IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INFORMATION AND COMMUNICATION TECHNOLOGY OF MACHINE LEARNING USED TO DETECT MALICIOUS ACTIVITIES OF BOTNET IN OSN

Ms.S. Geetha

Assistant professor

Department of Computer Science and Engineering

Mahendra Engineering College

Dhiyaneshwar.K.A, Arunkumar. P, Blesson Joshua. P, Gowtham.M

UG Students

Department of Computer Science and Engineering

Mahendra Engineering College.

ABSTRACT

Information and Communication Technology (ICT) security process to evaluate a system design that securely safeguards the information from various technologies. Cybersecurity has increasingly become a significant role in the platform of ICT that is adopted throughout the world. In ICT security is the ability to protect the Availability, Integrity, and Confidentiality of an organization's digital information resources. The responsibility and capabilities of ICT security should address the issue such as employee behavior on social network and inadequate public experience of digital information. Online Social network (OSN) most common type of interaction between people and botnet attacks on this network are currently corrupting the data and defined malicious data or intrusion of the network. Hence Machine learning algorithms are used to provide concurrence in cybersecurity for social networks in the infrastructure of ICT. One of the legitimate purposes of using Botnets to support the ITC channels operations using administrative rights on a specific process. Such goals do not meet with a large number of bots that have been seen in the research paper. The proposed research investigated to apply machine learning techniques to detect insider attacks to reduce network traffic, particularly in the area of botnet detection. The Support Vector Machine (SVM) algorithm is used for dynamic events and handles complex tasks coming from cyberspace which can be considered malicious activities from the unknown user in the ICT platform.

Index Term: Botnets, ICT, Cybersecurity, Online Social Network, Machine Learning, SVM, and Security analysis.

I. INTRODUCTION

A botnet is several collection bots that perform specific activities that were controlled by the botmaster. Among the various network attacks, the Botnet was defined as a dangerous attack [1, 2]. Numbers of malicious actions are performed by botnet attacks like DDoS attacks, phishing, theft of identity, fraud, spam email, etc [3, 4]. The bots are infected that is network-connected devices are infected then the botnet attacks are launched. Botnet itself identified as worm or computer viruses and their owner called as botmaster. To coordinate the attacks by conducting a botmaster by using command and control channels to exploit the illegal activities of spamming, confidential data, steal private and phishing, etc.

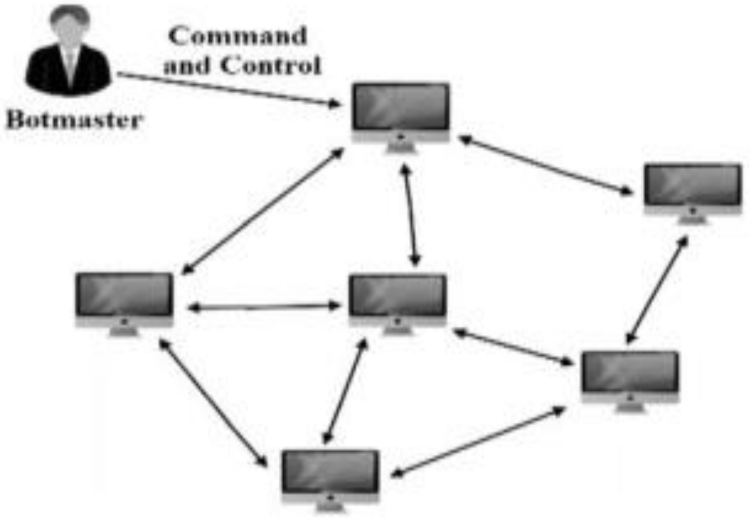

Figure 1: Illustration of Botmaster

In the cybersecurity world, botnet is one of the highly infected attacks on social networks. Day by day to find the presence of difficulties to detect the botnet the botmaster creates a new type of encrypted botnets. Several authors developed several techniques using a different method for detecting botnet some of the methods given below.

Zhi-juanjia et al. have described an algorithm of ant colony group-dividing for identifying a botnet from the network. The techniques of detecting have been improved the results of accuracy through the comparative analysis. An ant colony group-dividing searching method feasible for improving the highly effective implementation process. Later the author compared with various performance effects of a topological size that indicates the group by dividing the number a lower time of convergence in a single path by increasing a topology size by several node increases. By using this algorithm the right attack path which was located in the control center that may find it out easily [5].

For analyzing P2P botnet the developing a technique so non-trivial feature selection and suggest a problem for re-identifying to identify botnet. This technique able to show better features for two flow comparisons and botnet data was used to evaluate the performance of Monsieur Poirot and also compare the flow-based algorithm with a research paper. Effectiveness has been achieved experimentally by detecting malicious traffics.

II. PROPOSED METHODOLOGY

A) CYBERSECURITY

Our proposed approach is based on the behavior stages synchronization monitoring hosts to known the precedence of botnet attacks. The experimental evidence presented suggests the Command and control channel (C&C) respectively for the stages of binary download. This proposed research presented only a proof concept by implementing an approach to detect malicious users from an online social network (OSN). It may argue that is sufficient to observe a single host by engaging C&C communication to raise an early attack of alarm. Also, control observing the communication from multiple machines would reduce false alarms by synchronizing malicious activity using machine learning algorithms from botnets.

In the network attributes directly observe the social network from command and control channel from social bots by analyzing malicious activities by synchronization of same hosts communication. For example, if the indicator synchronized was different but the query from the same URL then it was taken as malicious activities. To monitor the network to generate the alarm when each indicator was observed malicious activities by the botmaster in the infrastructure of OSN for cybersecurity.

B) BOTNETS

One of the most important threats focused by facing enterprises network in the Bots was malicious activities happened on an online social network. Botnets are mainly used for cybersecurity such as internet attacks and breaking a secret against the target system.

A botmaster is a program that operates the agent from the users and runs automatic tasks over the internet. A collection of Bots network used to analyze malicious purposed that referred to Botnets. These attacks can range from localized attacks like keylogging t intensive network attacks DDoS, Spam, phishing, etc.

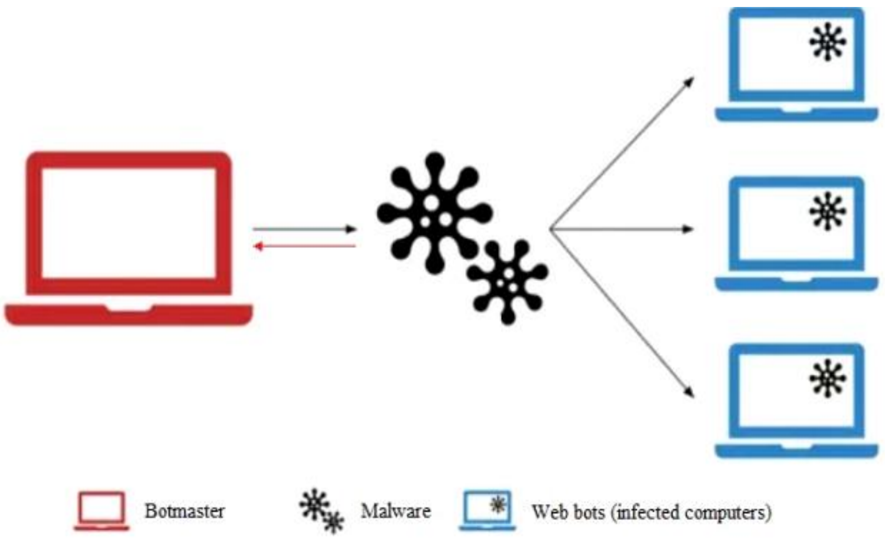

Figure 2: Architecture of Botnet

This proposed system, suggest a novel approaches that can detect the Bots. The solution adopts a two divided strategy which can classify into the standalone and network algorithms. The algorithm of Machine learning runs independently on each node on the network. This monitors the active process on the node to identify the bots process using parameters such as input traffic ratio, similar URL, and response time. The Botmaster process the social bots from the C&C to identify the malware by infected computer. Infected computer the deduce the bot pattern from the target user subsequently by using Botmaster onset.

C) Command and control channel (C&C)

The C&C channel link between the bot and botmaster and unique to bot malware the C&C defining characteristics. The C&C channel is used to send an instruction to the bots and receive information from bots. C&C channel is generally one of the three networks connect to the same C&C servers controlled by a single botmaster in an ICT environment.

Decentralized C&C design and architecture with the flexibility process in the botmaster by analyzing a malicious activity. The Center point of failure the ICT architectures, these botnets possess multiple paths for sending instructions. The decentralized C&C make usage of peer to peer (P2P) communication protocols as connecting the mean of infected machines. By combining this method the hybrid techniques seek to combine the principle of analyzing malicious activities from target users through an algorithm of machine learning SVM.

D) Support Vector Machine (SVM)

This is a supervised model associated with a learning algorithm of classification and regression model. In the proposed system is based on the machine learning framework using SVM algorithms to detect network anomalies. The novelty approaches embedding the ML procedure to analyze the behavior of network traffic happened because of the reason attacked by a malicious user. However, several network anomalies can reveal data with inspected together, such as DDoS attacks, Port/Range Scan, and Botnet C&C communications.

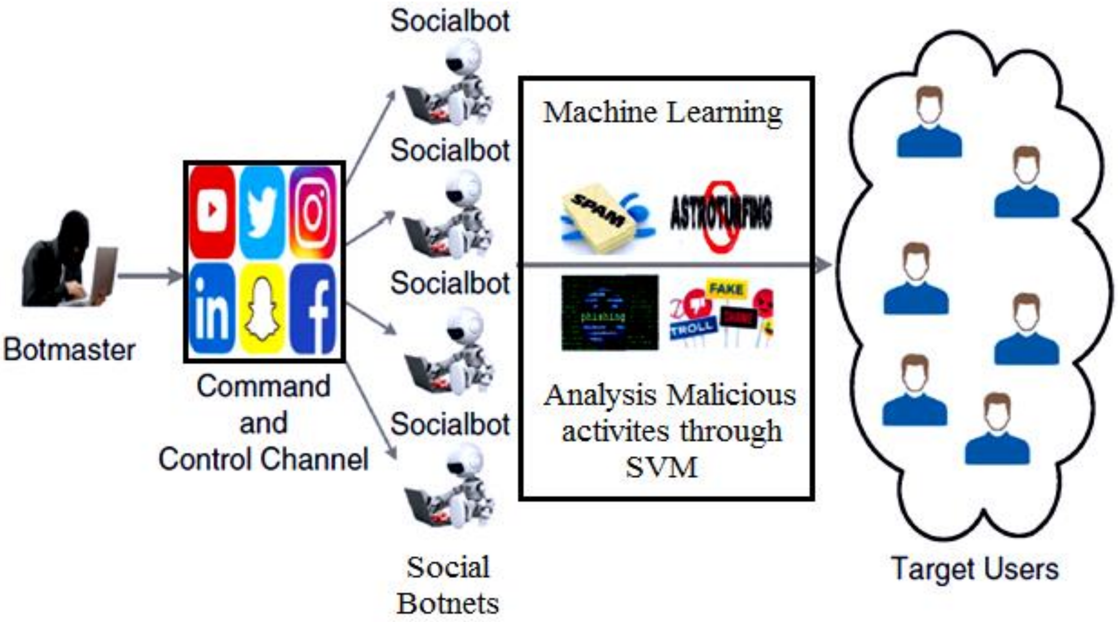

Figure 3: ICT Infrastructure of Social Botnet

Recently, using an SVM algorithm has been increasingly common because SVM can achieve high classification with training sets through machine learning techniques. The main purposes of SVM establish an optimal hyperplane to classify the data to build classification models. The botmaster controls the channel of social bonnets and analyzes the target users by attackers analyze using machine learning techniques. As a result, consider a batch recording ability to detect the abnormal behavior with a small set of training data using an SVM algorithm of machine learning.

III RESULT AND DISCUSSION

The statistical measures that can be considered some of the processes for evaluating the analyzing malicious activities which assume:

Accuracy (A)

$$A = \frac{TP+TN}{TP+FN+TN+FP} \quad (1)$$

Recall (R), or True Positive Rate (TPR) or sensitivity

$$R=\frac{TP}{TP+FN} \quad (2)$$

Specificity (S) or else True Negative Rate (TNR)

$$S=\frac{TN}{TN+FP} \quad (3)$$

A True Positive (TP) and False Negative (FN) of a specific classification of malicious activities through ML algorithm are considered by the detection methods. The False Positive (FP) and True Negative (TN) are discussed the classification of neural values from the botnets this is categorized as an accurate classification that specifies the false positive of the records.

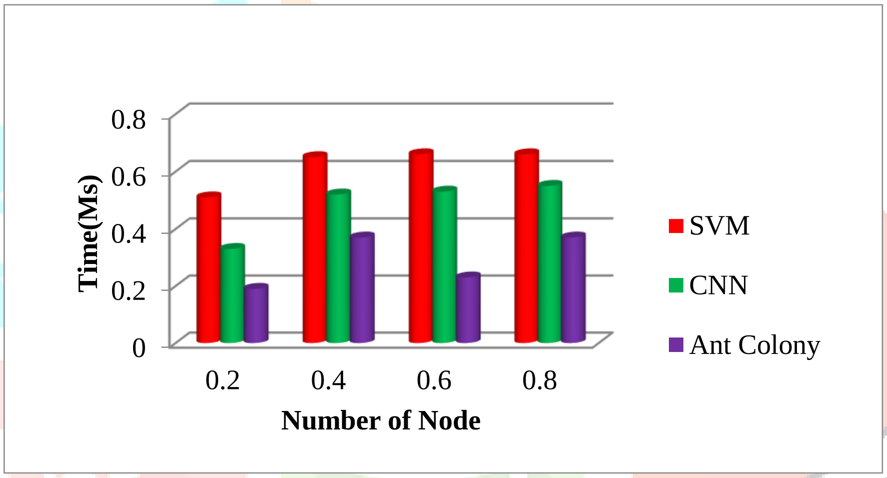

Figure 4: Malicious activities analyzed from botnet

The above chart demonstrated the malicious activities analysis using the proposed algorithm of Support Vector Machine (SVM) used to identify the target user from botnet attacks highly accurate malicious actives analyzed when it compared with an existing algorithm of Ant colony optimization, and Convolutional Neural Network (CNN).

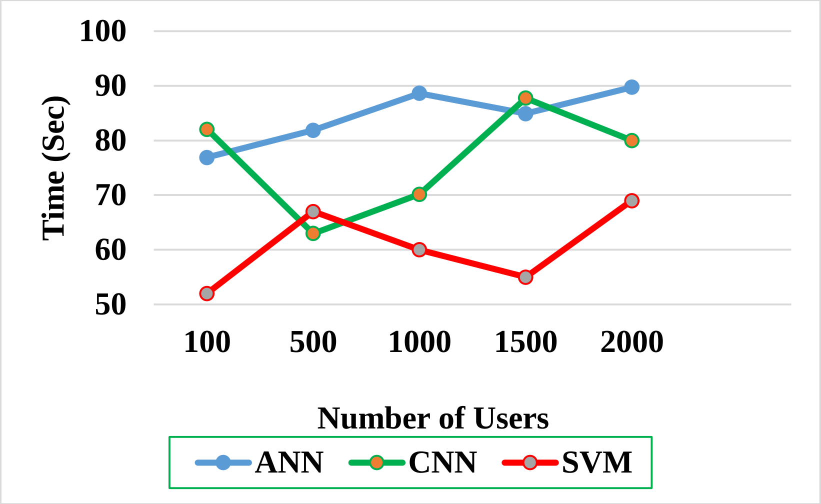

Figure 4: ML algorithm used for Social Botnet

Figure 4 shows the usage of botnets the machine learning algorithms taken a minimum amount of time even if the user increases more using the proposed algorithm the SVM is used to the taken minimum amount of time without any malicious attack compared with an existing algorithm of ANN and CNN. The proposed SVM algorithm of machine learning gives high accuracy with a minimum amount of time.

IV CONCLUSION

Increasing the number of internet users the commercial users generally bring several malicious attackers they potential to legitimate the user by threats. The aim of this research internet the security threats understanding malicious users and increased malware detection using machine learning. The proposed research, a detailed study involved the technology to control botnets and threat detection. The aim of the research concluded with the cybersecurity of botnet with a target user using a machine learning method. This paper proposed SVM, a novel machine learning technique to predict malicious activity users which means target user. Analyzing the whole network traffic is practical in the machine learning area due to user privacy issues and huge training and testing time detection using the proposed method.

REFERENCES

[1] Ms. P. C. Tikekar, Dr. S. S. Sherekar, Dr. V. M. Thakre, Ms. AlishaSherekar" Comparative analysis of mobile botnet detection techniques", The national conference on emerging trends in science(NCETS), India, ISSN:2348-7143, 1-2 February 2019.

[2]A. Malatras, E. Freyssinet, and L. Beslay, "Mobile botnets taxonomy and challenges," 2015 European Intelligence and SecurityInformatics Conference, Manchester, pp. 149-152.doi:10.1109/EISIC.2015.13,2015.

[3] D. A. Girei, M. Ali Shah and M. B. Shahid, "An enhanced botnet detection technique for mobile devices using log analysis", 201622nd International Conference on Automation &Coputing (ICAC). Colchester. pp. 450-455. doi:10.1109/IConAC.2016.7604961, 2016.

[4] H. Dhayal and Kumar, "Botnet and p2p botnet detection strategies: a review," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, pp. 1077-1082. doi: 10.1109/ICCSP. 2018.8524529,2018.

[5] Ms. P. C. Tikekar, Dr. S. S. Sherekar, Dr. V. M. Thakre "A study of botnet architecture & its defense mechanism", National Conference on Recent Advances In Science And Technology (AJANTA), India, ISSN: 2277-5730, 5-6 March 2019.

[6] S. Lysenko, K. Bobrovnikova and O. Savenko, "A botnet detection approach based on the clonal selection algorithm, " IEEE 9thInternational Conference on Dependable System, services and technologies (DESSERT), Kiev, pp. 424-428. doi:10.1109/DESSERT.2018.8409171,2018.

[7] F. K. Wai, Z. Lilei, W. K. Wai, S. Le, and V. L. L. Thing, "Automatedbotnet traffic detection via machine learning," TENCON 2018 IEEERegion 10 Conference, Jeju, Korea, pp. 0038-0043. doi: 10.1109/TENCON .2018.8650466,2018.

[8] Z. Jia, N. Wang, Y. Wamg and M. Hu," Traceability analysis of and research of botnet control center based on ant colony group dividing algorithm," 13 th IEEE Conference on Industrial electronics and applications (ICIEA), Wuhan, pp. 906-912. doi: 10.1109/ICIEA.2018.8397841,2018.

[9] W. Lee, A. Rezapour and W. Tzeng," Monsieur poirot, detecting botnet using reidentification algorithm and non-trivial feature-selection technique, " IEEE International Conference on Communication (ICC), Kansas City, MO, pp 1- 6. doi:10.1109/ICC.2018.8422081,2018.

[10] Di Zhuang and J. M. Chang, "Enhanced PeerHunter, detecting peer to peer botnet through network flow level community behavior analysis," In IEEE transactions on Information Forensics and security, vol. 14, no. 6, pp. 1485-1500, June. DOI: 10.1109/TIFS.2018.2881657,2019.