A Novel Framework Model for Implementing Defensive Auto-Updatable and Adaptable Bot Recommender System (DAABRS) for Cloud Computing

Menaka.N[1], and Jasmine Samraj[2]
[1]Research Scholar (Ph.D.), PG and Research Department of Computer Science,
Quaid-E-Millath Government College for Women (Autonomous), Chennai.
[2]Associate Professor, PG and Research Department of Computer Science,
Quaid-E-Millath Government College for Women (Autonomous), Chennai.

Abstract: Cloud Server Data Security widely uses data centres along with immediate available Edge System for potential transaction of large and privacy sensitive data. This type of Edge Systems are picked rental based on its utility where novel challenges are to be faced pertaining to its privacy and security issues. Due to dynamic mobility of Edge System selection utilization attacking threat risks are comparatively higher. In this proposed system the Cloud Centre determines the secured Edge System implementing Defensive Auto-updatable and Adaptable Bot Recommender System (DAABRS). Cloud Data Centre with Edge System involves various environments and users, in which attackers can easily invade with anonymity and interrupt the privacy in Edge System. Most relevant security mechanism for advancing threats and attacks for Edge System which rents extra cloud storage can be done by implementing Stealth Mode Bots inside data segments. Besides predicting and preventing the data attacks in Container, Tenant System or Edge System and Server Partitioning by infusing Stealth Mode Bots for each. Recommending feasible Bots for Tenants, Edge System or Containers for efficient security infused Stealth Mode Bots invoked when specific data segment got disconnected. The proposed system involves Updatable and Adaptive Bots in accordance with Edge System attacks. It also blocks highly attacked Data Container by invoking Stealth Mode Bots and specifications will be updated using Machine Learning for figuring out and blocking the subsequent attacks.

Keywords: *Adaptable and Updatable Bot, Cloud Data Centre, Containers, Defensive Bot, Defensive Auto-updatable and Adaptable Bot Recommender System (DAABRS), Edge System, Feasible Bot Selection, Stealth Mode Bots, Tenants.*

1. Introduction

Edge Systems, Containers or Cloud Data Centres faces novel challenges in data security and privacy protection. Utilising Edge Systems results in potential transaction of huge amount of data in which the consequences of data privacy is not assured. In Cloud Data Centres the Edge Node data has limited resources and supports complicated security system. As edge computing has high human vulnerability of different users and device resources the security mechanism provided also faces equal difficulties. Various edge computing threat models and attacks for edge computing have different defences and counter measures. Different types of web clients and web pages to track Bots and honey pot generates dynamically with different types of hyperlinks [1]. Analyzing the sequences of link requests possible to detect and acknowledge Bots dynamically generates various types of hyperlinks leads to other information about system. Optimize the whole bot operations intending to attack websites and extract sensitive information for classification of websites.

Collected data can be monitored with present activity of web bots in terms of quality for functioning and behaviour. Prevention of potentially malicious threats applied in web application firewall. Different sorts of honeypots in internet with spider trap, are reactive honey pot with advanced super next generation. There are various ways to protect web applications for users extend validity of SSL certificates with strict transport security. Load balancing along with protection against Distributed Denial of Service (DDoS) cyber security secures web applications in published blogs and methods of Hypertext Transfer Protocol (HTTP) requests classification of HTTP requests. Website protection from malicious internet traffic, process the data to create IP addresses collecting with connected data with anonymous ones. Honeypot installed software's depending on infrastructure to access application interfaces.

In detecting malicious social bots detection the prevention based on the possibility of clickstream sequences and clusters of supervised structures [2]. In online social networks analyzing probability of clickstream sequences illustrates the detection of accuracy. Different types of malicious social bots detect transition probability of clickstream increases detection based on user behavior. Social bots corresponding to various cloud stream increases the quality and efficiency of data transaction and data analysis from all social networks. Real time social bot detection and prevention from social platforms blocks malicious bots using semi supervised clustering methodologies. Fabricated detection of fake bots executes in timely manner in the background of websites. The hybrid transition feature and probability feature enhances robustness and improvises accuracy of social bots features with temporal and spatial dimensions [3]. The constrained K-means algorithm used for finding threshold error that finds number of iterations to procure social bot detection algorithm.

World Wide Web (WWW) significantly increases digital marketing and enables online payments which can overload the server of internet environment. Specific operations required for excessive bandwidth system connects with irrational Random Access Memory (RAM) with the power of processor in handling situations. Hard disc and Central Processing Unit (CPU) enables the server to handle the load of space in drive of virtual memory implies loads on server handles the linked server to be overloaded with global server. Cloud computing emerges in information technology with load balancing identifying the server issues [4]. Subspace in big data distribution model of network traffic of data. The neural network identification conducts real statistics analysis based of each websites network of data, website link between traffic and quality of hyperlink data with performance indicators.

Internet of Things (IoT) Botnet malware increases the substantial threats by compiling the synthesized data Botnet [5]. It detects and prevents device attackers known as Bot master. Crypto Botnet uses crypto currencies runs on embedded devices specified as routers, cameras and set top box powered computing devices. The ransom ware infected files are encrypted with files retrieves its legitimate owner which generates malicious activity on internet. Traditional bots detects and mitigates large amount of spam comprises of IoT devices which is triggered normally.

2. Literature Survey

Distributed computing for topology and location service in which the service oriented paradigm contains three main services like Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS). IaaS is a hardware structure contains storage servers and devices in data center. SaaS deliberately combines application in accordance with its needs. PaaS works in end user development and testing of applications in its operating system [6]. Cloud container used for optimized resources attain with tremendous rise demanding the cloud containers, tenants or edge system implemented for utilization purposes [7]. The cloud container sequentially allocates data received through streaming process. Streaming data from cloud center has rapid movement approaches the continuous stream data processed simultaneously. Both stream and batch processing are big operational modes of data center in streaming data [8]. The process of streaming data clarifies and analyzes the immediate streaming of allocating immediate data process in containers. Different batch processing sent and received through batches of data sets for analysis in database the results provided thereafter [9].

The resource management in cloud computing servers schedules job in accordance with key concepts related to scheduling strategies as stated. Garg et al. [10] states the utilization of boosting the resource allocation for cloud centre. The profit enhances the virtual machines in predicting the models for Artificial Neural Network (ANN). There are multiple objectives optimized through data segregation is constructed. Quality check fulfils the boosting algorithm prerequisite for agreement in service level users. Adhikari et al. [11] establish the resource allocation techniques along with optimization tasks that help with bat theory. The K-means algorithm helps minimizing the computational time and execution of each task.

Guerrero et al. [12] uses the sorting of genetic model II (NSGA-II) for optimizing the resource management in cloud containers where the container allocation follows different strategies for allocating the project to its target container which equally balances its workload evenly improvises the reliability of applications. It also reduces network load containing communication overhead. Kaur et al. [13] generates multiple objectives for scheduling models while implementing Fuzzy Particle Swarm Optimization (FPSO). FPSO system attains reduction of transmission time, consuming energy and processing power consumption with maximum attained resource utilization through virtual machine. Based on various container scheduling strategy for micro services with allocation of various methodologies as conferred by Lin et al. [14]. Several foregoing systems processes allocations of containers related to migration process. Kim et al. [15], recommends optimal container migrating the allocation of process in edge computing. The selected migration of cloud system reduces the traffic in network when it is in allocation process. Ouyang et al., [16] proposes a bandwidth of application area with artificial fish swarm algorithm for proper resource utilization of server.

The prediction behind random go through in social networks are faster and helps in recognizing Sybils and according to Zhou et al [17] actual accounts swiftly goes through random Sybils. At its higher level they deploy random nodes as sybils and in different perspectives of trusted nodes. Random go through in Sybil Infer methods where it deploys combinations Bayesian inference and Monte carlo sampling techniques so that they estimates actual Sybil users. Sybil Guard [18] assumes malicious users which can create many Sybils with fewer connections to trusted accounts. Various similar and trusted accounts are bounded to Sybil Limit [19] and they attempt isolation of Sybils based on random go through. Sybil Guard improvises optimal guaranteed networks and Sybil Ranks are predicted based on probability of short go through and escapes from its region of trusted nodes.

3. Proposed Methodology

In universal data transmission through Cloud Data Server, involves various strategies for highly secure mode of data transaction. This includes deployment of Cloud Data Centres, Tenants and most importantly Edge System. Anonymity and privacy for data transaction is secured in Edge System or Tenant based Server sharing system. Immediate solutions for Scalability Issues, Software Security of Edge Nodes are provided. Protocols and standards of Edge System are entrusted using lightweight cryptography tools. Social networks in online such as Facebook, Twitter or LinkedIn dominate public communication channels. The community allows people to involve, interact and share information efficiently and attracts its value [20]. According to Application oriented interactive environment that exploits, Social Bots where the software automates user activities which create pseudo posts looks alike human generated. It interacts with humans as if another human is interacting and sharing information with one another and attracts other human through such bots.

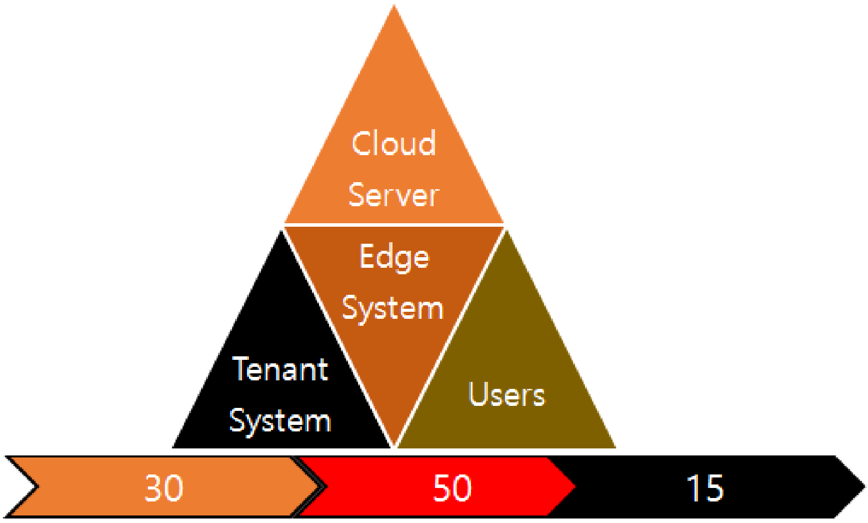

Fig.1 Cloud Storage Server and Bot Attacks System

Activities such as reposting posts, pictures and status of others, adding comments, likes and dislikes to others accounts according to the comfortable varied connections of Bots. Social Bots aggravates Dummy Bots and increases positive or negative impacts on News, Weather, Blogs or Reposts in Social Network. These kinds of Bots invade with comfortable conversations with humans and establish various impacts on society which can be used for good or bad intentions. These kinds of Bots are very difficult to be identified. Proposed System provides Recommendation for Edge System, Tenant System, and Container. The above mentioned Fig.1 predicts and prevents the blocks in data infringement. These servers can be procured rental based for flexible transaction even extra cloud storage can be added on requirement. Containers have efficient Server partitioning and data distribution system which is highly secured. Bots are imparted in Cloud Data Servers which selects number of Servers, Tenants, Edge Servers or Containers to be used and how efficiently secured they are to provide privacy and secured data. Thus the Bot Recommender System is formulated for Data Privacy and Bots are analyzed and chosen for selecting the Server.

Bot Recommender System deploys various Stealth Mode Bots liable to privacy issues through Edge Computing. Universal data transactions occur securely and privately using Servers from Cloud Centers, Containers, Edge Systems or Tenant Systems. Defending Bots and Adaptable bots are deployed to Cloud Centre with fast storage server and flexible capacity. Edge Server or Edge System can be used rental for fast download of receiving sensitive data. Tenant system is chosen based on speed, accuracy, efficiency, privacy, sensitivity for distribution of data in server. Once the Edge System's or Tenant System service is finished, it can be made available for subsequent tasks. In Edge System or Container Malicious imitation of actual people or Organization are in practice for identifying the fraudulent. Offensive speculations of promoting ones ideas through these Bot promotions where own speculations as real with their fake identities. Malicious activities following fraud activities with Sybil attacks considering large scale Bots Recommending Online Social Networks. Techniques distinctly detect malicious activities on Online Social Networks where Social Bots are detected with methodological categorization that reveals possible Bot Detection. Defensive Auto-updatable and Adaptable Bot Recommender System (DAABRS) has been shown in fig.2.

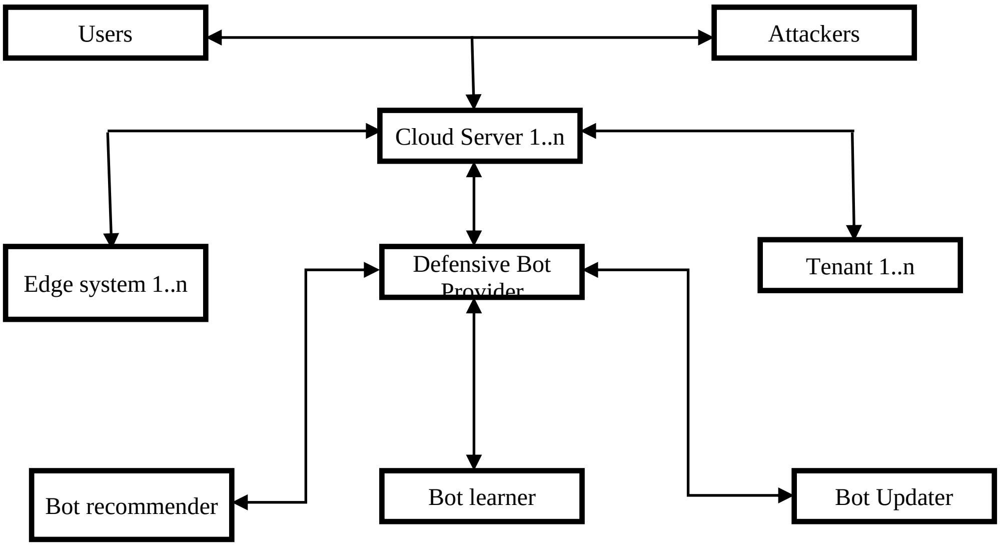

Fig.2. Defensive Auto-updatable and Adaptable Bot Recommender System (DAABRS)

Cloud server has many Bots for predicting and preventing attacks invading data and those are known as Defensive Bots which is also Adaptable and Auto-updatable when any novel attacks approached. It also infuses Stealth Mode Bots inside each data segments of tenant, container, edge server or cloud data centre which is intentionally hidden for most sensitive, private and secured data. Once the data segment is disconnected abruptly or accidentally then promptly the Stealth Mode Bots will be invoked and destroys the complete data without letting it to any malicious hands.

Securing cloud server data uses Elliptical Curve Cryptography (ECC) algorithm which is public key cryptography technique involved based on algebraic structure with elliptic curves. Key based security used in ECC algorithm with finite fields which secures efficiently. It also involves Long-Short Term Memory (LSTM) algorithm which is an Artificial Neural Network (ANN) based deep learning that requires feedback connections with recurrent neural network. It processes entire sequence of data by predicting data where tasks are segmented and prioritized. The Edge System, Cloud Server, Tenant System or Container Bot Recommender System detects in accordance with its data privacy level. It will be classified as Low, Medium and High level of security threat and the bots act accordingly. Bot recommender system in cloud service provider analyzes new attacks and classifies the threat level; if it is low then it predicts and notifies the user, if it is medium level it predicts and prevents the threat. In case of high level security attack the bot predict it and promptly block the attack and also notifies the user

Bots also acts as auto updatable and adaptive bots as in Fig.2 which processes in a disparate and customized manner exclusively for Edge System, Container, Tenant and Cloud Data Centre. Bot provider recommends Defensive Bots to secure data, Auto- updatable Bot to update new attacks and Adaptable Bot that adapts to novel attacks and learns new specifications of process through machine learning.

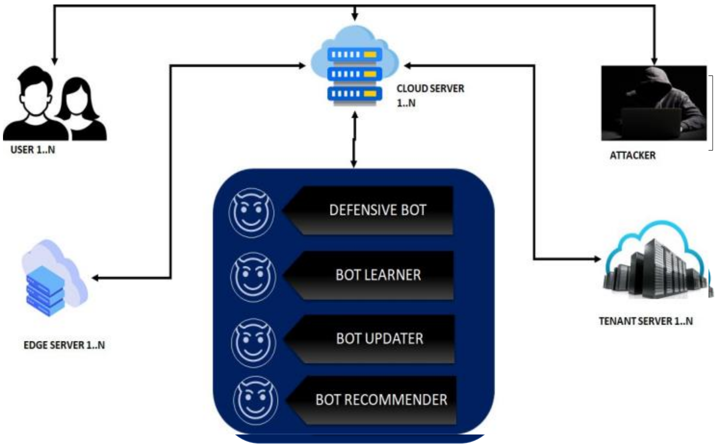

Fig.3 Architecture of Processing Recommender system

In above Fig.3 Cloud Server loads with N number of users and those data are stored securely using various Cloud Server, Tenant System or Edge System. All such systems are segregated into N number of Data Server and used on chatter based. Each user is allotted with server space that ensures data security with various segregated server space. In this, Defensive Bots are deployed by predicting and defending attackers. Bot learner learns and finds solutions to novel attacks and is updated with new bot learning. Bot Recommender System deploys with Stealth Mode Bots which are invoked once the connection is lost from cloud data centre. These Stealth Mode Bots are hidden and could not be recognized by any attackers or any techniques. Once the supervision from Cloud Data Centre or Edge Server or the Tenant System is lost, the Stealth Mode Bot is automatically invoked and destroys all the data in that data chunk. Thus no one can retrieve the data from that particular data segregation even if the attacker steals data it ends in vain. This kind of learning is updated and adapted in machine learning for subsequent defending process. The below described steps and Algorithm 1 depicts the work flow of proposed system.

Step 1: Bot provider tracks Cloud Server.

Step 2: Bot Recommendation for Cloud Server.

Step 3: Defensive Cloud Bot verify data for attacks.

Step 4: Defender bots are sent to tenant and Edge Systems for defense.

Step 5: Machine learning for attacks.

Step 6: Updating Bots with learnt data.

Step 7: Defensive Bot Recommendation analysis for Cloud Service Providers (CSP).

Step 8: Stealth Mode Bot Recommendation if needed.

Step 9: Acknowledging Stealth Mode Bots.

Step 10: Automatic activation of Stealth Mode Bots in critical condition.
Step 11: Data diffuser and destroyer activated in Stealth Mode Bots.
Step 12: Diffused data reaches to Bot Server if possible.
Step 13: Recommendation of Adaptive Bots for CSP.
Step 14: Adaptive code updater for Adaptive Bots.
Step 15: Self-destruction of unused and critical Bots.

```
Algorithm1. Defensive, Adaptive and Auto-Updatable Bots
Input:$B_{csp}$// Bots for CSP
Output:$P_{db}$//Protects Server by Defensive Bots
Initialization: Bot Allocation
While ($T_{csp}$) //CSP tracking
    $C_{sc}$csp←Security check
    $ES_a$←Edge Server analyses
    $TS_a$←Tenant Server analyses
    If ($R_t$<T) then // Risk lower than threshold
        $B_r$ for CSP minimum←Bot Recommendation for CSP
        If ($E_s$>0) then // Edge System is used
            $B_r$for Edge System←Bot Recommendation for Edge provided
            If ($Ec_u$) then // Edge System connection is unstable
                $S_{int}$←Stealth Mode Bots are initiated
            End if
        End if
        If ($T_s$>0) then // Tenant System is used
            $B_r$ for tenant system← Bot Recommendation for tenant system is  provided
            If ($Tc_u$) then // Tenant connection is unstable
                $S_{int}$←Stealth Mode Bots are initiated
            End if
        End if
    End if
    If ($R_t$==M) then // Risk level is medium
        $B_r$for CSP←Essential Bots Recommended for CSP
        If ($E_s$>0) then // Edge System is used
            $B_r$for edge system←Essential Bots Recommended for Edge Systems
            $S_{int}$←Stealth Mode Bots are initiated
        End if
        If ($T_s$>0) then // Tenant System is used
            $B_r$for tenant system←Essential Bots Recommended for Tenant Systems
            $S_{int}$←Stealth Mode Bots are initiated
        End if
    End if
    If ($R_t$>T) then // Risk level is above threshold
        $AB_{hs}$high security←Adaptive Bots Recommended for CSP
        If ($E_s$>0) then // Edge System is used
            $B_r$for CSP←high security Adaptive Bots Recommended for Edge Systems
            $S_{mon}$←continuous monitoring by Stealth Mode Bots
        End if
        If ($T_s$>0) then // Tenant System is used
            $B_r$for tenant system←High Security Adaptive Bots Recommended for Tenant System
            $S_{mon}$←continuous monitoring by Stealth Mode Bots
```

```
End if  End if End while
```

4. Results and Discussions

The below figured result analysis describes the number of Bots in Edge System, Cloud Server and Tenant System which is plotted against the number of Bots attacked and handled by Container storage system.

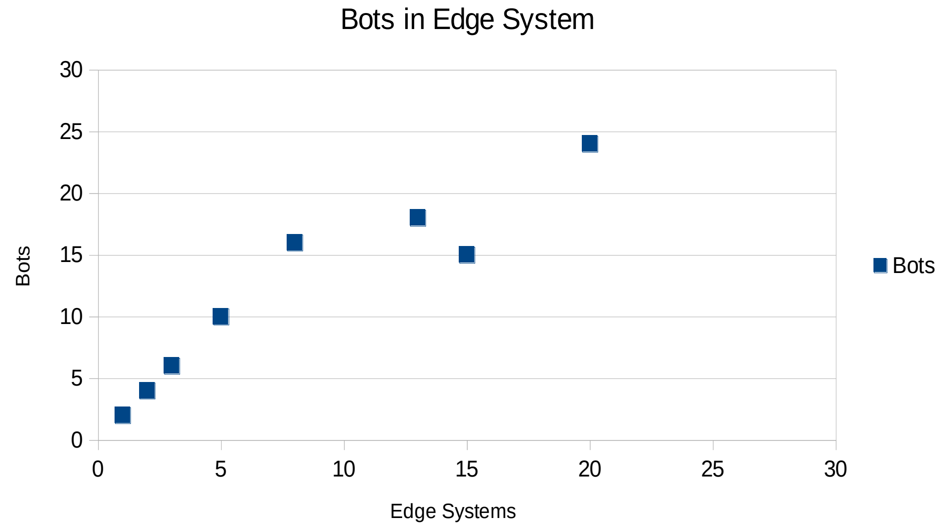

Fig.4 Number of Bot attacks in accordance with its Edge System

The above mentioned fig.4 describes the various number of Edge system Bots like 6, 16, 21… etc has number of Bots attacks and varied in accordance with their storage system. For increased number of edges, bots has increased due to insecurity. For example 20 number of edge system, proposed system has nearly 25 numbers of bots as illustrated in fig.4. Different Bot attacks in accordance with their Cloud Storage System such as Edge System, Tenant System and Cloud Storage System. New techniques used for accurate detection of malicious Bots results in social situation analysis of social media that interprets between users click stream methods. Number of Bots Recommended for Cloud Storage Servers provides efficient data storage. Stealth Mode Bots inside the data chunks makes data more secure with auto update and adaptable.

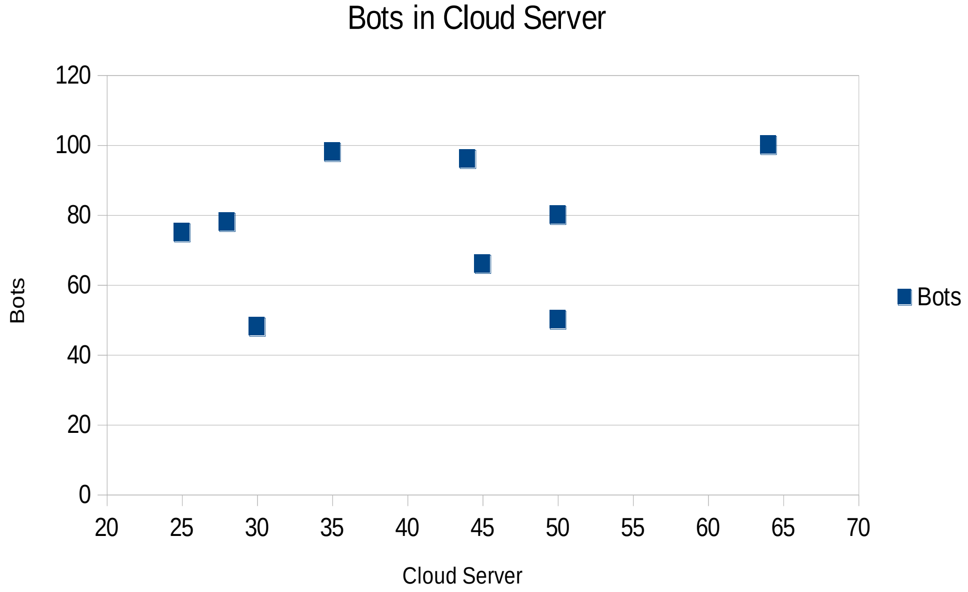

Fig.5 Number of Bot attacks in accordance with its Cloud Server System

The above mentioned fig.5 describes the various number of cloud server (20,25,30,35,40,45,50,55,,60,65, and 70) has gives Bots attacks. For increased number of cloud server, bots has increased due to insecurity. For example 65 cloud servers, in proposed system has nearly 100 number of bots as illustrated in fig.5.

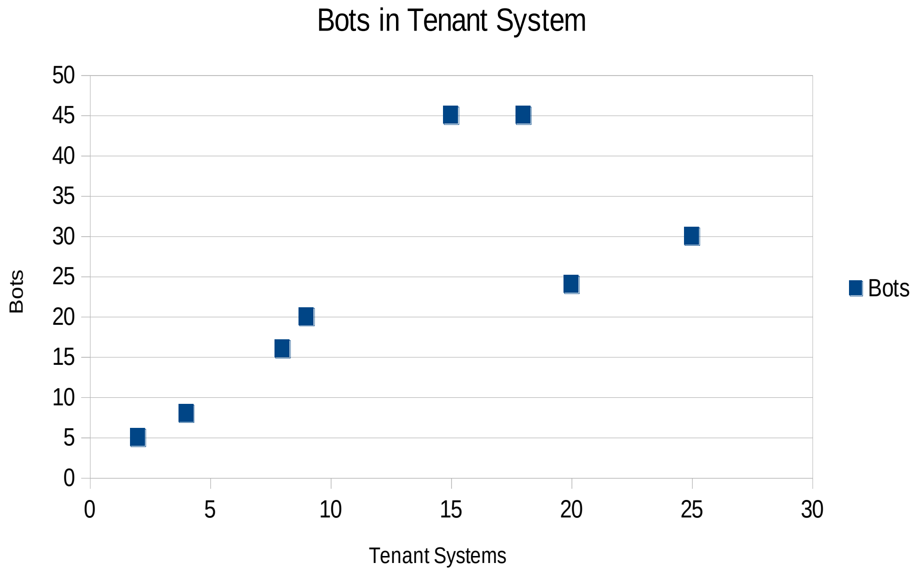

Fig.6 Number of Bot attacks in accordance with its Tenant System

The above mentioned fig.6 describes the various number of tenant system (5, 10,15,20,25, and 30) has gives Bots attacks. For increased number of cloud server, bots has increased due to insecurity. For example 25tenant system, proposed system has nearly 30 numbers of bots as illustrated in fig.6. The proposed system is developed and integrated not only to recommend secured bot it also predict and defend sensitive data which is adapted to defend further when new techniques arrives.

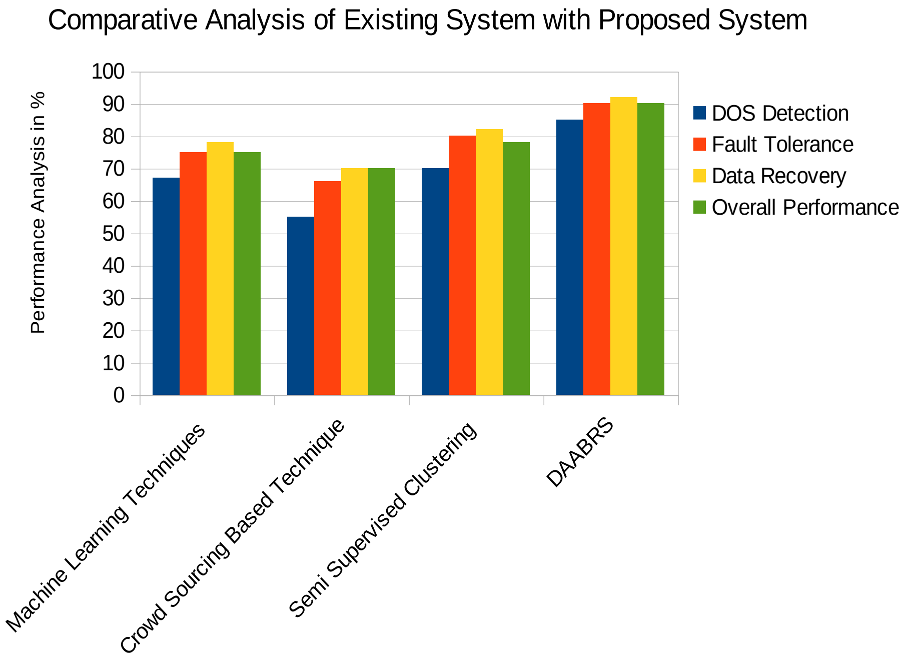

Fig. 7 Performance analysis of Proposed DAABR System along with existing Bot detection techniques using Machine Learning Techniques, Crowd Sourcing based approach and Semi Supervised Clustering system.

The Performance of Proposed Defensive Auto-Updatable and Adaptable Bot Recommender System (DAABRS) in Fig.7 are calculated based on its overall performance along with its Dos Detection ability, Fault Tolerance capability and it’s Speed of Recovery System. For comparison, various existing techniques are simulated and compared with Proposed Defensive Auto-updatable and Adaptable Bot Recommender System. Existing Bot Detection Systems used in this performance evaluation are Machine Learning techniques; Crowd Sourcing based approach and Semi Supervised Clustering. In all those existing techniques DoS detection speed is compared with defensive DoS detection system, then fault tolerance capability is compared and then recovery speed is analyzed. In accordance with all the above criteria's the overall performance are estimated and analyzed. Thus, the result of the proposed system is proved to have high performance percentage more than other existing approaches. Proposed system has higher performance of 89.82%, machine learning, crowd sourcing, and semi supervised clustering has lower performance of 76.51%,69.92%, and 78.95%

5. Conclusion and Future Work

The proposed work confronts a novel method to detect malicious Bots accurately, found in online social networks. Experiments shows that transition probability between user click streams based on the social situation analytics can be used to detect malicious bots in online social platforms meticulously. Additional behaviors of Malicious Social Bots are further considered and the proposed detection approach are extended and optimized to identify specific intentions and purposes of a broader range of malicious social bots. The proposed Defensive Bot and Adaptable Bot Recommender System is developed and integrated not only to recommend secured bot it also predict and defend sensitive data which is adapted to defend further when new techniques arrives. Machine learning is used and updated in global identification of novel solution to novel approach of attacks on sensitive data. As future enhancement such prospective methods of novel attacks and their novel solutions leads to further research to increase detection rate and intended to provide sensitive proof and attack proof data privacy and security.

References

[1] P. Lewandowski, M. Janiszewski and A. Felkner, "SpiderTrap—An Innovative Approach to Analyze Activity of Internet Bots on a Website," in IEEE Access, vol. 8, pp. 141292-141309, 2020, doi: 10.1109/ACCESS.2020.3012969.

[2] Peining Shi, Zhiyong Zhang, and Kim-Kwang Raymond Choo, "Detecting Malicious Social Bots Based on Clickstream Sequences", in *IEEE Access*, Vol 7, DOI 10.1109/ACCESS.2019.2901864.

[3] A. F. Costa, Y. Yamaguchi, A. J. M. Traina, C. Traina, Jr., and C. Faloutsos, ''Modeling temporal activity to detect anomalous behavior in social media,'' *ACM Transaction Knowledge Discovery Data*, vol. 11, no. 4, Aug. 2017, Article no. 49, https://doi.org/10.1145/3064884

[4] Fettweis, G., Nagel, W., &Lehner, W.," Pathways to servers of the future", *Design, Automation & Test in Europe Conference & Exhibition* (DATE), Dresden, 12.- 16.03.2012. *IEEE,* S. 1161-1166. ISBN 978-1-4577-2145-8. 2012, DOI: http://dx.doi.org/10.1109/DATE.2012.6176577

[5] Ben Stephens, ArashShaghaghi, Robin Doss, And Salil S. Kanhere, "Detecting Internet of Things Bots: A Comparative Study", in *IEEE Access*, Vol 9, 2021, Doi 10.1109/ACCESS.2021.3130714

[6] Rui, T. (2017). Research on resource scheduling strategy of container cloud platform based on Kubernetes [D]. University of Electronic Science and technology.

[7] A. C. Zhou, B. He, X. Cheng, and C. T. Lau, "A declarative optimization engine for resource provisioning of scientific workflows in geo-distributed clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 3, pp. 647–661, 2016, https://doi.org/10.1109/TPDS.2016.2599529

[8] H. Zhang, X. Geng and H. Ma, "Learning-Driven Interference-Aware Workload Parallelization for Streaming Applications in Heterogeneous Cluster," *in IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 1-15, 1 Jan. 2021, doi: 10.1109/TPDS.2020.3008725.

[9] Xinqian Zhang, Tingming Wu, Mingsong Chen, Tongquan Wei, Junlong Zhou, Shiyan Hu, Rajkumar Buyya,Energy-aware virtual machine allocation for cloud with resource reservation, *Journal of Systems and Software*,Volume 147,2019,Pages 147-161,ISSN 0164-1212, https://doi.org/10.1016/j.jss.2018.09.084.

[10] Garg, Saurabh & Toosi, Adel & Srinivasa, K. & Buyya, Rajkumar., "SLA-based virtual machine management for heterogeneous workloads in a cloud datacenter", *Journal of Network and Computer Applications.* 45. 108–120, 2014, Doi: 10.1016/j.jnca.2014.07.030.

[11] Adhikari, Mainak & Nandy, Sudarshan & Amgoth, Tarachand, “Meta heuristic-based task deployment mechanism for load balancing in IaaS cloud”, *Journal of Network and Computer Applications.* 128 ,2018, Doi: 10.1016/j.jnca.2018.12.010.

[12] Guerrero, C., Lera, I. & Juiz, C., “Genetic Algorithm for Multi-Objective Optimization of Container Allocation in Cloud Architecture.” *J Grid Computing* 16, 113–135, 2018, https://doi.org/10.1007/s10723-017-9419-x

[13] Kaur, Mandeep and Sanjay Kadam. “A novel multi-objective bacteria foraging optimization algorithm (MOBFOA) for multi-objective scheduling.” *Appl. Soft Comput.* 66, 183-195,2018, https://doi.org/10.1016/j.asoc.2018.02.011

[14] M. Lin, J. Xi, W. Bai, and J. Wu, ‘‘Ant colony algorithm for multi-objective optimization of container-based microservice scheduling in cloud,’’ IEEE Access, vol. 7, pp. 83088–83100, 2019, DOI:10.1109/ACCESS.2019.2924414

[15] T. Kim, M. Al-Tarazi, J. -W. Lin and W. Choi, "Optimal Container Migration for Mobile Edge Computing: Algorithm, System Design and Implementation," in *IEEE Access*, vol. 9, pp. 158074-158090, 2021, doi: 10.1109/ACCESS.2021.3131643.

[16] M. Ouyang, J. Xi, W. Bai and K. Li, "Band-Area Application Container and Artificial Fish Swarm Algorithm for Multi-Objective Optimization in Internet-of-Things Cloud," in *IEEE Access*, vol. 10, pp. 16408-16423, 2022, doi: 10.1109/ACCESS.2022.3150326.

[17] B. Carminati, E. Ferrari, and M. Viviani, "Security and trust in online social networks," *Synthesis Lectures on Information Security, Privacy, & Trust*, vol. 4, pp. 1-120, 2013.

[18] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Nodes using Social Networks," in *NDSS*, 2009,Available in: https://crysp.uwaterloo.ca/courses/pet/W11/cache/netfiles.uiuc.edu/mittal2/www/sybilinfer-ndss09.pdf

[19] Vasudevan, S. K., Sivaraman, R., & Karthick, M. R., “Sybil guard: Defending against sybil attacks via social networks”, *International Journal of Computer Applications,* 5(3), 27-42, (2010).

[20] Karataş, Arzum&Şahin, Serap, ”A Review on Social Bot Detection Techniques and Research Directions”, 2017, *Conference: ISCTurkey 10th International Information Security and Cryptology Conference*