IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

A Survey on Data Mining and Digital Forensics Techniques for Intrusion Detection and Protection System

M. Jayamagarajothi[1], P. Murugeswari[2]

PG Scholar, Computer Science & Engineering, Sri Vidya Engineering & Technology, Virudhunagar, India [1]

Professor, Computer Science & Engineering, Sri Vidya Engineering & Technology, Virudhunagar, India [2]

Abstract*:* With the dramatic increase in the internet applications, security is becoming a major issue of the network. Intrusive attacks on the network are increasing day-by-day. Intrusion Detection System (IDS) is used for ascertaining intrusion and preserves the security goals of information from attacks. Data mining techniques are used to monitor and analyze large amount of network data and classify these network data into anomalous and normal data. Data mining techniques such as classification and clustering are used to identify the intrusive attacks. An effective IDS requires high accuracy, high detection rate and low false alarm rate. This paper presents a survey on the different data mining techniques and digital forensics techniques for the Intrusion Detection and Protection System (IDPS). This enables effective detection of the both malicious and normal activities in the network, to develop a secure information system.

Keywords: Data Mining Techniques, Digital Forensics Techniques, Intrusion Detection System (IDPS), Intrusion Detection and Protection System (IDPS), Security.

I. INTRODUCTION

With the rapid escalation of the Internet applications, there is an increase in the threats caused by either individuals or any organization, to break the security of the network. The main objectives of the security are to ensure high confidentiality, integrity and data availability. Attacks on the network are referred as Intrusion. Intrusion means any set of malicious activities that attempt to compromise the security goals of the information. Conventionally various approaches such as encryption, firewalls, virtual private network, etc., are used. But they were not sufficient to secure the network completely. It is difficult to depend completely on the static defense techniques. This increases the need for developing the dynamic technique to identify the illegal activities. Hence, the network security is improved.

Intrusion Detection System (IDS) is defined as the security tools to reinforce the security of communication and information systems. The IDS is a combination of software or hardware for analyzing the network traffic and detecting the malicious patterns and alerting the abnormal activity to the proper authority. Figure.1 shows the IDS and Intrusion Protection System. The main functions of the IDS are

- Monitoring and analyzing the information gathered from both the user and system activities.
- Analyzing the system configurations and evaluating the file and system integrity.
- The abnormal pattern is found out for the static records.
- Static records are used to recognize the abnormal pattern and alert the system administrator.

The IDS involves four major stages. Initially, the data is collected from the network traffic. Then, the feature vector containing the required data is generated. It is determined whether the collected data is suspicious or not, using the data mining techniques and digital forensic techniques. The presence of attack is informed to the administrator.

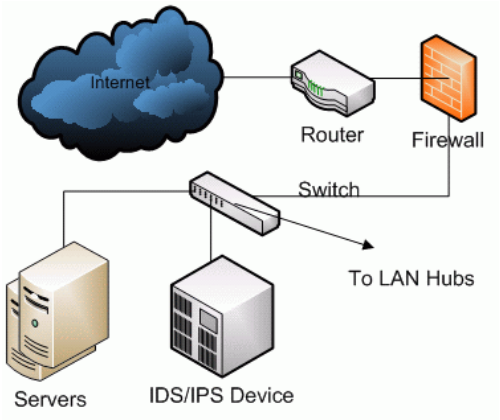

Figure.1 IDS/IPS

The IDS are classified as network-based and host-based IDS.

Network-based IDS

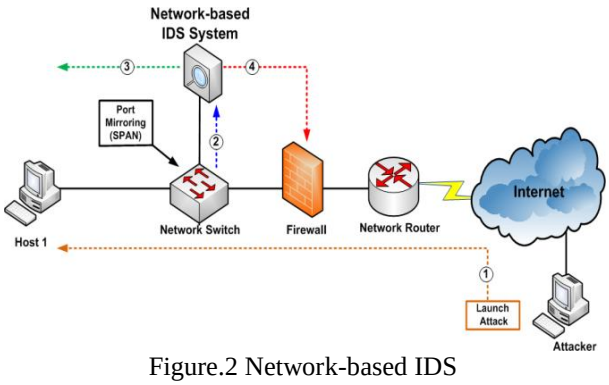

Figure.2 Network-based IDS

DOI 10.17148/IJARCCE.2015.41137

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Network-based IDS [1]monitors the packet that traverses through the network and analyzes the network activity to identify the attacks. It consists of hosts or a set of single-purpose sensors placed at various points in a network. It is most commonly deployed at a boundary between the networks.Figure.2 shows the network-based IDS.

Advantages

1. A large network is monitored easily by using a few network-based IDS
2. Network-based IDSs can be made invisible to many attackers to provide security against attack.
3. It can be fitted easily to the network without requiring much effort.

Host-based IDS

A host-based IDS [2] monitors the activities associated with a particular host and aimed at collecting the information about the activity on a host system or within an individual computer system, using separate sensors. Sensors monitors the event happening on the system and collect the data from the logs generated by the operating system, application activity, file access and modification.Figure.3 shows the Host-based IDS.

Advantages

1. By monitoring the local events of a host, the Host-based IDS can detect the attacks that are not detected by the network-based IDS.
2. It can detect the attacks involved in the software integrity breaches.

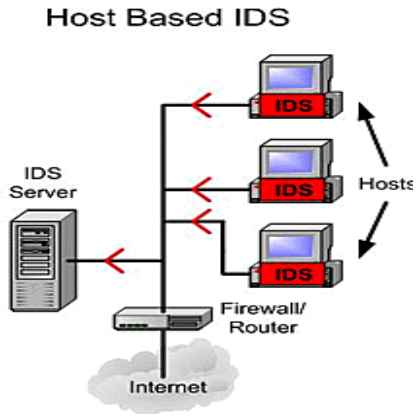

Figure.3 Host-based IDS

According to the techniques used for intrusion detection based on the attack pattern, the IDS is classified

- Signature-based detection system
- Anomaly detection system

Signature-based detection system: It identifies the patterns of traffic or application data that is presumed to be malicious. Signature-based IDS [1]detects the intrusion based on the behaviour of the known attacks. Antivirus software is an example of the signature-based IDS, which compares the data with the known code of the virus. In the signature-based detection, pattern of known malicious activity is stored in the dataset and identify the suspicious data by comparing the new instances with the stored pattern of attacks.

Anomaly detection system: It compares the activities against a normal defined behaviour. It is different from the signature-based detection. anomaly-based IDS [3], [4]monitors the new instances and compares it with the baseline such as load on the network traffic, protocol and packet size. If there is any deviation from the baseline, the data is notified as intrusion. Table I shows the comparative analysis about the merits and limitations of the signature-based and anomaly-based IDS.

Table I Comparative analysis of the Signature-based & Anomaly based

Signature-based IDS	Anomaly-based IDS
Merits 1. Higher detection rate and accuracy. 2. Simple and Effective Method. 3. Low False Alarm Rate.	**Merits** 1. Able to examine unknown and highly complicated intrusions. 2. Rate of missing report is low. 3. Detects new and unanticipated attacks.

Signature based Limitations	**Anomaly based Limitations**
1. Unable to detect only the unknown attacks. 2. Needs a regular update of the rules. 3. Unable to differentiate between the attack attempt and successful attack. 4. Rate of missing report is high.	1. Needs to be trained and tuned carefully to reduce the false positive detections. 2. Low detection rate and high false alarm rate. 3. It cannot identify the new attacks, since the intrusion detection depends on the latest model.

These remaining sections of the paper are organized as follows: Section II explains about the Data Mining Techniques for Intrusion Detection. Section III describes the computer forensic techniques and section IV presents the digital forensic tools. Section IV presents the conclusion of the survey.

II. DATA MINING TECHNIQUES FOR INTRUSION DETECTION

Network traffic is massive and the information is received from different sources, so the dataset for IDS becomes large. Hence, it is really hard for analyzing data in the case of large dataset. Currently, the data mining techniques [5], [6]play a vital role in the detection of the normal and abnormal patterns, since it can extract the hidden information and deal with large dataset. This section describes about different data mining techniques such as classification and clustering to obtain the information about vulnerability by monitoring the network data.

Association Rule

Association rule mining [7]identifies the association among the database attributes and their values. It is

pattern-discovery techniques that do not solve the classification problems and prediction problems. Association rule mining requires two thresholds i.e. Minimum support and Minimum Confidence.

Classification Techniques

Classification[5]is the task of assigning each and every instances of dataset to a particular class. It can be effective for both the signature-based and anomaly-based intrusion detection, but more frequently used for the signature-based detection.

Classification categorizes the data sets into predetermined sets. It is less efficient in the intrusion detection when compared to the clustering .Different classification techniques such as decision tree, Naive Bayes classifier, K-nearest Neighbour (KNN) classifier; Support Vector Machine (SVM), etc are used in IDS.

Decision tree

Decision Tree [8], [9], [10]is a recursive and tree-like structure for expressing classification rules. It uses divide and conquer method for splitting according to the attribute values. Classification of the data proceeds from root node to leaf node. Each root node represents the attribute and its value and each leaf node represent the class label of data. Tree-based classifiers have highest performance in case of large dataset. Different decision tree algorithms are described below

ID3 algorithm

It is a famous decision tree algorithm developed by Quinlan. ID3 algorithm [11]is an attribute based algorithm that constructs decision tree according to training dataset. The attribute having highest information gain is used as a root of the tree.

J48 Algorithm

C4.5 decision tree algorithm is known as J48 algorithm[12]. It construct decision tree using information gain. The attribute having highest information gain is selected to make decision. The main disadvantage of this algorithm is that it requires more CPU time and memory in execution.

Alternating Decision (AD) Tree

AD tree [13]is used for classification. It includes both the leaf node and root nodes as prediction node.

NB tree algorithm

NB tree algorithm [14] uses both decision tree and Naive Bayes classifier. Root node uses decision tree classifier and leaf nodes use Naive Bayes classifier.

Random Forest

Random Forest [15]is an ensemble classification technique that consists of two or more decision trees. In the Random Forest, every tree is prepared by randomly selecting the data from the dataset. It achieves high accuracy and prediction power, because it is less sensitive to the outlier data. It can easily deal with high dimensional data.

K-Nearest Neighbour

K-Nearest Neighbour[10]is one of the simplest classification technique. It calculates the distance between different data points on the input vectors and assigns the unlabeled data point to its nearest neighbour class. If k=1, then the object is assigned to the class of its nearest neighbour. When value of K is large, then it takes large time for prediction and influence the accuracy due to the effect of noise.

Naive Bayes classifier

Naive Bayes classifier[16], [17]is a probabilistic classifier that predicts the class according to the membership probability. It analyzes the relation between the dependent and independent variables to derive the conditional probability.

$$P(H/X) = P(X/H) \cdot P(H)/P(X) \rightarrow (1)$$

Where, X is the data record and H is the hypothesis that represents the data record and belongs to the class C. P(H) is the prior probability, P(H/X) is the posterior probability of H conditioned on X and P(X/H) is the posterior probability of X conditioned on H.

Construction of the Naive Bayes is easy without any complicated iterative parameter. It may be applied to large number of data points but there is increase in the time complexity.

Support Vector Machine (SVM)

SVM [18]is a supervised learning method used for prediction and classification. It separate data points into two classes +1 and -1 using hyper plane. +1 represents normal data and -1 represents suspicious data. The hyper plane is expressed as

$$W \cdot X + b = 0 \quad \rightarrow (2)$$

Where $W = \{w_1, w_2, \dots\dots, w_n\}$the weight vector for 'n' attributes is $X = \{x_1, x_2, \dots\dots, x_n\}$ is the attribute values and b is a scalar. The main goal of the SVM is to find a linear optimal hyper plane, for maximizing the margin of Separation between the two classes. The SVM uses a portion of the data to train the system. It is able to model both complex and nonlinear decision boundaries.

Fuzzy Logic

The Fuzzy logic [8], [19]is highly appropriate for intrusion detection applications, since there is no clear boundary between the normal and abnormal events. It is derived from fuzzy set theory that deals with reasoning that is approximate rather than precisely deduced from classical predicate logic. The application side of the fuzzy set theory deals with the real world expert values for a complex problem. In this approach, the data is classified on the basis of various statistical metrics.

Genetic Algorithms

Genetic algorithms[8] belong to the larger class of Evolutionary Algorithms (EA). They generate solution sto the optimization problems using the techniques inspired by natural evolution, such as inheritance, selection, mutation

and crossover. Genetic Algorithm (GA) is applied in the intrusion detection to derive a set of classification rules from the network audit data. The support-confidence framework is utilized as a fitness function to judge the quality of each rule. Significant properties of GA are its robustness against noise and self-learning capabilities. The advantages of GA techniques are high attack detection rate and lower false-positive rate. It provides a wider solution space and it is modified easily. It does not require any prior information of the problem space.

Neural Networks

Neural Network [8]is a set of interconnected nodes that are designed based on the functioning of the human brain. Each node has a weighted connection to several other nodes in neighbouring layers. Individual nodes take the input received from the connected nodes and use the weights together with a simple function to compute the output values. Neural networks can be constructed for supervised or unsupervised learning. The user specifies the number of hidden layers as well as the number of nodes within a specific hidden layer. Depending on the application, the output layer of the neural network may contain one or several nodes. The Multilayer Perceptions (MLP) neural networks produce more accurate results than other existing computational learning models. Hence, it is successful used in a variety of applications.

Markov Model

Markov-based techniques[20] are normally applied to the system calls. A Hidden Markov Model (HMM) has a definite set of states governed by a set of transition probabilities. In a special state, an observation can be generated according to the associated probability distribution. This process starts from one of the sestates and moves successively from one state to another.

Clustering Techniques

Since the network data is too huge, labelling of each and every instances or data points in the classification is expensive and time consuming. Clustering [5]is the technique of labelling data and assigning into groups of similar objects without using known structure of data points. Members of same cluster are similar and instances of different clusters are different from each other.

Farthest First Traversal (FFT)

FFT algorithm[21] is partitional clustering algorithm. This algorithm selects K objects as the canters of clusters and assigns other objects into the cluster. The center of the cluster that is highly dissimilar to the selected center of the cluster is chosen.

Hierarchical clustering

The BIRCH hierarchical clustering algorithm [22]stores fewer abstracted data points than the whole dataset. Each abstracted point represents the centroid of a cluster of data points. The BIRCH clustering algorithm can achieve high quality clustering with lower processing cost. The BIRCH can handle the noise effectively and it is memory-efficient because BIRCH only stores a few abstracted data points instead of the whole dataset.

K-means clustering algorithm

K-Means clustering algorithm[23] is simplest and widely used clustering technique proposed by James Macqueen. In this algorithm, number of clusters K is specified to classify the instances into a predefined number of clusters. The initial step of K-Means clustering is to choose k instances as a center of clusters. Then, each instance of the dataset is assigned to the nearest cluster. For the instance assignment, the distance between the centroid and each instance is measured using Euclidean distance. Each and every data point is assigned into the cluster according to minimum distance. K–Means algorithm requires less execution time, while applying on small dataset. When the data point increases, then it requires more execution time. It is a fast iterative algorithm but it is sensitive to outlier and noise.

K-Medoids clustering algorithm

K-Medoids[16], [23]is partitioning-based clustering algorithm. The most centrally situated instance in a cluster is considered as a centroid in the mean value of the objects in K-Means clustering. This centrally located object is called as reference point and medoid. It minimizes the distance between centroid and data points. K-Medoids algorithm performs better than the K-Means algorithm, when the number of data points is maximum. It is robust in the presence of noise and outlier, because medoid is less influenced by the outliers. However, it is really expensive.

III.COMPUTER FORENSIC TECHNIQUES

Forensic technologies are developed to extract evidence from a seized computer system. It analyzes and investigates about the spreading of computer virus, malware and malicious codes. During the recovery of data, the integrity of the original data should be maintained. The forensic analysis tools are used for recovering hard-disk information. The techniques used during the computer forensic investigations are described below

Cross-drive analysis

Cross-drive analysis [24]is a forensic technique that correlates the information found on multiple hard drives. This is used to identify social networks and perform anomaly detection.

Live analysis

This process performs extraction of evidence by examining the computers using the custom forensics or existing system admin tools. This analysis process is highly useful while dealing with the encrypting file systems.

Deleted file Recovery

A common technique used in the computer forensics is the recovery of deleted files. Modern forensic software include their own tools for recovering or carving out the deleted data[25]. Most operating systems and file systems

do not always erase physical file data. This allows the investigators to reconstruct it from the physical disk sectors. File carving involves searching for the known file headers within the disk image and reconstructing deleted materials.

Stochastic forensics

This method is used to investigate the activities that lack in the digital artifacts and data theft, by using the stochastic properties of the computer system.

Steganographic Analysis

Steganographic analysis[26] is used to obtain the details of the steganographic contents.

Digital Forensics Tools

The digital forensic tools are depicted in the Table. II.

Table II Digital Forensic Tools

Digital Forensic Tools	Operating Platform	Description
Encase [27]	Windows	Multi-purpose forensic tool including hash analysis for the classification of the known files.
Drive spy[28]	DOS/Windows	Inspects slack space and deleted file metadata.
Wire shark[29]	Cross-platform	Open-source packet capture/analyzer
SANS Investigative Forensics Toolkit – SIFT[30]	Ubuntu	Multi-purpose forensic operating system
Registry Recon[30]	Windows	It rebuilds the windows registries from anywhere on a hard drive and parses them for deep analysis.
DigitalForensics Framework[31]	Unix-like/Windows	Framework and user interfaces dedicated to Digital Forensics
FTK[32]	Windows	FTK is a multi-purpose court-cited digital investigations platform built for speed, stability and ease of use.
The Coroner's Toolkit[33]	Unix-like	A suite of programs for Unix analysis.
COFEE[34]	Windows	A suite of tools for Windows developed by Microsoft.
Xways[35]	Windows	Used for disk cloning and imaging.
The Sleuth Kit[36]	Unix-like/Windows	A library of tools for both Unix and Windows
Open Computer Forensics Architecture[37]	Linux	Computer forensics framework for CF-Lab environment

IV. CONCLUSION

This paper presented a survey on the different data mining techniques and digital forensics techniques for the IDPS. This enables effective detection of the both malicious and normal activities in the network, to develop a secure information system. The data mining techniques and computer forensic techniques are combined to detect the intrusion attacks and provide immediate response to the user. This results in the efficient detection of the attacks.

REFERENCES

[1] P. S. Kenkre, A. Pai, and L. Colaco, "Real Time Intrusion Detection and Prevention System," in Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, 2015, pp. 405-411.

[2] C.-M. Ou, "Host-based intrusion detection systems adapted from agent-based artificial immune systems," *Neurocomputing*, vol. 88, pp. 78-86, 2012.

[3] S. K. Shrivastava and P. Jain, "Effective anomaly based intrusion detection using rough set theory and support vector machine," *International Journal of Computer Applications*, vol. 18, pp. 35-41, 2011.

[4] X.-s. Gan, J.-s. Duanmu, J.-f. Wang, and W. Cong, "Anomaly intrusion detection based on PLS feature extraction and core vector machine," *Knowledge-Based Systems*, vol. 40, pp. 1-6, 2013.

[5] D. K. Denatious and A. John, "Survey on data mining techniques to enhance intrusion detection," in *International Conference on Computer Communication and Informatics (ICCCI), 2012*, 2012, pp. 1-5.

[6] M. Ektefa, S. Memar, F. Sidi, and L. S. Affendey, "Intrusion detection using data mining techniques," in *International Conference on Information Retrieval & Knowledge Management,(CAMP)*, 2010, pp. 200-203.

[7] S. Mabu, C. Chen, N. Lu, K. Shimada, and K. Hirasawa, "An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,*, vol. 41, pp. 130-139, 2011.

[8] O. Chandrakar, R. Singh, and L. B. Barik, "Application of Genetic Algorithm in Intrusion Detection System," *Control Theory and Informatics*, vol. 4, pp. 50-57, 2014.

[9] C. Xiang, M. Chong, and H. Zhu, "Design of mniple-level tree classifiers for intrusion detection system," in *IEEE Conference on Cybernetics and Intelligent Systems*, 2004, pp. 873-878.

[10] H. Tribak, B. L. Delgado-Marquez, P. Rojas, O. Valenzuela, and H. Pomares, "Statistical analysis of different artificial intelligent techniques applied to Intrusion Detection System," in *International Conference on Multimedia Computing and Systems (ICMCS)* 2012, pp. 434-440.

[11] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, pp. 2670-2679, 2015.

[12] B. Senthilnayaki, K. Venkatalakshmi, and A. Kannan, "An intelligent intrusion detection system using genetic based feature selection and Modified J48 decision tree classifier," in *Fifth International Conference on Advanced Computing (ICoAC)*, 2013, pp. 1-7.

[13] S. Thaseen and C. A. Kumar, "An analysis of supervised tree based classifiers for intrusion detection system," in *International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME)* 2013, pp. 294-299.
[14] A. H. Bhat, S. Patra, and D. Jena, "Machine learning approach for intrusion detection on cloud virtual machines," *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 2, pp. 56-66, 2013.
[15] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely, and M. M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," *Ain Shams Engineering Journal*, vol. 4, pp. 753-762, 2013.
[16] D. Upadhyaya and S. Jain, "Hybrid Approach for Network Intrusion Detection System Using K-Medoid Clustering and Naïve Bayes Classification," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, pp. 231-236, 2013.
[17] L. Koc, T. A. Mazzuchi, and S. Sarkani, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier," *Expert Systems with Applications*, vol. 39, pp. 13492-13500, 2012.
[18] S.-J. Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L. Lai, *et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert systems with Applications*, vol. 38, pp. 306-313, 2011.
[19] R. Shanmugavadivu and N. Nagarajan, "Network intrusion detection system using fuzzy logic," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, pp. 101-111, 2011.
[20] A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, "Credit card fraud detection using hidden Markov model," *IEEE Transactions on Dependable and Secure Computing*, , vol. 5, pp. 37-48, 2008.
[21] M. Panda and M. R. Patra, "A novel classification via clustering method for anomaly based network intrusion detection system," *International Journal of Recent Trends in Engineering*, vol. 2, pp. 1-6, 2009.
[22] S. H. Oh and W. S. Lee, "An anomaly intrusion detection method by clustering normal user behavior," *Computers & Security*, vol. 22, pp. 596-612, 2003.
[23] T. Velmurugan and T. Santhanam, "Computational complexity between K-means and K-medoids clustering algorithms for normal and uniform distributions of data points," *Journal of computer science*, vol. 6, p. 363, 2010.
[24] S. L. Garfinkel, "Forensic feature extraction and cross-drive analysis," *digital investigation*, vol. 3, pp. 71-81, 2006.
[25] A. Philipp, D. Cowen, and C. Davis, *Hacking exposed computer forensics*: McGraw-Hill, Inc., 2009.
[26] B. Dunbar, "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment," *Sans Institute*, vol. 2002, pp. 1-9, 2002.
[27] S. Garfinkel, "Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus," *Digital Investigation*, vol. 9, pp. S80-S89, 2012.
[28] J. M. Kizza, "Computer and Network Forensics," in *Guide to Computer Network Security*, ed: Springer, 2015, pp. 299-324.
[29] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using Wireshark," *International Journal of Security and Networks*, vol. 10, pp. 91-106, 2015.
[30] G. Shrivastava and B. Gupta, "An Encapsulated Approach of Forensic Model for digital investigation," in *Consumer Electronics (GCCE), 2014 IEEE 3rd Global Conference on*, 2014, pp. 280-284.
[31] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, pp. 71-80, 2012.
[32] E. Sohl, C. Fielding, T. Hanlon, J. Rrushi, H. Farhangi, C. Howey, *et al.*, "A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, 2015, pp. 113-122.
[33] S. Garfinkel, "Digital forensics XML and the DFXML toolset," *Digital Investigation*, vol. 8, pp. 161-174, 2012.
[34] M. S. Bashir and M. Khan, "Triage in Live Digital Forensic Analysis," *International journal of Forensic Computer Science*, vol. 1, pp. 35-44, 2013.
[35] F. Brennan, M. Udris, and P. Gladyshev, "An Automated Link Analysis Solution Applied to Digital Forensic Investigations," in *Digital Forensics and Cyber Crime*, ed: Springer, 2014, pp. 189-206
[36] G.Fenu and F. Solinas, " COMPUTER FORENSICS INVESTIGATION AN APPROACH TO EVIDENCE IN CYPERSPACE ",in The Second International Conference on Cyber Security Cyber Peace fare and Digital Forensic ,2013
[37] C. Federici, "AlmaNebula: a computer forensics framework for the Cloud," *Procedia Computer Science*, vol. 19, pp. 139-146, 2013.
[38] V. R. Ambhire and B. Meshram, "Digital Forensic Tools," *IOSR Journal of Engineering*, vol. 2, pp. 392-398, 2012.
[39] M. Kaart, C. Klaver, and R. van Baar, "Forensic access to Windows Mobile pim. vol and other Embedded Database (EDB) volumes," *Digital Investigation*, vol. 9, pp. 170-192, 2013.