A Survey on Techniques to Detect Malicious Activites on Web

Dr.Abdul Rahaman Wahab Sait[1]
Asst. Professor
King Faisal University
Al Ahsa
Kingdom of Saudi Arabia

Dr.M.Arunadevi[2]
Asso. Professor
Department of Compute Science
Cambridge Institute of Technology
Bengaluru, India

Dr.T.Meyyappan[3]
Professor
Department of Computer Science
Alagappa University
Karaikudi, India

***Abstract*—The world wide web is more vulnerable for malicious activities. Spam–advertisements, Sybil attacks, Rumour propagation, financial frauds, malware dissemination, and Sql injection are some of the malicious activities on web. Terrorist are using web as a weapon to propaganda false information. Many innocent youths were trapped by web terrorist. It is very difficult to trace the impression of malicious activities on web. Many researches are under development to find a mechanism to protect web users and avoid malicious activities. The aim of the survey is to provide a study on recent techniques to find malicious activities on web.**

***Keywords*—Malware detection; malicious behavior; spam detection; web terrorism; Sql injection**

I. Introduction

The application of web is increasing exponentially in various fields. E–commerce, social networks, mobile applications, and search portals are some of the applications of web. Machine learning applications are under development to provide flexible interface to web users. Recent studies from Netcraft [1] show that there are more than 1.8 billion websites in web. In 2016, Google [2] has stated that the number of hacked websites rose by 32% comparing to previous year. The reason for the malicious activity is some sort of compromisation in security.

Hackers are monitoring the web using robots, and web cookies. When users have tried to open an anonymous websites, the cookies will be stored into their system. The malicious cookie will send the activities of users and their navigation pattern. They will trap the users using the information collected from their system.

Robots are used to scrawl content from web, monitor user activity and communicating the pattern to the robot owners. Search engines are using robots to index the websites. Hacking is not only a malicious activity; web terrorism is also a part of it. Web terrorist are using web as a weapon to spread falser information about a community, an organization and a country. Rohingya incidents of Myanmar were the proof for the rumor propagation on social networks [3]. Researchers are focusing on malicious behaviors on web. Existing studies are helping to find out the malware, and culprits but there is no tool to intimate users about the suspicious activities [4]. The following Fig. 1 will show the malicious activities on web.

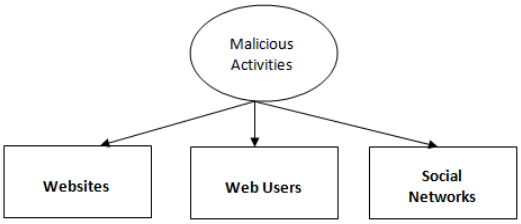

Fig. 1. Malware Activities on Web.

Spam, malware, and rumour propagation are the keys of malicious activities on web. Spam are used to redirect the users towards anonymous activity [5]. Malware are software or cookies which monitor user activity. Rumour propagation is used on social networks. Terrorist are using rumour propagation technique to trap innocent people into terrorist activity. Hackers are targeting websites, web users and social networks. A cyber-attack can be anything which targets the users of a website and a social network. The following part of the survey is organized as follows: Section 2 will provide review of literature on malicious activities. Section 3 will give information about the malicious attacks on web. Section IV will describe the techniques which can be used to find suspicious activities on web. Finally, the conclusion part will conclude the survey.

II. Review of Literature

Frank Vanhoenshoven et al., [6] have proposed a method to detect malicious URLs as a binary classification problem and studied the performances of machine learning methods like Naïve Bayes, support vector machine(SVM), Multi-layer perceptron, Decision trees, Random forest(RF), and K–nearest neighbours. The blacklists services are array of techniques which combines manual reporting, honey pots, and web crawlers with site heuristics. The authors have discussed the merits and demerits of techniques based on machine learning methods. The study has suggested that RF or SVM are competitive methods for the classification of web data. The process of feature selection will be difficult for a dataset consisting of over 2 million entries. In that case, the pattern detection and correlation become more complex or difficult for computation. They have used a group of three feature set for the purpose of experimentation. Each features are binary than non–zero value to describe the information about the URL.

They have compared the methods with the metrics like accuracy, precision, and recall. 121 datasets were used as the test set; a non–stratified independent random sample with equal probability is used from a set of row numbers between 1 and 20000. All predictions have achieved 65% of overall classification accuracy. RF and SVM have achieved an average accuracy of 97.6% and 96.10%.

R.V. Bhor and H.K. Khanuja [7] have developed a security mechanism and attack detection technique to avoid sql injection attack. Sql injection and Denial of service (DOS) are the threats found in web applications. Sql injections attack is the process of altering Sql statement by the use of web forms. DOS is the attack on network resources. The authors have developed a distributed vulnerability and attack detection tool (DVADT) to protect web users from sql injection and DOS attacks. It is necessary to find out the attacks efficiently to reduce its effect on the web. The existing system for the attack detection is limited to 50% to 60%. Monitoring stage, Injection stage, Attack payload creation stage, Exploit stage, Detection and testing stage, and Classification stage are the stages involved in DVADT. The monitoring stage will monitor the communication between the web browser and web application. The injection stage will detect the locations which are vulnerable for injection attack. The concept of vulnerability operator is to find the vulnerable location and protect code location. The attack payload creation stage is used to generate payload to avoid malicious attacks. The set of possible malicious activities will be generated with possible solutions. The exploit stage is used to upload vulnerable source into web application. Sql probe and HTTP probe are used to capture the interaction data between the web server and the web browser. The detection and testing stage is used to observe the communication between the web application and the database server. The classification stage is used to analyse the type of attacks. A neural network classifier is used to classify the data sent by DVADT. The experimental results have shown that the security policies and mechanism related to web applications are inversely proportional to rate of attacks.

K. Srividya and A.Mary Sownjanya [8] have developed a method for the analysis of internet messaging and detection of malicious activity. The authors have discussed the adverse effect of internet messaging in social networking sites like Facebook and Whatsapp. The methodology of the research is based on the Latent semantic analysis (LSA). The text messages were processed and alarm if malicious activity were following the emotion analysis technique rather than proper attention to internet messaging. Social networking service consists of a representation of a user profile and their social links and different types of additional services. Keyword matching, semantic analysis and frequency counting are the phases involved in the process of behavioural analysis and malicious activity detection. The keyword matching phase is the difficult phase, finds abusive words using bag of words technique. The words were categorized as flagged, non–flagged, and highly–flagged according to their general usage and the number of occurrences is used to signify an abusive and explicit meaning. Tokenization technique is used to extract data from messaging service. The semantic analysis phase is used to extract data from messaging service. The semantic analysis phase is used to derive the meaning of the message. LSA algorithm is used for the analysis of data. A custom score is used to extract the different emotions like joy, anger, sadness and so on. The frequency counting phase is used to predict the exact score of a message which are processed by the previous phases. An average cumulative score is computed for the entire message and compared with threshold values. The results have proved that some improvement in the process of detection of malicious activity comparing to its peers.

Shahab saquib and Rashid Ali [9] have proposed a technique to investigate malicious behaviour in online social network (OSN). They have analysed the suspicious and unusual behaviour in OSN. A framework for the detection of malicious behaviour was developed by the research. The data about the users of OSN will be stored by the OSN provider. Rumour propagation is one of the malicious activities present in all the OSNs. The study has classified malicious behaviour analysis into two parts: Illegitimate content analysis and illegitimate user detection. The authors were argued about an attack called Sybil. A Sybil attack is the process of creating fake accounts to create fake forums and deceive user into it. Illegitimate content analysis is used to identify and suspend the malicious node in OSN. It has three functions namely rumour spread mechanism, rumour containment strength and source of information. The rumour spread mechanism is used to analyse the rumours which were spread in OSNs. A randomized rumour spreading model is deployed to calculate the ratio of rumours in OSNs. The rumour containment strategy is the study of cost involved in rumour containment, rumour containment within a deadline and marking protector nodes in OSNs. The source of information part is used to detect the source of rumour in order to give punishment to users. K – suspector problem technique is employed to detect the K – top most suspended source of rumour. Illegitimate user detection has two parts namely attack mechanism and defence strategy. The attack mechanism was discussing possibilities to understand the psychology of illegitimate user. The defence strategy is used to find the deceptive users in OSN. The framework which is proposed by the research has analyzed the details of individual user and the content published by different users. The output of the research will be useful to study the users in social network.

Pedro Marques et.al.,[10] have proposed a method to detect web scraping activity using diverse detectors. Robots were employed to extract content and data from a website. Search engine bots, and price comparison bots are considered as legitimate web scraping robots. Copyrighted content scraping and Boosting sale robots are illegitimate robots. A commercial tool and an in – house tool called Arcane were employed in the research for the detection of web scraping activity. An Apache HTTP access log from an e-commerce application is used for the experimentation purpose. The authors have analyzed the similarity and diversity in finding the alerting behaviour by the two tools. Both tools were similar in generation of alert for 1.2 millions HTTP request but there is a difference of 43,648 HTTP requests by commercial tool and 9305 HTTP request by Arcane only. They have also analyzed the breakdown of those alerts based on the HTTP status. The study had the ability to analyze trade – offs between false positives and false negatives.

The result has proved that their system can protect the network from malicious web scraping activity.

Devan Gol and Nisha Shah [11] have discussed the detection of web application vulnerability based on Rational Unified Process (RUP). The authors were argued that the existing vulnerable detection tools are failed to detect latest attacks in web. The research has demonstrated the vulnerabilities in web applications. Vulnerabilities were occurring from improper codes, computer viruses, or a cross sided script (XSS) and SQL injection attack (SQLIA). SQLIA is against a database driven application. It will inject invalid input strings into the database and modify for the deliberate usage. A successful attack will pass a SQL attack code into the back – end system and execute the vulnerable application. The XSS attack is the process of passing client side script into a web server to perform malicious activities. The four phases of RUP framework are inception, elaboration, construction, and transition. The initial module of the framework is used to crawl a set of websites for the system. The second module is used to launch the attacks against the collected websites. The third module is used to analyse and verify whether the attack was successful or not. The last module is used to provide a report of whole process involved in vulnerability scanning method. The framework which is proposed in the research will be useful to detect vulnerability in the network. The research did not provide any proofs to show the performance of the framework in real time network.

III. Types of Malicious Attack

A malicious attack is an online code executed by a programmer with an intension to break the privacy of an individual or an organization. Hackers, web terrorists and eavesdropper are some of the titles for the programmer who executes the malicious code [12]. The following part of the section will discuss the types of malicious attacks on web.

A. Websites–Malicious Attacks

The prime target of malicious attackers is the websites. Fig. 2 shows the classification of attacks targeting websites. A website will have more number of visitors and a malicious code can easily broadcasted into visitors' system.

1) DOS: It is an attack that blocks the user from using the resources of a network. Web servers of organizations such as Bank, E–Commerce, Service portals, and Media portals are the targets of DOS attack.

Flooding a crashing services are the general concepts of DOS. Buffer overflow attacks, ICMP flood, and Sync flood are the familiar flood attacks under the concept of flooding services. Slowloris, NTP amplification, and Zero – day are the familiar methods under the concept of crashing services [13]. A distributed DOS is a multitude of Dos attacks. Fig. 3 is the illustration of DOS attack. An attacker can employ flooding or crashing services to block the services to the customer or user of an organization.

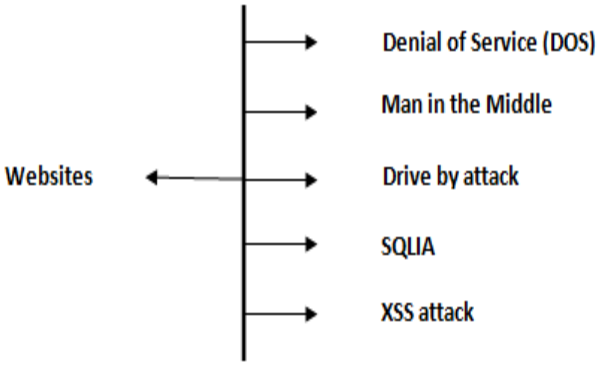

Fig. 2. Websites Related Malicious Attacks.

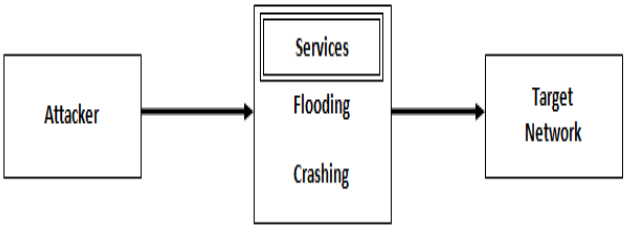

Fig. 3. DOS Attack.

2) Man in the middle: It is a type of attack which intercepts the message between the sender and the receiver. Both parties are not aware of the attack [14]. The attacker will find out the loopholes of the security of a network and inject malware. They have the ability to modify all messages communicating between two victims. Authentication, tamper detection, and forensic analysis are the detection techniques to detect the attack. Fig. 4 shows the scenario of man in the middle attack.

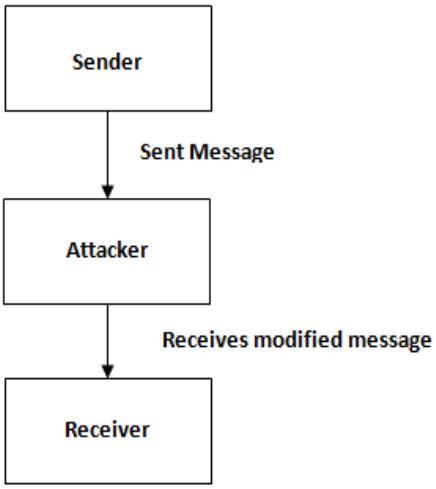

Fig. 4. Man in the Middle Attack.

3) Drive by attack: It is also called as Drive by downloads attack. The criminal will search a insecure websites and attach a malware script with HTTP and spread the malware into visitors' system. The installed malware may create a IFRAME and redirect the visitor to a site maintained by the criminal. This kind of attack will wait for the visitor to visit the website to pass a malware code.

4) XSS attack: XSS is a cross–side script used by the criminals to inject a malicious code into vulnerable website. Stored and Reflected are the two types of XSS. The stored XSS is also called as persistent XSS. The persistent XSS is activated when a malicious code is triggered by the vulnerable web application. It is very dangerous and cause more damage to the website. The reflected XSS is passed to the user browser when a user is trying to open a web page. Fig. 5 is the illustration of XSS attack.

5) SQLIA: It is an older method to gain access of a website. The attacker will search a weaker website and apply a coding technique to enter into website. It is applied against data–driven applications. Many sql statements which are useful for injection attack are available in Internet. Modern prevention techniques are developed to challenge the SQLIA. Cyber criminals are still using SQLIA to steal the valuable information of a website.

B. Web User-Malicious Attacks

The intention of cyber-criminal is to steal individual information to access of their resources. The prime focus of criminals on a website and their final target is the individual who is visiting the particular website. Cookies are the key for the criminals to gather information about the information. Some websites are pretending as a legitimate site and offer software for free to users. Users will provide some of their real data to the site and accessing the software provided by them. The software will plant malicious code and cookies into the user system. The malicious code and cookie will communicate with the server and pass information about the user. The criminals will use the valuable of the user for monetary benefits. The following part will discuss the malicious activities related to web users.

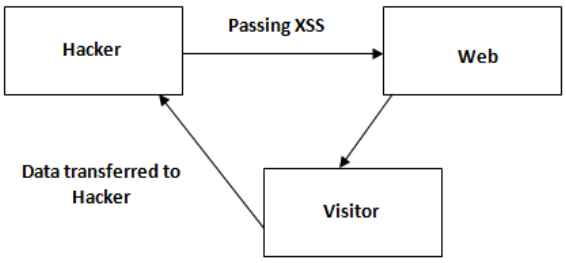

Fig. 5. XSS Attack.

1) Password attack: Password is an attribute of security mechanism to authenticate a user into a website or a network. The password attack is against the user privacy. Generally, attackers are applying brute–force, dictionary attack, and key–logger methods to break the user password. Brute force method is a guessing technique based on random approach by trying various combinations. Dictionary attack method will supply a set of common passwords to gain user access. A key –logger attack is a latest technique to track users' key strokes. The attacker will use a key logger program to store user key stokes during a day or a session.

2) Phishing: It is a type of attack which is used to steal user information. An attacker will recreate or clone a legitimate site and invite users with an intention to steal their credentials and apply the details on the legitimate site. Installation of malware, blocking of antivirus and firewall of a system, loosing valuable information and ransomware attacks are the consequences of phishing attack. Spear phishing is the typical kind of phishing attack which cannot be traced out by the highly secured organization. E–Mail spoofing is one of the examples of spear phishing.

3) Birthday attack: The cyber criminal will use hash function and generate message digest (MD) and replace it with a user message. The Birthday attack is recently discovered in web and difficult to identify the original message. It is basically a cryptographic attack based on the birthday problem in probability theory.

4) Malware attack: Malware is a computer worm or virus that has the capability to spread all over the system. The malware is injected by the attacker through a legitimate application or website. It is a proper code or software written by an experienced programmer to damage a network and a computer. Macro viruses, polymorphic viruses, boot infectors, Trojans, logic bombs, adware, and spyware are the common types of malware exist in web.

5) Spam dissemination: Spam is an advertisement that disseminates malware into a client computer. It is a primary contact of a cyber criminal to know the behaviour of a user or a recipient of spam. Criminals are using web cache, and cookie to study the user attitude on web. Many countries have restricted the spam dissemination on web. Many innocent people were trapped by spam benign advertising methods.

C. Social Networks–Malicious Activities

Social network is a communication tool for people to communicate with friends and relatives. Whatsapp, Facebook, Twitter, and Instagram are the familiar social network medium on web. Criminals are using the medium to trap people. Rumour propagation and Sybil attack are the major problems in social networks.

1) Rumour propagation: Criminals are using a social media as an instrument to spread rumours. They will make fake identities and form a group to gather more people. Rumours were created more problems in all over the world. Terrorism on social medium has become a threat for national security. Rumours are the prime reason for the communal violence. There is no tool available to detect the rumour seeders.

2) Sybil attack: The attacker will use the loop holes of social media security to gain access and make fake identities. Recent security breaches in Facebook were an example of Sybil attack. The Facebook management has declared that 50 millions of user identities were exposed by the security breach. Identity – based validation method will be a solution to protect identity of a user from Sybil attack. The censorship–free nature of social medium will not allow implementing identity – based validation technique.

IV. Detection Methods

The detection of malicious ad suspicious activities on web is a complex process. Existing methods are not up to expectation in finding malicious activities. There is a need of intelligence in the detection of malwares. Machine learning methods are the better replacement for the existing detection methods. RF, SVM, Artificial neural network (NN) and Q – Learning are the machine learning techniques which can be applied in the process of detection of malicious activities on web. The remaining part of the section will discuss the details of the machine learning methods.

A. RF

RF is a supervised learning technique and useful for classification and regression problems. It is based on decision tree algorithm [15]. It is a flexible machine learning algorithm which will produce optimum results for complex or difficult problems. The RF has the ability to handle the missing values or outliers. The number of trees in RF will not over fit the model. The number of decision trees will be increased depend on the situation of a problem. Figure 6 shows the process involved in RF. The possible solutions for a problem will be divided into multiple decision trees. A voting method will be followed for each trees and generate the final solution. The following procedure is followed in RF to make a decision for a problem. Time and space should be calculated for each machine learning methods to evaluate the performance.

1) Procedure–RF

Step 1: Input the dataset.

Step 2: K–features will be selected randomly where k<<m.

Step 3: Best split point will be applied to calculate a node.

Step 4: Step 2 to 3 will be repeated until a perfect number of node is generated for the trees.

Step 5: Step 2 to 4 will be repeated to build forest.

Step 6: Select a test feature and apply rules to predict outcome from generated forest.

Step 7: Calculate the votes for predicted outcomes.

Step 8: Consider the high voted predicted outcome as final prediction.

2) Advantages

- RF will not be affected by overfitting problem.
- It can be used for the extraction of important features from dataset.

3) Disadvantages

- Generation of large number of decision trees lead to make algorithm slower and generation of decision will take more time.
- It is purely depend on the bootstrap sampling.
- The algorithm may not notice rare behaviour and impressions of user.

B. SVM

The algorithm is based on the structural risk minimization principle. It is a supervised learning method widely used for classification and regression tasks.

SVM is using the concept of train and test dataset [16]. The classifier will be trained with target values and features in train set. The trained classifier will be tested with new features without target value. The algorithm will produce high dimension of generalization than the original set of data.

1) Procedure

Step 1: Pre–process the dataset.

Step 2: Split the dataset into train and test set.

Step 3: Input the train set with attributes.

Step 4: Input the target value.

Step 5: Calculate the time and space of the classifier during training phase.

Step 6: Input the test set with attributes for the generation of target values from classifier.

Step 7: Generation of target values.

Step 8: Calculate the time and space of the classifier during testing phase.

2) Advantages

- Computation speed will be more comparing to RF.
- There is no possibility of overfitting problem in SVM.
- Interpretation of features will be easy.
- Parameters will be optimized according to the model.

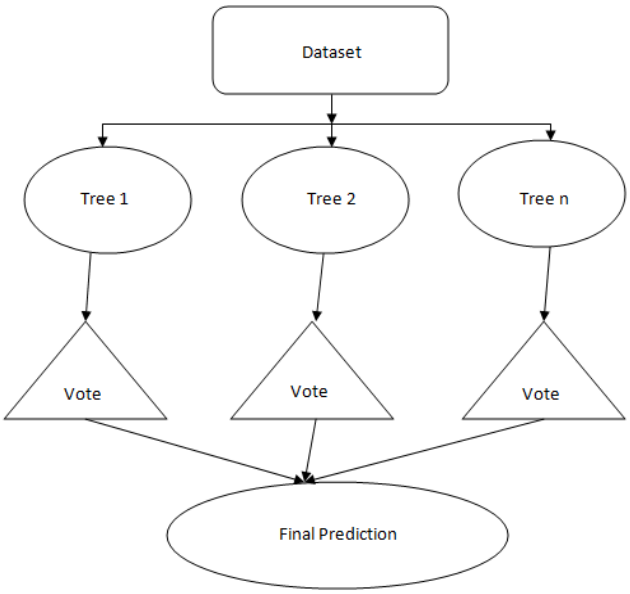

Fig. 6. Processes-RF.

3) Disadvantages

- It is an older technique. Training phase will take more time comparing to testing phase.
- Determination of parameter is a difficult process.
- Consume more space for the computation of results.

C. ANN

ANN is a tool to develop machine learning applications [17]. It is also called as multi-layer perceptron. Input, output, and hidden layers are the part of ANN. The hidden layer will perform operations related to the given problem. The user can have multiple hidden layers to get the optimum results. ANN environment provides Feed forward, Recurrent, Convolutional, Botlmann machine, and Hopfield networks to the users.

1) Procedure

Step 1: Split the dataset into train and test dataset.

Step 2: Train ANN with train set.

Step 3: Teach ANN with possible target values.

Step 4: Calculate time and space.

Step 5: Test ANN with test set.

Step 6: Generation of target.

Step 7: Calculate time and space

2) Advantages

- It has the ability to model non–linear and linear applications.
- It can find hidden pattern from the target dataset.
- It does not have any restriction on input variables.

3) Disadvantages

- Training time will be more for larger dataset.
- Computation cost will be more.
- A fine – tune is required to attain better performance.

D. Q–Learning Method

Q–learning method is also called as reinforcement learning method. It is based on Markov decision process technique [18].

The method will work according to the policy. State and action are the input variables. It will instruct an agent to take action from state to state. A reward or a punishment will be given to the agent for the performance. A successful performance of an agent will yield more rewards.

1) Procedure

Step 1: State and action variable has to be assigned for the environment.

Step 2: Input the policy

Step 3: Train with train dataset with target values.

Step 4: Agent will learn to achieve target with maximum rewards.

Step 5: Test with test set.

Step 6: Generation of results.

Step 7: Calculate time and space.

2) Advantages

- Accuracy of the results will be more.
- Computation cost will be less.
- Generalization of high dimensional data will be high.

3) Disadvantages

- Training time will be more.
- A small error in the system will affect whole model.

V. Conclusion

A malicious activity is an act of security breach which affects an individual privacy on web. The survey has provided the information about malicious attacks and methods to detect malicious activities. A web user is a final target of cyber criminals. A website will be used by the criminals to inject malware into the user machine. RF, SVM, ANN, and Q–learning methods were discussed in the survey. Machine learning methods are the solution for the detection of malicious activities. The future work will be a development of detection technique to detect malicious activities on web.

References

[1] https://news.netcraft.com/archives/2018/01/19/january-2018-web-server-survey.html

[2] https://webmasters.googleblog.com/2017/03/nohacked-year-in-review.html

[3] https://www.cbsnews.com/news/rohingya-refugee-crisis-myanmar-weaponizing-social-media-main/

[4] https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Password%20attack

[5] http://press-files.anu.edu.au/downloads/press/n2304/pdf/ch30.pdf

[6] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[7] Frank vanhoenshoven, Gonzalo Napoles, Rafael Falcon, Koen Vanhoof, and Mario Koppen, " Detecting malicious URLs using machine learning techniques",IEEE Symposium series on computational intelligence, 6 - 9 Dec - 2016.

[8] R.V.Bhor and H.K. Khanuja," Analysis of web application security mechanism and attack detection using vulnerability injection technique",International Conference on Computing Communication Control and automation (ICCUBEA), 12 - 13 August 2016.

[9] K.Srividya and A.Mary Sowjanya, " Behavioral analysis of internet messaging and malicious activity detection", International Conference on Advances in Human Machine Interaction (HMI), March 2016.

[10] Shahab Saquib and Rashid Ali, " Malicious behavior in online social network", IEEE Workshop on Computational Intelligence: Theories, Applications and Future Directions (WCI),14 - 17 Dec - 2015.

[11] Pedro Marques, Zayani Dabbabi, Miruna - Mihaela Mironescu, Olivier Thonnard, Alysson Bessani, Frances Buontempo, Illir Gashi, " Using diverse detectors for detecting malicious web scraping activity", 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops,2018.

[12] Deven Gol and Nisha Shah, " Detection of Web Appication Vulnerability Based on RUP Model ",National Conference on Recent Advances in Electronics & Computer Engineering, RAECE -2015, Feb.13-15, 2015, liT Roorkee, India.

[13] https://searchsecurity.techtarget.com/definition/malware

[14] Muna Al–Hawawreh, Nour Moustafa, and Elena Sitnikova, " Identification of malicious activities in industrial internet of things based on deep learning models", Journal of Information security and applications", volume 41, August 2018, Pages 1 -11.

[15] https://towardsdatascience.com/the-random-forest-algorithm-d457d499ffcd

[16] https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example-code/

[17] https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/

[18] Abdul Rahaman Wahab Sait and T.Meyappan "An automated web page classifier and an algorithm for the extraction of navigational pattern from the web data", Journal of web engineering, Rinton Press,ISSN: 1540-9589, Vol.16(2017), pp. 126–144.