A Cyber-Threat Intelligence Framework for Improved Internet Facilitated Organized Crime Threat Management

Oluwafemi Oriola
[#] *Ph.D. (InfoSec), Department of Computer Science, Adekunle Ajasin University, Akungba Akoko, Nigeria*

Abstract

Internet Facilitated Organized Crime Threats are internet aided forms of cyber-crime activities that target citizens and organizations in large scale. They have been commonly propagated through botnets and worms. At times, they exhibit as advanced persistent threats. Presently, different models have been developed for assessing the threats with the aim of combating the trends. However, such models are deficient in the technological intelligence needed for managing the threats cost-effectively and cost-efficiently. This paper thus reviews the state-of-the-arts in Cyber-Threat Intelligence with focus on Threat Management. The paper identifies the strengths and limitations of the works and proposes a Cyber-Threat Intelligence framework that maintains the strengths in the existing models and addresses the limitations for improved Internet-facilitate Organized Crime Threat Management.

Keywords

Internet-facilitated Organized Crime Threats, Cyber-Threat Intelligence, Incident, Information Sharing, Information Analysis

I. INTRODUCTION

Internet is one of the greatest innovations that has benefitted human race since the nineteenth century. It has eliminated the boundary among groups in the societies. Now, it can be accessed everywhere via web, phones or cloud. In particular, hackers have been using internet media to access unauthorised resources on the internet. A hacker or attacker could steal confidential information or commit financial fraud through the internet. Some of the methods employed include phishing, masquerading, spoofing and crypto-analysis.

Apart from the individual usefulness of internet in causing harms to resources online, groups of users do benefit from it. Some Attackers collaborate and cooperate via internet to exploit the vulnerability of victim systems and cause damage in Organised manner.

According to Global Agenda Council on Organised Crime Report for 2011/2012 in [1] and Internet Organised Crime Threat Assessment Release for 2014 in [2], these kinds of threats are referred to as Internet-facilitated Organised Crime Threats and they make use of three common methods in achieving their missions: Botnet, Worm Propagation and Advanced Persistent Threats (APT).

Botnet otherwise known as zombies are set of interconnected computers that could attack a single host or multiple hosts [3]. They may be Organized as Server-Client or Peer-to-Peer computers. Each of the computers is known as bots and nowadays, distributed hosts are being taken over as slaves without authorization by master remotely in order to improve complexity and sophistication of their exploits. The Worm is a malicious program that could replicate itself to damage other useful programs in single host, different hosts or multiple networks with various manifestations [4]. Initially, APT was used to describe nation-states stealing of data or damage to other nation-states for strategic gain. But the definition has now been expanded by security vendors and media to include similar attacks carried out by cybercriminals stealing data from businesses for profit [5]. It is 'Advanced' because it is targeted and sophisticated and 'Persistent' because it usually continues over some period until the aim is achieved.

The emergence of these Internet-facilitated Organised Crime Threats has increased the violation of network security policies, disruption of assets' services and loss of assets. Symantec [6, 7] reported that majority of these threats are discovered in large organisations. [7], only thirty one per cent (31%) of the Internet Threats were targeted at organisations with less than two hundred and fifty personnel in 2012. It was also reported that a single Threat was discovered in 2011 to have infected six hundred thousand (600,000) mac machines in 2012. Arbor Networks [8] reported that *distributed denial of service* (DDoS) caused by Bots was the most perpetrated between the period of

October 2010 and September 2011. Kaspersky [9] identified about fifteen million unique samples of malware specimens in 2009, which means that one unknown sample was discovered roughly every two seconds. This high level of occurrence and distribution might be attributed to Internet-facilitated Organised Crime Threats. In the reports by Symantec [7], the insurgence and sophistication of these threats have also been justified. It was reported that as at 16th March 2011, approximately 88.2 per cent of all spam was distributed by spam-sending botnets. Also Worms (including viruses) were accounted for more than 70 per cent of the malicious codes discovered in 2012. In recent years, perpetrations of Advanced Persistent Threats have continued to increase. For example, Malwares such as Stuxnet, Duqu, and Flamer & Disttrack in 2010, 2011 and 2012 respectively have persistently showed high levels of sophistication and danger.

As Internet connectivity continues to spread in the world, citizens and organizations will be subjected both to a larger volume of cyber attacks, and to attacks from previously under-connected areas of the world. Combating cybercrime will therefore require strategic and operational partnerships. Centralized coordination of intelligence gathering, analysis, training, and partnership management is a way to actualize this.

II. CYBER-THREAT INTELLIGENCE

Cyber-Threat Intelligence is defined as "knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise." [10].

It is threat intelligence related to computers, networks and information technology. Intelligence is, "the information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding, is the product that provides battlespace awareness" [11]. Clark [12] described intelligence as being actionable information. Additionally, cyber threat intelligence can be strategic or tactical. Strategic intelligence includes things like motivation of adversaries. Tactical intelligence includes things like 'tactics, techniques and procedures (TTP)' and 'indicators of compromise (IOCs)'. IOCs are one of the most easily actionable types of CTI and are often the focus standards and tools. Some of the most commonly used IOCs are IP addresses, domain names, uniform resource locators (URLs) and file hashes. The Intelligence is formed from the fusion of information from collaborative partners. It provides both insight and foresight to the end user based on the degree of understanding of complex situations by consideration of the provenance, pedigree and context of the source material, the processing methods and the documents that verify the findings [13]. Thus, Cyber-Threat Intelligence will involve incident information sharing and analysis and decision making.

III. INCIDENT INFORMATION SHARING

Many Incident Information Sharing Standards exist.

A. Incident Information Sharing-based on Collection Strategy.

This includes:

1) ***Internal Collection Strategies****:* The internal threat category encompasses any Cyber-Threat Intelligence that is collected from within the organization. This can include reported information from security tools such as firewalls, intrusion prevention systems (IPS) and host security systems like anti-virus. A valuable source of threat intelligence information comes from computer forensic analysis. The analysis can yield intelligence that is not readily visible and may be very useful in detection of other attacks.

2) ***Community Collection Strategies****:* The community category includes any Cyber-Threat Intelligence shared via a trusted relationship among multiple members with a shared interest. This can be an informal group with member organisations that are in the same industry sector or that have other common interests. There are formal community groups such as the Information Sharing and Analysis Centres (ISACs) Organised under the National Council of ISACs [14]. ISACs are formed for specific sectors such as higher education or financial services. There are over a dozen ISACs under the National Council of ISACs. One example of a community sharing group is Research and Education Networking (REN) ISAC. REN-ISAC is a trusted community for research and higher education. They are the main organization behind the Collective Intelligence Framework. Another example of a community group is the Defense Industrial Base Collaborative Information Sharing Environment (DCSIE). This group provides a hub for CTI sharing between U.S. government defense contractors.

3) ***External Collection Strategies****:* The external category includes CTI from sources outside an organization and not part of a community group. There are two types of external sources. The first is public sources. Public sources are available to anyone and

generally there is no cost associated with access. While public feeds can be available at no cost, there can be problems. Amoroso points out data quality problem with volunteered data [15]. An example of a public Cyber-Threat Intelligence feeds is MalwareDomains [16]. MalwareDomains provides a list of domains known to be involved in malicious activity. The lists are available in multiple formats and can be used to block access to the malicious domains.

The other type of an external Cyber-Threat Intelligence source is private. Private sources are typically only available on a paid basis. An organization can subscribe to a threat feed from a vendor to receive regularly updated Cyber Threat Intelligence. These feeds have the advantage in that there may be a service level agreement on data quality. Many security products include some type of cyber threat intelligence update mechanism. CTI services can also be purchased separately. One example is the Emerging Threats ETPro Ruleset [17]. Emerging threats offers subscription services for IDS rules and IP reputation.

B. Incident Information Sharing based on Exchange standard.

In the review, [18] Indicators are used.

- Information Leakage: This has to do with the ability of CTI tool and standard to manage of integrity and privacy of information.
- Interoperability: This has to do with the ability of CTI tool and standard to provide rich semantics that support both human and machine parsing.
- Validation of Information Quality and Reliability: This concerns the ability of CTI tool and standard to provide quality and trustworthy information.

1) Incident Object Description Exchange Format, RFC **[19]**

The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.

An attribute is defined as an enumerated value with a default value of "private". In other classes where this attribute is used, no default is specified. The indicators are Public (there are no restrictions placed in the information); Need-to-Know (the information may be shared with other parties that are involved in the incident as determined by the recipient of this document); Private(the information may not be shared); and Default (the information can be shared according to an information disclosure policy pre-arranged by the communicating parties).

2) IODEF for Structured Cyber Security Information, RFC 7203 **[20]**

IODEF for Structured Cyber Security Information" (IODEF-SCI) is an extension to the IODEF standard that supports additional data. It is a standard proposed by the MILE working group [20]. The additional information includes: attack pattern, platform information, vulnerability, weakness, countermeasure instruction, computer Incident log, and severity. IODEF-SCI supports the additional data by embedding existing standards within the IODEF document. The following standards are also included in IODEF-SCI: Common Attack Pattern Enumeration and Classification (CAPEC), Common Incident Expression (CEE), Common Platform Enumeration (CPE), Common Vulnerability and Exposures (CVE), Common Vulnerability Reporting Format (CVRF), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), Open Checklist Interactive Language (OCIL), Open Vulnerability and Assessment Language (OVAL), Extensible Configuration Checklist Description Format (XCCDF), Distributed Audit Service (XDAS) and ISO/IEC 19770.

3) Real-time Inter-network Defense (RID), RFC **[21]**

Real-time Inter-network Defense (RID) outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident-handling solution. Combining these capabilities in a communication system provides a way to achieve higher security levels on networks. Policy guidelines for handling incidents are recommended and can be agreed upon by a consortium using the security recommendations and considerations. RID functions via five message types: Request, Acknowledgement, Result, Report and Query. The RID standard includes a Policy Class which would allow different policies to be applied based on the relationship with the sharing parties. Some of the relationships considered are Client-to-SP (Service Provider), SP-to-Client, Intra-Consortium, Peer-to-Peer and Between-Consortiums. This flexibility would allow for direct organisation to organisation sharing via the Peer-to-Peer relationship

or within a community using the Intra-Consortium relationship. The problems with the standard are that some of the default information may disclose certain level of privacy; it does not provide mechanism for ensuring trust among the exchange partners and caters for additional security risk-related information that could ensure quality.

1) MITRE Standards: CybOX, STIX, TAXII [22]

MITRE developed three standards that each fills different needs for a Cyber Threat Intelligence. The first is Cyber Observable eXpression (CybOX), which provides a standard for defining indicator details known as observables. The second is Structured threat Information Expression (STIX) which provides a standard to define patterns of observables in context. The third is Trusted Automated eXchange of Indicator Information (TAXII) which provides a standard to exchange Cyber Threat Intelligence. It has been adopted as a planned standard by Microsoft as part of its 'Microsoft Active Protections Program' (MAPP) [23]. TAXII is also in use by Financial Services Information Sharing Analysis Centre (FS-ISAC) [24]. This standard defines eight extension classes, namely Attack Pattern, Platform, Vulnerability, Scoring, Weakness, Incident Report, Verification, and Remediation.

The review shows that *IODEF* for Structured Cyber Security Information, RFC 7203 [20] is the most quality cyber-threat intelligence message exchange standard because it offers additional information, which is relevant to this study. It is therefore adapted for this work. However, some of its default information may disclose certain level of privacy and it does not provide mechanism for ensuring trust among the exchange partners.

IV. CYBER-THREAT INTELLIGENCE SYSTEMS

The works presented below are Cyber-Threat Intelligence Systems with state-of-the-arts information sharing, analysis and decision making techniques. The review employs the following methodology:

a. *INFOSEC sensors:* This stands for the number of information security devices or vulnerability sources. They were either single or multiple sensors.
b. *Information Sources:* It may be internal, external or community sources
c. *Administrator:* Population of administrators that participated in the administration of security. They were either be single or multiple.
d. *Incident Exchange Standard:* The RFC standards for information exchange.
e. *Point of Analysis:* It represented the location of threat analysis. They were either central or distributed.
f. *Stage of Threat Analysis:* This referred to the point at which the analysis takes place. They were either by pre-incident or post-incident. The pre-incident analysis is also referred to as Predictive Analysis.
g. *Perspective of Threat Analysis:* This referred to the point of view in which threat analysis were performed. The perspectives were either Attacker or Victim.
h. *Type of Threat Identified:* These were the kinds of threats that were identified. These types included: Minor, Major and All.
b. *Method of Threat Identification:* This is the method that was used to recognize and understand the threat. They were mainly by Single Step, Step-by-Step and Attack Pattern. Some attack patterns were based on predictive analysis.
c. *Type of Threat Prioritised:* These were the kinds of threats that are prioritised. These types included: Minor, Major and All.
d. *Method of Threat Prioritisation:* These are the methods that were used to rate threats. They included Vulnerability-based Threat Prioritisation Severity-based Threat Prioritisation, Likelihood-based Threat Prioritisation, and Risk-based Threat Prioritisation.
e. *Type of Threat Mitigation:* These are the kinds of threats that were mitigated. These types include: Minor, Major and Arbitrary Threat Mitigation.
f. *Method of Threat Mitigation:* These were the method used to select the configuration options. This included Arbitrary, Cost-effective and Cost-benefit.

The following are the systems:

AlienVault [25] is a relatively recent entrant to the commercial SIEM market. AlienVault's Unified SIEM provides SIEM, vulnerability assessment, network and host intrusion detection, and file integrity monitoring functions via software or appliance options. AlienVault Unified SIEM is composed of proprietary and open-source components. Open Source Security Information Monitoring (OSSIM) is an open-source security management platform that has been available since 2003. It provides support for NetFlow. Its unified SIEM lacks native support for Database Active Management (DAM) and there is no integration with third-party technologies.

CorreLog [26] integrates log management and SIM functions and provides basic capabilities. It targets midsize businesses, and have been validated with small deployments in the range of 50 to 75 servers. The solution includes agent-based Incident filtering and file integrity monitoring for Windows, Unix, and Linux platforms. CorreLog [26] does not provide Incident source integration for packaged applications. CorreLog does not provide Incident source integration for third-party DAM technologies, but there is limited support for monitoring database activity through native audit functions. In fact, CorreLog's predefined compliance reporting is limited to Payment Card Industry (PCI) only.

IBM's Tivoli Security Information and Incident Manager (TSIEM) [27] software provides SIM and Security Incident Monitoring functionality, and allows customers to have a starting point with log management. TSIEM provides capabilities for privileged user monitoring, compliance reporting, log management and basic real-time SEM. A typical deployment is focused on user activity monitoring and involves 100 or fewer servers. TSIEM integrates with a wide set of IBM and third-party Integrity and Access Monitoring technologies and applications. The technology is not well-suited for moderate or large deployments that require network security monitoring.

OSSEC [28] is an open source host-based intrusion detection system(HIDS). It is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows." The OSSEC HIDS can be installed as a stand-alone tool to monitor one host or can be deployed in a multi-host scenario, one installation being the server and the others as agents. The server and agents communicate securely using encryption. OSSEC also has intrusion prevention features, being able to react to specific Incidents or set of Incidents by using commands and active responses. The system allows the creation of new commands which can be bound to Incidents. The system comes with some predefined active response tools, but the administrator can add others.

McAfee IntruShield Network Security Products [29] delivers an integrated hardware and software solution, which delivers comprehensive detection *and* protection from known, first strike (unknown), DoS, and DDoS attacks from several hundred Mbps to multi-gigabit speeds. The architecture integrates patented signature, anomaly, and Denial of Service detection on a single purpose-built appliance. This not only enables highly accurate detection, but also empowers administrators with smart tools and processes, and enables flexible and scalable deployment for global businesses and vital government agencies. The IntruShield architecture employs a combination of threshold-based and patented self-learning, profile-based detection techniques that delivers unmatched intelligence to intrusion detection. With straightforward threshold-based detection, administrators can configure data traffic limits to ensure their servers will not become unavailable due to overload. Its self-learning methodologies enable studying of the patterns of network usage and traffic over time.

Caswell and Roesch [30] developed Snort, which is one of the most popular open source security tools. Since then, the product evolved both as features and as portability: currently Snort is available for most major platforms including Windows, BSD, Solaris or Mac OS X. This can be considered as a big advantage since the availability of signatures for new attacks can be faster than for most commercial IDS tools. Snort can run in different modes: Sniffer mode; Packet Logger mode; NIDS mode; and Inline (IPS) mode. Working as an IDS, Snort uses preprocessors and rules. Snort Preprocessors allow the functionality of Snort to be extended by allowing users and programmers add modular plug-ins. While Snort does not offer a GUI, there are many complementary open-source tools like Analysis Console for Intrusion Detection (PHP-based), Sguil, or BASE (Basic Analysis and Security Engine) which provide the GUI functionality for Snort.

Kang et al. [31] provided the design, evaluation, and deployment of Sequoia, a robust communication architecture for distributed Internet-scale security monitoring systems. Sequoia supports a rich set of communication patterns for regional and global sharing of monitor observations, collaborative decision-making among monitors, and timely delivery of security information to monitors. Highly secure communication is achieved through a comprehensive set of security mechanisms for trust management of participating monitors and trust-based routing. In addition, Sequoia offers high-quality and reliable communication services using a scalable self-organizing structure that is resilient and adaptive. Sequoia's communication architecture supports aggregation, integration, and dissemination of blacklists using a publisher-subscriber paradigm. Sequoia comprises three key protocols through which monitors self-organize into a two-level hierarchy on which scalable, fast and trustworthy message delivery can be

achieved: The Monitor Neighbour Discovery Protocol (MND) is used to form a topology-aware flat overlay among monitors, with every monitor connected to nearby nodes as its neighbours. The goal of the Distributed Dominator Selection Protocol (DDS) is to form a two-level communications hierarchy from the flat neighbour overlay constructed by MND. A monitor in the higher level of this hierarchy (dominators) must meet minimum requirements regarding trustworthiness and routing performance. The Communication Path Discovery Protocol (CPD) discovers multiple delivery paths from one or more senders to one or more destinations, considering both efficiency and security constraints. This is achieved by mapping the highly trusted dominator nodes into a structured overlay network.

Yegneswaran et al. [32] described and evaluated DOMINO, a cooperative intrusion detection system. DOMINO is designed to enable intrusion information sharing in a globally distributed network consisting of: trusted axis nodes Organised in a peer-to-peer overlay, satellite nodes associated with each axis node that are hierarchically arranged, terrestrial nodes, which are deployed at the leaves of the infrastructure, that provide daily intrusion summaries. DOMINO's design is based on heterogeneous data collection through NIDS, firewalls and active-sinks. This architecture enables DOMINO to be secure, scalable, fault tolerant, and facilitates data sharing. The evaluation clearly demonstrates the utility of sharing information between multiple nodes in a cooperative infrastructure. We use an information-theoretic approach to show that perspective on intrusions can be greatly enhanced by cooperation of a relatively small number of nodes. Using the 2002 and 2003 SQL-worm outbreaks, it is demonstrated that false-alarm rates can be significantly reduced in DOMINO and that reaction time for outbreak detection can be similarly reduced. Finally, we provide an initial evaluation of the effectiveness of active-sinks in discriminating between types of attacks based on examining payload data. The results clearly demonstrate that active-sinks provide important insight in this regard. Based on these analyses, it is concluded that DOMINO offers a significant opportunity to improve intrusion and outbreak detection capability in the Internet.

Chen et al. [33] presented a new distributed approach to detecting DDoS flooding attacks at the traffic flow level. The new defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP). At the early stage of a DDoS attack, some traffic fluctuations are detectable at Internet routers or at gateways of edge networks. A Distributed Change-point Detection (DCD) architecture is developed using change aggregation trees (CAT). The idea is to detect abrupt traffic changes across multiple network domains at the earliest time. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider. The system is built over attack-transit routers, which work together cooperatively. Each ISP domain has a CAT server to aggregate the flooding alerts reported by the routers. CAT domain servers collaborate among themselves to make the final decision. To resolve policy conflicts at different ISP domains, a new secure infrastructure protocol (SIP) is developed to establish the mutual trust or consensus. Sixteen network domains were simulated on the DETER testbed. Experimental results showed that 4 network domains are sufficient to yield a 98% detection accuracy with only 1% false-positive alarms. The security coverage is wide enough to safeguard most ISP core networks from real-life DDoS flooding attacks.

Dondo [34] presented a fuzzy systems approach for assessing the relative risk associated with computer network assets. He used the approach to rank vulnerabilities so that analysts can prioritise their work based on the potential risk exposures of assets and networks and associated vulnerabilities to individual assets, and therefore networks. Fuzzy models of the vulnerability attributes were developed in which fuzzy rules is used to make an inference on the risk exposure and the likelihood of attack, which allows ranking of the vulnerabilities and shows which ones need more immediate attention. The work did not address threat identification while the Threat Prioritisation used only vulnerability information to rate threats.

According to Mell et al. [35], Common Vulnerability Scoring System is standard approach used to quantitatively analyse vulnerabilities and rank risk between 0 and 10. It can qualitatively described risk as low, medium and high. It based its risk estimation on three factors: base factors, temporal factors and environmental factors. This approach has the advantage that it takes into consideration vulnerability attributes, and uses them to calculate a score for relative comparison. However, CVSS's rough estimates of the number of assets affected by vulnerability, its course-grained inclusion of asset values and the limited variability of its temporal metrics makes its vulnerability prioritisation less accurate. Also, it is limited by the fact that its risk estimation was based on the presence of availability of Common Vulnerability and Exposure Identification.

Ahmed et al. [36] presented Risk based proactive seCurity cOnfiguration maNAger (ROCONA). They proposed a security metric

framework that quantifies objectively the most significant security risk factors, which include existing vulnerabilities, historical trend of vulnerability of the remotely accessible services, prediction of potential vulnerabilities for any general network service and their estimated severity and finally propagation of an attack within the network. The risks were obtained based on the information in National Vulnerability Databases. The result show high accuracy and confidence of the proposed metrics.

Locastor et al. [37] presented Worminator, which extracts relevant information from alert streams and encodes it in Bloom Filters. This information forms the basis of a distributed watchlist. The watchlist can be distributed via a choice of mechanisms ranging from a centralized trusted third party to a decentralized P2P-style overlay network. They adopt two mechanisms in order to cope with the difficulties of distributed correlation and the potential volume of data being correlated. The Bloom filters by Worminator is employed to protect the confidentiality of the data being exchanged between domains. Second, efficient information exchange is accomplished with a distributed correlation scheduling algorithm. The scheduling algorithm dynamically calculates subsets of correlation peers that should communicate to exchange Bloom filters. Since information is also compacted by the Bloom filter, correlation between peers becomes extremely cost-effective in terms of bandwidth and processing power. The Worminator also has privacy preserving mechanism.

In [38], DShield is discussed. DShield aggregates firewall and intrusion detection system logs from networks throughout the global Internet. Each log entry provided by a network represents one or more packets that violated a local rule. DShield transforms all of the logs into a normalized form. Each entry in the DShield trace includes: time-detected, submitter's ID, count, source IP, source port, destination IP, destination port, protocol exploited, and flags. The source IP can be used for identifying a malicious/infected scanning source if the IP address is not spoofed. Broadly speaking, the DShield trace provides a unique opportunity to extract the spatial-temporal characteristics of attacking machines.

Ning et al. [39] presented the development of TIAA, a visual toolkit for intrusion alert analysis. TIAA is developed to provide an interactive platform for analyzing potentially large sets of intrusion alerts reported by heterogeneous intrusion detection systems (IDSs). To ensure timely response from the system, TIAA adapts main memory index structures and query optimization techniques to improve the efficiency of intrusion alert correlation. TIAA includes a number of useful utilities to help analyze potentially intensive intrusion alerts, including alert aggregation/disaggregation, clustering analysis, focused analysis, frequency analysis, link analysis, and association analysis. Moreover, TIAA provides several ways to visualize the analysis results, making it easier for a human analyst to understand the analysis results.

Ntoukas et al. [40] presented a collaborative Workstation platform called Storm to improve security in distributed and complex information Systems with critical data and services. This platform makes use of advanced open source technologies and interactive software tools. The tool was applied to Port Information Systems security and the results show the effectiveness of Collaborative Workstation in Distributed System.

The aim of Chen et al. [41] was to mitigate Botnets, which consisted large number of bots that generate huge volumes of spam or launch Distributed Denial of Service (DDoS) attacks on victim hosts. To address these problems, a practical collaborative Workstation system was proposed with an effective collaborative Unified Threat Management (UTM) and traffic probers. A distributed security overlay network with a centralized security centre leverages a peer-to-peer communication protocol used in the UTMs collaborative module and connects them virtually to exchange network Incidents and security rules. Security functions for the UTM were retrofitted to share security rules. In the work, they proposed the design and implementation of a cloud-based security centre for network security forensic analysis. The cloud storage kept collected traffic data and enabled processing of data with cloud computing platforms to find the malicious attacks. The cloud based security centre could instruct each collaborative UTM and prober to collect Incidents and raw traffic, send them back for deep analysis, and generate new security rules. These new security rules were enforced by collaborative UTM and the feedback Incidents of such rules are returned to the security centre. By this type of close-loop control, the collaborative Workstation system could identify and address new distributed attacks more quickly and effectively. The Collaborative Workstation System did not address uncertainty and trust issues posed by incident sharing and analysis.

Porras et al. [42] described a mission-impact-based approach for the analysis of security alerts produced by spatially distributed heterogeneous information security (INFOSEC) devices, such as firewalls, intrusion detection systems, authentication services, and antivirus software. The objective of the work was to deliver an automated capability to reduce

the time and cost of managing multiple INFOSEC devices through a strategy of topology analysis, alert Prioritisation, and common attribute-based alert aggregation. They developed a prototype system called the Mission Impact Intrusion Report Correlation System, or MCorrelator. M-Correlator was intended to provide analysts (at all experience levels) a powerful capability to automatically fuse together and isolate those INFOSEC alerts that represent the greatest threat to the health and security of their networks. Once translated to an internal incident report format, INFOSEC alerts are augmented, and, where possible, fused together through a chain of processing. A relevance score was produced through a comparison of the alert target's known topology against the vulnerability requirements of the incident type, which was provided to M-Correlator by an Incident Handling Fact Base. Next, a priority calculation was performed per alert to indicate the degree to which the alert was targeted at critical assets and the amount of interest the user had registered for this alert type. Last, an overall incident rank was assigned to each alert, which brings together the priority of the alert with the likelihood of success. Once ranked, the M-Correlator attempted to combine related incident alarms with an attribute-based alert clustering algorithm. The resulting correlated incident stream represents a filtered, lower-volume, content-rich security-incident stream, with an incident-ranking scheme that allows the analyst to identify those incidents that pose the greatest risk to the monitored network. The M-Correlator was able to combine information from different sources but did not address or state how it addressed the issues that affect this kind of framework. Also, no mechanism was develop to address bias modelling and mitigation of Minor Threats.

Yu et al. [43] proposed a general collaborative architecture for multiple IDS products by combining intelligent agents and knowledge-based alert evaluation. They evaluated the alert priority, based on asset characteristics, and they used it as the input to their correlation system. No mechanism was developed to address bias modelling and mitigation of Minor Threats and it did not address or state how it addressed the issues that affect the Collaborative framework.

Årnes et al. [44] proposed a network risk assessment using several strategies including examining the composition of risks to the individual host and applying the Hidden Markov Model (HMM) to represent the likelihood of transitions between security states. The model was static and so could not address the continuously emerging threats.

Alshubi et al. [45] proposed a fuzzy-logic based technique for scoring and prioritizing alerts generated by intrusion detection systems. In addition, they presented an alert rescoring technique that led to further reduction of the number of alerts. The IDS alerts were evaluated based on a number of criteria representing the seriousness of the alerts. A Fuzzy Logic Inference Mechanism was developed to score alerts. The approach was therefore applied to the alerts generated by scanning in DARPA 2000 LLDOS 1.0 dataset which successfully prioritized the most critical alerts along with their preparation steps. They did not addressed how alert priority changes with time, that is action based alerts.

A very popular Threat Model is DREAD [46]. It makes use of a static Threat Modelling approach.The ratings can fall in the range of 5–15. The risk determination factors are organised into five descriptions. Damage potential: How great is the damage if the vulnerability is exploited? Reproducibility: How easy is it to reproduce the attack? Exploitability: How easy is it to launch an attack? Affected users: As a rough percentage, how many users are affected? Discoverability: How easy is it to find the vulnerability? It usually makes use of STRIDE Threat Identification Model Hernan et al. (2006) to identify threats. As such, it is not suitable for modelling complex scenario threats.

Data mining approach was applied in generating attack graphs in [47] through Association Rule Mining without training, the algorithm generated multi-step attack patterns from historical intrusion alerts which comprised the attack graphs. The algorithm also calculated the predictability of each attack scenario in the attack graph which represented the probability for the corresponding attack scenario to be the precursor of future attacks. The algorithm predicted most major threats with very high accuracy and confidence; however, minor threats were predicted less accurately with low confidence.

Haslum [48] developed Distributed Intrusion Prediction and Prevention System. A Probabilistic Hidden Markov Model (HMM) that captures the interaction between the attacker and the network was provided. The interaction between various Distributed IDS and integration of their output were achieved through a HMM. He modelled the interaction between the attackers and the system using a Markov model and assumed the system to be in one of the following states: Normal (N) indicating that there is no on-going suspicious activity, Intrusion Attempt (IA) indicating suspicious activity against the network, Intrusion in

Progress (IP) indicating that one or more attacker have started an attack against the system, and Successful Attack (SA) one or more attackers have already broken into the system. By using a Markov model, he assumed that next state transition only depend on current state. The risks of the predicted attacks were estimated based on severity, resistance, frequency, etc using fuzzy logic. The risks determined the response options. The prediction was static while the prioritisation relied on expert knowledge which is scarce in network security domains.

Another data mining technique to discover, visualize, and predict behavioural pattern of attackers in a network based system was developed by [49]. They proposed a system that was able to discover temporal pattern of intrusion which revealed behaviours of attackers using alerts generated by Intrusion Detection System (IDS). They used data mining techniques to find the patterns of generated alerts by generating Association rules. Their system was able to stream real-time Snort alerts and predict intrusions based on the learnt rules. The algorithm is not suitable for complex scenario attack and emerging threats.

Jumaat [50] proposed a framework for modelling risk through incident prioritisation and responding to the intrusion. It prioritised and responded to incident using their urgency and criticality. A Risk Index Model (RIM) was used to estimate the risk while a Response Strategy Model (RSM) dynamically maps incidents into different types of response, with serious incidents being mapped to active responses in order to minimise their impact, while incidents with less impact have passive responses. Through the results gathered, the study demonstrated that that alerts priorities change with time and prioritisation process can feasibly be used to facilitate the response selection process in Intrusion Response Systems. However, the incident prioritisation scheme did not address bias against Minor Threats while the response applied a single sensor. The survey for some of the review works is presented in Table 1.

V. CYBER-THREAT INTELLIGENCE FRAMEWORK FOR IOCT MANAGEMENT

The methodology for this work is premised on the fact that the collaboration of local stations will assist in Cyber-Threat Intelligence. The Framework consists of Incident Sharing, Incident Analysis and Security Configuration Decision Making Components. The components are organized as a Server-Client Architecture consisting of a Central Administrative System, which serves as the server and local stations that are the clients. The Incident Sharing Component has Data Collection and Information Sharing Units while the Incident Analysis has Threat Prediction Unit and Threat Prioritisation Unit.

A. Incident Sharing Component

1) Data Collection Model

Due to the strength of Incident Object Description Exchange Format for Structured Cyber Security Information (IODEF-SCI) [20] *(Takahashi, 2013)* in providing additional information, which is important to our model, we operationalised incident data layout consisting of the following fields for the proposed Incident Sharing Model.

TABLE 1: Survey of Cyber-Threat Intelligence System

S/N	Tool	INFOSEC Sensor/Sources	Administrator / exchange method	Point of Analysis	Mode of Analysis	Perspective of Analysis	Stage of Threat Analysis	Type of Threat Identified	Method of Threat Identification	Type of Threat Prioritised	Method of Threat Prioritisation	Type of Threat Mitigation	Focus of Threat Mitigation
1	**DREAD (**Microsoft Inc in Meier et al., 2006**)**	Single/ External Source	Single/ DREAD standard	Central	Offline	Victim	Pre-incident	All	Single Step	All	Risk	NA	NA
2	**Collaborative Architecture**	Multiple/ Internal	Single /No	Central	Online	Victim	Post-incident	All	Attack Pattern	All	Risk	NA	NA

	(Yu et al., 2004)	source	specified standard						(Predictive)				
3	**CVSS** (Mell et al., 2009**)**	Multiple/ Commu-nity Source	Single/ IODEF-SCI sub-standard	Central	Offline	Victim	Pre-incident	All	Single Step	All	Vulnera-bility	Arbitrary	Arbitrary
4	**Fuzzy System Approach** [34]	Multiple/ Commu-nity Source	Single/ No specified standard	Central	Offline	Victim	Pre-Incident	All	Single Step	All	Vulnera-bility	Major	Cost-effective
5	**SNORT (**Caswell and Roesch, 1998)	Single/ Commu-nity Source	Single/ No specified standard	Central	Online	Victim	Pre-incident	All	Single Step	All	Severity	Arbitrary	Arbitrary
6	**Incident Prioritisation for Intrusion Response** (Jumaat, 2012)	Single/ Internal & External Source	Single/ No specified standard	Central	Online	Victim	Post-Incident	All	Single Step	All	Risk	Major	Cost-effective
7	**ROCONA** (Ahmed *et al.*, 2010)	Single/ External Source	Single/ No specified standard	Central	Online	Victim	Post-incident	Major	Attack Pattern (Predictive)	Major	Risk	Major	Cost-effective
8	**DIPPS** [48]	Multiple/ Internal Source	Single/ No Specified Standard	Central	Online	Attacker	Post Incident	All	Attack Pattern	All	Risk	Major	Cost-effective
9	**M-Correlator** (Porras et al., 2002)	Multiple/ Internal & External Source	Colla-borative/ No Specified Standard	Distri-buted	Online	Victim	Post-incident	All	Single step	All	Risk	Major	Cost-efficient
10	**FuzMet** [45]	Multiple/ Internal Source	Single/ No Specified standard	Central	Online	Victim	Post-incident	All	Step-by-step	All	Risk	Minor	Cost-effecient
11	**Network Risk Assessment** (Årnes *et al.*, 2006)	Single/ Intenal Source	Single/ No specified standard	Central	Online	Victim	Pre-incident	All	Step-by-Step	All	Risk	Major	Cost-effective
12	**Sequential**	Multiple/	Single/	Central	Offline	Attack	Post-	All	NA	NA	NA	NA	NA

	Association Mining without Training [47]	Internal Source	No specified standard			-er	incident						
13	**Sequential Association Mining with Training** [49]	Multiple/ Internal Source	Single/ No specified standard	Central	Offline	Attack -er	Post-incident	All	NA	NA	NA	NA	NA

The Takahashi [20] consists of the following Incident and Incident Class attributes:

- *Incident_ID*
- *Alternative_ID*
- *Related_Activity*
- *Detect_Time*
- *Start_Time*
- *End_Time*
- *Report_Time*
- *Assessment*
- *Method*
- *Incident_Data*
- *History*
- *Additional_Data*

The IODEF-SCI data model is adapted as Incident Fact Base.

2) Information Sharing Model

In Figure 1, the Layout of the Information Sharing Model is presented. The Collaborating Network Security Managers submit incident information to the Central Controller Fact Base in Structured Query Language (SQL) interoperability format such as Comma Separated Value (.csv) and Extensible Mark-up Language (.xml). The Central Administrative System filters the information and performs analysis based on the request of the Managers. The outcomes of the analyses are reported by the Central Administrative System to the Security Managers.

B. Incident Analysis and Decision Making Component

The Incident Analysis Component of the Collaboration Framework consists of Threat Prediction and Threat Prioritisation Units while the Decision Making focuses on efficient and effective Security Configuration.

1) Threat Prediction

The Central Administrative System performs Data Mining activities, which is summarized into Data Pre-processing, Data Mining and Interestingness Analysis. The Local Workstation receive the results of the data mining via their contacts and make use of them in managing the Internet-facilitated Organised Crime Threats.

2)Threat Prioritisation

The Threat Prioritisation unit consists of Attacker and Victim-based Threat Rating, Threat Rating and Ranking components.. The Attacker-based Threat Rating Component consists of Vulnerability Measurement, Vulnerability Reconciliation, Attacker-based Threat Rating units. The Vulnerability Measurement unit uses the Attacker's Perspective of Intrusion Detection to characterise vulnerability. The Vulnerability Reconciliation unit uses Dempster-Shafer Decision Fusion Technique to map qualitative value of vulnerability criteria to quantitative value. The Threat Rating units rate Threat with respect to the asset criticality using Expectation Theory. The Victim-based

3) Threat Mitigation

The reputable Risk Control Security Configuration advices are provided by the Central Administrative System on both the Minor Threats and Major Threats. Each Network Security Managers uses the feedback from the Central Administrative System to perform effective and efficient IOCT Management.

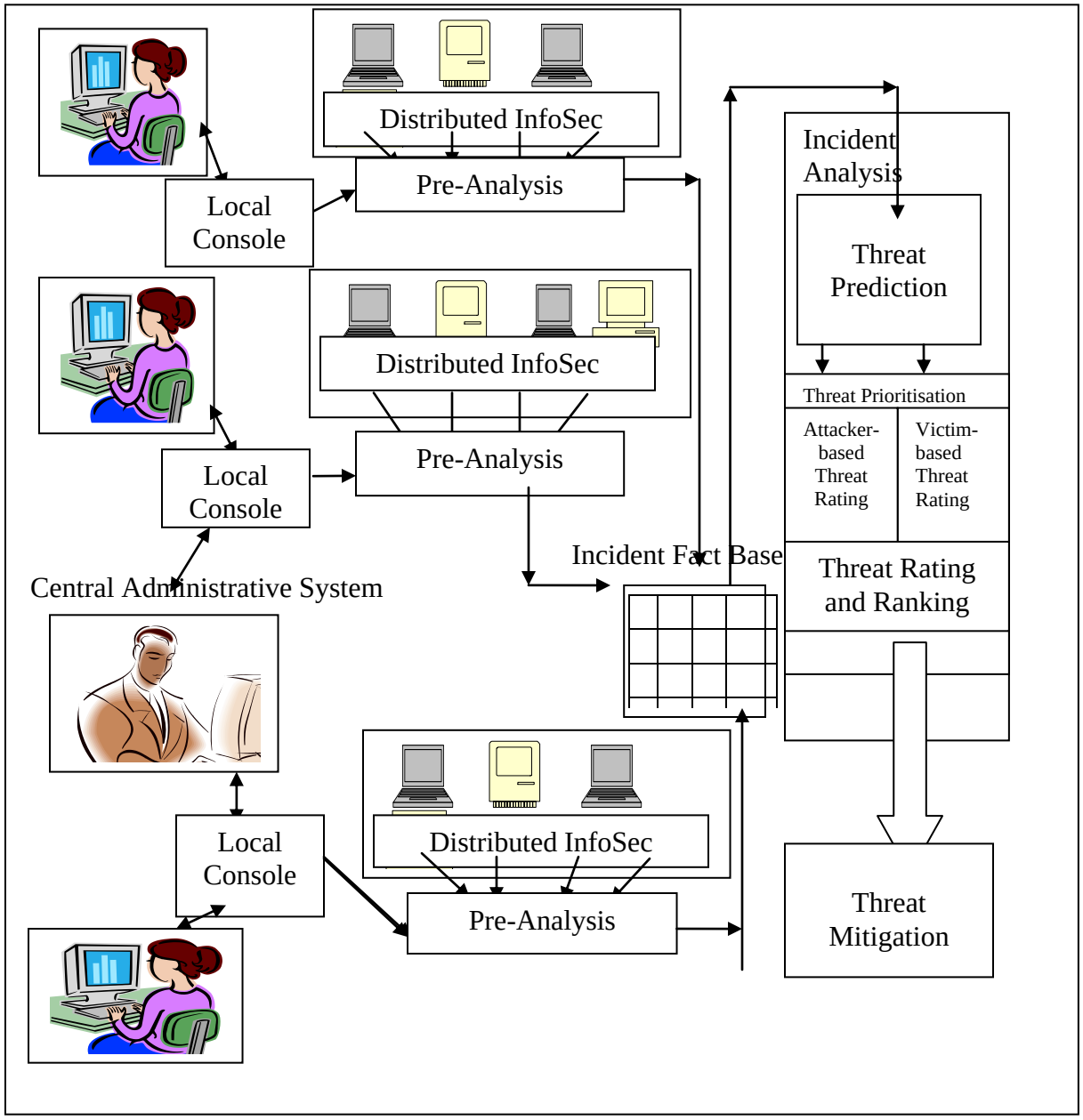

Fig 1: Cyber-Threat Intelligence Framework for Improved IOCT Management

VI. CONCLUSION

The above framework emanated from the following findings as presented below.

Sequential Association Mining Algorithms [47] and [49] were able to predict scenario threats dynamically. Li et al. [47] performed better than [49] with Major Threats in simple attack scenario of LLDOS 1.0 by yielding minimum confidence above 0.5. However, it performed poorly with Minor Threats in the same scenario by yielding maximum confidence of 0.26. Therefore, Sequential Association Mining Algorithm without minimum support is proposed for this study with modifications to predict actionable Minor Threats from different networks accurately.

All the works reviewed were biased in prioritising Minor Threats leading to inaccurate ratings. Haslum [48], Dondo [34] and Alsubhi et al., [45] however prioritised threats and addressed Information Reconciliation, Fusion and Uncertainty using Fuzzy Logic, which needed expert knowledge, large data or prior information. These requirements are scarce in network security domain. A Belief Function that does not need such requirements and could reconcile, fuse and remove uncertainty is proposed to prioritise threats based on Attacker and Victim Perspectives of Intrusion.

Existing works focusing on Cost-effective decision making mitigated only Major Threats to ensure compliance with the scope of Network Threat Management. None of the reviewed works mitigated harmful Minor Threats. Hence, the standard Risk Mitigation Model [51] would be adapted to allow for mitigation of harmful Minor Threats from Internet-facilitated Organised Crime Threats.

All the SIEMs performed well by effectively detecting threats. Chen *et al.* (2007) Collaborative-based change point detection for DDoS, Ntoukas *et al.* (2011) Storm, and Chen *et al.* (2013) Cloud-based Collaborative Network Security Management for Forensic Analysis performed well in effectively managing Internet-facilitated Organised Crime Threats. However, they were not applied to Threat Modelling involving Minor Threats and would not manage all the Incident Sharing and Analysis Issues such as Privacy, Multidimensionality, Uncertainty, Trust, Interoperability and Quality. Hence, a new Collaborative Network Security Management Framework involving multiple network security managers, multiple sensors and multiple networks that addressed the issues of Incident Sharing, Analysis, cost-effectively and efficient Security Configuration is proposed.

REFERENCES

[1] Weforum. 2012. "Organised Crime Enablers," Retrieved 2nd May, 2014 https://www.weforum.org

[2] Europol. 2014. "The Internet Organised Crime Threat Assessment," Retrieved 2nd May, 2014 from https://www.europol.europa.eu/sites/default

[3] Banday, M.T., Qadri, J.A., Shah, N.A. (2009). "Study of Botnets and Their Threats to Internet Security," . Sprouts: Working Papers on Information Systems, 9(24). Retrieved I9th May, 2012 from http://sprouts.aisnet.org/9-24.

[4] CAIDA .2003. Slammer Worms. Retrieved 4th May, 2014 from www.caida.org.

[5] Websense. 2011. "Advanced Persistent Threats and Other Advanced Attacks: Threat Analysis and Defense Strategies for SMB, Mid-Size, and Enterprise Organisations," Retrieved 2nd May, 2014 from https://www.websense.com

[6] Symantec .2012. Internet Security Threat Report, Volume 17 Retrieved 19th January, 2014 from www.symantec.com/content

[7] Symantec .2013. Internet Security Threat Report, Volume 18 Retrieved 19th January, 2014 from www.symantec.com/content

[8] Arbor Networks. 2012. Arbor Special Report: Worldwide Infrastructure Security Report 2011. Volume VII. Retrieved 8th January, 2013 from www.arbornetworks.com/report.

[9] Kaspersky Security Bulletin. 2009. Malware Evolution 2009. Retrieved 4th April, 2014 from http://kaspersky.com

[10] Friedman, J. and Bouchard, M.2015. Definitive Guide to Cyber-Threat Intelligence, iSight Partner, Retrieved 4th June, 2016 from http://isightpartners.com

[11] Waltz, E. 1998. Information warfare principles and operations. Norwood, MA: Artech House, Inc. In Proceedings of Network and Distributed System Security Symposium (NDSS 2004).

[12] Clark, R. 2010. Intelligence analysis: A target-centric approach. (Third ed.). Washington, DC: CQ Press.

[13] Payment Council.2014. Cyber Threat Intelligence. Retrieved 3rd May, 2017 from http://www.paymentsuk.org.uk

[14] NCI. 2013. National council of isacs. Retrieved 5th February, 2014 from http://www.isaccouncil.org/home.html

[15] Amoroso, E. 2011. Cyber Attacks: Protection National Infrastructure. Burlington, MA: Elsevier.

[16] MalwareDomains. 2013. DNS-bh – malware domain blocklist. Retrieved 4th April, 2014 from http://www.malwaredomains.com

[17] EmergingThreats. 2013. Enhance your intrusion detection system with etpro™ ruleset. Retrieved 4th December, 2013 from http://www.emergingthreats.net/solutions

[18] Saklikar, S. 2013. Sharing Threat Intelligence Analytics. RSA Conference, Asia-Pacific 2013. CLT-05 Intermediate Class.

[19] Danyliw, R.,Meijer, J.and Demchenko, Y. 2007. The Incident Object Description Exchange Format. Network Working Group, RFC 5070. Retrieved 2nd April, 2014 from www.ietf.org

[20] Takahashi, T. 2013. Iodef-extension for structured cybersecurity information. Retrieved 4th April, 2014 from http://tools.ietf.org/html

[21] Moriarty, K. 2012. Real-time Inter-network Defense (RID), RFC 6545. Retrieved 2nd April, 2014 from www.ietf.org

[22] Farnham, G. 2013. Tools and Standards for Cyber Threat Intelligence Projects. GIAC (GCPM) Gold Certification.

[23] MAPP (2017) Microsoft Active Protections Program. Retrieved April 9, 2018 from https://technet.microsoft.com/enus/security/dn467918.aspx

[24] FS-ISAC(2014) Financial Services Information Sharing Analysis Centre. Retrieved April 4, 2014 from https://www.fsisac.com/

[25] AlienVault. Retrieved April 4, 2014 from http://www.alienvault.com

[26] CorreLog. Retrieved 4th May, 2014 from https://correlog.com

[27] IBM, Retrieved May, 2014 from http://ww.ibm.com

[28] OSSEC (2018) Open Source HIDS Security. Retrieved 10th May, 2017 from https://www.ossec.net/

[29] McAfee. Retrieved 4th May, 2014 from www.mcafee.com

[30] Caswell, B. and Roesch, M. 1998. Snort: The open source network intrusion detection system. Retrieved 10th April, 2014 from http://www.snort.org .

[31] Kang, X., Zhou, D., Rao, D., Li, J. and Lo, V. 2004. Sequoia – A Robust Communication Architecture for Collaborative Security Monitoring Systems. Retrieved 4th

April, 2014 from http://netsec.cs.uoregon.edu/research/sequoia.php

[32] Yegneswaran, V., Barford, P. and Jha, S. 2004. Global Intrusion Detection in the DOMINO Overlay System.

[33] Chen, Y., Hwang, K and Ku, W. 2007. Collaborative Detection of DDoS Attacks over Multiple Network Domains. IEEE Transactions on Parallel and Distributed Systems, TPDS-0228-0806.

[34] Dondo, M. 2009. A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System. DRDC Ottawa Defence R&D Canada – Ottawa, Technical Memorandum DRDC Ottawa TM 2007-090.

[35] Mell, P., Scarfone, K. and Romanosky, S .2009. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", Rerieved 1st May 2014 from http://www.first.org/cvss/cvss-guide.html

[36] Ahmed, M.S., Al-Shaer, E., Taibah, M., Khan, L. 2010. Objective Risk Evaluation for Automated Security Management.

[37] Locasto, M.E., Parekh, J.J., Keromytis, A.D., Stolfo, S.J. 2005. Towards Collaborative Security and P2P Intrusion Detection. Proceedings of the 2005 IEEE Workshop on Information Assurance and Security T1B2 1555 United States Military Academy, West Point, NY, 15.

[38] Ullrich, J. 2004 \Dshield home page." Retrieved 19th January, 2014 from http://www.dshield.org/.

[39] Ning, P., Peng, P., Hu, Y., and Xu, D. 2003. TIAA: A Visual Toolkit for Intrusion Alert Analysis. Retrieved 4th April, 2014 from http://www.iss.net.

[40] [40] Ntouskas, T., Pentafronimos, G. and Papastergiou, S. 2011. STORM - Collaborative Security Management Environment. Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless CommunicationLecture Notes in Computer Science Volume 6633, 2011, pp 320-335.

[41] Chen, Z., Han, F., Cao, J., Jiang, X., and Chen, S. 2013. Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System. Tsinghua Science and Technology ISSN 1007-0214 05/12 pp40-50 Volume 18, Number 1.

[42] Porras, P.A., Fong, M.W. and Valdes, A. 2002. A mission-impact-based approach to INFOSEC alarm correlation", Proceedings of the 5th International Symposium Recent Advances in Intrusion Detection, Zurich, Switzerland, Vol. 2516, pp. 95-114.

[43] J. Yu, Y.V. R. Reddy, S. Selliah, S. Reddy. TRINETR: An architecture for collaborative intrusion detection and knowledge-based alert evaluation. Advanced Engineering Informatics, 19 (2005) 93–101.

[44] Årnes, A., Valeur, F., Vigna, G. and Kemmerer, R. 2006. Using Hidden Markov Models to Evaluate the Risks of Intrusions: System Architecture and Model Validation", Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID), Hamburg, Germany, pp. 145–164.

[45] Alsubhi, K., Al-Shaer, E. and Boutaba, R. 2008. Alert Prioritisation in Intrusion Detection Systems, Proceedings of the IEEE Network Operations and Management Symposium, Salvador, Brazil, pp. 33-40.

[46] Meier, J.D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. and Murukan, A. 2003. Improving Web Application Security: Threats and Countermeasures, Threat Modelling, Microsoft Corporation.

[47] Li, Z., Lei, J., Wang, L., and Li D. 2007. A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction. Computer Communications 29.

[48] Haslum, K. 2010. Real-time network intrusion prevention. Doctoral theses at NTNU, 2010:168.

[49] Katipally, R., Cui, X. and Yang, L. 2010. Multi stage attack Detection system for Network Administrators using Data Mining.

[50] Jumaat, A. N. B. 2012. Incident Prioritization for Intrusion Response. University of Plymouth, Unpublished Ph.D. Thesis.

[51] Hillson, D. 1999. Developing Effective Risk Responses, Proceedings of the 30th Annual Project Management Institute 1999 Seminars & Symposium, Philadelphia, Pennsylvania, USA.