark-up Language) signature and XML encryption to increases the security of browser. They also used the simple object access protocol. They also use access control policy language (ACPL) for describes the policies in cloud and also use access control oriented ontology system (ACOOS) to provide semantic information. In this, main concept is building trust on the cloud in future research area.

In 2012, Modi et.al[3] include the cloud computing suffers from different types of attacks at the network layer such as DoS attacks, DDoS attacks , Man in the Middle attacks, Routing Information Protocol (RIP) attack, DNS poisoning attack as etc. But the DoS and DDoS attacks are the insider attacks. These different types of attacks can affect the integrity, confidentiality of resources or the data that are provided by cloud. In this Paper, use the Bayesian classifier for the anomaly detection and snort based NIDS[16] is used as detection based on signature and there are different postions of NIDS in cloud such as:

1. On front end.
2. On back end.
3. On Virtual machine.

For showing the results of proposed NIDS based on performance and quality, they used eucalyptus and installed it on ubuntu operating system and sending the custom packets on the network by using scapy tool and to monitor the traffic by installed wireshark on front end and back end of cloud and show the results on different base rates with different size of data. In this paper, the snort based IDS is not properly defined but mention in the starting. But in general our proposed NIDS is capable of detect higher number of intrusions with false negatives and low false positives for cloud computing environment and also detect well known and unidentified attacks. By improving the number of partitions, then the accuracy of the proposed system is also increase. But, the problem arises is that the cost of computational is also increases.

In 2012, Gonzalez Nelson et.al[4] includes the analysis of security concerns and solution of cloud computing. It describes the security is considered as a key requirement for cloud computing as a feasible multipurpose solutions. It includes the availability of data, confidentiality of data. It describes the three services of cloud that are SaaS, IaaS and PaaS. In cloud computing security, each category includes the various security problems and that are divide into seven parts:

1. Network security
2. Interfaces
3. Data security
4. Virtualization
5. Governance
6. Compliance
7. Legal issues

In this paper, they use the Pie Charts for Security concerns; security Concerns with group categories, solution citations and then shows the comparison between citations and grouped types. Comparison between security concerns and security solutions using radar charts. They also used the cloud security alliance to identify top threats. But, this paper is not feasible because in this not proper define how to detect threats and provide security solutions.

In 2013, Keiko Hashizume et.al[5] shows the relationship between the threats, vulnerabilities and countermeasures. They use the different countermeasures like hypersafe that is the approach that provides control flow integrity. The main task of hypersafe to protect the hypervisors by using the technique is non bypassable 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) [17] allows users to describe the environment before installing the virtual machine. It is concerns with the analysis of security issues for cloud computing. The Traditional security methods cannot perform well in cloud computing due to the complex structure that is used for combine different technologies. In future, we have to make this architecture easier by using different mechanisms.

In 2014, Jen-Ho Yang et.al[6] in architecture of Cloud Computing, authentication scheme based on user is an essential security tool since it offers authentication based on accounting for the clients of cloud. They proposed user authentication scheme centred on new ID. Before this proposed scheme, there are many authentication scheme based on the ID like remote user authenticate scheme based on Dynamic ID, its permits clients to change and select the password free of cost and do not keep[11] some verifier table. In this das, demanded that this scheme is fully secure against various attacks. But Wang notices that it is run on the insecure channel, so it is unsecure[13]. Then the Improvement has been done on the existing scheme user authentication scheme centred on new ID. But, there are many security problems, security flaws, high communication and computational cost are found in these schemes. Due to these problems, yang and pie propose a new scheme and in this scheme includes three different parts:

1. User
2. Server
3. ID Provider

Each of these has different responsibility. In this novel scheme, they use the two phase's, first phase is that in which the user register and second is that phase in which both the user and the server verify its identity earlier communication starts. They use one way hash function and XOR to reduce the computational and communication cost. This scheme can be applied on the multiple servers so the client preserve single message of authentication to sign in several virtual machine and they also analyze the performance amongst technique which is planned and existing scheme and also show the security analysis of different attacks such as replay attack, impersonation attack, insider attack and outsider attack.

In 2014, D. Nimmy K et.al[7] includes an essential technology of cloud computing is proper authentication that defines connection to outside environment are mutual and risks are high. They planned propose a new mutual authentication based scheme where the user and the cloud server can authenticate one another. In 2015, Shashi Kant Shankar, et.al[21] have proposed unique novel technique of mutual authentication and ECC in Wireless Sensor Network. In this, they use the steganography to cover the image and data and also use the secret key that is shared between both the cloud server and user. One of the main challenges is mutual authentication because both the user and server can authenticate themselves before the communication begins. There are various methods of authentication like plain password etc. The various existing schemes such as user authentication scheme based time bound, mutual authentication scheme based new ticket[14] that using smart cards, strong and reliable user authentication scheme[15] in which each user and the server has proven its identity. But in these schemes has found many security problems and the novel mutual authentication scheme for cloud computing using secret sharing and steganography has been proposed. In the proposed scheme, different phases are used that are:

1. Registration Phase
2. Login Phase
3. Mutual Authentication Phase
4. Password Change Phase

This scheme has also show the security analysis of different attacks and analyses the resistivity of this scheme to various attacks such as replay attack, masquerade attack, DoS attack, insider attack. A significant scheme based on mutual authentication for cloud computing with several features of security such as the user and cloud server shared the session key, change the password and mutual authentication. In this novel technique based on scheme that can use the out of band (OOB) authentication to provide the interaction with human that builds the scheme stronger and none use of any software and the hardware for the end users. But this paper has not shown any comparison related to performance with the schemes that already exists. This scheme can oppose many widespread attacks such as masquerade attack, insider attack, replay attack and DoS attack. But this propose scheme do not resist any other attack such as zombie attack and do not detect the zombie nodes from the cloud network.

In 2014, Anurag Singh Tomar et.al[8] Cloud computing is a collection of various technologies of IT. The security issues about the data in cloud involve accessing the data securely from cloud. Before accessing the service from the cloud, user will exchange the key with cloud service provider securely. Firstly, with the help of Primitive Root[18, 19, 20] of group, user will generate the key and after that user will send the information about key and with the help of CSP can compute the key. In this, cloud service provider can perform authentication based on Image authentication. To authenticate the user in cloud, they use the RSA algorithm and after that they encrypt the data with the help of symmetric algorithm. In this paper, they can use secure mechanism to access the data from cloud. In this secure mechanism, they can use the three phases are-

1. Registration phase
2. Image based authentication phase
3. Key exchange phase.

In the First phase, the user was interacting with the CSP to register itself to access the data from the cloud securely. Then the CSP provides some images to the user and out of these images the user is sanctioned to select the images in the form of order and also provides password corresponds to those images. In the second phase, the user can generate the key and also compute some parameters and send those parameters to the CSP. After that the CSP received that parameters that is send by user and find the key from those parameters by using the different steps of key generation. The mechanism that is used is secure against different attacks such as impersonation attack, man in the middle attack and insider attack.

In 2015, E. Prachi Deshpande et.al[9] Cloud computing is a collection of sources in order to enable resource sharing in terms of scalability, services that are delivered on demand over the network. Classification and analyze on different threat related to security in the environment of cloud computing alongside with classification of intrusion detection system in short term. Different threats are commenced onto cloud private model and finding and avoidance carried out through snort technique. The snort is freely available which usages the procedure related to name for identifying malicious users. Snort is free and widely usages. Its platform like GNU, windows, Linux and regularly updated. Snort Captures data packets related to network, then check contents through by default well-known packet pattern to some association. Basically, the way of snort exist inline and protects system. To analyze efficiency by using the two threats of security: the Flooding attack and Port scan attack. Threats associated with security such as port scan and flooding sprang onto open Nebula frontend to authenticate the cloud behaviour with the help of hping. In future work, we proposed deploy and design of comprehensive IDS for detection of threats of security with a capacity.

3. PROPOSED WORK

Due to number of reasons, Cloud computing unavoidably presents novel challenging threats of security. Initially, Cloud Computing is not a data warehouse of third party. The data that is stored in the cloud might be modified, deleted and reordered by the malicious users in cloud. Data can be accessed by any user at any time so data accuracy is another issue in cloud. Analysis of performance and security shows that the technique that is planned is extremely resourceful and hardy in contradiction of failure of Byzantine, server crashing attacks and malicious data changing attack. In this proposed work, to detect and isolate the zombie attack, novel authentication technique has been proposed which is based on the server authentication.

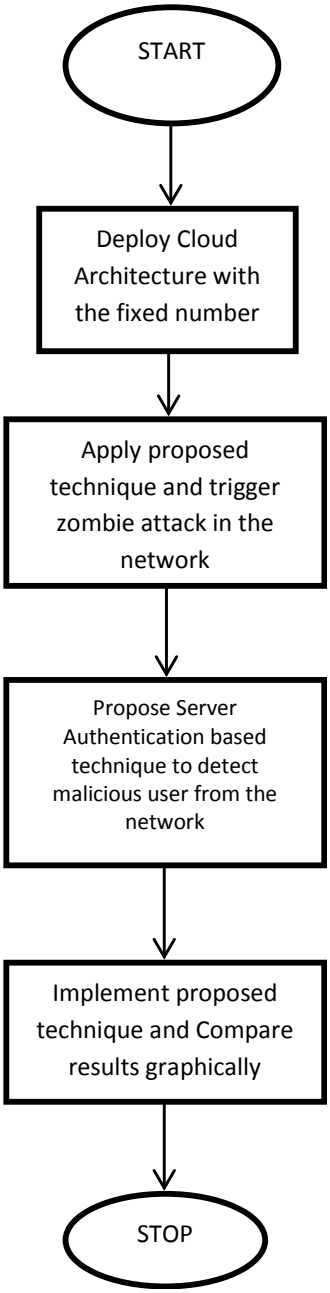

Figure 1: Proposed Technique Work Flow

Table 1
Proposed Authentication Mechanism

User	*Virtual Machine*
Where g is primitive root; x is shared secret between user and virtual machine; r is the random number; ID is the identity of the user and it is known to Virtual machine; y is any number; H1, H2 and H3 are three parameters using by user. **1.** User computes first parameter, $H1 = gx + ID + r$ **2.** Then again user computes second parameter, $H2 = H(ID \| x \| r)$ **3.** Then again user computes third parameter, $H3 = (ID \| y)$ where $y = x$ XOR r **4.** Then user concatenates three parameters, H1||H2||H3 H1||H2||H3 ⟶	Upon receiving these three parameters, virtual machine performs following operations based on mutual authentication: **1.** Virtual machine checks the values of parameter H3 and match the ID of the user with the ID that is stored in its database, if it is match. **2.** Then Virtual machine computes $r = y$ XOR x **3.** Then Virtual machine checks the value of H2 and calculate $H(ID \| x \| r)$, if it is equal, it means user is legitimate, otherwise not legitimate. **4.** If User is legitimate, then virtual machine checks the value of H1 parameter and computes: $gx + ID + r / gx + ID = gr$ **5.** If computed value (gr) is match with the genuine value of the user, it means user is legitimate user.

4. PROPOSED WORK IMPLEMENTATION

In this proposed work, implementation has been done based on two cases; firstly when user can send the original data to the virtual machine and secondly, when an attacker can capture the data and send modified data to the virtual machine. These two cases have been implemented following:

4.1. When Original Data is Send

4.1.1. Common Parameters Agreement

User can choose any prime number and send it to the virtual machine, if both user and virtual machine are agree upon this prime number, then user can find primitive root of that prime number. User can also enter the Shared Secret key between the user and the virtual machine.

Figure 2: Parameters agreement

4.1.2. Computation

User can generate the random number for this particular session and also enter the ID of the user and then compute H1, H2, *y*, H3. User can send original data that contain H1||H2||H3 to virtual machine after data computation.

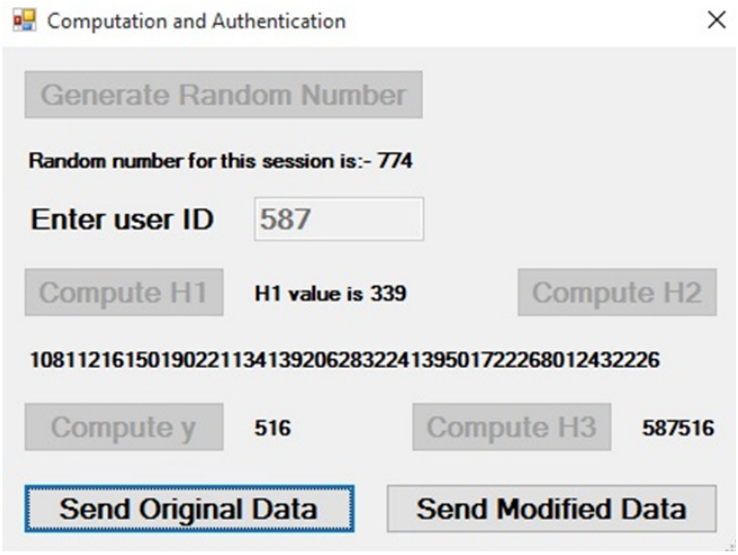

Figure 3: Data Computation and Original Data

4.1.3. On Virtual Machine Side

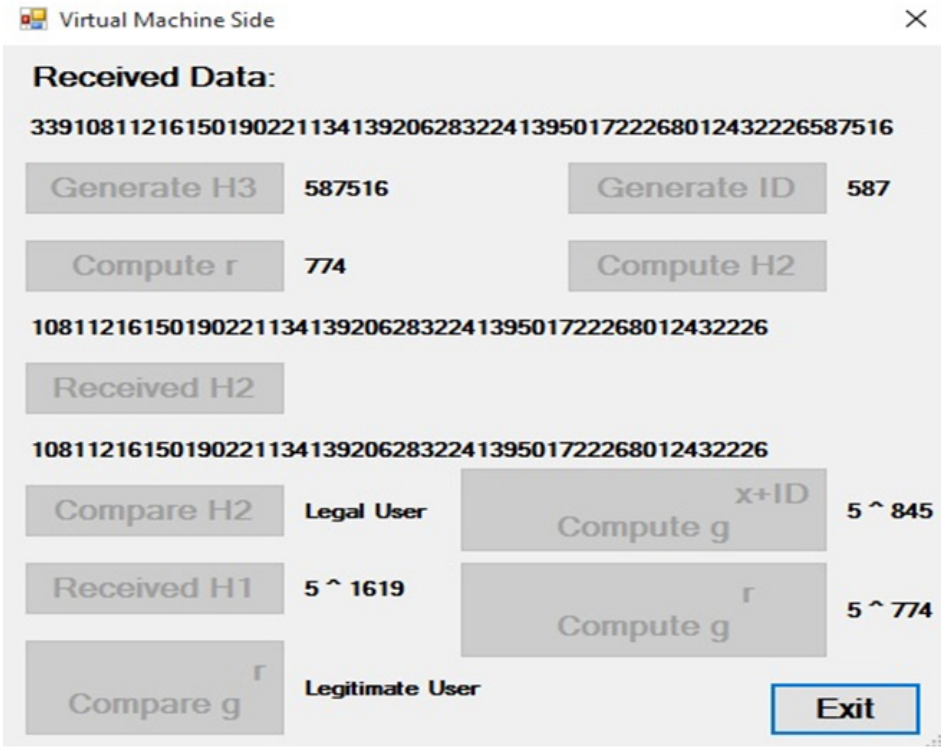

Figure 4: Legitimate User

Virtual machine received the data that is sent by the user and after receiving the data, it performs various operations:

1. Generate H3 and ID by the virtual machine.
2. Compute r and H2.
3. Compare the received value of H2 with the computed value of H2, if both H2 value is match, it means user is legitimate.
4. Then compute g^{x+ID} and g^{r}. After that virtual machine compare g^{r} with the genuine value of the user, if it is match then user is legitimate.

4.2. Attacker capture and Modified Data

4.2.1. Computation

Send modified data to virtual machine after data computation by an attacker.

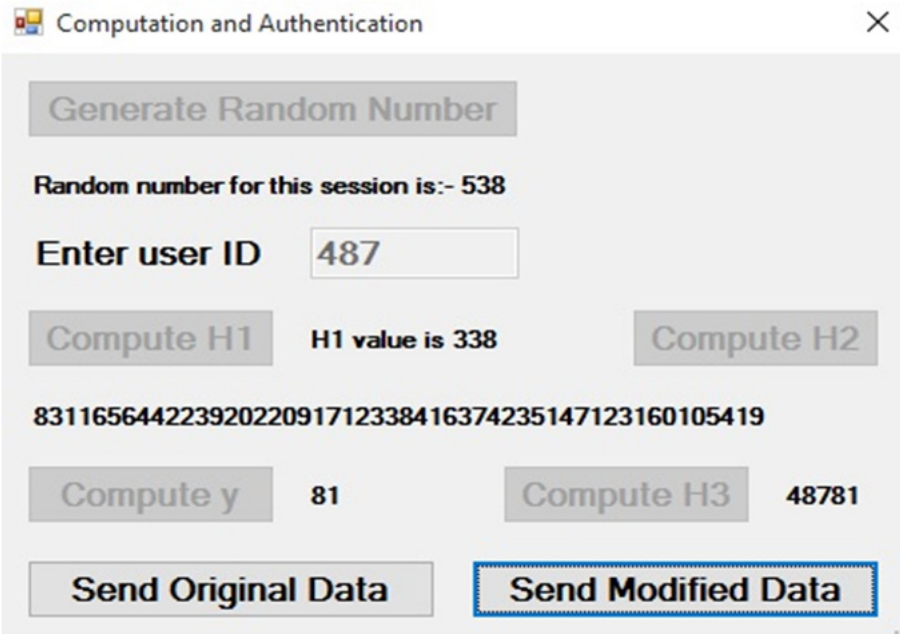

Figure 5: Data Computation and Modified Data

4.2.2. On Virtual Machine Side

The data is received at virtual machine that is sent by an attacker.

1. Compare the received value of H2 with the computed value of H2 by virtual machine, if both H2 value is not match, it means user is illegal.

   Proposed technique has been implemented on .NET framework 4.5 in C# using Visual Studio 2012 IDE. Windows Forms Application which is a very lightweight application that is used for implementation. The hardware used for the implementation is 4th Gen Intel i5 Processor with processing capability of 2.50GHz. 4GB RAM with 64-bit Windows 8.1 single-language Operating System having Microsoft Visual Studio Location Simulation Sensor.

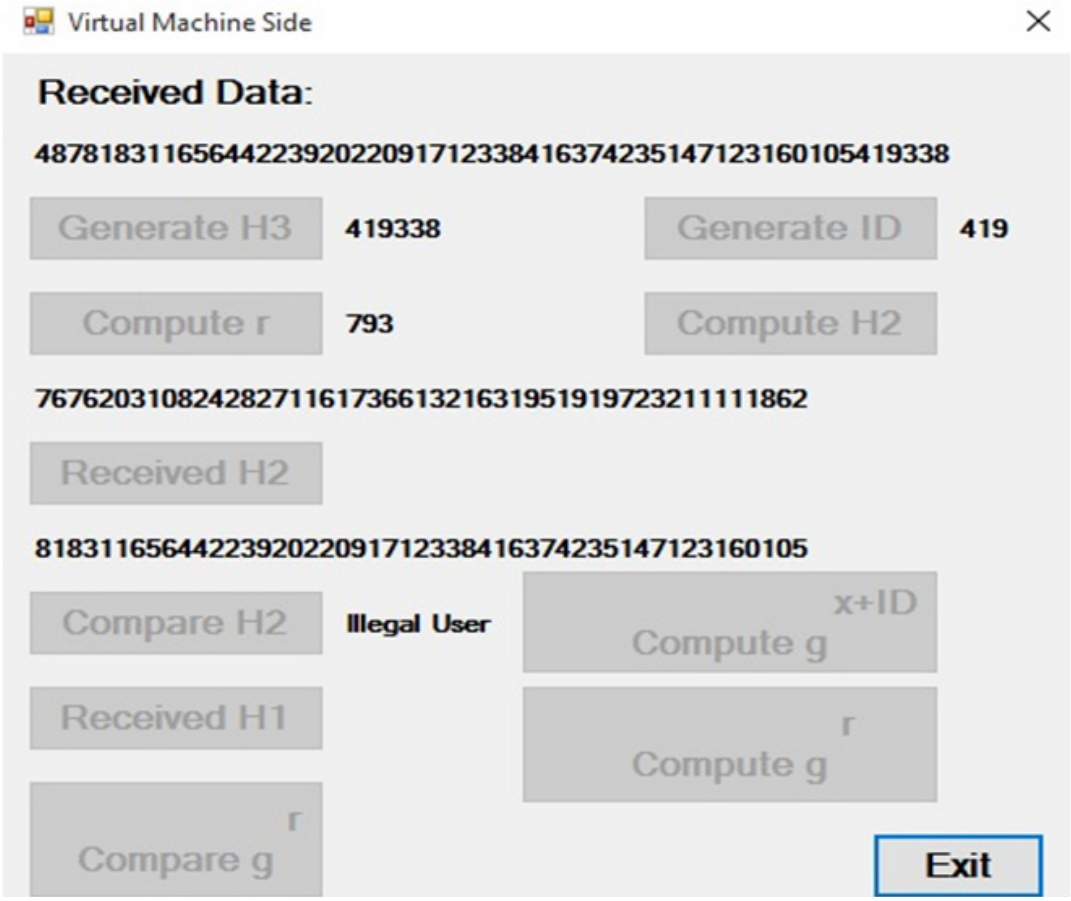

Figure 6: Malicious User

5. SECURITY ANALYSIS

Analyze the proposed technique security based on mutual authentication by using some possible attacks as follows:

5.1. Denial of Service (DoS) Attack

An Attacker obtains ID and y' and then computes ID || y' and sends to virtual machine, then virtual machine captures ID and y' of an attacker and computes y' XOR x and find r' then calculate H2, if calculated H2 is not match with the H2 of the legal user. It means user is illegal and this attack is not feasible.

5.2. Impersonation Attack

An Attacker obtain an ID of the User, But an attacker does not knows x and r because x is shared between the user and the virtual machine, and r is random number that is valid for only one session. So, this attack is infeasible.

5.3. Man in the Middle Attack

If an attacker obtain ID and y, and it can change x and r and then sends to virtual machine. Virtual machine computes H2 and if computed H2 is not equal to the H2 of the legitimate user. It means the user is illegitimate user and attack is not feasible.

5.4. Replay Attack

If an attacker obtain ID and y' and sends to virtual machine and then virtual machine computes y' *xor* x and find r'. After that an attacker again sends the h (ID|| x'|| y') and then again virtual machine computes the H2 and matches its H2 with the H2 of the user, if it is not same then user is illegal. Then again virtual machine computes H3 = ID||y', if again its H3 is not match with the H3 of the legal user. Then it means the user is legal and this attack is not feasible.

6. CONCLUSIONS

In the cloud architecture, some malicious nodes may join the network which is responsible to trigger zombie attack in the network. These zombie nodes can spoof the information of the legitimate user and communicate with virtual machine on the behalf of legitimate user. This will leads to reduction in network performance in terms of delay and bandwidth consumption. In this proposed work, detection of malicious user from the network has been done based on strong and server authentication.

REFERENCES

[1] Tupakula, Udaya, Vijay Varadharajan and Naveen Akku. Intrusion detection techniques for infrastructure as a service cloud. In Dependable. Autonomic and Secure Computing (DASC). IEEE Ninth International Conference.2011; pp. 744-751.

[2] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing 63.2012; pp. 561-592.

[3] Chirag N. Modi, Dhiren R. Patel, Avi Patel and Rajarajan Muttukrishnan. Bayesian Classifier and Snort based network intrusion detection system in cloud computing. In Computing Communication & Networking Technologies (ICCCNT). Third International Conference, 2012; pp. 1-7.

[4] Gonzalez, Nelson, Charles Miers, Fernando Redígolo, Marcos Simplicio, Tereza Carvalho, Mats Näslund, and Makan Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing 1, 2012; pp. 1-18.

[5] Hashizume, Keiko, David G. Rosado, Eduardo Fernandez-Medina, and Eduardo B. Fernandez. An analysis of security issues for cloud computing. Journal of Internet Services and Applications 4. 2013; pp. 1-13.

[6] Jen-Ho Yang and Pei-Yu Lin. An ID-Based User Authentication Scheme for Cloud Computing. Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2014; pp. 98-101.

[7] Nimmy K and M. Sethumadhavan. Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography. Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT) – Bangalore. India. 2014; pp. 101-106.

[8] Anurag Singh Tomar, Gaurav Kumar Tak and Ruchi Chaudhary. Image based Authentication with Secure Key Exchange Mechanism in Cloud. International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom) 2014; pp. 428-431.

[9] Prachi Deshpande, S.C. Sharma, and P. Sateeshkumar. Security Threats in Cloud Computing. International Conference on Computing, Communication and Automation (ICCCA2015). 2015; pp. 632-635.

[10] Tiwari, Pradeep Kumar, and Bharat Mishra. Cloud Computing Security Issues, Challenges and Solution. International Journal of Emerging Technology and Advanced Engineering. 2012; pp. 306-310.

[11] M. L. Das, A. Saxena, and V. P. Gulati. A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics. vol. 50. no. 2. 2004; pp. 629-631.

[12] Singh, Ajey, and Maneesh Srivastava. Overview of attacks on cloud computing. International Journal of Engineering and Innovative Technology (IJEIT). 2012; pp.1- 4.

[13] Y. Wang, J. Liu, F. Xiao, and J. Dan. A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, vol.32. no.4. 2009; pp. 583-585.

[14] Z. Hao, S. Zhong, and N. Yu. A Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing. Int. J. of Computers, Communications & Control. Vol. VI (2011). No. 2 (June). 2006; pp. 227- 235.

[15] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee. A Strong User Authentication Framework for Cloud Computing. in Services Computing Conference (APSCC). IEEE Asia-Pacific. 2011; pp. 110 –115.

[16] Raghav, Iti, Shashi Chhikara, and Nitasha Hasteer. Intrusion Detection and Prevention in Cloud Environment: A Systematic Review. International Journal of Computer Applications 68, 2013; pp. 7-11.

[17] Santos N, Gummadi KP, Rodrigues R. towards Trusted Cloud Computing. In the conference on hot topic in cloud computing. San Diego. California. CA.USA. 2009.

[18] Anurag Singh Tomar, Jaidhar C.D., S. Tapaswi. Secure Session key generation Technique for group communication. International Journal of Information and Electronics engineering. vol. 2. 2012; pp. 831-834.

[19] Mohit kumar Gokhroo, Jaidhar C.D., Anurag Singh Tomar. Cryptanalysis of SIP secure and efficient authentication scheme. International Conference on Information and computer networks. 2011; pp. 308-310.

[20] Anurag Singh Tomar, Gaurav kumar Tak, Manmohan Sharma. Secure Group Key Agreement with node Authentication. International Journal of Advanced Research in Computer Engineering and Technology. vol. 3. 2014; pp. 1455-1458.

[21] Shashi Kant Shankar, Anurag Singh Tomar, Gaurav Kumar Tak. Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs. 4th International Conference on Eco-friendly Computing and Communication Systems (ICECCS). 2015; pp. 455-461.