A Framework for Self-Protection of Resources in Cloud from Location Specific Attacks

Gumpina Babu Rao*[1], Prof. Nistala V.E.S.Murthy[2] , Dr. G.Lavanya Devi[3]

[1]Assistant Professor, Department of computer science, GITAM (Deemed to be University),Visakhapatnam, Andhra Pradesh, India

[2]Prof. N.V.E.S. Murthy, Head, department of Mathematics, J.V.D. College of Science and Technology, Visakhapatnam, Andhra University, Andhra Pradesh, India

[3]Assistant Professor, Department of Computer Science and Systems Engineering

Andhra University, Visakhapatnam, Andhra Pradesh, India

Abstract— *Improvements in the cloud computing algorithms, techniques and services have forced majority of the services to migrate on to the cloud. These migrations have increased the security risks on the cloud systems in terms of data protection, application or service protection and resource protection. The modern data centres are capable of dealing with high volume applications and loads. In order to justify the high loads, the data centres are generally distributed over multiple geodetic locations and thus leverage access to a wide variety of clients and data auditors. It is highly challenging to maintain a single security policy for the completely distributed data centre resources due to the policy variation of data access rules in various countries. A number of research attempts are carried out for providing a single time security policy and process for the entire data centres. Nonetheless, the failure rates are very high due to the above mentioned complexity. Thus, after analysing various methods for resource security, this work proposes a self-protecting framework for cloud data centre based resources. During the testing and simulation, the proposed framework has demonstrated nearly 96% detection and avoidance of the security attacks on the resources.*

Keywords— ***Secure Channel Communication, Attack Characterisation, Meta Information Sharing, SAT, SADM, VESPA, CPCS, MICSP, CTMS, SMVR, SPDS***

I. INTRODUCTION & LITERATURE REVIEW

The security for the cloud computing is one of the key areas for research and due to less number of research attempts, this area also catches attention from various attackers.Thus, the demand of the modern research is to provide a multiple frameworks for securing the data, applications and the resources on cloud. The novel work by G. Qu et al. [1] was the very first attempt to make the cloud resources capable of own protection. Nevertheless, the method by G. Qu et al. [1] focuses on the resources security only during the access by the identified client application. In case of any unidentified client request, the system demonstrates weak behaviours. In order to overcome this and few other limitations, the work of A. Carpen-Amarie et al. [2] was proposed. This solution was majorly focusing on the data resources of cloud data centres and can self-protect for any types of accesses. The work was widely accepted. Nonetheless, in the search of complete protection for all types of cloud resources, another notable outcome from A. Wailly et al. [3] must be considered. This method is capable of handling all types of resource protection policies. However, the complexity of the model made it significantly difficult to implement in all situations and for all application types.

In the due course of study, it became understandable that for providing best level of security for the cloud resources, the research attempts must consider the attack characteristics and then to nullify the characteristics design the frameworks or the algorithms on the resources.

Considering the fact of attack characteristics, once again this research domain has witnessed many new research outcomes. The work by E. Benkhelifa et al. [4] has demonstrated that the design of any framework for preventing the attacks on the cloud resources can be highly effective, if the attack types are known. Enhancing this concept, the work of P. Manuel et al. [5] has showcased that for improving the quality of the services majorly depends on nullifying the attacks on the cloud data centres, specifically the resources.

The work by R.D. Di Pietro et al. [6] has pointed out towards a newer challenge of the cloud resource security. The resources on the data centres are virtualized and many of the physical properties cannot be detected during the service time. This challenge was justified by the work of A.Y. Sarhan et al. [7] by deploying security agents on the cloud resource pools.

Further, in the recent advancements of the security algorithms, many of the parallel researches have challenged the above stated algorithms and frameworks to be having high impact on the scheduling times. The work of S. Singh et al. [8] has benchmarked and demonstrated the effects on the additional security policies on the resource allocation and scheduling.

Henceforth, this work undertakes the challenge of providing a framework for self-protecting the cloud resources without compromising the performance of the cloud data centre to a high scale.

The rest of the work is furnished as in the Section – II, the popular security attack types are discussed, in Section – III, the proposed framework is elaborated, in Section – IV, the driving algorithm of the framework is elaborated, the results obtained from the proposed framework is discussed in the Section – V and the work presents the final conclusion in the Section – VI.

II. Analysis of Location Specific Attack Types

Based on the literature review carried on by this work, it is natural to understand that realizing the characteristics of the attack types are important for building any self-sustainable model. Thus the attack types are realized in this section [Table – 1].

TABLE I
ATTACK TYPES CHARACTER IDENTIFICATION AND RANKING

Name of the Attack	**Attack Characteristics**	**Attack Type**	**Ranking based on Severity**
SMURF	High Network Traffic - Random	DoS	1
LAND	Violation of QoS	DoS	2
SYN Flood	Spoofing	DoS	3
HTTP Flood	High Client Requests	Distributed DoS	7
Zero Day	Finding Random Guesses for Cloud Network Flaws	Distributed DoS	4
SPY	Remote Control	Remote Access	10
Password Guessing	Random Requests	Remote Access	5
IMAP	IMAP access violation	Remote Access	6
Rootkits	Incorrect Privilege Request	Root Violation	7
Buffer Overflow	Illegal Data Access	Root Violation	8
Ports Sweeps	Manipulation of the Network Access Table	Breaching	9
NMAP	Port Scanning and Illegal Access	Breaching	10

The ranking made on these types of attacks will certainly help in deciding the self-sustainable protection framework. The ranking is visualized graphically here [Fig – 1].

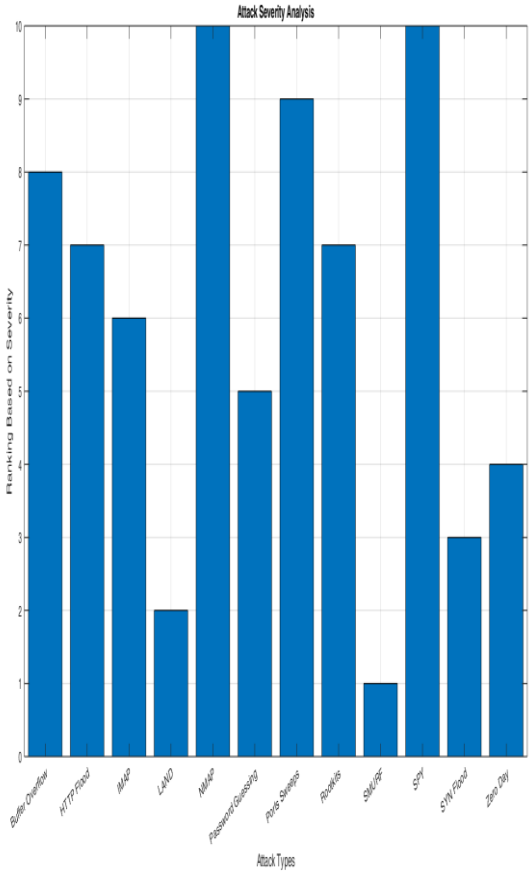

Fig. 1 Attack Types Ranking Analysis Based on Severity

Further, this work analyses the type density of the attacks on cloud [Table – 2]. The information is provided by Microsoft research in India [9].

TABLE II
ATTACK TYPES AND ATTACK DENSITY IN INDIA

Attack Type	**Number of Attacks**
DoS	4933
Distributed DoS	6333
Remote Access	6714
Root Violation	4900
Breaching	9261

The density is visualized graphically here [Fig – 2].

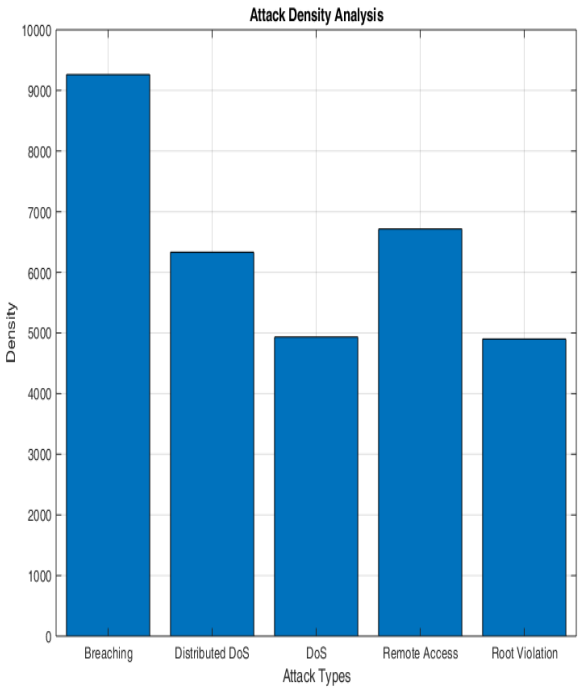

Fig. 2 Attack Density in India

Henceforth, based on the severity of the attacks and similarities of the attacks resulting into density of the attacks, in the next section this work proposes the framework for self-protecting security of the cloud resources.

III. An Automated Location Specific Attack Detection

In this section of the work, the proposed framework is elaborated with component descriptions. The novelty of the framework is to deploy the security threat information over the secure channel for all resource managers [Fig – 3].

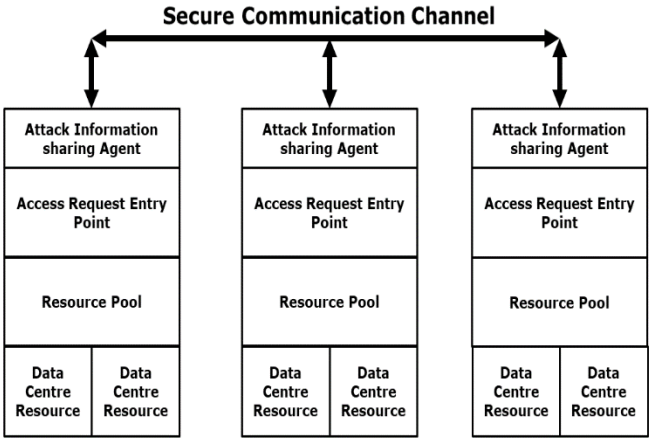

Fig. 3 Framework for Attack Sharing via Secure Communication Channel

This framework ensures the attack information sharing via a secure communication channel over all the resource pools in the cloud data centres.

This proposed framework is catering the following advantages over the existing systems:

1. The attack information is shared over all the resource pools, so that the other resource pools can be alert on the attack presence.
2. Once the attack characteristics are analysed at one resource pool, the other resource pools can utilize the same benefits without processing the requests again. This reduces the time complexity to higher scale.
3. The attack characteristics are analysed before the entry point, thus the resources on the cloud data centre are safer than before.

IV. PROPOSED ALGORITHM

In this section of the work, the driving algorithm for the framework is elaborated and analysed.

Algorithm: Self – Protection
Step-1. Establish the Connection request between the data centre request manager
Step-2. Establish the secure connection between resource pools
Step-3. Accept the Connection Request from data centre request manager
Step-4. For each connection
a. Check for High Network Traffic
b. Check for Violation of QoS
c. Check for Spoofing
d. Check for High Client Requests
e. Check for Finding Random Cloud Network Flaws
f. Check for Remote Control Access Request
g. Check for Random Requests
h. Check for IMAP access violation
i. Check for Incorrect Privilege Request
j. Check for Illegal Data Access
k. Check for Manipulation of the Network Access Table
l. Check for Port Scanning and Illegal Access
Step-5. End
Step-6. Share the connection request status via secure channel

The algorithm is visualised graphically here [Fig – 4].

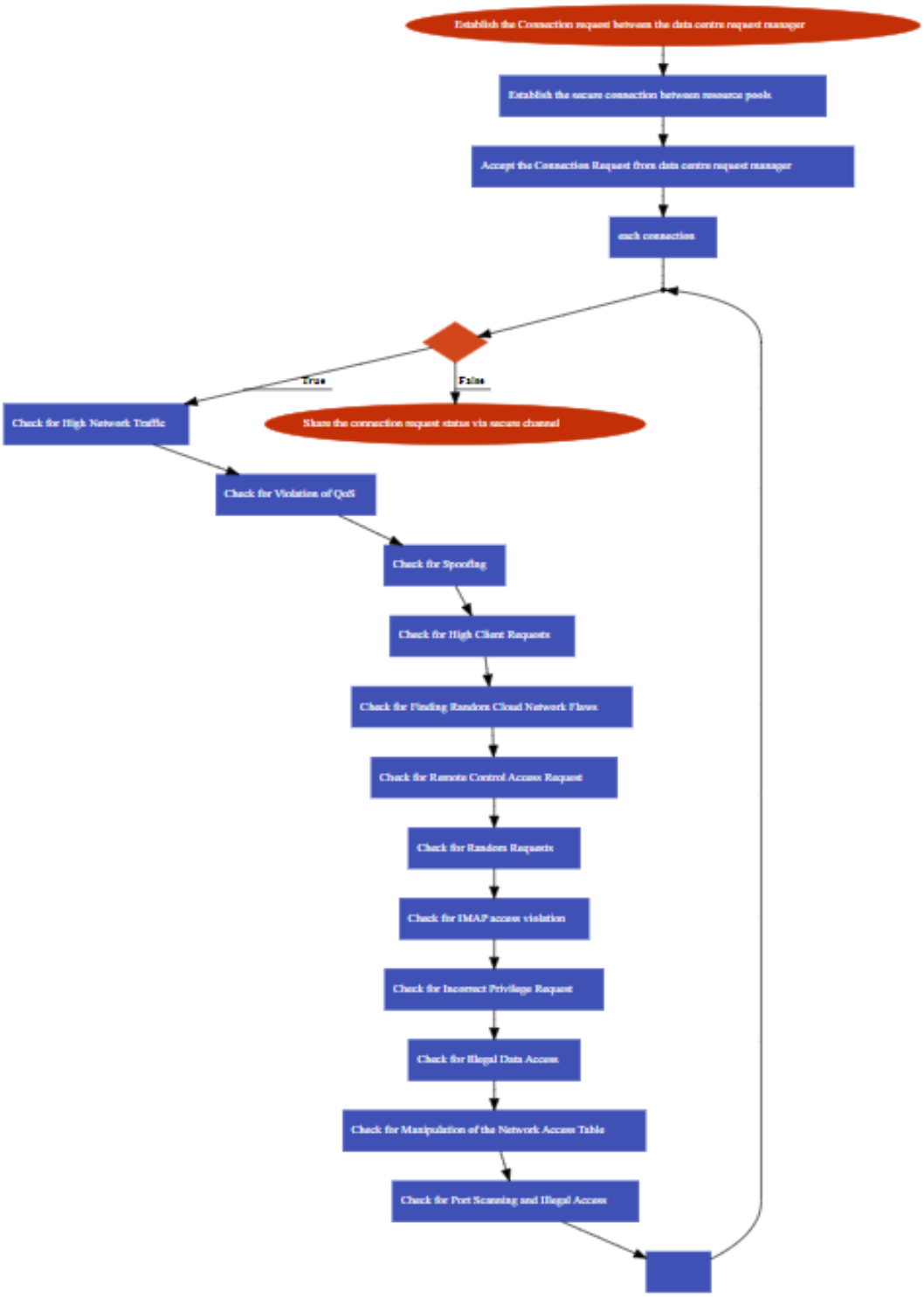

Fig. 4 Proposed Algorithm

Henceforth, the results obtained from this proposed framework is furnished and discussed in the next section.

V. RESULTS AND DISCUSSION

In this section of the work, the results obtained from various parallel research attempts are compared with the proposed secure channel method [Table – 3].

TABLE III NUMBER OF ATTACK DETECTION AND PREVENTION COMPARISON

Name of the Attack	Proposed Method	SAT	SADM	VESPA	CPCS	MICSP	CTMS	SMVR	SPDS
SMURF	5344	1710	1861	2064	1519	1499	1323	1368	2147
LAND	2588	1933	1852	1372	1973	1794	2374	1720	1389
SYN Flood	4808	1450	2391	1236	1883	1561	2119	1386	2002
HTTP Flood	1720	1389	1385	1308	1836	1262	1943	2217	2413
Zero Day	4014	1397	1913	1553	2107	1956	1904	2284	1674
SPY	2907	2388	2373	1622	2367	1781	1394	1887	1713
Password Guessing	4638	1686	1784	1958	1601	1951	2175	2183	1821
IMAP	4013	1836	1760	1298	1599	2259	2493	1551	2182
Rootkits	4977	1348	1708	2220	1395	2307	1441	1551	1710
Buffer Overflow	2971	1246	1934	1232	1871	1558	2433	2360	1395
Ports Sweeps	5042	1382	2050	2310	1790	1725	2130	2197	2030
NMAP	1239	1674	1983	1703	2340	2369	1322	1777	1947

It is natural to understand, that the number of attacks detected by the proposed method is significantly high.

The results are analysed visually here [Fig – 5].

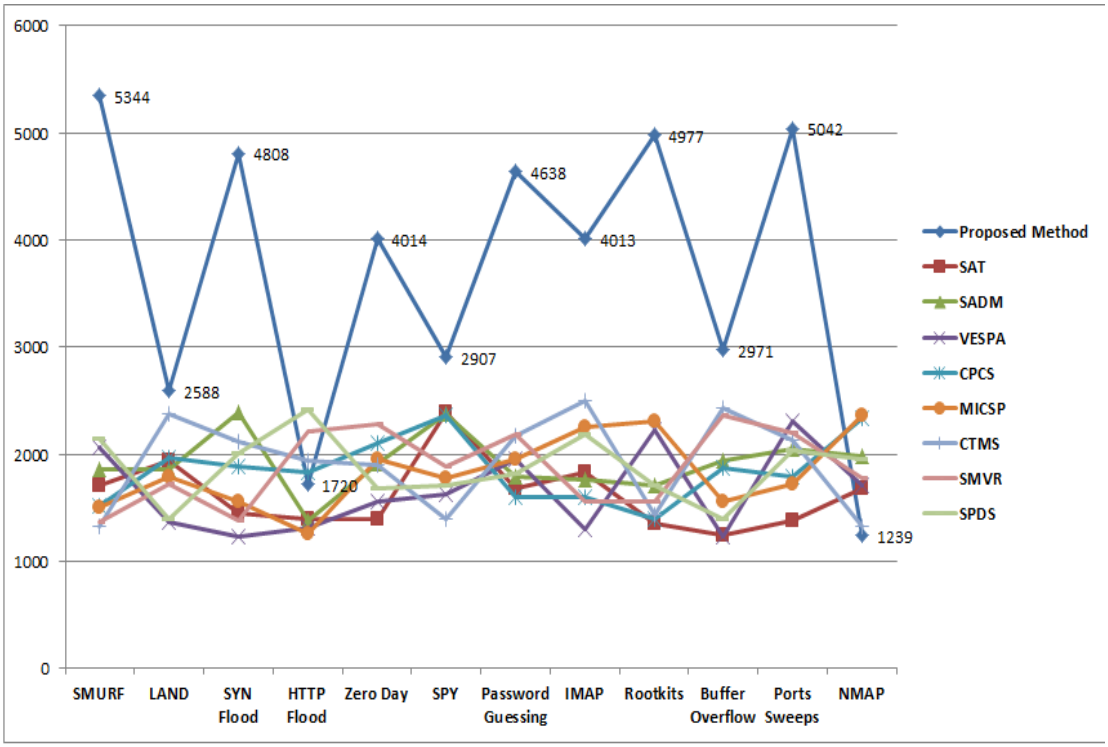

Fig. 5Result and Comparative Analysis of Attack Detections

The work presents the conclusion in the next section.

VI. CONCLUSION

The growth in the cloud computing and migration of the existing systems in to the cloud have forced the researchers to analysed the cloud security aspects. The major challenge of the cloud security is securing the resources on the cloud. The existing security methods cannot deal with the fact of securing the cloud data centre resources as desired. Thus this work provides a new method of securing the cloud resources in a self-sustainable method. The proposed framework demonstrated a high accuracy of detecting attacks compared to the parallel outcomes of the researchers. The novelty of proposed framework is to share the attack meta information over the secure channel and proven to be the newer dimension of the research for making the cloud security better than before.

REFERENCES

[1] G. Qu, O.A. Rawashdeh, and D. Che, "Self-Protection against Attacks in an Autonomic Computing Environment," International Journal of Computer Applications (CAINE), vol. 17, no. 4, 2010, pp. 250–256.
[2] A. Carpen-Amarie, "Towards a self-adaptive data management system for cloud environments," IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW 11), 2011, pp. 2077–2080.
[3] A. Wailly, M. Lacoste, and H. Debar, "Vespa: Multi-layered self-protection for cloud resources," Proceedings of the 9th International Conference on Autonomic Computing (ICAC 12), 2012, pp. 155–160.
[4] E. Benkhelifa and T. Welsh, "Towards Malware Inspired Cloud Self-Protection," Proceedings of the 2014 International Conference on Cloud and Autonomic Computing (ICCAC 14), 2014, pp. 1–2.
[5] P. Manuel, "A trust model of cloud computing based on Quality of Service," Annals of Operations Research, vol. 233, no. 1, 2015, pp. 281–292.
[6] R.D. Di Pietro, F. Lombardi, and M. Signorini, "Secure Management of Virtualized Resources," Security in the Private Cloud, CRC Press, 2016; doi.org/10.1201/9781315372211-14.
[7] A.Y. Sarhan and S. Carr, "A Highly-Secure Self-Protection Data Scheme in Clouds Using Active Data Bundles and Agent-Based Secure Multi-party Computation," Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud 17), 2017, pp. 228–236.
[8] S. Singh and I. Chana, "QRSF: QoS-aware resource scheduling framework in cloud computing," The Journal of Supercomputing, vol. 71, no. 1, 2015, pp. 241–292.
[9] Microsoft Security Intelligence Report, Volume 22 | January through March, India, 2018.