International Journal of Computer Applications Technology and Research
Volume 5– Issue 4, 226 - 233, 2016, ISSN:- 2319–8656

A Review of Intrusion Alerts Correlation Frameworks

Joseph Mbugua Chahira
GarissaUniversityCollege,
Garissa- Kenya

Jane Kinanu Kiruki, Chuka University,
Chuka- Kenya

Peter Kiprono Kemei
Egerton University,
Nakuru- Kenya

Abstract : The advancement of modern computers, networks and internet has led to the widespread adoption and application of Information Communication Technology in modern organizations. As a result, large amount of information is generated, processed and distributed through digital devices. On the other side, digital crimes have increased in number and sophistication and they compromise the organization's critical information infrastructure affecting the confidentiality, integrity and availability of its information resources. In order to detect these malicious activities, organizations deploys multiple Network Intrusion Detection Systems (NIDSs) in their corporate networks. They generate huge amount of low quality alerts and in different formats when an attack has already taken place. Thus Alert and event correlation is required to preprocess, analyze and correlate the alerts produced by one or more network intrusion detection systems and events generated from different systems and security tools to provide a more succinct and high-level view of occurring or attempted intrusions. This work will review current alert correlation systems in terms of approaches and propose design consideration for an efficient alert correlation technique. We conclude by highlighting the opportunity to include attack prediction component in a real time multiple sensors environment.
Key words alert correlation, Intrusion Detection Systems, Attacks prediction, Attack strategy, Network security.

1.0 INTRODUCTION

The modern enterprise relies on network enabled applications, distributed rather than centralized computing resources and internet access to every networked device to conduct and improve business transactions. As a result large amount of information is generated, processed and distributed electronically (Sommer, 2009). Against the background of these accelerating technological changes and disruptive business models, enterprises with online presence are at a high risk of cyber-attacks and threats. Cyber crimes have increased in frequency and their degree of sophistication has also advanced ((Healy, 2008, Alharbi, 2011). Finding the most effective way to secure information systems, networks and sensitive data based on the current trends is a challenging task experienced by many organisation.

Information Assurance and Security (IAS) is a crucial component in the corporate environment to ensure legitimate access to critical information resources and prevent illegal alterations, protect the trustworthiness of information and maintain secrecy of sensitive information against unauthorized access. The organizations have implemented various Intrusion Detection and Prevention Systems (IDPS)on protecting the information on a secured network. However, they are unable to provide bullet proof protection that copes with the large amounts of information to be protected, the advancement of cyber threats and attacks and also the current manual way of analyzing alerts which istedious, time consuming and error prone for the security analyst to manage and verify true alerts (Maheyzah at el, 2015; wang at el, 2005).

In order to optimally discover the complete relationships among alerts from multiple sources a more practical and efficient Alert Correlation system is required (Maheyzah at el, 2015; Rahayu at el, 2009). This will address the problem of huge volumes of low quality alerts, computational requirements and increase the accuracy of generated output. Indeed, the complete discovery can reveal the behavior of the attacker and predict the next steps of action in a proactive step to assist response systems react before the network is compromised.

The following section presents the overview of the main correlation approaches and proposed frameworks that falls in these areas of intrusion alert correlation approaches. Section Three provides a summary of these approaches in terms of the strengths and limitations and design Considerations for an effective alert correlation technique. Lastly, we conclude the paper and present potential future work.

2.0 ALERT CORRELATIONS SYSTEMS

The research on alerts clustering and correlation techniques have been carried out for several years to provide a global view of attacker's behavior by analyzing low-level alerts produced by the IDS sensors and other security systems. The main objective of alerts correlation is to build an automated abstract modeling of alerts by reducing the number of meta alerts generated from alert aggregation process (Fatma at el,2013; Bateni et al., 2012). The correlation system achieves this by identifying and suppressing false alerts, grouping alerts that refer to the same incident together, constructing attack scenarios, prioritizing the alerts, attack detection and prediction (Maheyzah at el, 2015; Rahayu at el, 2008). The main approaches of alert correlation techniques can be divided into: Similarities of Alert Attributes technique, Predefined Attack Scenario, Prerequisites and Consequences of Attacks, and data mining and expert based

2.1 Similarities of Alert Attributes

This approach focuses on improving the quality of alerts reduction by comparing an alert to all alert threads that have similar attributes or features (such as Source IP address, source port number, destination IP address, destination port number, and time stamps). A correlation score is calculated between these alerts and then correlates alerts with a high degree of feature similarity if match or a new thread is created if none is match depending on the score. This method is simple and easy to implement, but is unable to detect complex attacks due to its reliance only on expert knowledge to determine the similarity degree between attack classes (Karunasekera at el, 2010, rahayu at el , 2008). In addition, it fails to discover the causal connection between alerts when alerts with different attributes have been induced in a single attack. In this case, not all the attacks can be detected.

Collection mechanism and reduction of IDS alert framework (CMRAF) (Al-Saedi at el, 2012) was proposed to remove the duplicates IDS alerts and reduce the number of false alerts. They use information gain ratio algorithms to extract the similarities between set of alerts and provide the highest weight to the most effective features based on the class of alerts belonging to the algorithm.

Alert correlation using a novel clustering approach, (Mohamed et al. 2012), applied an incremental clustering approach to reduce the amount of alerts generated by IDS. Three attributes, destination IO, signature-id, and timestamp had been extracted and hashed by using MD5. The hash value from the next input tuple is checked against hash value of the existing clusters. The hashing technique is used to speed up the comparison in checking the similarities of alert attributes.

An improved framework for intrusion alert correlation, (Elshoush at el, 2012), divided alert correlation into 10 main components and contained them in the Data Normalization Unit, Filter-based Correlation Unit and Data Reduction Unit. Similar alerts are fused based on seven extracted features, namely EventID, timesec, SrcIPAddress, DestPort, DestIPAddress, OrigEventName, and SrcPort in order to remove duplicate alerts created by the independent detection of the same attack by different sensors.

Valdes et al. (2008), proposed a probabilistic-based approach to correlate and aggregate security alerts by measuring and evaluating the similarities of alert attributes. They use a similarity metric to fuse alerts into meta-alerts to provide a higher-level view of the security state of the system. Alert aggregation and scenario construction are conducted by enhancing or relaxing the similarity requirements in some attribute fields. But similarity calculations the only way for them to aggregate the alerts. They have to compare all the alert pairs and have to determine lot of thresholds with expert knowledge which lead to their huge volume of computing workload.

2.2 Predefined Attack Scenario

This technique utilizes the fact that intrusions often require several actions to take place in order to succeed. Every attack scenario has corresponding steps required for the successfulness of the attack. Low- level alerts from IDS are compared against the pre-defined attack scenario before the alerts can be correlated. It is restricted to known attack and misuse detection only and specified by human users or learned through training datasets.

The main advantage for this method is that it is able to accurately detect well-documented attacks derived from the libraries. But if it is a novel attack, the method will fail to detect the intrusion (Osman at el, 2010, Alsaidi, at el 2012, Benferhat at el, 2012) Limitations of this approach are the need of more complete and comprehensive scenario libraries; time and cost to build and maintain them are the main concerns. In-depth knowledge on various attack scenarios is required to manually define the attack conditions. Thus, it may not be practical for complex and large-scale networks.

An alert fusion model inspired by artificial immune system, (Mahboubian at el, .2012) which is an aggregating method inspired by Danger Theory to aggregate the generated alerts based on the prediction of attack scenarios. They categorized network attacks into three general groups which are One-to-One, Many-to-One, and One-to-Many. Each alert will be grouped and a priority value will be given. Then each group is checked with predefined rules for the possibility of raising the danger alarm by using the Danger Theory.

Automatic attack scenario discovering based on a new alert correlation method (Ebrahimi at el, 2012) introduced a method to automatically extract multi-step attack scenarios. They arrived alert had been determined as to which alerts scenario it belongs to and inserted in an alert tree. Sub scenarios in each scenario and meta-alerts are extracted. Finally, the multi-step attack graph is constructed for each attack scenario from the produced meta-alerts.

A novel algorithm for the alert correlation generated by signature-based network IDS (NIDS) had been presented by (Marchetti at el, 2012). The proposed algorithm called pseudo Bayesian alert correlation is based on Bayes's theorem of conditional probability. This algorithm aims to identify and highlight groups of intrusion alerts based on their detection time and on the past alert history generated by same NIDS. In this case, the previous alert history was analysed periodically while recent intrusion alerts are received from the NIDS and analysed as soon as they are generated.

2.3 Prerequisites and Consequences of Attacks

Most attacks today are not isolated but related to each other as different stages of attack sequences with the earlier attacks paving way for consequent attacks. In order to ensure the attack is successful, the prerequisite of an attack is the necessary condition (Ning at el, 2004). In this approach, a set of detailed criteria is used to learn the causal relationship between alerts and the weights of such relations. The main benefit to network analysts when using this method is that they do not have to specify all the possible scenarios but they are still able to detect unknown attacks. Nonetheless, it is expensive (in terms of human expertise) to build a complete attack database which consists of every attack action with its pre- and post-conditions (Karunasekera at el, 2010, fatma at el, 2013). Similar to predefined attack scenario approach discussed in

the previous section, this approach may not be practical in production networks due to the complexity of the design and user behaviour.

Bayesian network-based alert correlation, (Anbarestani at el, 2012) discovers attack strategies without the need for expert knowledge. The approach extracted attack scenarios using classification by taking into account the sequence of actions. It then leverages upon historical data from log sources and classifies them based on observed intrusion objective as class variables. The possible attack scenarios constructed from hyper alerts sequences are examined and the most plausible strategies for constructing a cooperative attack are extracted.

Zhaowen at el (2010), used an on-line prerequisite-consequence-based correlation method to analyze and discover attack scenario behind alerts. The assumption here states that the component attacks are usually not isolated, but related to different stages of the attacks, with the early ones preparing for the later ones. They introduce the notion of hyper alerts to represent the prerequisite and the consequence of each type of alert by using logical predicates. Each hyper-alert is a tuple (fact, prerequisite, consequence), where fact is the set of alerts attribute's names, and prerequisite and consequence are two different sets, each one consisting of a logical combination of predicates expressed as mathematical conditions on the variables contained in the set fact. The model employs distributed agents to collect alert information online and adopts prerequisite-consequence correlation method to analyse and discover attack scenario and intent intrusion behind the alerts.

An alert correlation method, based on causal approach, had also been proposed by (Zali at el, 2012). In this method, the knowledge base of attack patterns is represented as a graph model called causal relations graph. Some trees related to alerts probable correlations are constructed offline while the correlations of each received alert in real time with previously received alerts will be identified by performing a search only in the corresponding tree.

Alserhani at el (2010), developed a rule based correlation language MARS, a Multi-stage Attack Recognition System which is based on prerequisite-consequence-based correlation method to analyze and discover attack scenario behind alert. Unlike others, they add another two parameters for modeling attack consequences, i.e., vulnerability and extensional consequences. MARS is mainly based on the phenomena of cause and effect. It has two main components: online and offline. The main purpose of the online component is to receive raw alerts and generates hyper-alerts. Then, multi-stage attack recognition is applied to correlate hyper-alerts based on rules provided by the offline component

Ning et al. (2004), proposed alert correlation model based on prerequisites and consequences of individual detected alerts. A knowledge database "Hyper-alert Type Dictionary" contains rules that describe the conditions where prior behaviors prepare for later ones. Attack strategy is represented as a Directed Attack Graph (DAG) with constraints on the attack attributes considering the temporal order of the occurring alerts. The nodes of the DAG represent attacks and the edges represent causal and temporal relations. Similarities between these strategies are measured to reduce the redundancy. A technique of hypothesizing and reasoning about missing attacks by IDS is presented to predict attribute values of such attacks. The significance of their work is the reduction of the huge number of security incidents and to report a high-level view for the administrator. However, the proposed system is useful as a forensic tool where it perform offline analysis. In addition, building the knowledge database containing rules of the applied conditions is a burdensome wang at el (2008). However, authors have not provided a mechanism to build the Hyper Alert dictionary. Also, the generated graph is huge even with.

2.4 Expert System and Data Mining

Data mining is a process of discovering significant and potentially useful patterns especially in a large volume of data. Correlation mining is much effective because of the large number of correlation relationships among various kinds of suspicious alerts (karim at el, 2013). This method employs data mining algorithms on training data-set and using knowledge-base derived from human experts to identify attack scenarios on intrusion patterns and relationships among alerts. In this approach, statistical analysis of alerts can be done by identifying the co-occurrence of alerts within a predefined time window. Some relation rules or patterns will be created from correlation relationships that satisfy some statistical criteria. This involves pair-wise comparison between alerts since every two alerts might be similar and therefore can be correlated (Sadoddin at el, 2009). In this case, the repeated comparisons between alerts will lead to a very huge computational overload especially in largescale networks. Besides this, this approach requires a lengthy initial period of training (Mahboubian at el 2013).

A self-regulated alert correlation model had been proposed by (Yang at el, 2010). This model incorporated advantages of the associated component-based approach and alert information correlation based on preconditions. The model introduced data mining techniques in alert correlation and made improvements on alert correlation using improved Apriori algorithm.

In general, the Apriori algorithm states that any super-pattern of a non-frequent pattern is also not frequent (Zerin at el, 2011). In this proposed algorithm, it divided the alert information into several disjoint subsets with destination IP as a unit and then mined them separately before associating the correlation rules set for generating the results correlation rules set.

Alert correlation technique to automatically extract attack strategies from a large volume of intrusion alerts without specific prior knowledge about these alerts was proposed by (Zhu at el, 2007). The proposed approach is based on two different neural network approaches, which are multilayer perceptron (MLP) and support vector machine (SVM) to estimate the alert correlation probability by storing correlation strengths of any two types of alerts in an alert correlation matrix (ACM). For pattern recognition, SVM is a recommended classifier with its better performance (Phinyomark at el, 2011).

An algorithm to mine attack behaviour patterns from a large number of intrusion alerts without prior knowledge of

the attacks was proposed by (Kavousi at el, 2012). The proposed engine has two components. The first, an offline component that periodically learns multi-step attack behaviour patterns from historical alerts using a Bayesian causality analysis and the second is an online component that correlates alerts in real time using a hierarchical method and based on the attack behaviour patterns extracted by the offline component.

Zhitang at el (2008), employed different data mining algorithms for real-time correlation to discover multi-stage attacks. Off-line attack graph is constructed using manual or automatic knowledge acquisition and then attack scenarios are recognized by correlating the collected alerts in real-time. The incoming step of an attack can be predicted after detection of few steps of attack in progress. The association rule mining algorithm is used to generate the attack graph from different attack classes based on historical data. "Candidate attack sequences" are determined using a sliding window.

In Zhang, et al (2007), AprioriAll algorithm which is a sequential pattern matching technique is used to generate correlation rules based on temporal and content constraints. The work adopted a classical sequential mining method GSP to find the maximal alerts sequence and then to discover the attack strategy. The limitation of their work is the use of only attack class and temporal as features.

Cuppens et al. (2002), Proposed MIRADOR correlation approach for alert clustering, merging and then correlation. Explicit correlation of events based on security experts is used to express the logical or topologic links between events. Attack is specified using five fields and based on the language of LAMBDA. Partial matching techniques are adopted to build the model. In addition to explicit correlation, implicit correlation is used to overcome possibly missing events.

Qin at el (2005), proposed a combination of statistical and knowledgebase correlation techniques. Three algorithms are integrated based on assumption that some attack stages have statistical and temporal relations even though direct reasoning link is not existent. Bayesian-based correlation engine is used to identify the direct relations among alerts based on prior knowledge. In contrast to previous approaches, knowledge of attack steps incorporates as a constraint to probabilistic inference to avoid the exact matching of pre and post conditions. Causal Discovery Theory-based engine is developed to discover the statistical of one-way dependence among alerts. In addition, Granger Causality-based algorithm is used by applying statistical and temporal correlation, to identify mutual dependency. However, the problem of selection time window for temporal correlation is still an open problem. Attackers can exploit the slow-and low attack to avoid detection. Attack reduction also relies on prior knowledge where zero-day attack is not detected and also the analysis of results may result to huge computing work load Wang at el (2008).

3.0 DISCUSSION AND ANALYSIS OF ALERT CORRELATION TECHNIQUE

3.1 Comparison of Alert Correlation Techniques

All the discussed techniques have their advantages and disadvantageous as summarized in Table 1 below

Table 1: comparison of alert correlation techniques

Technique	Advantages	Disadvantages
Similarities of Alert Attributes technique	Can reduce large number of redundant alert generated by multiple sensors.	-Suitable for known alerts. -Not able to discover causality of alerts and statistical relationships. -Limited to discover complicated attacks.
Predefined Attack Scenario	is able to accurately detect well-documented attacks Can reduce large number of redundant alert generated by multiple sensors	Could generate large number of false positive alarm • it requires that users specify attack scenarios manually • It is limited to detection of known attacks or misuse detection and not anomaly detection. • multi-step attack alert is disregarded intrusion (Osman at el, 2010, Alsaidi, at el 2012, Benferhat at el, 2012)
Prerequisites and Consequences of Attacks	Multi-step attack can be detected to provide a high-level view of the attack associated with a security compromise • can generate useful graph to determine the attacker's objective	The approach may not be practical in production networks due to the complexity of the design and user behavior It is expensive to build a complete attack database which consists of every attack action with its pre- and post-conditions (Karunasekera at el, 2010, fatma at el, 2013).

data mining and Expert system	Does not need pre-defined knowledge about attack scenarios. • Using anomaly detection technique • new attack scenarios can be identified • can be used as pre-process alerts or meta-alert signatures.	a very huge computational overload especially in large scale networks This approach requires a lengthy initial period of training (Mahboubian at el 2013).
Hybrid technique	Performs multiple types of correlations (structure, cause & statistical) No predefined rules Recognize known and unseen alerts No manual parameters settings	May lead to complex architecture (Maheyzah at el 2015)

3.2 Proposed Design Consideration for Alert Correlation Technique

From the discussed alert correlation techniques, we have identified the significant issues within each technique which can be solved to improve the effectiveness of NIDS performance. Among the issues include alert Normalization and aggregation, alert correlation architecture, false alerts, alert prioritization, attack prediction, test data and the visualization techniques applied. This section briefly examines each issue and proposes a solution to fix it.

Table 2: Issues analysed in NIDS

Design consideration	Description	Proposed solution
Alert normalization	the majority of organizations implement different types of NIDSs (heterogeneous NIDSs), accordingly they produce alerts in different data format ((Maheyzah at el 2015, Rahayu at el, 2009)	Convert different alert data formats from multiple intrusion sensors into a standard format to be appropriate and acceptable by the other correlation components.
Attack scenario construction (study behavior of the attacker)	Attacks are likely to generate multiple related alerts. Current IDS do not make it easy for security officers to logically group related alerts (wang at el 2006; Xiao at el 2010)	To group or cluster alert which has a related event or event threaded. 2. classify the alerts into the corresponding cause effect paradigm
Alert correlation architecture (To solve problem of alert flooding)	IDS are prone to alert flooding as they provide a large number of alerts to the security officer, who then has the difficulties coping with the load (Bin at el, 2006,Rahayu at el, 2009)	To reduce number of alert generated from IDS and improve the alert correlation performance in terms of the processing time and quality of alerts by adopting alert filtration and alert aggregation
False Alert	Existing IDS are likely to generate false positives or false negatives alert (Rahayu at el, 2009)	To reduce number of false alerts through filtering 2. To identify known attack using misuse detection 3. To identify unknown attack using anomaly detection
Alert Severity/Prioritization	Not all generated alerts are equally important (Ghorbani at el2010; Maheyzah at el 2015, Alsubhi at el, 2008)	need to separate important alerts from the rest and calculate scoring and prioritizing alerts
Attack Prediction/ execution mode	Technologies are not effective in predicting the future attacks. (Maheyzah at el 2015; Wang at el, 2009; Rahayu at el 2008)	A proactive approach is to anticipate and conduct possible attacks to prevent damage
Test Data	The effectiveness of a component depends heavily on the nature of the data-set analysed to evaluate the system.	latest attack scenario data-sets to include IPv6 attack to ensure its efficiency and effectiveness in producing a good and quality output

Table 3: A summary of related works with design considerations

	Correlation application				Execution mode		Attack scenario		Correlation architecture		Test data set			
Alert correlation technique	Similarities	Predefined	Prerequisite	Expert system and data	Online	offline	Single	Multistage	Centralized	Distributed	selected	Darpa1999	Darpa2000	IPv4 or IPv6
Alserhania at el [2008]		✓	✓	✓		✓		✓	✓		✓		✓	
Bateni at el.[2013]		✓	✓	✓		✓		✓	✓		✓		✓	IPv4
Al-Saedi At el.[2012]	✓	✓	✓			✓	✓		✓			✓		IPv4
Mohamed at el.[2012]	✓				✓		✓			✓				IPv4
Osman at el[2012]	✓		✓			✓		✓	✓		✓		✓	
Anbarestani at el[2012].			✓	✓		✓		✓	✓				✓	
Zhaowen at el[2010]			✓		✓			✓		✓				IPV6
Zali at el[2012]			✓		✓			✓		✓			✓	
Kavousi at el [2012]				✓	✓			✓		✓			✓	IPv4
Mahboubian at el[2012]	✓	✓			✓			✓	✓				✓	IPv4
Amiri at el[2011].				✓		✓		✓		✓				
Ebrahimi at el [2011]		✓				✓		✓	✓				✓	
Marchetti at el [2011]		✓		✓		✓		✓	✓					IPv4
Taha at el[2010]		✓		✓		✓		✓		✓	✓		✓	IPv4
Tabia at el [2010]		✓		✓		✓		✓	✓					IPv4
Yang at el [2010]		✓	✓			✓		✓	✓		✓			IPv4
Tian at el [2009]	✓		✓			✓		✓		✓	✓		✓	
Huang at el[2010]		✓		✓				✓	✓				✓	IPv4
Ahmadinejad at el [2009]	✓					✓		✓	✓				✓	IPv4
Valdes at el [2008]	✓					✓		✓	✓				✓	
Ning at el [2004]	✓					✓		✓	✓				✓	
Zhitang at el [2008]	✓					✓		✓	✓				✓	
Zhang	✓					✓		✓	✓				✓	
Wang at el 92008)	✓					✓		✓	✓				✓	

An efficient correlation system should achieve the following objectives

i. Alert normalization to convert different alert data formats into a standard format
ii. Reducing and eliminating redundant of intrusion alerts
iii. Ability to discover complete attacker strategy with known and unknown attack
iv. A unified hybrid architecture that leverages capabilities of the various correlation techniques
v. Filtering and prioritizing intrusion alerts to improve the quality of alerts.
vi. A proactive approach to predict the next attacker action in real time
vii. graphical based approach for analysis and presenting alerts
viii. Take different types of dataset to measure components effectiveness

4. CONCLUSION

Several techniques of alert correlation have been proposed to help identify and discover the relationships amongst alerts from multiple sources. However, most of these techniques suffers from complex correlation rules definition, they have limited capabilities to discover new and complicated attack, depends on human expert's knowledge to update the correlation knowledge as well as they do not provide a proactive action when attack activities are going on. As a result researchers have begun to look for a hybrid approach that leverages capabilities of the various correlation techniques

Future work should be based on scalable, structured and computationally techniques which do not require prior knowledge, not dependable on security expert to frequently update rules and are able to detect known and unknown attacks. Additionally, as the Internet enters a new era and domain such as mobility and Internet of Things and its ever-growing user's base, a more flexible and intelligent intrusion alert which is able to detect and predict the incoming alerts at sensor level and in real time is desired to complement IDSs to secure information systems, networks and sensitive data

5. REFERENCES

1. Alserhani, F., Akhlaq M., Awan I.U., Cullen A.J., Mirchandani P., (2010). "MARS: Multi-stage Attack Recognition System", 24th IEEE International Conference on Advanced Information Networking and Applications (AINA)
2. Zhaowen Lin, Shan Li and Yan Ma,(2010). "Real-Time Intrusion Alert Correlation System Based on Prerequisites and Consequence", 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)
3. Zhi-tang Li, Jie Lei, Li Wang, Dong Li, 2007,"A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction," Fuzzy Systems and Knowledge Discovery, Fourth International Conference on, vol. 4, pp. 307-311, Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007) Vol.4
4. Ai-fang Zhang, Zhi-tang Li, Dong Li, Li Wang, 2007"Discovering Novel Multistage Attack Patterns in Alert Streams," Networking, Architecture, and Storage International Conference on Networking, Architecture, and Storage (NAS 2007)
5. Jie Ma, Zhi-tang Li, Wei-ming Li, 2008."Real-Time Alert Stream Clustering and Correlation for Discovering Attack Strategies," Fuzzy Systems and Knowledge Discovery, Fourth International Conference on, vol. 4, pp. 379-384, 2008 Fifth International Conference on Fuzzy Systems and Knowledge Discovery,
6. PengNing, Yun Cui, Douglas S. Reeves, 2002"Constructing Attack Scenarios through Correlation of Intrusion Alerts," in Proceedings of the 9th ACM Conference on Computer & Communications Security, pages 245--254, Washington D.C.
7. P. Ning, D. Xu, C. Healey, R. St. Amant,2004 "Building Attack Scenarios through Integration of Complementary Alert Correlation Methods," in Proceedings of the 11th Annual Network and Distributed System Security Symposium
8. X. Qin. 2005A Probabilistic-Based Framework for INFOSEC Alert Correlation. PhD thesis, Georgia Institute of Technology
9. X. Qin and W. Lee2004. Attack plan recognition and prediction using causal networks. In ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), pages 370-379, Washington, DC, USA,. IEEE Computer Society.
10. W.Wang, T.E.Daniels,(2008). A graph based approach toward network forensics analysis, ACM Transactions on Information and Systems Security
11. Li Wang, Ali Ghorbani, and Yao Li Automatic Multi-step Attack Pattern Discovering,International Journal of Network Security, Vol.10, No.2, PP.142{152, Mar. 2010
12. Siti Rahayu Selamat, R. S. (2008). Mapping Process of Digital Forensic Investigation Model. *IJCSNS International Journal of Computer Science and Network Security* , Vol. 8(No. 10): p. 163-169.
13. Alharbi, S. e. (2011). The Proactive and Reactive Digital Forensics Investigation ProcessInternational Journal of Security and Its Applications Vol. 5 No. 4, October, 2011
14. pandaLabs, Annual Report Panda Security's AntiMalwa re Laboratory 2009. 2010, Panda Security
15. Siti Rahayu Selamat, Shahrin SahibA Forensic Traceability Index in Digital Forensic Investigation ,Journal of Information Security, 2013, 4, 19-32
16. Ricci S.C, I. F. (2006). Digital forensics investigation model that incorporate legal issues. *Digital Investigation* , 29-36
17. S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," in 2nd International Conference on i-Warfare and Security, 2007, p. 77.
18. Sebastian Roschke, Feng Cheng, and ChristophMeinel (2011), A New Alert Correlation Algorithm Based on Attack Graph, In Proceedings of the 4th International

Conference on Computational Intelligence in Security for Information Systems (CISIS 2011), Torremolinos,
19. Wang, L., Liu, A., Jajodia, S (2006): Using attack graphs for correlation, hypothesizing, and predicting intrusion alerts. Journal of Computer Communications
20. FatmahBahareth, OmaimaBamasak, 2013, Constructing Attack Scenario using Sequential Pattern Mining with Correlated Candidate Sequences. The Research Bulletin of Jordan ACM,
21. C. V. Zhou, C. Leckie, and S. Karunasekera. 2010,"A survey of coordinated attacks and collaborative intrusion detection,"Comput. Secur., Vol. 29, no. 1, pp. 12440,
22. RobiahYusof, ,SitiRahayuSelamat, Shahrin Sahib 2008, Intrusion Alert Correlation Technique Analysis for Heterogeneous Log, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9K. H. Al-Saedi, S. Ramadass, A. Almomani, S. Manickam, and W. A. A. Alsalihy, 2012, collection mechanism and reduction of IDS alert, International journal for Compututer Application., Vol. 58, no. 4
23. A. B. Mohamed, N. B. Idris, and B. Shanmugum, 2012, Alert correlation using a novel clustering approach, in International Conference on Communication Systems and Network Technologies (CSNT), Gujarat, India, May 1113, pp. 7205.
24. H TagelsirElshoush, Izzeldin Mohamed Osman, 2012,An improved framework for intrusion alert correlation, in The World Congress on Engineering, London, UK, Jul. 46, pp. 51823
25. TagelsirElshoush, Izzeldin Mohamed Osman, 2011, Alert correlation in collaborative intelligent intrusion detection systems—a survey, *Applied Soft Computing*, Vol. 11, 7, pp. 434965
26. A. Ebrahimi, A. Z. H. Navin, M. K. Mirnia, H. Bahrbegi, and A. A. A. Ahrabi, 2011, Automatic attack scenario discovering based on a new alert correlation method, in IEEE International Systems Conference M. Marchetti, M. Colajanni, and F. Manganiello, 2011, Identification of correlated network intrusion alerts, in Third International Workshop on Cyberspace Safety and Security (CSS), Milan, Italy, pp. 1520.
27. P. Ning, Y. Cui, D. S. Reeves, and D. Xu,2004, .Techniques and tools for analyzing intrusion alerts, ACM Trans. Inf. Syst. Secur. (TISSEC), Vol. 7, no. 2, pp. 274318
28. Z. Zali, M. R. Hashemi, and H. Saidi, 2012,"Real-time attack scenario detection via intrusion detection alert correlation,"in 9th International ISC Conference on Information Security and Cryptology (ISCISC), Tarbiz, Iran, Sep. 1314, , pp. 95102
29. M. Karim, C. F. Ahmed, B. S. Jeong, and H. J. Choi, 2013, "An efficient distributed programming model for mining useful patterns in big datasets," IETE Tech. Rev., Vol. 30, no. 1, pp. 5363
30. Reza. Sadoddin, and A. A. Ghorbani,"An incremental frequent structure mining framework for real-time alert correlation," Comput. Secur., Vol. 28, no. 3, pp. 15373, May 2009
31. M. Mahboubian, N. I. Udzir, S. Subramaniam, and N. A. W. A. Hamid, 2012An alert fusion model inspired by artificial immune system, in International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia
32. L. Yang, and D. Xinfa, 2010.Alert correlation model design based on self-regulate, in Second International Conference on Multimedia and Information Technology (MMIT), Kaifeng, China,
33. S. F. Zerin, and B. S. Jeong 2011, A fast contiguous sequential pattern mining technique in DNA data sequences using position information, IETE Tech.
34. Bin Zhu and Ali A. Ghorbani, 2006 Alert Correlation for Extracting Attack Strategies, International Journal of Network Security, Vol.3, No.3, PP.244–258,
35. A. Phinyomark, P. Phukpattaranont, and C. Limsakul2011,"A review of control methods for electric power wheelchairs based on electromyography signals with special emphasis on pattern recognition,"IETE Tech. Rev., Vol. 28, no. 4
36. F. Kavousi, and B. Akbari, 2012Automatic learning of attack behavior patterns using Bayesian networks, in Sixth International Symposium on Telecommunications (IST), Tehran, Iran
37. C. J. Huang, C. F. Lin, C. Y. Li, J. J. Liao, Y. W. Wang, and K. W. Hu, 2010An adaptive rule-based intrusion alert correlation detection method, in First International Conference on Networking and Distributed Computing (ICNDC), Hangzhou, China
38. B. Abdulrazak, and Y. Malik, 2013Review of challenges, requirements, and approaches of pervasive computing system evaluation, IETE Tech .Rev., Vol. 29
39. ShameliSendi A, Dagenais M, Jabbarifar M, Couture M. 2012Real time intrusion prediction based on optimized alerts with Hidden Markov model. Journal of Networks.
40. Alsubhi K, Al-Shaer E, Boutaba R., 2008, Alert prioritization in intrusion detection systems. Proceedings of IEEE Network Operations and Management Symposium. NOMS.
41. Ghorbani AA, Lu W, Tavallaee M.,2010, Alert management and correlation. Journal of Network Intrusion Detection and Prevention..
42. Ning P, Cui Y, Reeves DS, Xu D. 2004Techniques and tools for analyzing intrusion alerts. ACM Transactions on Information and System Security (TISSEC)..
43. Bateni M, Baraani A, Ghorbani, 2012,A. Alert correlation using artificial immune recognition system. International Journal of Bio-Inspired Computation..
44. Xiao F, Jin S, Li X. 2010, A novel data mining-based method for alert reduction and analysis. Journal of Networks..
45. MaheyzahMdSiraj, Hashim Hussein TahaAlbasheer and Mazura Mat Din,2015,Towards Predictive Real-time Multi-sensors Intrusion Alert Correlation Framework Indian Journal of Science and Technology, Vol 8(12)