The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 6 ||Pages|| 19-25||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

# Characterization and Trends of Development in Data Mining Techniques For Intrusion Detection Systems (IDS)

Idowu S.A, Ajayi Adebowale
Babcock University, Ilishan-Remo, Ogun State, Nigeria

**----------ABSTRACT----------**

*In Information Security, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Data mining is the process of extracting useful and previously unnoticed models or patterns from large data stores. This work is focused on the characterization and trends of development in data mining techniques for intrusion detection systems. We present a comparative analysis of these techniques vis-à-vis their performance.*

***Keywords:-*** *Information Security, intrusion detection, data mining, intrusion detection systems*

Date Of Submission: 20 May 2013 Date Of Publication: 10, June.2013

## I. INTRODUCTION

As the demand for the use of Internet increases, there is a need for corresponding security of content and services. Computer scientists seek new ways of securing networks as the attackers constantly change their attack patterns. Intrusion Detection Systems (IDS) have consequently become a standard component in security infrastructures as they allow network administrators to detect policy violations. These policy violations run the gamut from external attackers trying to gain unauthorized access (which can usually be protected against through the rest of the security infrastructure) to insiders abusing their access (which often times is not easy to protect against) [18]. Detecting such violations is a necessary step in taking corrective action, such as blocking the offender (by blocking their machine at the parameter, or freezing their account), by reporting them (to their ISP or supervisor), or taking legal action against them [11].

Alternatively, detecting policy violations allows administrators to identify areas where their defenses need improvement, such as by identifying a previously unknown vulnerability, a system that was not properly patched, or a user that needs further education against social engineering attacks [2].

Traditional methods for intrusion detection are based on extensive knowledge of signatures of known attacks that are provided by human experts. The signature database has to be manually revised for each new type of intrusion that is discovered. A significant limitation of signature-based methods is that they cannot detect emerging cyber threats. In addition, once a new attack is discovered and its signature developed, often there is a substantial latency in its deployment across networks [3]. These limitations have led to an increasing interest in intrusion detection techniques based upon data mining.

Given its success in commercial applications, data mining holds great promise for the development of tools for gaining fundamental insights into the network traffic data, thereby allowing system administrators and network engineers to automatically detect emerging cyber attacks [3] [13].

## II. DATA MINING AND KNOWLEDGE DISCOVERY IN DATABASES (KDD)

Data Mining is the automated process of going through large amounts of data with the intention to discover useful information about the data that is not obvious. Useful information may include special relations between the data, specific models that the data repeat itself, specific patterns, and ways of classifying it or discovering specific values that fall out of the "normal" pattern or model [18]. However, in literature this same definition is sometimes given to describe Knowledge discovery in databases (KDD). This work adopts the view that KDD is the broader discipline, of which data mining is merely a component, specifically pattern extraction, evaluation and cleansing methods. In practice KDD is an interactive and iterative process involving numerous steps, some of which are listed below.

i. Understanding the application domain: This involves understanding the application domain, the relevant background knowledge and the specific goals of KDD.

ii. Data integration and selection: This is concerned with the integration of multiple data sources and the selection of relevant subsets of data.

iii. Data mining: Application of algorithms for extracting patterns from data.

iv. Pattern evaluation: At this stage, the discovered patterns are evaluated and validated. The goal of this step is to guarantee that actual knowledge is being discovered.
iv. Knowledge representation: This step involves documenting and using the discovered knowledge.
Data mining techniques are basically pattern discovery algorithms [3]. Some techniques such as association rules are unique to data mining but most are drawn from fields such as statistics, machine learning or pattern recognition [24].

## III. INTRUSION DETECTION AND DATA MINING

Intrusion detection is mainly concerned with the detection of security violations to information management. Intrusion detection is a passive approach to security as it monitors information systems and raises alarms when security violations are detected. Examples of security violations include the abuse of privileges or the use of attacks to exploit software or protocol vulnerabilities. Traditionally, intrusion detection techniques are classified into two broad categories: misuse detection and anomaly detection [4].

Misuse detection systems, encode and match the sequence of "signature actions" of known intrusion scenarios. The main shortcomings of such systems are: known signatures have to be hand-coded into the system and they are unable to detect any future intrusions that have no matched patterns stored in the system. Anomaly detection on the other hand establishes a model of normal user or system behavior or and marks any significant deviations from this model as potentially malicious. The strength of anomaly detection is its ability to detect previously unknown attacks. Its deficiency however is the high false alarms it generates, as previously unseen but normal system behavior gets to be flagged as an intrusion. A more extended taxonomy of IDS can be found in [25].

In recent times a growing number of research works have applied data mining to intrusion detection. This work presents a trend of development in this area of research and provides a characterization of data mining techniques in intrusion detection.

### 1.1 DRAWBACKS OF IDS

In other to understand the role of data mining in IDS, it is important to be aware of the deficiencies and challenges of IDS. The following may be considered significant setback in IDS.
(i). Current IDS are usually tuned to detect known service level network attacks. This leaves them vulnerable to original and novel malicious attacks.
(ii). Data overload: Another aspect which does not relate directly to misuse detection but is extremely important is how much data an analyst can efficiently analyze. The amount of data he needs to look at seems to be growing rapidly. Depending on the intrusion detection tools employed and the size of the network there is the possibility for logs to reach millions of records per day.
(iii). False positives: A common complaint is the amount of false positives an IDS will generate. A false positive occurs when normal attack is mistakenly classified as malicious and treated accordingly.
(iv). False negatives: This is the case where an IDS does not generate an alert when an intrusion is actually taking place.(Classification of malicious traffic as normal)

Data mining can help improve intrusion detection by addressing the above mentioned problems in the following ways.
(i). Removal of normal activity from alarm data to allow analysts to focus on real attacks
(ii). Identifying false alarm generators and "bad" sensor signatures
(iii). Finding anomalous activity that uncovers a real attack
(iv).Identifying long, ongoing patterns (different IP address, same activity)

To accomplish these tasks, data mining experts employ one or more of the following techniques:
(i). Data summarization with statistics, including finding outliers
(ii). Visualization: presenting a graphical summary of the data
(iii). Clustering of the data into natural categories
(iv). Association rule discovery: defining normal activity and enabling the discovery of anomalies
(v). Classification: predicting the category to which a particular record belongs.

## IV. DATA MINING TECHNIQUES AND IDS

This section presents a trend of development in data mining techniques in IDS.

[A]. Feature Selection

Feature selection, also known as subset selection or variable selection, is a process commonly used in machine learning, wherein a subset of the features available from the data is selected for application of a

learning algorithm. Feature selection is necessary either because it is computationally infeasible to use all available features, or because of problems of estimation when limited data samples (but a large number of features) are present [12].

In IDS research, connection log is the most popular data format for analysis. The connection record format affords more power in the data analysis step, as it provides multiple fields that correlation can be done on (unlike a format such as command histories) [4]. Researchers apply various analysis procedures to the accumulated connection data, in order to select the set of features that they think maximizes the effectiveness of their data mining techniques. Table I below contains some examples of the features selected. Each of these features offers a valuable piece of information to the System. Extracted features can be ranked with respect to their contribution and utilized accordingly.

Lee et al [15] note that the timestamp, source address and port, destination address and port, and protocol uniquely identify a connection, making them essential attributes. They go on to note that "association rules should describe patterns related to the essential attributes." Specifically, at least one of those attributes must be present in the antecedent of a rule in order for that rule to be useful. They call this the axis attribute for the rule. For example, a rule that is based solely on the number of bytes transferred really does not convey any useful information. Likewise, if the value of some feature must be kept constant through the processing of a set of records (for instance, the destination host), that feature is called a reference attribute [14] [15] [16].

Dickerson and Dickerson [7] found that their best results were achieved when they limited their rules to only use a key consisting of the source IP, destination IP, and the destination port, which they call the sdp.

Hofmeyr and Forrest [12] used the same approach, although they assign all connections with unassigned privileged ports to one service group, and all connections with unassigned non-privileged ports to another group.

A Table of Features extracted in the process of Applying Data Mining Techniques to IDS

| | |
|---|---|
| % of same service to same host | # different services accessed |
| % on same host to same service | # establishment errors |
| average duration / all services | # FIN flags |
| average duration /current host | # ICMP packets |
| average duration / current service | # keys with outside hosts |
| bytes transferred / all services | # new keys |

Table I

[B]. STATISTICAL TECHNIQUES

Statistical techniques, also known as "top-down" learning, are employed when we have some idea as to the relationship we are looking for and can employ mathematics to aid our search. Three basic classes of statistical techniques are linear, nonlinear (such as a regression-curve), and decision trees. Statistics also includes more complicated techniques, such as Markov models and Bayes estimators. Statistical patterns can be calculated with respect to different time windows, such as day of the week, day of the month, month of the year, etc or on a per-host, or per-service basis.

Denning [25] described how to use statistical measures to detect anomalies, as well as some of the problems and their solutions in such an approach. She described five statistical measures for anomaly detection; the operational model, the mean and standard deviation model, the multivariate model, the Markov process model, and the time series model. She noted that the time series model was similar to the mean and standard deviation model in terms of applicability, and that the time series model stood to provide more accurate results, however it was more costly than the standard deviation model. The models themselves are built in an off-line environment due to the cost of their construction. These statistical measure models may be further assisted by the availability of a data warehouse to do mining from. For instance, if the system or analyst decides that the system should detect anomalies in the mean and standard deviation of duration of FTP sessions, the necessary mean and standard deviation can be constructed from the data warehouse on the fly, rather than having to wait for the collection of new data.

Javitz and Valdes [12] provided more details on the individual statistical measures used in intrusion detection. They also provided formulas for calculating informative statistic metrics.

Staniford et al [13] uses a similar approach by employing a Bayes network to calculate the conditional probabilities of various connection features with respect to other connection features. These probabilities are then used to determine how anomalous each connection is.

**[C]. MACHINE LEARNING**

Machine Learning is the study of computer algorithms that improve automatically through experience. In contrast to statistical techniques, machine learning techniques are well suited to learning patterns with no a priori knowledge of what those patterns may be [25]. Classification and clustering are probably the two most popular machine learning problems [4]. Various techniques addressing these two problems have been applied in IDS research.

**i. Classification Techniques:**

In a classification task in machine learning, the task is to take each instance of a dataset and assign it to a particular class [20]. A classification based IDS attempts to classify all traffic as either normal or malicious. The challenge in this is to minimize the number of false positives (classification of normal traffic as malicious) and false negatives (classification of malicious traffic as normal) [2]. The following techniques have been applied for classification in IDS

**a. Inductive Rule Generation**

In the attribute based inductive learning paradigm, the aim of induction is to determine conceptually meaningful generalized patterns (rules) from a set of training data (instances) [20]. The rules in turn are used to classify new non-training data to one class of the domain.

Since the training data is pre-classified, the view could be adopted that the inductive rule generation process starts with k-clusters of data (k is the number of decision classes of the domain). Each cluster consists of the data items that belong to one decision class. The aim of induction becomes the creation of sub clusters of the initial clusters, so that each sub cluster will be given a simple conceptual description, based on the attributes that define the domain [20]. This conceptual description is the condition part of a rule. The conclusion part of the rule is the class of the instances that belong to the sub cluster from which the rule has been generated.

The **RIPPER** System is probably the most popular representative of this classification mechanism. **RIPPER** is a rule learning program [6]. **RIPPER** is fast and is known to generate concise rule sets. It is very stable and has shown to be consistently one of the best algorithms in past experiments [11]. The system is a set of association rules and frequent patterns that can be applied to the network traffic to classify it properly [6]. One of the attractive features of this approach is that the generated rule set is easy to understand; hence a security analyst can verify it. Another attractive property of this process is that multiple rule sets may be generated and used with a meta-classifier.

**b. Genetic Algorithms:**

In the field of artificial intelligence, a genetic algorithm is a search heuristic that mimics the process of natural evolution [11]. While GAs were originally introduced in the field of computational biology, they have been applied in various fields with promising results. Fairly recently, researchers have tried to integrate these algorithms with IDSs.

In IDS research, genetic algorithms are used in conjunction with other data mining algorithms [5]. GA's are applied at the pre-processing or post-processing stage of the connection records. GA's help in selecting the most useful features from the dataset and consequently enhances the performance of data mining algorithms on the preprocessed data.

The REGAL System is a concept learning system based on a distributed genetic algorithm that learns First Order Logic multi-modal concept descriptions. REGAL uses a relational database to handle the learning examples that are represented as relational tuples [17].

**c. Fuzzy Logic:**

Fuzzy logic is derived from fuzzy set theory dealing with reasoning that is approximate rather than precisely deduced from classical predicate logic [4]. It can be thought of as" the application side of fuzzy set theory dealing with well thought out real world expert values for a complex problem. In Dickerson and Dickerson [7] the authors classify the data based on various statistical metrics. They then created and applied fuzzy logic rules to these portions of data to classify them as normal or malicious. They found that the approach is particularly effective against scans and probes.

**d. Neural Networks:**

The application of neural networks for IDSs has been investigated by a number of researchers. Neural networks provide a solution to the problem of modeling the users' behavior in anomaly detection because they do not require any explicit user model. Neural networks for intrusion detection were first introduced as an alternative to statistical techniques in the IDES intrusion detection expert system to model.

McHugh [22] pointed out that advanced research issues on IDSs should involve the use of pattern recognition and learning by example approaches for the following two main reasons:

**i.** The capability of learning by example allows the system to detect new types of intrusion.

**ii.** With learning by example approaches, attack "signatures" can be extracted automatically from labeled traffic data. This basically eliminates the subjectivity and other problems introduced by the presence of the human factor.

**e. Support Vector Machine:**

Support vector machines (SVMs) are a set of related supervised learning methods used for classification and regression. They belong to a family of generalized linear classifiers. SVMs attempt to separate data into multiple classes (two in the basic case) through the use of a hyper-plane.

Eskin et al [9], and Honig et al [11] used an SVM in addition to their clustering methods for unsupervised learning. The SVM algorithm had to be slightly modified to operate in the unsupervised learning domain. Once it was, its performance was comparable to or better than both of their clustering methods.

Mukkamala, Sung et al [23] used a more conventional SVM approach. They used five SVMs, one to identify normal traffic, and one to identify each of the four types of malicious activity in the KDD Cup dataset. Every SVM performed with better than 99% accuracy, even using seven different variations of the feature set. As the best accuracy they could achieve with a neural network (with a much longer training time) was 87.07%, they concluded that SVMs are superior to neural nets in both accuracy and speed [13].

**ii. Clustering Techniques:**

Data clustering is a common technique for statistical data analysis, which is used in many fields, including machine learning, data mining, pattern recognition, image analysis and bioinformatics [9]. Clustering is the classification of similar objects into different groups, or more precisely, the partitioning of a data set into subsets (clusters), so that the data in each subset (ideally) share some common trait - often proximity according to some defined distance measure [11].

In Machine learning, data clustering is typically regarded as a form of unsupervised learning. Clustering is useful in intrusion detection as malicious activity should cluster together, separating itself from non-malicious activity. Clustering provides some significant advantages over the classification techniques already discussed, in that it does not require the use of a labeled data set for training.

Frank [10] breaks clustering techniques into five areas: hierarchical, statistical, exemplar, distance, and conceptual clustering, each of which has different ways of determining cluster membership and representation .

Portnoy et al [12] presented a method for detecting intrusions based on feature vectors collected from the network, without being given any information about classifications of these vectors. They designed a system that implemented this method, and it was able to detect a large number of intrusions while keeping the false positive rate reasonably low. There are two primary advantages of this system over signature based classifiers or learning algorithms that require labeled data in their training sets. The first is that no manual classification of training data needs to be done. The second is that we do not have to be aware of new types of intrusions in order for the system to be able to detect them. All that is required is that the data conform to several assumptions. The system tries to automatically determine which data instances fall into the normal class and which ones are intrusions. Even though the detection rate of the system they implemented is not as high as of those using algorithms relying on labeled data, they claim it is still very useful. Since no prior classification is required on the training data, and no knowledge is needed about new attacks, the process of training and creating new cluster sets can be automated. In practice, this would mean periodically collecting raw data from the network, extracting feature values from it, and training on the resulting set of feature vectors. This will help detect new and yet unknown attacks.

Bloedorn et al used k-means clustering techniques on connection logs looking for outliers, which represent anomalies in the network traffic [2].

Marin et al (2001) employed a hybrid approach that begins with the application of expert rules to reduce the dimensionality of the data, followed by an initial clustering of the data and subsequent refinement of the cluster locations using a competitive network called Learning Vector Quantization.

**D. Ensemble Approaches**

"In reality there are many different types of intrusions, and different detectors are needed to detect them" [1]. One way to improve certain properties, such as accuracy, of a data mining system is to use a multiplicity of techniques and correlate the results together. The combined use of numerous data mining methods is known as an ensemble approach, and the process of learning the correlation between these ensemble techniques is known by names such as multi-strategy learning, or meta-learning [7].

Lee and Stolfo [10] stated that if one method or technique fails to detect an attack, then another should detect it. They propose the use of a mechanism that consists of multiple classifiers, in order to improve the effectiveness of the IDS.

Axelsson [1] proposes the modeling and analysis of both possible types of traffic (normal and malicious). Having results from both patterns can help improve the overall performance of the system [1].

Lee and Stolfo used meta-classification to improve both accuracy and efficiency (by running high cost classifiers only when necessary), and combined the results using boolean logic. The classifiers are produced using cost factors that quantify the expense of examining any particular feature in terms of processing time, versus the cost of responding to an alert or missing an intrusion [10].

Didaci et al applied a meta-classification approach [5]. The authors applied three different classification methods - the majority voting rule, the average rule, and the ”belief” function to the outputs of three distinct neural nets. The Neural nets had previously been trained on different features sets from the KDD tcpdump data. They found that these multistrategy techniques, particularly the belief function, performed better than all three neural nets individually.

**E. Predictive Analysis**

Ideally, data-mining based IDS will do more than just detect intrusions that have already happened: we would like it to provide some degree of predictive analysis. Lee [10] noted that “a typical attack session can be split into three phases: a learning phase, a standard attack phase, and an innovative attack phase.” Given that, we should be able to predict standard and innovative attacks to some degree based on prior activity. Another area that predictive analysis may be useful is in early detection of worms. Typically, retrospective analysis of worms such as Code Red has shown similar activity of the worms a number of weeks before its widespread outbreak [8]. Additionally, statistical trending should be able to detect the start of a worm’s characteristic exponential curve before the infection rate begins increasing steeply, at least for traditional worms such as Code Red or Nimda [13]. Unfortunately, fast infection rate worms, such as the SQL Slammer worm, will most likely have completed their exponential growth before the connection data can be fused and mined.

## V. CONCLUSION

This paper has presented a development trend in the use of data mining techniques for IDS. We describe an explicit characterization of the techniques over time, highlight strengths and weaknesses of each of the techniques. Further Work in this respect include a comparative analysis of some popular data mining algorithms applied to IDS and enhancing a classification based IDS using selective feedback methods (Ensemble approach).

## REFERENCES


[1]. Axelsson, S. (2000). “The base-rate fallacy and the difficulty of intrusion detection”, ACM Trans. Information and System Security 3 (3), pp. (186-205).

[2]. Barbara, D., Wu, N. and Jajodia, S. [2001]. “Detecting Novel Network Intrusions Using Bayes Estimators”, Proceedings Of the First SIAM Int. Conference on Data Mining, (SDM 2001), Chicago,.

[3]. Bloedorn et al. (2003). Data Mining for Network Intrusion Detection: How to Get Started. The MITRE Corporation McLean, VA.

[4]. Carbone, P. L. (1997). “Data mining or knowledge discovery in databases: An overview”, In Data Management Handbook, New York: Auerbach Publications.

[5]. Chittur, A. (2001). “Model generation for an intrusion detection system using genetic algorithms”, High School Honors Thesis, Ossining High School in cooperation with Columbia University.

[6]. Cohen, W. (1995). “Fast effective rule induction” (Prieditis, A. & Russell, S. (Eds.). Proc. of the 12th International Conference on Machine Learning (pp. 115 123), Tahoe City, CA: Morgan Kaufmann.

[7]. Dickerson, J. E. & Dickerson, J.A. (2000). “Fuzzy network profiling for intrusion detection”, In Proceedings of North American Fuzzy Information Processing Society (NAFIPS) 19th International Conference of the North American Fuzzy Information Processing Society (pp. 301-306), Atlanta.

[8]. Didaci, L., Giacinto, A. & Roli, F. (2002). “Ensemble learning for intrusion detection in computer networks”, Proceedings of AI*IA, Workshop on “Apprendimento automatico: metodi e applicazioni”, Siena, Italy.

[9]. Eskin, E., Arnold, A., Preraua, M., Portnoy, L. and Stolfo, S. J. (2002). “A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data”, (Barbar & Jajodia Eds.), Data Mining for Security Applications. Boston: Kluwer Academic Publishers.

[10]. Frank, J. (1994). ”Artificial intelligence and intrusion detection: Current and future directions”, In Proc. of the 17th National Computer Security Conference, Baltimore, MD. National Institute of Standards and Technology (NIST).

[11]. Honig, A., Howard, A., Eskin, E. and Stolfo, S.J. (2002). “Adaptive model generation: An architecture for the deployment of data mining based intrusion detection systems” (Barbar, D. & Jajodia, S. Eds.). Boston: Kluwer Academic Publishers

[12]. Kesavulu, E., Reddy, V. N. & Rajulu, P. G. (2011). “A Study of Intrusion Detection in Data Mining”.Proceedings of the World Congress on Engineering 2011 Vol IIIWCE 2011, July 6 - 8, 2011, London, U.K.

[13]. Lappas, T. and Pelechrinis, K. (2006). Data Mining Techniques for (Network) Intrusion Detection Systems, Department of Computer Science and Engineering Riverside, Riverside CA.

[14]. Lee, W. & Stolfo, S.J. (1998). Data mining approaches for intrusion detection, In Proc. of the Seventh USENIX Security Symp., San Antonio, TX.

[15]. Lee, W., S. J. Stolfo, & Mok, K. W. (1999). “A data mining framework for building intrusion detection models,” In Proc. of the 1999 IEEE Symp. On Security and Privacy (pp. 120-132), Oakland, CA: IEEE Computer Society Press.

[16]. Lee, W., Stolfo, S.J. & Mok, K.W. (1999). “Mining in a data-flow environment: Experience in network intrusion detection,” (Chaudhuri, S. & Madigan, D. Eds.). Proc. of the Fifth International Conference on Knowledge Discovery and Data Mining (KDD-99) (pp. 114-124), San Diego, CA: ACM,

[17]. Lee, W. & Stolfo, S.J et al. (2000). ”A data mining and CIDF based approach for detecting novel and Distributed intrusions”, In Proc. of Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000), Toulouse, France.

[18]. Manganaris, S., M. Christensen, D. Zerkle, and K. Hermiz 2000. "A data mining analysis of RTID alarms", Computer Networks, 34, p. 571-577.
[19]. Mithcell Rowton, Introduction to Network SecurityIntrusion Detection, December 2005.
[20]. Neri, F. (2000). "Comparing local search with respect to genetic evolution to detect intrusion in computer networks", In Proc. of the 2000 Congress on Evolutionary Computation CEC00 (pp. 238-243), La Jolla, CA: IEEE Press.
[21]. Marin, J. A., Ragsdale, D. & Surdu, J. (2001). "A hybrid approach to profile creation and intrusion detection", In Proceedings of DARPA Information Survivability Conference and Exposition, Anaheim, CA. (pp. 12-14) IEEE Computer Society.
[22]. McHugh, J. (2000). "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory", ACM Trans. Information System Security 3 (4), (pp. 262-294).
[23]. Mukkamala, S. & Sung, A. H. (2003). "Identifying significant features for network forensic analysis using artificial intelligent techniques", International Journal of Digital Evidence 1 (4), (pp. 1-17).
[24]. Rendell, Larry (1986). " A general framework for induction and a study of selective induction". Machine Learning 1 (2):177-226.
[25]. Tan, Pang-Ning; Steinbach, Michael; and Kumar, Vipin (2005); Introduction to Data Mining, ISBN 0-321-32136-7

**Authors**


| | |
|---|---|
|  | **Sunday Idowu Phd** is currently the Head of department of the computer science and engineering, Babcock University, Ilishan-Remo, Ogun State, Nigeria. He holds a Masters degree in Software Engineering, and Ph.D in computer science from the University of Ibadan, Oyo State, Nigeria. His research areas are Software Engineering, Web Application Development and Security. He has published works in several journals of international repute. He can be contacted at |
|  | **Ajayi Adebowale** Received a B.Sc degree in Mathematics (computer science) from University of Agriculture Abeokuta 2007, he is a Cisco Certified Network Associate and is currently working on his M.Sc degree in Computer science at Babcock University. He can be contacted at |