An Effective Data Transmission Process in Interconnected Federated Cloud using Decision Tree Algorithm

M. S. Premalatha
Research Scholar, Manonmanium Sundaranar University, Abishekapatti, Thirunelveli – 12, Tamil Nadu, India.
premalatha_ms@yahoo.co.in

Dr. B. Ramakrishnan
Associate Professor, Department of Computer Science and Research Centre, S.T. Hindu College, Nagercoil, Tamil Nadu, India.
ramsthc@gmail.com

Abstract – The main objective of this research is to predict the behaviour of the packets in interconnected united cloud victimization ID3 classifier. Basically, the system consists of 4 modules like (i) Feature selection (ii) Rule generation process, (iii) Decision tree generation and (iv) Prediction of traditional and attack Packets. At first, an interconnected united cloud with the physical configuration of knowledge centres with brokers and virtual machines is meant. Then, the quantity of packets from knowledge homeowners to knowledge centers is shipped. After that, choose the necessary options for every packets victimization using flower fecundation algorithmic program. Then, the chosen options area unit is given to prefix span algorithmic program to form a rule. After that, supported the foundations there is a tendency to produce decision tree algorithmic program. Finally, in testing, the choice tree detects a given packet as traditional or attack.

Index Terms – Decision Tree, Packets, Attack, ID3 Classifier, Flower Pollination Algorithm, Prefix Span Algorithm, Feature Selection, Interconnected Federated Cloud, Transmission System.

1. INTRODUCTION

Cloud computing is a system put together with conditions for those concentrations with respect to sharing calculations or assets. Everything considered, clouds are Internet-based and it endeavours to disguise flightiness for clients. Cloud computing implies both the applications passed on as administrations above the web with the hardware and programming in the server that gives those administrations [1]. Cloud providers use virtualization joined with self administration capacities with respect to computing resources by methods of a framework. In cloud circumstances, a couple of sorts of virtual machines are encouraged on indistinct physical server from establishment. In cloud, customers should pay for what they use and have not to pay for neighbourhood resources which they need to, for instance, storing or system. These days, there exist three kinds of cloud: Public, Private, and Hybrid clouds [2]. An open cloud is standard model which suppliers build some assets, for instance, request and capacity, reachable to the common population. Out in the open clouds which they are running applications remotely by tremendous administration supplier which suggests a couple of points of interest over private clouds. Private Cloud suggests administrations of a business that isn't available for common people. Fundamentally private cloud is an advancing term for building that gives encouraged administrations to explicit social affair of people behind a firewall. Cross breed cloud is a space that an association gives and controls a couple of benefits inside and has some others for open use [3].

In addition, Inter-cloud is an interconnected clouds around the world. The expression was initially proposed with respect to cloud computing in 2007 when preached that "over the long haul we'll have the communication between clouds, the cloud of clouds". It ended up unmistakable in mid-2009 and has been used to portray the server farm of things to come. The Inter-cloud is interconnected around the world group of clouds [7]. It can give a development of computing and limit capacity to a lone cloud. These structures make sure the information, framework and establishment safety for a secure and trust based cloud systems. The cloud scheme must reinforce information and effective device broadcast among cloud structures [8].The security and execution assessment of the convention demonstrates its prevalence over the cutting edge between cloud information movement [9]. Between cloud information relocation is a general new issue and its security ensures have not acquired the due consideration. The secure information relocation between clouds has additionally been discussed about in [9].

As examined in [4], it can change a huge bit of the IT business, making programming altogether logically appealing as an administration and embellishment the way in which IT gear is arranged and purchased. At the present time, it is progressing as an optimal computing stage for distributing assets with establishment assets, programming resources, and others [5]. In any case, with the immense proportion of benefits on the web, these cloud systems are going up against genuine security issues. Appropriated attack ambush can be considered as an essential peril to cloud computing. This strike will impede the certified access to the servers, exhaust their advantages, for instance, orchestrate exchange speed, computing influence and even lead to amazing budgetary hardships as showed in [6]. Security issues that may exist in the cloud are high to the point, that even the entire IT industry has experienced a transformation; in any case, it isn't immaculate [10]. Existing security innovations still can't tackle a portion of the issues related with cloud security; there are such huge number of security attributes of the cloud that are hard to give complete show. Security approach is expected to guarantee sound and stable improvement of cloud computing. Along these lines, the security based information transmission framework is quickly required.

2. LITERATURE SURVEY

Bunch of analysts have clarified about the information transmission in interconnected combined cloud. Among them a portion of the papers are displayed in the writing audit; Joseph et al. [11] have clarified security attacks. It was considered as a standout amongst the most genuine dangers to developing cloud computing foundations. It goes for contradicting admission to the cloud foundation by making it inaccessible to its clients. This was the reason that essential financial and hierarchical harm contingent upon the kind of utilizations running on the cloud that have turned out to be inaccessible. This acquainted an expansion with unified cloud engineering to utilize versatility and relocation of virtual machines to manufacture adaptable cloud barriers against attacks. The engineering was approved by appearing three DDoS assault situations taken care of by the DDoS countermeasures.

M. Ficco et al. [12] have specified Intrusion Detection in Cloud Computing. Digital assaults speak to a genuine peril, which bargains the nature of service conveyed to the clients. The paper shows a distributed design for giving interruption identification in Cloud Computing, which empowers Cloud suppliers to offer security arrangements as a service. It was a various levelled and multi-layer engineering intended to gather data in the Cloud, utilizing different distributed security segments, which can be utilized to perform complex connection examination.

Bing Wang et al. [13] have mentioned a DDoS assault insurance. Here, they address the imperative security issues. They found that SDN innovation really assists undertakings with defending against DDoS assaults if the safeguard engineering was planned legitimately. Keeping that in mind, they clarified a DDoS assault relief engineering that coordinates a profoundly programmable.

Wanchun et al. [14] have identified a certainty based sifting technique for DDoS assault guard in cloud condition. Solidly, the technique was conveyed by two periods, i.e., non-assault period and assault period. All the more uncommonly, real parcels were gathered in the non-assault period, for removing credit sets to create an ostensible profile. With the ostensible profile, the CBF technique was advanced by figuring the score of a specific parcel in the assault time frame, to decide if to dispose it or not. Finally, broad reproductions were led to assess the plausibility of the CBF technique.

Reehan et al. [15] have mentioned a strategy for information examination and handling by means of inadequate regularized enhancement that chooses a little subset from the first component factors to display the information with the end goal of arrangement. A direct SPLR expects to choose the discriminative highlights from the archive of datasets and study the parameters of the straight classifier. Contrasted and the component choice methodologies, similar to channel (positioning) and wrapper techniques that differ in the element choice and characterization issues, SPLR can consolidate determination and grouping into a brought together system.

K.Abirami1 et al. [16] have explained that Vampire assault was emptying of hub life out of remote impromptu sensor systems. Asset exhaustion assault forever incapacitates arranges by rapidly depleting hubs battery control. Vampire assaults were extremely hard to recognize in light of the fact that they assault the hub just by sending convention consistent messages. PLGP with validations (PLGP-an) is issued for recognizing malignant assault. M-DSDV directing convention is utilized to identify and dispense with the asset exhaustion assault from the system.

Jiachen et al. [17] have clarified a Multimedia proposal and transmission framework dependent on cloud stage. This paper displays a film proposal framework as per scores that the clients give. In perspective of the motion picture assessment framework, the effects of access control and interactive media security was dissected, and secure cross breed cloud stockpiling design is displayed. Versatile Edge Computing (MEC) innovation was utilized in the general population cloud which ensures the high productivity necessities of the communication of the sight and sound substance. The procedures of the framework including enlistment, client login, job task, information encryption and information unscrambling were likewise portrayed. Finally, the execution of the proposed plan is broke down which further demonstrates that the different conceivable assaults can be moderated by means of the proposed framework.

3. INTER CLOUD SYSTEM

In an inter cloud system, centre that points on a cloud would use assets, management or knowledge from varied clouds. The essential target of a bury cloud structure is to create strait edges that may direct the swap and transportability of knowledge from a cloud to the others. To structure these options, there's a necessity of constructing a capable tradition to interchange information to clouds. Affiliations ought to be developed on the contraptions which is the limit of the cloud. All cloud traditions ought to have the flexibility to be silent distinctive traditions that has got to be affordable in varied clouds.

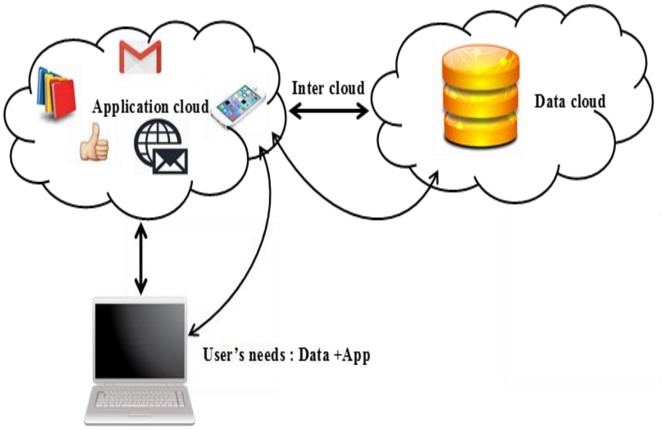

Figure 1. Message transmission over clouds

4. PROPOSED DATA TRANSMISSION SYSTEM IN INTER CLOUD FEDERATION SYSTEM

Cloudlets are the owner who sends the data to the Data Center which is managed by Brokers and processed by Virtual machines. With the advent of this new technology several new issues arise specially related to the Security. It is an imperative worry amid the transmission of information whether in wired or in remote correspondence. When we transfer the packets to the data center, sometimes malicious attack happen on the original packets information and discard some of the information. This is one of the main problems in the data transmission system. Hence in our proposed work a more improved framework is implemented for data transmission system which consists of Interconnected Federated Cloud where Data Packets send from various Cloudlets is send through Brokers. The behaviour of the packets is computed using four modules such as (i) Feature selection using FPA, (ii) Rule generation, (iii) Decision tree generation and (iv) Prediction of behaviour of packets. Initially, an Interconnected Federated Cloud is designed with the physical configuration of data centers with brokers and virtual machines. Then, number of packets are send from data owners to data centers via brokers. To reduce the response time of the brokers, in this paper border brokers are connected in parallel. After the Interconnected Federated Cloud design, the behaviour of the packets is predicted. In this, the important features from each packet is selected using flower pollination algorithm that reduces computational burden and enhances performance of ID3 classifier system. Then, the obtained packet with subset of attributes is given to the prefix span algorithm, to generate the logical rules. Then, the obtained rules are given to ID3 classifier to design a decision tree based on rules. After that, the packets are tested and predict the packet as normal or attack using frequency behaviour. The proposed Interconnected Federated Cloud architecture is given in Figure 2.

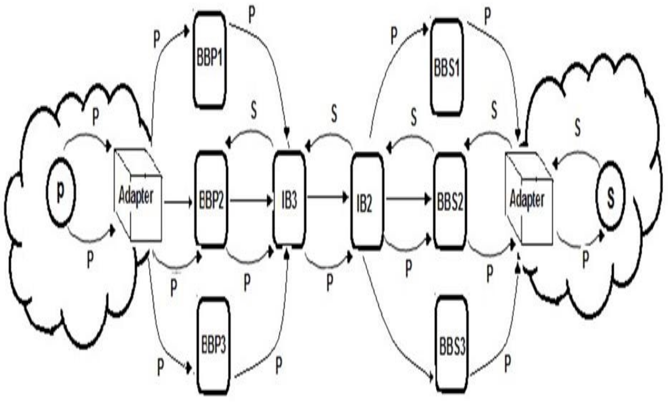

Figure 2. Architecture of Interconnected Federated Cloud

4.1 Feature selection

In this paper, the KDD glass 99 dataset is used for interruption recognition framework. This dataset is huge with every parcel made out of 41 highlights; formation of a standard set is extremely dull. Besides, all highlights won't be important or completely contribute in recognizing an assault. So the quantity of highlights must be diminished so as to create effective standard set for arrangement. There are a few techniques for highlight significance examination. Here, improvement calculation is utilized for highlight selection.

4.2 Rule generation

After the highlight selection process, the standards are produced dependent on highlights utilizing Prefix Span calculation. Prefix Span (i.e., Prefix-anticipated Sequential example mining) is a novel consecutive example mining technique, which investigates prefix projection in successive example mining. Prefix Span mines the total arrangement of examples however significantly lessens the endeavours of applicant subsequence age. Besides, prefix-projection generously diminishes the extent of anticipated databases and prompts effective handling. Consider the reduced dataset with class value. Before, we generate the rule; we have to convert the features values into discretization format (i.e., Low, High, and Medium). The step by step process of rule generation using prefix span algorithm is explained below.

4.3 Decision Tree creation using ID3 classifier

After the standard age, we need to create the decision tree utilizing ID3 classifier. ID3 calculation is a customary decision tree characterization calculation which makes utilization of information gain as an attribute selection technique. To demonstrate the grouping procedure, a tree is developed utilizing the decision tree method. When a tree is constructed, it is connected to every parcel in the database and this outcome in arrangement for that bundle. The decision tree calculation depends on Entropy, its primary thought is to outline guides to various classifications; its inside is to choose the best game plan property from condition characteristic sets. The computation picks data gain as quality determination criteria; generally the property that has the most bewildering data gain is picked as the part trait of the present center. Branches can be set up subject to different estimations of the traits and the methodology above is recursively moved towards each branch to influence diverse center points and branches until all of the precedents in a branch have a place with a comparable grouping. To pick the part traits, the thoughts of Entropy and Information Gain are used. Here, the most outrageous data trait is picked as the root center.

5. CONCLUSION

Nowadays, system security is one of the major worries because of different attacks and vulnerabilities in cloud. As a result, attack detection is an imperative segment in system security. Here, ID3 and optimization algorithm is explained based on the behavior of packet prediction in inter cloud federation system. The Optimization algorithm is used to select the important features from packets. The ID3 classifier is used to make the decision tree. After various stages of training process, test dataset is given as input and finally the classified output is obtained. The experimental results using the KDD CUP 1999 dataset demonstrates the effectiveness of the approach which provides better successive rate than the existing method.

REFERENCES

[1] Hassan and Qusay "Demystifying Cloud Computing", The Journal of Defense Software Engineering, CrossTalk, 2011 (Jan/Feb): 16–21.

[2] F.M. Aymerich, G. Fenu, and S. Surcis, An approach to a cloud computing network. Applications of Digital Information and Web Technologies, 2008. ICADIWT 2008, pp. 113 –118, August 2008.

[3] Chengpeng Wu, Junfeng Yao and Songjie, “Cloud computing and its key techniques”, Electronic and Mechanical Engineering and Information Technology, vol. no. 1, pp. 320-324, 2011.

[4] M. Armbrust, et al., “A view of cloud computing”, Communicaton ACM 53 (4) (2010) 50–58.

[5] L. Zhang, Q. Zhou, “CCOA: cloud computing open architecture” in Proceedings of the IEEE International Conference on Web Services, 2009, pp. 607–616.

[6] T. Peng, C. Leckie, K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems”, ACM Computing Survey 39 (1) (2007) 3.

[7] D. Bernstein, E. Ludvigson, K.Sankar, S. Diamond, and M. Morrow, “Blueprint for the intercloud protocols And formats for cloud computing interoperability,” in Internet and Web Applications and Services, 2009.

[8] IETF, “Extensible messaging and presence protocol (xmpp): Core rfc6120,” 2011. [Online]. Available: http:// datatracker.ietf.org/doc/rfc6120/

[9] Qingni Shen; Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "SecDM: Securing Data Migration between Cloud Storage Systems," Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference, pp. 636,641, 12-14 Dec. 2011.

[10] Ramgovind S, Eloff MM, Smith E., “The Management of Security in Cloud Computing”, IEEE 2010.

[11] Joseph Latanicki, Philippe Massonet, Syed Naqvi, Benny Rochwerger and Massimo Villari, “Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks*”,* Towards the Future Internet - Emerging Trends from European Research Source: DBLP, 2010.

[12] M. Ficco, L. Tasquier, and R. Aversa, “Intrusion Detection in Cloud Computing,” in 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2013.

[13] Bing Wang, Yao Zheng, Wenjing Lou and Y. Thomas Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking", Computer Networks 81 (2015) 308–319.

[14] Wanchun Dou, Qi Chen and Jinjun Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment", Future Generation Computer Systems, vol. 29, pp.1838–1850, 2013.

[15] Reehan Ali Shah,Yuntao Qian, Dileep Kumar, Munwar Ali and Muhammad Bux Alvi, “Network Intrusion Detection through Discriminative”, Feature Selection by Using Sparse Logistic Regression", Journal of Future Internet 2017.

[16] K.Abirami1, R.Saranya, P.Jesu Jayarine, *“*Maintaining Lifetime of Wireless Ad-hoc Sensor Networks by Mitigating Resource Depletion Attack using M-DSDV*”,* IJRDE 2014.

[17] Jiachen Yang, Huanling Wang, Zhihan Lv, Wei Wei, Houbing Song, Melike Erol-Kantarci, Burak Kantarci and Shudong He, "Multimedia recommendation and transmission system based on cloud platform”, Future Generation Computer Systems, 2015.

Authors

M. S. Premalatha received BSc degree in Computer Science from Nesamony Memorial Christian College, Marthandam. She received Master of Computer Applications from Bishop Heber College, Thiruchirapalli and Master of Philosophy in Computer Science at Manonmanium Sundaranar University, Thirunelveli. She is currently working as Assistant Professor in the Department of Computer Applications, Nesamony Memorial Christian College, Marthandam. She is a Research Scholar in Computer Applications at Manonmanium Sundaranar University, Thirunelveli. Her field of interest is Mobile communications, Green computing and Cloud computing.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 30 years. He has 23 years of research experience and published more than 70 research articles in reputed international journals (14 Science Citation Index Expanded research articles and 25 SCOPUS indexed research articles). Further, he has authored a book titled “Vehicular Ad Hoc Network and Web Vehicular Ad Hoc Network an Overview” published by the International book publisher LAP Lambert Academic Publishing with the ISBN:978-3-330-02628-5. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.