ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

INTRUSION DEFENSE MECHANISM USING ARTIFICIAL IMMUNE SYSTEM IN CLOUD COMPUTING (CLOUD SECURITY USING COMPUTATIONAL INTELLIGENCE)

SANTHANALAKSHMI L, SAKKARAVARTHI R

School of Computing Science and Engineering, VIT University, Chennai Campus, Chennai, Tamil Nadu, India. Email: sakkaravarthi.r@vit.ac.in

Received: 23 January 2017, Revised and Accepted: 03 March 2017

ABSTRACT

Cloud is a general term used in organizations that host various service and deployment models. As cloud computing offers everything a service, it suffers from serious security issues. In addition, the multitenancy facility in the cloud provides storage in the third party data center which is considered to be a serious threat. These threats can be faced by both self-providers and their customers. Hence, the complexity of the security should be increased to a great extend such that it has an effective defense mechanism. Although data isolation is one of the remedies, it could not be a total solution. Hence, a complete architecture is proposed to provide complete defense mechanism. This defense mechanism ensures that the threats are blocked before it invades into the cloud environment. Therefore, we adopt the mechanism called artificial immune system which is derived from biologically inspired computing. This security strategy is based on artificial immune algorithm.

Keywords: Artificial immune system, Cloud security, Computational intelligence.

DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19602

INTRODUCTION

As the demand for cloud computing increases day by day in the industrial communities, the security has become a serious concern in the industry. It is encountering various security issues. Typically, uncertainty about all the security level leads the industrial communities to consider security as the rank one concern with regards to cloud computing. Some of the traditional security mechanisms such as authentication and authorization are not enough for today's cloud environment. A serious threat may lead to misuse of the resources stored in the cloud environment. To provide with an effective architecture, the methodology of artificial immune system (AIS) is adopted. This methodology is similar to biological immune system (BIS) preventing the cloud environment from the intruders.

This research focuses on the following objectives,

- To identify the self- and nonself-discrimination attempting to gain the unauthorized access into the cloud environment.
- To analyze the vulnerability index of the identified nonself-discrimination using the common vulnerability scoring system (CVSS).
- To develop a hybrid fuzzy model for the defense mechanism for the statistical parameters for the protocol.

LITERATURE REVIEW

A multilayer network defense system using AIS

- A complete system is formed using innate and adaptive layer.
- Innate layer prevents 70% of the threats from entering the cloud environment.
- Adaptive layer identifies the visible threats.
- The overall network traffic is observed by network monitor, which emits danger signals.

Performance evaluation of a fraud detection system based on AIS

- Evaluation of fraud detection system.
- Produces higher accuracy in detection rate.
- Associated with generating and processing large data sets.

AIS architecture for cloud security application

- Detection, identification, and elimination of malicious codes and packets.
- Integration of adaptability, capability, and flexibility of information management.

Intrusion detection system adapted from agent-based AIS

- Proposal for multi-agent intrusion detection system.
- Detects unusual and untrusted network behavior.
- Ensures flow of untrustfulness from aggregated connection.

CHALLENGES IN THE EXISTING SYSTEM

Security issue in cloud computing has become the top priority in the industrial community. Hence, the traditional methods such as key management using public cryptography, contains empty spaces which produces various consequences such as data breaches, intruder access et al. Then, the cloud service providers face serious issues during the data migration because these data are backed up in several places. Simultaneously, data migration should be given prior consideration in a dynamic cloud environment. Finally, improper data storage structure has a serious threat to management. However, data security in cloud computing plays a major role in complete data management.

DETAILED PROBLEM SOLUTION

Cloud computing is a standout among the most famous innovation that eventually goes for cost streamlining. The qualities of cloud computing are on-request abilities, expansive system get to, asset pooling, fast flexibility, and measured administration. These qualities have a few security issues such as information accessibility, information classification, and assurance of touchy information kept up at the specialist organization's end.

In this way, so as to beat these security issues, we apply the idea of AIS got from BIS. AIS utilizes this idea as a part of the way that the BIS keep our body from the antibodies. This framework likewise makes a system security circumstance mindfulness, which gives the fundamental data about the gatecrashers. In this way, we propose a three-module instrument to distinguish, assess, and give a protection component utilizing artificial invulnerable framework.

The AIS has some similarities with the BIS which are as per the followings: the biological immune framework is named as network

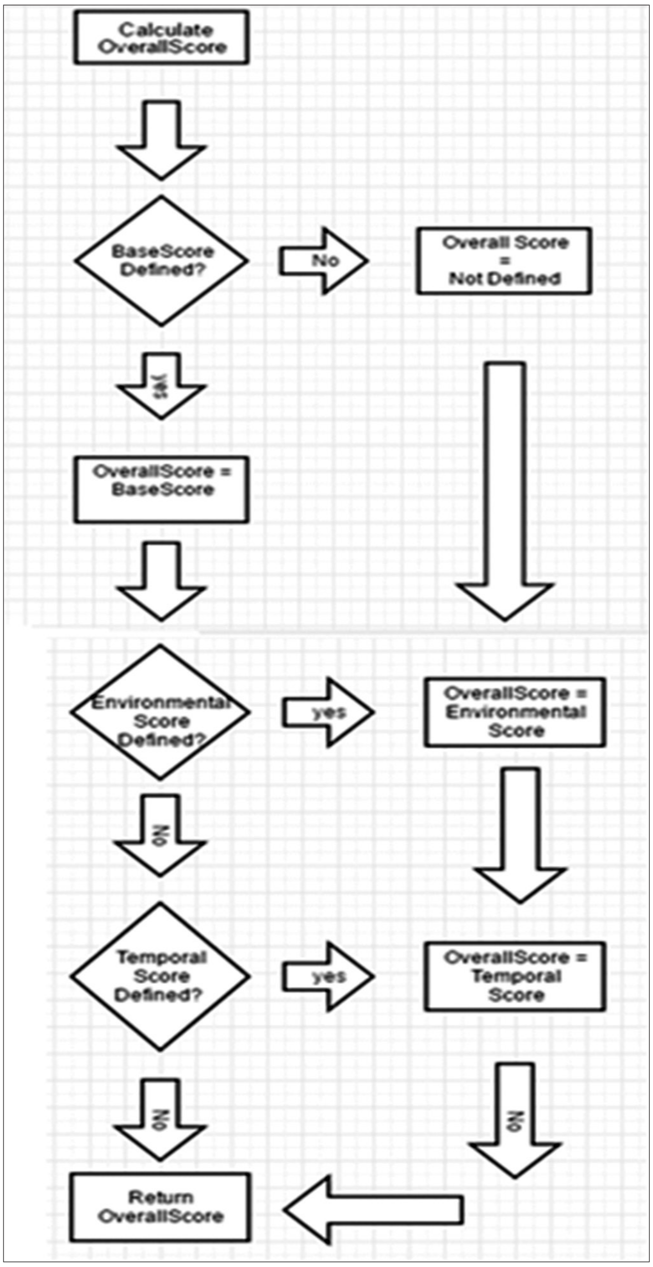


Fig. 1: Common vulnerability scoring system workflow

intrusion detection system, organism is signified by network, organ is the network segment, cell is called as the host computer, antigens are the binary characters extricated from the internet protocol parcels, and cell clone is the duplication of the antibodies.

Fig. 1 captures the workflow of the CVSS used for evaluating the security vulnerability.

SOLUTION METHODOLOGY

The answer for this specific research can be given utilizing the negative selection algorithm. At first, in the main module, we make utilization of the negative selection algorithm enlivened by the self–nonself-segregation conduct. The self- and nonself-separation standard recommends that the expectant suppositions made in clonal determination are sifted by locales of infeasibility (protein adaptations that dilemma to self-tissues). Advance, the self- and nonself-immunological worldview proposes the demonstrating of the obscure area by displaying the supplement of what is known. This is unintuitive as the characteristic slant is to classify obscure data by what is not the same as that which is known, as opposed to speculating the obscure data and sifting those theories by what is known.

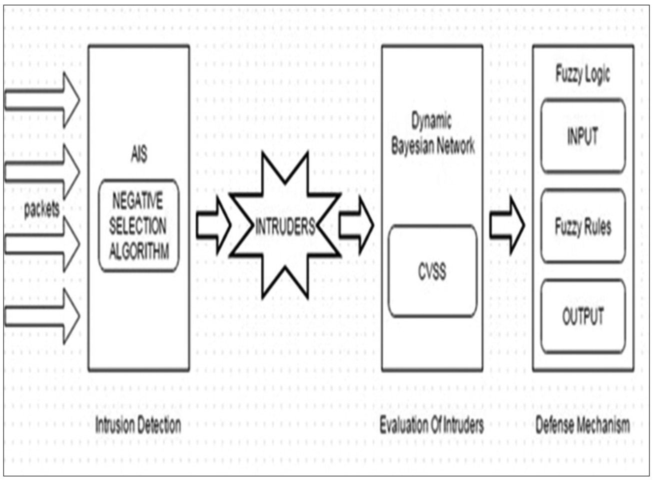


Fig. 2: Intrusion defense system

The data handling standards of the self- and nonself-separation prepare by means of negative determination are that of peculiarity and change recognition frameworks that model the expectation of variety from what is known. The rule is accomplished by building a model of changes, irregularities, or obscure information by producing designs that do not coordinate a current corpus of accessible examples. The arranged non-ordinary model is then used to either screen the current typical information or floods of new information by looking for matches to the non-ordinary examples.

As the second module, the severity of the interlopers is cautioned through the Agent information in the cloud environment. The seriousness of the interlopers is measured in this stage utilizing the agent information. Along these lines, we present the technique dynamic Bayesian network. For the most part, the seriousness of the interlopers is disregarded in the system measurements.

It is exceptionally fundamental to gauge the helplessness of the danger, in light of the fact that the outcome may change over the time. The defenselessness is less when the sellers misuse the patches and though the powerlessness is high when the code turns out to be generally spread. In this manner, it is here and there inadequate to rate the vulnerabilities with settled scores.

Along these lines, we propose dynamic Bayesian network model to include important worldly variables. The fleeting components are the accessibility of the endeavor codes or fixes. At that point utilizing CVSS, we infer the last estimation of the seriousness. What's more, the later part is the protection arrangement of the engineering which keeps every one of the interlopers from entering the Cloud Environment.

EXPERIMENTATION

The implementation is done via three modules which are as follows,

- Detection of self- and nonself-discrimination using negative selection algorithm.
- Evaluation of the security vulnerability using CVSS.
- Proposal of fuzzy intrusion defense mechanism.

Detection of self- and nonself-discrimination using negative selection algorithm

The exhibit issue is a two-class characterization issue where tests are drawn from a two-dimensional space. Those specimens are named self and whatever is left of the space has a place with the nonself-class. Tests are drawn from the self-class and displayed to the calculation for the arrangement of example indicators for grouping imperceptibly tests from the nonself-class.

The calculation makes an arrangement of identifiers that do not coordinate the self-information and are then connected to an arrangement of arbitrarily produced tests from the area. The calculation utilizes a genuine esteemed representation. The Euclidean separation capacity is utilized amid coordinating and a base separation esteem is determined as a client parameter for estimated coordinates between examples. The algorithm includes the additional computationally expensive check for duplicates in the preparation of the self dataset and the locator set.

Calculation negative selection

Input: A S⊂U ("self-set"); a set M⊂U ("screen set"); a whole number n

Yield: For every component m∈M, either "self" or "nonself."

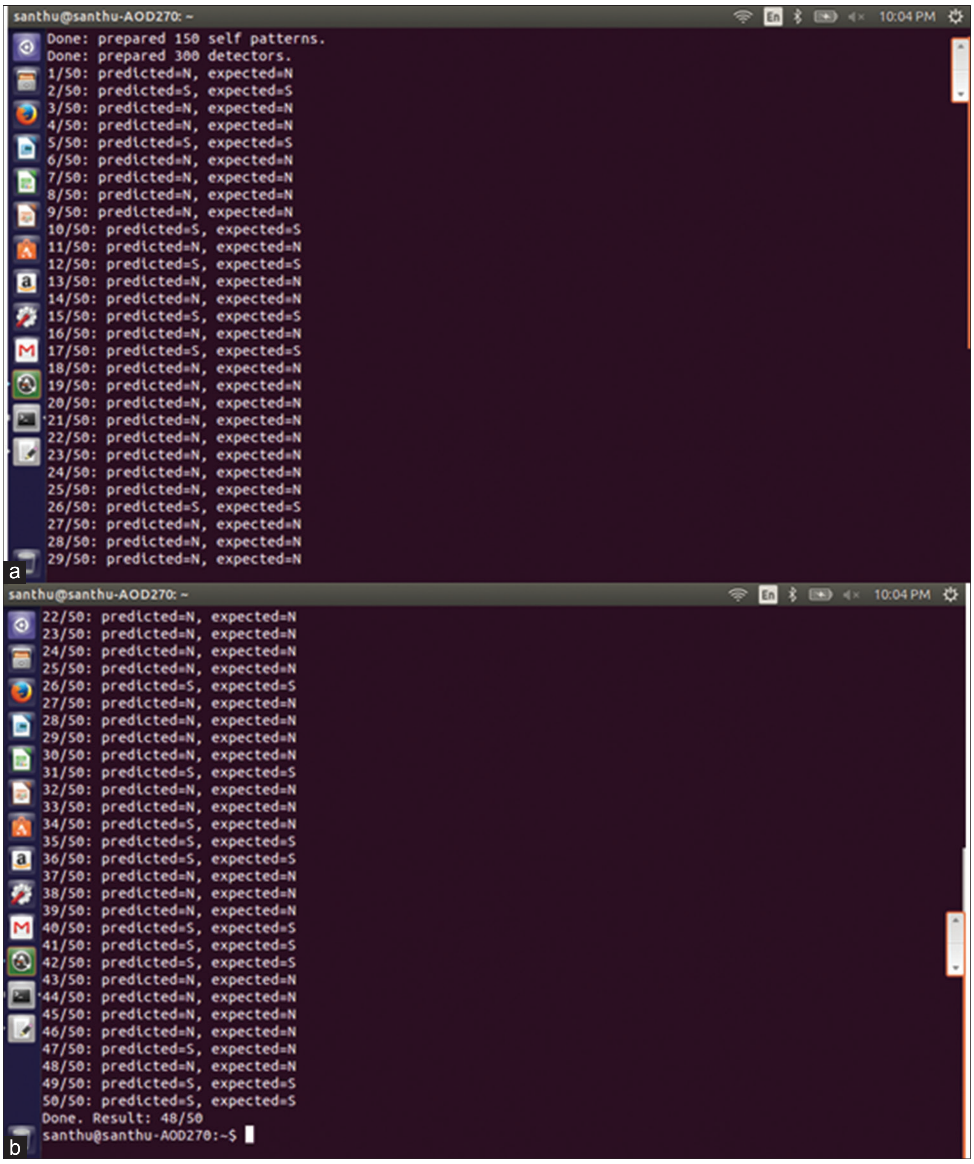
/preparing stage

- d ← discharge set
- while |D|<n do
- d ← irregular finder
- if d does not coordinate any component of S then

Evaluation of the security vulnerability using *CVSS*

The seriousness of the gatecrashers is measured in this stage utilizing the agent information. In this way, we present the system dynamic Bayesian network. For the most part, the seriousness of the interlopers is disregarded in the system measurements. It is extremely fundamental to gauge the defenselessness of the risk, in light of the fact that the result may change over the time.

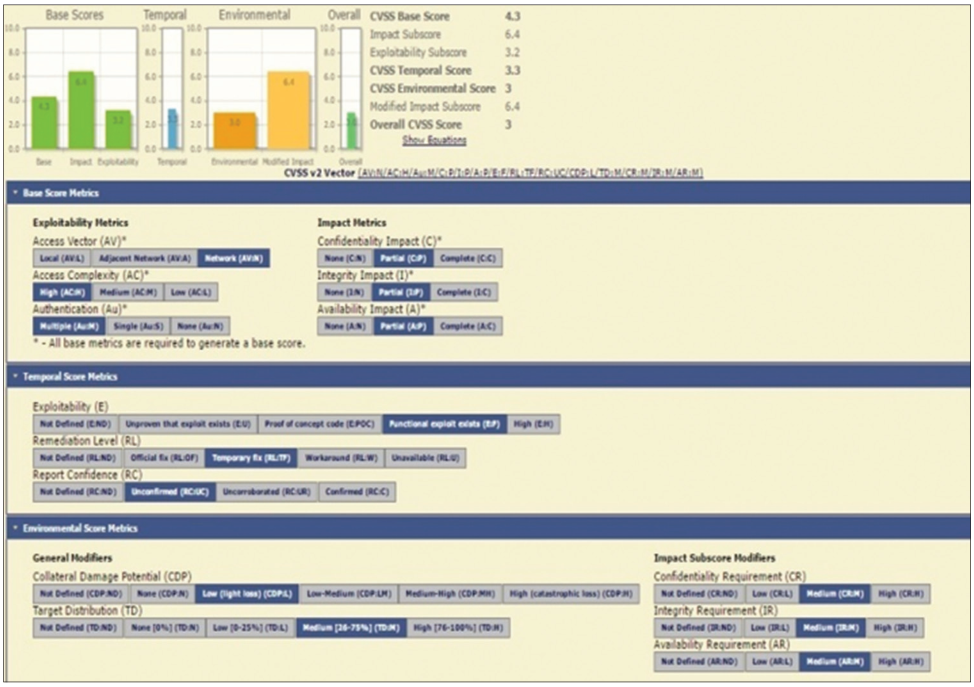
The helplessness is less when the merchants abuse the patches and while the powerlessness is high, when the code turns out to be broadly spread. Subsequently, it is some of the time lacking to rate the vulnerabilities with settled scores. In this way, we propose dynamic Bayesian network model to include important fleeting components. The fleeting components are the accessibility of the endeavor codes or fixes. At that point, utilizing CVSS, we determine the last estimation of the seriousness. CVSS endeavors to allocate seriousness scores to vulnerabilities, permitting responders to organize reactions and assets as per risk. Scores are ascertained in light of a recipe that relies on upon a few measurements that surmised simplicity of endeavor and the effect of adventure. Scores are computed in light of the metric values each conveying an arrangement of equations for the effect of endeavor. Scores may change from 0 to 10, where 10 has the most extreme possibilities for powerlessness. Here, the CVSS framework is utilized to



```
Done: prepared 150 self patterns.
Done: prepared 300 detectors.
1/50: predicted=N, expected=N
2/50: predicted=S, expected=S
3/50: predicted=N, expected=N
4/50: predicted=N, expected=N
5/50: predicted=S, expected=S
6/50: predicted=N, expected=N
7/50: predicted=N, expected=N
8/50: predicted=N, expected=N
9/50: predicted=N, expected=N
10/50: predicted=S, expected=S
11/50: predicted=N, expected=N
12/50: predicted=S, expected=S
13/50: predicted=N, expected=N
14/50: predicted=N, expected=N
15/50: predicted=S, expected=S
16/50: predicted=N, expected=N
17/50: predicted=S, expected=S
18/50: predicted=N, expected=N
19/50: predicted=N, expected=N
20/50: predicted=N, expected=N
21/50: predicted=N, expected=N
22/50: predicted=N, expected=N
23/50: predicted=N, expected=N
24/50: predicted=N, expected=N
25/50: predicted=N, expected=N
26/50: predicted=S, expected=S
27/50: predicted=N, expected=N
28/50: predicted=N, expected=N
29/50: predicted=N, expected=N
```

```
22/50: predicted=N, expected=N
23/50: predicted=N, expected=N
24/50: predicted=N, expected=N
25/50: predicted=N, expected=N
26/50: predicted=S, expected=S
27/50: predicted=N, expected=N
28/50: predicted=N, expected=N
29/50: predicted=N, expected=N
30/50: predicted=N, expected=N
31/50: predicted=S, expected=S
32/50: predicted=N, expected=N
33/50: predicted=N, expected=N
34/50: predicted=S, expected=N
35/50: predicted=S, expected=S
36/50: predicted=S, expected=S
37/50: predicted=N, expected=N
38/50: predicted=N, expected=N
39/50: predicted=N, expected=N
40/50: predicted=S, expected=S
41/50: predicted=S, expected=S
42/50: predicted=S, expected=S
43/50: predicted=N, expected=N
44/50: predicted=N, expected=N
45/50: predicted=N, expected=N
46/50: predicted=N, expected=N
47/50: predicted=S, expected=N
48/50: predicted=N, expected=N
49/50: predicted=S, expected=S
50/50: predicted=S, expected=S
Done. Result: 48/50
santhu@santhu-AOD270:~$
```

Fig. 3: (a and b) Identification of self and nonself-class using data sets



CVSS Base Score	4.3
Impact Subscore	6.4
Exploitability Subscore	3.2
CVSS Temporal Score	3.3
CVSS Environmental Score	3
Modified Impact Subscore	6.4
Overall CVSS Score	3

Show Equations

CVSS v2 Vector (AV:N/AC:H/Au:M/C:P/I:P/A:P/E:F/RL:TF/RC:UC/CDP:L/TD:M/CR:M/IR:M/AR:M)

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*
Local (AV:L) | Adjacent Network (AV:A) | [✓ Network (AV:N)]

Access Complexity (AC)*
[✓ High (AC:H)] | Medium (AC:M) | Low (AC:L)

Authentication (Au)*
[✓ Multiple (Au:M)] | Single (Au:S) | None (Au:N)

* - All base metrics are required to generate a base score.

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | [✓ Partial (C:P)] | Complete (C:C)

Integrity Impact (I)*
None (I:N) | [✓ Partial (I:P)] | Complete (I:C)

Availability Impact (A)*
None (A:N) | [✓ Partial (A:P)] | Complete (A:C)

Temporal Score Metrics

Exploitability (E)
Not Defined (E:ND) | Unproven that exploit exists (E:U) | Proof of concept code (E:POC) | [✓ Functional exploit exists (E:F)] | High (E:H)

Remediation Level (RL)
Not Defined (RL:ND) | Official fix (RL:OF) | [✓ Temporary fix (RL:TF)] | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)
Not Defined (RC:ND) | [✓ Unconfirmed (RC:UC)] | Uncorroborated (RC:UR) | Confirmed (RC:C)

Environmental Score Metrics

General Modifiers

Collateral Damage Potential (CDP)
Not Defined (CDP:ND) | None (CDP:N) | [✓ Low (light loss) (CDP:L)] | Low-Medium (CDP:LM) | Medium-High (CDP:MH) | High (catastrophic loss) (CDP:H)

Target Distribution (TD)
Not Defined (TD:ND) | None [0%] (TD:N) | Low [0-25%] (TD:L) | [✓ Medium [26-75%] (TD:M)] | High [76-100%] (TD:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)
Not Defined (CR:ND) | Low (CR:L) | [✓ Medium (CR:M)] | High (CR:H)

Integrity Requirement (IR)
Not Defined (IR:ND) | Low (IR:L) | [✓ Medium (IR:M)] | High (IR:H)

Availability Requirement (AR)
Not Defined (AR:ND) | Low (AR:L) | [✓ Medium (AR:M)] | High (AR:H)

Fig. 4: Evaluation of the vulnerabilities using common vulnerability scoring system

- embed d into D.

/arrangement stage
- for every m∈m do
- if m coordinates any indicator d∈D then
- yield “m is nonself” (an abnormality)
- else
- yield “m is self.”

break down the defenselessness in a cloud domain utilizing the three metric values, for example, base scores, temporal scores, and ecological scores.

Proposal of fuzzy intrusion defense mechanism

A fuzzy logic system (FLS) can be characterized as the nonlinear mapping of an information set to a scalar yield information. A FLS comprises four principle parts: fuzzifier, rules, surmising motor, and defuzzifier. The resistance instrument against the gatecrashers is produced utilizing the fuzzy logic as a part of the artificial intelligence. Fuzzy-based resistance system screens the activity progressively, breaks down and assesses based on surmising rules. The fuzzy standards are characterized in restrictive route in IF-ELSE frame to decide the logic. The entropy hypothesis assumes a noteworthy part in the fuzzy logic for cloud environment resistance system.

The primary strides considered in making the interloper barrier instrument utilizing fuzzy logic is,
- Setup security list system.
- Index quality and fuzzy assessment.
- Fuzzy extensive assessment of system security.

Fuzzy logic algorithm
1. Define the phonetic factors and terms (instatement).
2. Construct the participation capacities (instatement).
3. Construct the run base (instatement).
4. Convert fresh info information to fuzzy qualities utilizing the participation capacities (fuzzification).
5. Evaluate the guidelines in the govern base (surmising).
6. Combine the consequences of every govern (surmising).
7. Convert the yield information to non-fuzzy qualities (defuzzification).

Fig. 2 depicts the architecture of the mechanism.

RESULT AND ANALYSIS

The different investigations of the intrusion defense component using AIS in cloud computing are made. The proficiency of the proposed system has been broke down and different studies have been made in the space of artificial intelligence, AIS, computational intelligence, and Bayesian Network. Fig. 3a and b gives the distinguishing proof of the self- and nonself-class which are recreated by the information sets utilizing the negative choice calculation. The classes are resolved with the assistance of changes and irregularities in the system.

In the second module, the dynamic Bayesian network utilizes the time stamp to perform analysis of the vulnerabilities. . It is very essential to measure the vulnerability of the threat, because the aftermath may change over the time. At that point utilizing CVSS, we determine the last estimation of the seriousness.

Fig. 4 captures the evaluation metrics of the security vulnerability.

CONCLUSION

The Artificial Immune System possess the characteristics of the Biological Immune System are capable of handling the issues concerned with the security of the Cloud Environment. With this research a proactive Defense mechanism can be designed and implemented. This design can also act as tool for surveillance in the real time for the cloud environment.

REFERENCES

1. Available from: http://www.en.wikipedia.org/wiki/Cloud_Computing.
2. Sangkatsanee P, Wattanapongsakorn N, Charnsripinyo C. Practical real-time intrusion detection using machine learning approaches. Comput Commun 2011;34(8):2227-35.
3. Elshoush HT. Alert correlation in collaborative intelligent intrusion detection systems-a survey. Appl Softw Comput 2011;11:4349-65.
4. Kuzhalisai M, Gayathri G. Enhanced security in cloud with multi-level intrusion detection system. Int J Comput Commun Technol 2012;3(3):66-9.

5. Modi C, Patel D, Borisanya B, Patel A, Rajarajan M. A novel framework for intrusion detection in cloud. ACM, International Conference on Security of Information and Networks; 2012. p. 67-74.
6. Zarrabi A. Internet intrusion detection system service in a cloud. Int J Comput Sci 2012;9(5):308-15.
7. Gonzalez N, Miers C. Top threats to cloud computing. A quantitative analysis of current security concerns and solutions for cloud computing. Cloud Security Alliance; 2012.
8. Tanase M. The Future of IDS; 2001. Available from: http://www.securityfocus.com/infocus/1520.
9. Debar H, Becker M, Siboni D. A neural network component for an intrusion detection system. In: Proceedings. IEEE Computer Society Symposium; 1992. p. 240-50.
10. Available from: http://www.nvd.nist.gov/CVSS/v2-calculator#score.
11. Yan X, De-ming Z. Research on network security evaluation based on fuzzy method. Meas Control Technol 2009;28(2):79-82.
12. Dongmei Z, Yuqing Z, Jianfeng MA. Fuzzy Risk Assessment of Entropy Weight Coefficient Method Applied in Network Security; 1997.
13. Prowell S, Kraus R, Borkin M. Seven Deadliest Network Attacks. 1st ed. Burlington: Syngress Publishers; 2010.
14. Shun-Chieh L, Tseng SS. Constructing detection knowledge for DDoS intrusion tolerance. Int J Expert Syst Appl 2004;27(3):379-90.
15. Leland WE, Taqqu MS, Willinger W, Wilson DV. On the self-similar nature of ethernet traffic (extended version). IEEE/ACM Trans Netw 1994;2(1):1-15.
16. Jose N. Politically motivated denial of service attacks. In: Czosseck C, Geers K, editors. The Virtual Battlefield: Perspectives on Cyber Warfare. Amsterdam: IOS Press; 2009. p. 163-81.
17. Segura V, Lahuerta J. Modeling the economic incentives of DDoS attacks: Femtocell case study. In: Economics of Information Security and Privacy. US: Springer US Publishers; 2010. p. 107-19.