International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 6, Issue 6, June 2017)

A Review on Cloud Data Security using Frequency Variation and Hard Logarithmic based Algorithm

Ankur Jain[1], Asst. Prof. Dr. L. K. Vishwamitra[2]
[1,2]*Department of Computer Science & Engineering, Oriental College of Technology, Bhopal, India*

***Abstract*--Offering real-time data security for Peta-bytes of data is important for Cloud Computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern.**

I have reviewed paper "Towards achieving Data Security with the Cloud Computing Adoption Framework" and found that this paper is using multilayered architecture for data security.

There are three lyres in this paper :

1. **firewall and access control;**
2. **identity management and intrusion prevention and**
3. **convergent encryption**

This paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. This paper explains the overview, rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security.

This paper has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 Trojans and viruses. The CCAF multi-layered security can block 9,919 viruses and Trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated.

The experiments show although the percentage of blocking can decrease for continuous injection of viruses and Trojans, 97.43% of them can be quarantined.

Our CCAF multi-layered security has an average of 20% better performance than the single-layered approach which could only block 7,438 viruses and Trojans.

I. INTRODUCTION

The express increase of the Internet and the appearance of cloud calculating have permitted an innovative drift of acquiring and overwhelming Material Knowledge amenities. Cloud calculating has transported new chances to the Material and Announcement Knowledge industry permitting productions to subcontract their IT amenities to cloud wage-earners and circumventhigh-class up-front assets of founding their own infrastructures and resulting costs of conservation and advancements.

By earnings of cloud amenities, cloud clienteles can admittance all their obligatory competences i.e., computational re-sources, information, and submissions over the Internet, use what they necessity, and recompense for what they use deprived of actuality anxious with the fundamental organization (see Figure 1). As a consequence, patrons involvement the coziness of outmoded conveniences such as water, electricity, gas, and telephony. compensation such as a utility representation in totaling to convenience, scalability, and ease of organization have fashioned an industry-wide modification concerning cloud figuring explanations. Cloud computing initiates a foremost transfer in the IT liberation representation by donation computing possessions for hosting requests as an effectiveness which provides businesses and organizations to admittance sophisticated IT amenities existing by shade provider without the exclusive up-front reserves obligatory to create their own communications [1].

II. LITERATURE REVIEW

In this thesissuggests [9] an interconnection clarification for Cloud coalitions based on allocate/recruit military. Here they introduced an original flexible amalgamated Cloud building in which the sustenance bordered by the anxious society is based on a ascendable distribute/promise middleware for active and translucent interconnection of manifold classes of incomes/objects over mixed Internet-based announcement structures. The projected [9] Int Cloud Ware context theoretical and recapitulates the interacted possession accessible within the coalesced Cloud into controllable and energetically provisioned objects, enable relaxed and low-priced descriptions that make imaginable perpendicular and straight announcement amongst the intricate wage-earners gifted complete appropriate borders, supportive the mandatory trustworthiness and ease of use environments of present-day location-independent Cloud tenders.

On the additional pointer such construction suggests new. approaches for realizing DoS boutdiscovery, anticipation, and salvage.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 6, Issue 6, June 2017)

Here they established that in an interconnection organization for joined Clouds the penalties of a DoS dose can broadcast inversely contingent on influences for instance communication gratified and the upkeep of national in the machineries of the middleware. Untried consequence demonstrations that the stuff of DoS bouts that mature the dispersed brokerage, the communication content-complexity and the location defense. Specific retrievals gadgets have to be de-signed with the determination of with stand predictable regulator over presentation and answer periods of such compound organizations.

In an amalgamated Cloud, breadwinners can reciprocally cooperate to portion their incomes and accomplish the request amongs teach other's. For occurrence, a wage-earner can subcontract requirements to other workers when obliging requirements within in digeno us substructure is not conceivable for instance in crowning hours. Unquestionably, this is the circumstance when the fore see able incomes from these purchasers' requirements is greater than the custody of subcontracting them. Consequently, the worker attains developed revenue since it can deliver provision for more patrons without opposite principal costs of gaining IT apparatus which capacity be costly. Similarly, a provider that has underutilized belongings might license part of them to other earner in the alliance [10]. The effectiveness of a mist contractor in a amalgamate situation exceptionally be contingent on widespread range of strictures such as the breadwinner's conventional assignment, the charge of subcontract in gadded incomes, the income of rental underutilized volume, or the cost of preserving the wage-earner's possession seffective. Consequently, cloud workers necessitate partaking an understandable caring of the disadvantage of every conclusion they make. Goiri et al. [10] commend a monetary symbol that symbolizes circumstances that assist conclusions in a amalgamated incomprehensible, such as when to commission possessions to other wage-earners, when to acknowledge requirements from other wage-earners, and how much volume to underwrite to the coalition.

S. Yu, et al. [11], planned a self-motivated stock portion method for defensive discrete clienteles of mist throughout DDoS attack safeguarding excellence of provision throughout attack. The cloud setting is accomplished of supervisory the reserve distribution since it has hugeamount of possessions to apportion to separateoperator.

The standby helping method used in clouds theaters vigorous role in extenuating the impression of dose by philanthropic admittance to capitals. In cloud situation the accomplishment of attack or protection be contingent upon who is property more resources, aggressor or cloud user. The active further standby portion a vertsmal nutrition, thus defensivein contradiction of DDoS bout. They also accessible queue based classical of reserve apportionment under numerous attack situations. They used dependable planet statistics set standing on DDoS attack for investigation of reserve apportionment. In average municipal of activities, the real-world associated in mist has disturbance prevention organization (IPS) for sanctuary determination and column that preserves the list of received packets. Through attack conditions, great number of package licenses finished the column as botnets are used for introduction DDoS attacks there ascend a need of replicating the possessions to upsurge the intrusion expectation systems. This is made conceivable by go-ahead reserve provision. They appraised the exhibition of developed mock-up through imitations in standard and bout circumstances and using Amazon EC2 cloud for procurementconsequences.

M. Glenn [12], in "A instant of DOS/DDOS avoiding, nursing and alleviation technique in an overhaul supplier atmosphere", demonstrates that the incidence and intricacy of Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) on the Internet are quickly snow balling. Provision wage-earners are below cumulative force to avoid, mitigate and monitor DoS/DDoS attacks heading for in the direction of their clientele and their organization. The Internet is portion of the thoughtful countrywide organization but is exclusive in that it has no unvarying limitations to guard it from doses. Attacks that are production a dissimilarity every day on the Internet include philosophical attacks, shortest attacks, remote controlled attacks, viruses and worm. Explicit attacks expressed at a service provider's infrastructure can be very damaging and cause wide spread. Here this paper covers these attacks and talk about techniques to avoid attacks as well as good safety measures policies, latest updated product safety measures tough, and space supervision, spoofed container dropping (uRPF) and IPS/IDS/firewall use in a examine contributor environment. Security of the provider's communications is another key characteristic and that is addressed in this paper.

Fasheng Yi, et al. [13], in "Source-Based Filtering Scheme against DDOS Attacks", describes that IP address spoofing is make use of a lot of DDoS attack tools.

Generally of the existing research on DDoS attack packet filtering depends on collaboration among routers, which is inflexible to achieve in authentic promotions. Consequently, in this dissertation proposition a narrative filtering format based on starting place in sequence in this dissertation to care for against different source IP deal with spoofing.

C. Lin, et al [14], in "An efficient main concern Queue-Based method to lessen spiteful Packet Flows from disseminated DoS Attacks", demonstrates that a DoS attack affects the resources or bandwidth of a targeted system. By flooding networks and distracting access to services, it may reason that harm on multimedia network services and Internet Service Providers. In this paper, the authors propose to evaluate the activities of packet flows and implement a main concern queue-based procedure that allocate packet from standard users to a elevated main concern row and packets from supposed attacker to a low main concern queue. Here they justify by using NS2 simulator to proposed priority queue-based scheme is valuable in blocking attacking traffic while maintaining constant flows for legal users.

Yi Xie, et al [15], in "Monitoring the Application-Layer DDoS Attacks for Popular Websites", illustrates that Distributed denial of service (DDoS) attack is a continuous dangerous threat to the Internet. Originated from the low layer, new application-layer-based DDoS attack make use of legal HTTP requests to overcome victim resources are more untraceable. The case may be more serious when such attacks take off or occur during the flicker crowd occurrence of a popular Website. Mainly these attacks are focusing on the detection for such new DDoS attacks; a design based on manuscript reputation is established. An Access Matrix is defined to imprison the spatial-temporal patterns of a common blaze host. Autonomous constituent psychotherapy and most important constituent psychiatry are practical to theoretical the multidimensional admittance Matrix. A work of fiction anomaly detector based on concealed semi-Markov model is proposed to explain the dynamics of Access Matrix and to detect the attacks. The entropy of manuscript attractiveness correct to the reproduction is used to identify the budding function layer DDoS attacks. Some results based on real Web traffic data are presented to express the effectiveness of the proposed method.

T. Peng, et. al [16] , "Protection from distributed denial of service attacks using history-based IP filtering" describes that this paper, introduce a convenient design to protect against dispersed refutation of service (DDoS) attacks based on IP foundation lecture to filtering. The boundary router keeps a history of all the legal IP addresses which have formerly become visible in the network. When the boundary router is exceed, this record is used to choose whether to acknowledge an incoming IP packet. Distinct additional proposals to defend against DDoS attacks, here there proposal works well during highly-distributed DDoS attacks, i.e. from a large number of sources. The author nearby quite a lot of heuristic methods to create the IP address database correct and robust, and the experimental results shows that effectiveness of their design in defending against highly-distributed DDoS attacks.

Saman Taghavi Zargar.et al,[17] were focus on DDoS flooding attacks and defense mechanisms in wired networked systems. Here, there goal is to categorize the existing DDoS flooding attacks and to provide a broad ranging survey of defense mechanisms categorized based on where and when they become aware of and take action to DDoS flooding attacks. Such a learning of DDoS flooding attacks and the current survey is important to identify with the significant issues related to this essential network security problem so as to put together additional extensive ranging and valuable defense mechanisms. When they avoid, detect, and respond to the DDoS flooding attacks. Furthermore, they highlight do with for a broad distributed and joint defense approach. Our most essential purpose for this work is to support the research community into developing inspired, widespread prevention, detection, and response mechanisms, valuable, proficient, and that address the DDoS flooding problem before, during and after an authentic attack.

DefCOM [18,19] is a distributed framework for DDoS defense. It contains assorted resistance nodes prearranged in a peer-to-peer complex, communicate to realize a energetic supportive resistance and it approved out fatality end, source end, and network core defenses mechanisms to perform attack detection, traffic differentiation and rate-limiting, respectively.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 6, Issue 6, June 2017)

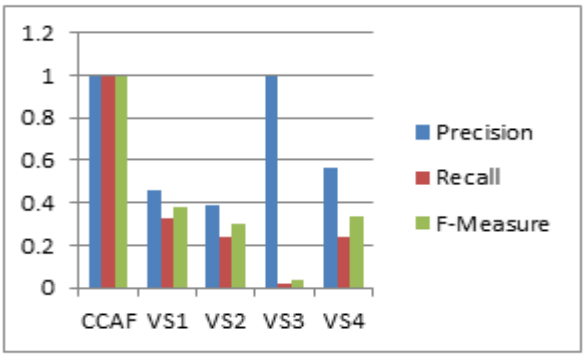
III. Experimental Evaluation

Here I experimentally evaluate the paper "Towards achieving Data Security with the Cloud Computing Adoption Framework " and found that this paper is using multilayered architecture 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption. To validate CCAF, this paper has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 Trojans and viruses. The CCAF multi-layered security can block 9,919 viruses and Trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated. The experiments show although the percentage of blocking can decrease for continuous injection of viruses and Trojans, 97.43% of them can be quarantined. Our CCAF multi-layered security has an average of 20% better performance than the single-layered approach which could only block 7,438 viruses and Trojans.

IV. Experimental Result

Services	Precision	Recall	F-Measure
CCAF	1	0.9919	0.996
VS1	0.455	0.323	0.378
VS2	0.388	0.241	0.297
VS3	1	0.019	0.037
VS4	0.567	0.241	0.338

Results in Table 1 show that the CCAF multi-layered security can provide a much better service CCAF can be used on each VM and each server to check all the incoming data to see whether they are clean, quarantine and free of suspected malicious files. Suspected files will be alerted and moved to the quarantine section ready for further checks. Since experiments have been conducted over 125 hours with 99.19% PTe, 99.98% STe, 100% precision, 99.19% recall and 99.5% F-measure, there is a good reliability. The use of CCAF mutli-layered security can ensure the high level of protection and safeguard of data security for the organizations.



DDOS attacks are huge form of DOS attack where assailants produce anenormous quantity of necessities to injured through cooperated congregation called zombies against computers (zombies), with the intend of deny ordinary examine or belittling of the eminence of armed forces. Disseminated Denial of Service (DDoS) bouts are a mounted form of DoS bouts where manifold attack bots2are working in an prearranged manner to method an attack system for aggressive a specific board. DoS and DDoS attacks are unfortunate for the most of the part after that to be an appropriate for very much perceptive intentions similar to Critical Information Infrastructure (CII). A fine and conventional communication is an example of a DoS attack is a SYN flooding attack [5], which is nearly everyone admired. A piece of information which is frequently acknowledged by safety measures investigators over and done with the globe is no difficulty by means of which grave DoS and DDoS occurrences can be doubtles permitted.

Additionally, the analysis [6] also instigate that the crest of 40 gigabit DDoS attacks almost creased in 2008 associated with the previous year. The grounds following this singularities is that the arrangement safety measures people does not have positive and resourceful suggestion back methods to establish attackers as it is informal for aggressors to camouflage themselves by enchant ingrecompenses of the predispositions of the World Wide Web, such as the self-motivated, circumstances, and indeterminate countryside of the Internet[7][8]. Denial of service is an intentional attempt to entirely interrupt or worse naccessibility of package/possessions to genuine/ authorized user by attackers. DoS attacks more insensitive and easy to execute.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 6, Issue 6, June 2017)

On the other hand, with the ahead of certainty progress of the Internet throughout the recent years, a progressively more large number of susceptible systems are now available to attackers. Attackers can now employ a large number of these susceptible hosts to launch an attack as an alternative of using an on its own server, an approach which is not very valuable and become aware of easily. Generally, this type of attacks create a problem during at system downtime, missing profits, and the substantial effort fit into placed to be acquainted by means of and formulate moving ahead creating such attacks.

V. Conclusion

Our paper has demonstrated the CCAF multi-layered security for the data security in the Data Center under the proposal and recommendation of CCAF guidelines. We explained the rationale, overview, components in the CCAF, where the design was based on the requirements and the implementation was illustrated by its multilayered security. We explained how multi-layered security was a suitable method and recommendation, since it offered multiple protection and improvement of security for 10 PB of data in the Data Center based at the University of London Computing Center (ULCC). We explained the technical details in each layer of security and propose an integrated solution to check all the data when data is intensively used. We used the Business Process Modeling Notation (BPMN) to simulate the cases of how the data can be used, either at rest, in use, or in motion. All simulations could be completed within 2 seconds. Our BPMN simulation results showed that it could take up to 50 hours to protect all the 2PB data and up to 125 hours to raise an alarm to take control of the situation in the ULCC Data Center. This means that an integrated approach was required to ensure data protection, in case that the data center is under the attack or potential threat from the rapid rise of data growth in the data center, which can be due to the external intrusion or the internal rapid consumption. We then used FGSM for the penetration testing. 10,000 viruses and trojans were injected into Data Center with two experiments performed. The first experiment showed that firewall, identity management and encryption could block 5,423, 3,742 and 842 viruses and trojans respectively. The remaining 81 could be either quarantined or isolated. The second experiment showed that continuous injection of 10,000 viruses and trojans could make the blocking rate decreased from the 99.19% to 76.00% in 125 hours.

Despite of this result, the CCAF multi-layered security could quarantine and isolate 97.53% of viruses and trojans. Our work can demonstrate that the use of CCAF multi-layered security can protect the data center from the rapid data growth due to the security breach, and the use of BPMN can calculate how much time required for rescue action if the data security is compromised. In this way, we can work out the better tactics and plans for data recovery and security. In this paper, we demonstrated that CCAF multilayered security could provide the additional protection for all 10 PB of data in 125 hours when the Data Center was under the security threat and attack. Data security in the Cloud is an important issue for Cloud adoption. We demonstrated that our approach could provide real-time protection of all the data, block the majority of threats and quarantine the petabyte systems in the Data Center. We plan to improve our method and code in the simulation and choose the right type of algorithms to improve the overall performance in execution time of data security and blocking viruses/trojans in real-time. We will develop more services and proofs-of-concept in CCAF to improve the performance of BPMN simulation and penetration testing. Existing studies on cloud security [11, 14, 20- 24; 28-29, 33] have been focused on either identify management, general issues concerning cloud security, access control or architecture layers. Our approach provides an integrated solution to cloud security based on a clear framework, business process modeling to study the impact on the performance of a user accessed service which is often learned on the fly which is costly and a CCAF three layered model.

REFERENCES

[1] John Reumann. GooPS: Pub/Sub at Google, Lecture & Personal Communications at EuroSys & CANOE Summer School. 2009.

[2] G. Loukas, and ¨G. Oke, “Protection against denial of service attacks: A survey.” Computer. Journal. 53, pages-1020–1037. (2010)

[3] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita “Surveying port scans and their detection methodologies.” Computer. Journal., 54, Pages-1565–1581,(2011)

[4] H. J. Kashyap, and D. K. Bhattacharyya “,ADDoS attack detection mechanism based on protocol specific traffic features.”, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India, 26-28 October, pp. 194–200. ACM. , (2012).

[5] Eddy, W. TCP SYN flooding Attacks and Common Mitigations. http://tools.ietf.org/html/rfc4987. RFC 4987, IETF published document, 2007.

[6] IP Flow Based Technology", Arbor Networks, http://www.arbornetworks.com, 2010.

[7] C.Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks," The Internet Protocol J., vol. 7, no. 4, pp. 13-35, 2004.

[8] T. Peng, C. Leckie, and K. Rama mohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys, vol. 39, no. 1, p. 3, 2007.

[9] Christian Esposito, Massimo Ficco, Francesco Palmieri, Aniello Castiglione, "Interconnecting Federated Clouds by Using Publish-Subscribe Service" Cluster Comput (2013) 16:887–903

[10] I. Goiri, J. Guitart, and J. Torres, "Economic model of a cloud provider operating in a federated cloud," Information Systems Frontiers, vol. 14, no. 4, pp. 827–843, 2011.