A

Dissertation

On

"Unified Model for Integrated Cyber Security"

Submitted in Partial fulfilment of the requirement

For the award of Degree of

MASTER OF TECHNOLOGY

Computer Science & Engineering

Delhi Technological University, Delhi

SUBMITTED BY

RAJESH KUMAR MEENA

University Roll No: 2K11/CSE/10

Under the Guidance of:

Mr. VINOD KUMAR

Associate Professor

Delhi Technological University

DEPARTMENT OF COMPUTER ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

BAWANA ROAD, DELHI-110042

2012-2013

CERTIFICATE

This is to certified that **Mr. RAJESH KUMAR MEENA, Roll No. 2K11/CSE/10**, student of **M.Tech. in Computer Science & Engineering, Department of Computer Engineering, Delhi Technological University,** has submitted the dissertation entitled **"Unified Model for Integrated Cyber Security"** under my guidance towards partial fulfilment of the requirements for the award of the degree of **Master of Technology (Computer Science & Engineering).**

The dissertation is a bonafide work record of project work carried out by him under my guidance and supervision. This matter embodied in this project work has not been submitted earlier for the award of any degree or diploma in any university/institution to the best of our knowledge and belief. His work is found to be outstanding and his discipline impeccable during the course of the project.

I wish him success in all his endeavours.

(Mr. VINOD KUMAR)
Project Guide
Associate Professor
Department of Computer Engineering
Delhi Technological University

PUBLICATION

Cyber Times International Journal of Technology & Management

310 Suneja Tower-II, District Centre, Janak Puri, New Delhi-110058.

Ph: 011-25595729, +91-9312903095

Website: http://Journal.CyberTimes.in Email: editor@cybertimes.in

ACKNOWLEDGEMENT

Greetings from ***"Cyber Times International Journal of Technology & Management", dated:*** 22/06/2013.

Thanks for your contribution to CTIJTM for your Paper ***(Cyber Security A Review)*** submission. This is pleased to inform you that your paper has been selected and approved for the Final publication in our upcoming Edition in September 2013, in Vol. 6 Issue 2 of "Cyber Times International Journal of Technology & Management".

ACKNOWLEDGEMENT

First of all, let me thank the almighty god, my parents and my dear friends who are the most graceful and merciful for their blessing that contributed to the successful completion of this project.

I would like to devote my gratitude and thanks to my guide **Sh. Vinod Kumar**, **Associate Professor, Department of Computer Engineering, Delhi Technological University, Delhi** for his valuable guidance, constant encouragement and helpful discussions throughout the course of this work. Obviously, the progress I had now will be uncertain without his guidance.

I would like to thanks to my Co-Guide **Dr. V. K. Panchal** for his incredible support in helping me to understand my project work.

I would also like to thank **Prof. (Dr.) Daya Gupta**, **H.O.D. Computer Engineering Department, Delhi Technological University, Delhi** for providing me better facilities and constant encouragement.

I would like to take this opportunity to express the profound sense of gratitude and respect to all those who helped us throughout the duration of this project. DELHI TECHNOLOGICAL UNIVERSITY, in particular has been the source of inspiration, I acknowledge the effort of those who have contributed significantly to this project.

RAJESH KUMAR MEENA

(Roll No.: 2K11/CSE/10)

TABLE OF CONTENTS

Title Name **Page No.**

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

This thesis examines the guidance that is being given to developing a unified cyber security monitoring and management system. The proposed rules and regulations are largely relevant for developed a unique cyber security system. In promoting better guidance, the thesis identifies and discusses several challenges related to cyber defence. Another such difference is the common lack of a private cyber security sector and different expectations of government. This thesis concludes with discussing unexpected results. The most fundamental problem of cyber security is cyber threats. Most of the cyber defence techniques are more effective day by day, but cyber threats are growing more fast compare to cyber defence solutions. At the beginning, a nuclear war may not be on the immediate horizon, but a cyber war is and it has the potential to bring major cities worldwide to a standstill, affecting everything from banking, traffic networks, hospitals and even electricity grids. These are now the focus of a new security front worldwide. It's pretty clear now there is underway a type of cyber arms race, both to be able to pick up and also to secure data per second, but also, in fact, to be able to target or to defend those countless crucial functions of a contemporary society.
Thus the highest realization of warfare is to attack the enemy's plans; next is to attack their alliances; next to attack their army; and the lowest is to attack their cities. Warfare is the greatest affair of state, the basis of life and death, the Way to survival or extinction.

In this thesis we survey, review, analyze and design various current cyber security strategies to find out the robust, reliable, efficient and quick responsive results during cyber security operation for cyberspace superiority in cyber warfare. The Federated Cyber Defence System (FCDS), its architecture, protocols and security mechanisms, are quite relevant to the current environment. Cyber forces, refers to cultivated personnel's that can perform network computer operations and hold cyber security technology such as cyber intelligence collection, cyber-attack, cyber defence, and cyber forensics. Cyber intelligence capability includes cyber surveillance/reconnaissance, cyber order of battle and cyber damage assessment. Technical-socio framework encompasses the cyber security warning systems. A real-time intrusion detection system that changes its behavior according to the patterns occurred in the new received data, the framework uses a semi rule-based approach to classification in order to make the model more understandable for human experts and facilitate the user interference in the learning process.

CHAPTER: 1

INTRODUCTION

1.1 OBJECTIVE

The objective of this thesis is to analysis and design a new unified model for integrated cyber security (UMICS) system. This model is working effectively and accurately to find the solutions of cyber threats. Our model can provide an efficient solution for the cyber threats problem of the cyber security. The fundamental problem in designing a unified model is integration cyber security techniques, centrally controlled and monitoring the system. Traditional methods for cyber security models are not properly handles the cyber threat problems. Many cyber security models working but these are not fulfilling the end user requirements. Some techniques are more useful with assigned some special works in UMICS system.

The cyber security techniques such as FCDS, cyber physical system (CPS), cyber security strategies, next generation- intrusion detection system (NG-IDS,) early warning system (EWS) and technical-socio cyber security (TSCS) warning system are reviewed in this thesis .The integration of all techniques in a single platform for the controlling and monitoring purpose of the developed system . Federated cyber defence system (FCDS) is developed to minimize the number of threats and attacks that may affect the domain connected to the open network. FCDS is the system that cooperates in federation of systems (FoS). FoS is an association of loosely coupled countries, states, companies, societies, or organizations, each retaining control of its own network. Domains in FoS are so connected or related as to produce results beyond those achievable by the individual systems. The lack of synchronization among network administrators causes that network security level depends on employed solutions and system administrator awareness and skills. Exchange of information on threats, detected attacks and verified security metrics improves situational awareness in federated domains. The advantage of FCDS is a capability to collect and correlate events gathered by various sensors spread in its own and federated domains. In FCDS a response is prepared and applied to reactions elements of protected domain as fast as an attack is detected

[14]. CPS has close relationships with embedded systems, sensors, and wireless network, but has its own characteristics, for example, the complexity and dynamics of environment. The problem space and solution space are closely related with the environment and the requirement for high reliability of the system [19].

Cyberspace superiority should be firstly achieved to win in cyber warfare. Cyber strategy is required superiority in term of national defence strategy [15]. Being technical-socio in nature, successful information systems security process relies on two pillars: technology and humans. In cyber space, information security is not anymore limited within a local entity; given it is a working group, an organization or even a whole nation. If the security process to be managed effectively and efficiently, then those people has the correct and expected understanding and good thinking about security mechanisms [2]. Harmful activities cover broad spectrum of cyber threats and potential cyber attacks. Everybody relies on networks, and nothing can operate unless the networks are functioning correctly. They can influence communication links, data resources, their integrity, confidentiality and availability. General Douglas MacArthur once said "There is no security on this Earth, there is only opportunity" [3].

1.2. PROBLEM STATEMENT

The objective of this research work is to provide a cyber threats free, safe cyber space for future internet, which can achieve high accuracy and many other useful functionality of the system. So that, UMICS model can be used in place of expensive and poor response cyber security systems.

The desired model must be generic and can be customized for any cyber security application. It must also be adaptable with the changing needs and requirements of the future cyber security environment.

1.3. MOTIVATING FACTOR

The Internet is currently structured as a global and borderless computer network. The ability to communicate easily with any other device has enabled the Internet to have great benefits, but this also enables cyber security problems in one part of the globe to easily impact users somewhere else. As a result of this architecture, the cyber security situations in all

organisations are interrelated. Consequently, it is the global interest to have all countries working to reduce the amount of malicious traffic exiting their organisations. International Communication Techniques (ICT) emerging nations are the target of this thesis for multiple reasons. There is a perception that these governments are not taking the issue of cyber security seriously, because few have created substantial programs to secure cyberspace. This is important because if the cyber security situation is poor they will emanate malicious traffic which will harm the global Internet. In addition, because these countries are at the early stages of ICT development, they have an opportunity to structure their ICT infrastructure for cyber security in ways that were not done when other nations adopted the Internet. These pressing reasons create a need for better guidance for policy makers. The goal of this thesis is thus to provide research and analysis to help others provide better guidance.

In recent time, we have observed a trend toward exploitation of new or otherwise unprotected computers in increasingly shorter periods of time. This problem is exacerbated by a number of issues, including:

- Many computers' default configurations are insecure.
- New security vulnerabilities may have been discovered between the time the computer was built and configured by the manufacturer and the user setting up the computer for the first time.
- When upgrading software from commercially packaged media (e.g., CD-ROM, DVD-ROM), new vulnerabilities may have been discovered since the disc was manufactured.
- Attackers know the common broadband and dial-up IP address ranges, and scan them regularly.
- Numerous worms are already circulating on the Internet continuously scanning for new computers to exploit.

As a result, the average time-to-exploitation on some networks for an unprotected computer is measured in minutes. This is especially true in the address ranges used by cable modem, DSL, and dial-up providers. Standard advice to home and organisations users has been to download and install software patches as soon as possible after connecting a new computer to the Internet. However, since the background intruder scanning activity is pervasive, it may not be possible for the user to complete the download and installation of software patches before the vulnerabilities they are trying to fix are exploited. This Technical Tips offers advice on how

to protect computers before connecting them to the Internet so that users can complete the patching process without incident

1.4 ORGANIZATION OF THE DISSERTATION

This thesis work is organized as follows Chapter 1 deals with providing the objective, problem statement, motivation of undertaking this research work as well as organization of this dissertation.

Chapter 2 deals with basic overview of the cyber security concept. It also provides the basic knowledge of various challenges associated with cyber security models. This chapter includes the importance of cyber security environment and classified the various types of cyber threats. The cyber threats problem is also explained to helps us in better understanding of needs and requirement of a designing a unified model for cyber security.

Chapter 3 provides introduction to the unified model for integrated cyber security (UMICS) model approaches and basic analysis techniques of the unified models, which are basis for our approach. It also provides knowledge about various analysis tools are involved in designing a unified models for monitoring and management systems.

Chapter 4 begins with description of our research work. It describes the basic design of our approach. We have explained various steps involved in our model; we explained every techniques in detailed and proposed a new techniques using in UMICS systems.

Chapter 5 gives the final conclusion and outcomes of the research. It also lays the ground to design, develop and implement a unified model in the future work in this direction.

CHAPTER: 2

LITERATURE REVIEW

2.1 CYBER SECURITY – AN OVERVIEW

The Cyber Security is a set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware devices and software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security.

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three NWs were set up: INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure; NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central government with the state governments and district administrations, and the Education and Research Network (ERNET), to serve the academic and research communities. The target for broadband is 160 million households by 2016 under the National Broadband Plan. The government has ambitious plans to raise cyber connectivity. There has been a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace.

The cyber security scenario in India is one of relative chaos and a sense of insecurity arising out of the periodic reports of cyber espionage, cyber terrorism, cyber warfare and cyber crime. The complexity of the issue has resulted in a virtual paralysis. Legal and law enforcement mechanisms have not shifted gears fast enough to grapple with growing cyber crime. The lack of a coherent cyber security policy will seriously interfere with India's national security and economic development. It is essential that more attention at the highest levels is paid to ensuring that cyber-related vulnerabilities that can impact on critical sectors are identified and removed. A coherent and comprehensive cyber security policy will have several major elements, including accurate conceptualisation of cyberspace threats, building of robust cyberspace through a variety of measures, including technical, legal, diplomatic, international

cooperation creation of adequate organisational structures, strengthening of PPPs, HR development and implementation of best practices and guidelines. India's approach to cyber security has so far been ad hoc and piecemeal. A number of organisations have been created but their precise roles have not been defined nor synergy has been created among them. Meanwhile, many countries are seriously engaged in attending to their cyber security doctrines and strategies.

Cyber security is becoming an indispensable dimension of information security. The rapid growth of information communication techniques (ICT) has contributed immensely to human welfare but has also created risks in cyberspace, which can destabilise international and national security. Global and national critical infrastructure is extremely vulnerable to threats emanating in cyberspace. Given the positive as well as negative potential of cyberspace, there has been talk of devising an international convention on cyber security which would ensure that states behave responsibly in cyberspace. Cyber security must balance the cost of implementing security measures against the likelihood and impact of any security breaches. This balancing of cost vs. impact must take into account that excessive costs could impact customer rates, but that inadequate security measures could allow unnecessary power outages to those same customers. The cost/impact balancing also must recognize that no single security measure is 100% effective in preventing a security breach. Therefore, layered security measures must be applied, and methods must be developed for deterring, detecting, and coping with security attacks, along with audit trails for forensic analysis, possible legal actions, and training.

Cyber security solutions must ultimately be implementation-specific, driven by the requirements for security of all of the functions in the system. The cyber security requirements address the confidentiality, integrity, and availability of data using "Information Technology (IT)" security solutions such as cryptography, certificates, and physical access control [20].

Cyber Ethics is the code of responsible behavior on the Internet. We should all employ the basic tenets of Cyber Ethics to be good "cyber citizens." Cyber ethics must be taught and reinforced at every level of computer use—from the novice user just learning to navigate a computer and the Internet, to an information professional whose job requires significant use of online resources. The power of the Internet means that anyone can communicate at anytime, with anyone, anywhere.

2.2 BASICS OF CYBER SECURITY ENVIRONMENT

In this section, we discuss basics of cyber security environment tactics. A fundamental CPS solution for controlling large volumes of manned and unmanned air traffic is through using Automatic Dependent Surveillance Broadcast (ADS-B) and Internet Protocol (IP) technology. The main focus of earlier research was on CPS architecture, real-time control, security assurance, integration mechanism. The main advantage of general CPS architecture, based on Service-Oriented Architecture (SOA), is the integration flexibility of services and components. This model, based on "bottom up" initiative is to help secure a nation in a grass root. Our cyber strategy will provide prior decision of action to operate desired effects in cyberspace [19].

The Privacy Petri Nets (PPN) technique incorporates application dynamic behavior analysis with network traffic analysis. It presents a robust model which is more applicable to various applications and more meaningful to users. Private information leak has become serious and challenging problem to cyber security. PPN should be consisted of different privacy leak data sources and network connections to analyze the detail of private information leak. The analysis of a large-scale cyber network in which each component is either in a healthy state or an abnormal state. Private information leak mainly includes three categories: local file leaks, application associated data leaks and system associated data leaks. With the increasing size, diversity, and interconnectivity of the cyber system, intrusion detection faces the challenge of scalability and locating intrusions and anomalies in a large dynamic network with limited resources [18].

There are two basic approaches for intrusion detection, namely, active probing and passive monitoring. Active-probing based approaches need to choose judiciously, the components from the network for probing, in order to reduce network overhead. Passive-monitoring based approaches need to determine how to sample the network so that real-time processing of the resulting data is within the computational capacity of the IDS. Cyber security researchers aim to design and develop various cyber defence systems to secure information management systems against intentional and potentially malicious threats.

Solution for the various cyber security problems can be categorized into two: proactive and reactive solutions. Proactive approaches require user authentications, information protection,

and capable software for avoiding programming errors. In contrast, reactive security solutions detect intrusions based on the information from the log files and network flow, so that similar attacks can be prevented in the future. An intrusion detection system (IDS) monitors and restricts user access to the computer system by applying certain rules. These rules are based on expert knowledge extracted from skilled administrators who construct attack scenarios and apply them to exploit system. The intrusion detection problem is dynamic in nature. In other words, there is always the possibility that new attacks can happen and the system can fail to detect them because it has not learned patterns occurred in unknown attacks during the training phase [16].

Botnets are the main driver of cyber attacks, such as distributed denial of service (DDoS), information phishing and email spamming. Botnets are the engine for malicious activities in cyber space. These attacks are pervasive in nature and often cause great financial loss. Motivated by huge financial reward, attackers find it worthwhile to organize sophisticated botnets as attack tools. Botnets owners exhaust their strength to mimic legitimate cyber behavior by flying under the radar, flash crowd mimicking attacks on popular websites. In order to secure from the various botnets a statistical discrimination algorithm was proposed. The scheme was inspired from the various factors like, there are a lots of legitimate network events which do not involve a large number of users. Botnet owners do have the capability to perform perfect mimicking attacks, such as membership recruitment, performance degradation attacks and so on. In certain scenarios the botnet owners may cooperate to establish a super botnet so that it satisfies the sufficient number of conditions to execute mimicking attacks.

The security analysts (SA) are responsible for detecting cyber threats by perusing continual floods of data such as intrusion alerts and network logs. The researchers and the analysts face challenges which attempts to understand, measure, and impact of SA in the cyber arena. An adaptive risk management framework is capable of preventing, identifying and responding in critical time to threats. Mimicking the way immunity works in biological organisms the system can dynamically adapt to embrace new risk situations and can dynamically create and learn new risk models as it encounters new risk situations. A holonic Cyber security system is a system that can unfolds itself into an emergency response management infrastructure. The holonic cyber security system is capable of reacting in due time to unknown and new kinds of threats/attacks. A holonic system consists of three main types of holarchies: risk, infrastructure and support. All these holarchies dynamically interact through the inter agent

communication. Due to which the system is capable to learn, respond and adapt to new situations much like biological organisms adapt and respond to threats in their struggle for survival [22].

Cognitive task analysis (CTA) focuses on teams of analysts and the subsequent preliminary study conducted using a cyber defence simulation environment.CTA based on its findings built CyberCog. It is the system that can adapt to changing environment through self-organizing organic capability. The objective of CTA was to design a dynamic probing strategy that can minimize the long-term network cost incurred at all abnormal components. The phrase "risk management" has a broad definition and is applied in a number of diverse disciplines e.g. statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory. The CTA show that a cyber security defense analyst team can often be characterized as a group of individuals working independently with less communication or in a collaborative effort with team members. CTA identified three possible contributing factors to breakdown of team performance in the cyber security defense task: team structure, team communication, and information overload. The cyber security defense task must be restructured at the process level while utilizing new technologies and strategies to be team-based by sharing the workload and information efficiently, while interacting effectively to remedy the security threats. The CyberCog findings are emblematic of the findings in the CTA and only begin to scratch the surface of this vastly complex area, means to respond to emerging needs for safety and security in today's dynamic world[3].

2.3 IMPLEMENT CYBER SECURITY BEST PRACTICES

Protecting our network is a team effort, it requires the combined efforts of every citizens, employee and IT cyber security staff member. It is expected that everyone applies the three rules of data security: confidentiality, integrity and availability (CIA).Some useful best practices should be implement inside the organizations, offices, and homes are discussed below:

1**. Use "anti-virus software" and keep it up to date**. Make sure you have anti-virus software on your computer. Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be

sure to update your anti-virus software regularly. The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Most of the organizations owned networks are configured with antivirus software and centrally managed to receive regular virus definition file updates.

2. **Don't open e-mails or attachments from unknown sources**. Be suspicious of any unexpected e-mail attachments even if they appear to be from someone you know. A simple rule of thumb is that if you don't know the person who is sending you an e-mail, be very careful about opening the e-mail and any file attached to it. Should you receive a suspicious e-mail, the best thing to do is to delete the entire message, including any attachment. If you are determined to open a file from an unknown source, save it first and run your virus checker on that file, but also understand that there is still a risk. If the mail appears to be from someone you know, still treat it with caution if it has a suspicious subject line or if it otherwise seems suspicious. Also be careful if you receive many copies of the same message from either known or unknown sources. Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. When in doubt, delete all the complete materials including attachments. If you receive an e-mail from a trusted vendor or organization, be careful of phishing, a high-tech scam used to deceive consumers into providing personal data, including credit card numbers, etc.

3. **Protect your computer from Internet intruders - use "firewalls".** Firewall is an equipment of your computer. Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet.

4. **Regularly download security updates and "patches" for operating systems and other software.** Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes bugs are discovered in a program that may allow a criminal hacker to attack your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that they post on their web sites. You need to be sure you download and install the patches. Check your software vendors' web

sites regularly for new security patches or use the automated patching features that some companies offer. Ensure that you are getting patches from the correct patch update site. Many systems have been compromised this past year by installing patches obtained from bogus update sites or e-mails that appear to be from a vendor that provides links to those bogus sites. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you.

5. **Use hard-to-guess passwords**. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. Passwords will only keep outsiders out if they are difficult to guess. Don't share your password, and don't use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places. The golden rules of passwords are:

- A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters, symbols and numbers, e.g., xk2&LP97.
- Change passwords regularly, at least every 90 days.
- Do not give out your password to anyone. For enhanced security, use some form of two-factor authentication. Two-factor authentication is a way to gain access by combining something you know (PIN) with something you have (token or smart card).

6. **Back-up your computer data on disks or CDs regularly**. Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Many people make weekly backups of all their important data, and make sure you have your original software start-up disks handy and available in the event your computer system files get damaged.

7. **Don't share access to your computers with strangers**. Learn about file sharing risks. Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don't pay close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers.

8. **Disconnect from the Internet when not in use**. Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer, and if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet and help protect others for disconnect.

9. **Check your security on a regular basis**. When you change your clocks for daylight-savings time, reevaluate your computer security. The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year - do it when you change the clocks for daylight-savings. Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area.

10. Set Screensaver Passwords to 5 Minutes: As more and more of our information is stored on our computers and network storage, securing data is an increasing concern. Most of us do not log out of our computers when we leave our office for short periods of time. Rather than logging off, you can lock your computer by pressing Ctrl-Alt-Delete and selecting Lock Workstation. This will secure your computer and leave any programs currently running while you're away from your desk. You must re-enter your password to unlock the computer when you return, but the computer will not have to go through the complete login procedure. Another security feature is to have a screen saver that requires your password to unlock the computer. This feature is accessed by right-clicking in a blank portion of the desktop and selecting Properties. The Display Properties dialog box will open:

- Click the Screen Saver tab
- Make sure the On Resume, password protect box is checked
- Set a wait time of 5 minutes
- Click OK.

11**. Secure your online transaction**. When submitting your sensitive information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission. Also be sure that "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure," and indicates that communication with the webpage is encrypted.

- Don't reveal too much personal information online.

- Protect your laptop, smart phone, or other portable devices when travelling.
- Be aware that public computers and public wireless access are not secure.
- Understand if and how location data is used
- Do not e-mail sensitive data
- Dispose of information properly

2.4 CURRENT CYBER SECURITY ISSUES & CHALLENGES

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialised has seen the use of cyberspace expand dramatically in its brief existence. The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU).The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security [12].

The success of the Internet has partly been attributed to its relative openness and low barriers to entry. The uniqueness of the Internet in being an open structure with few barriers to entry is the outcome of the circumstances in which it was conceptualised and a result of the worldview of its initial champions. The fact that the technology did not belong to any one company saw the implementation of standards for its various protocols, which was responsible for continuing innovation and improvements of its capabilities. In the early stages of development of the Internet, much of the task of developing cyberspace was in the hands of line organisations such as the Department of Information Technology (DIT) at the national level or the ITU at the international level, and other expert bodies. While these organisations were competent in their own right, they were unable to bring a holistic perspective to the issue, given their domain-specific focus on issues. The Internet Engineering Task Force (IETF) was set up in 1986. It comprised a number of experts on various aspects of the Internet who worked through a cooperative consensus-based decision-making process. The Internet

Corporation for Assigned Names and Numbers (ICANN) was created in 1998 on similar principles to manage the Domain Name System (DNS), another key infrastructure of the Internet. Most of the ICANN's powers and functions were devolved to it by the US government, which either to controlled DNS. The US has had a major influence on the development of cyberspace by virtue of the fact that much of the initial infrastructure and use was centred in that country and it continues to be a major force in its development and use. The US has thus been in a position to fend off periodic attempts to challenge its supremacy, and those times when it has been forced to shed some of its control, as in the case of ICANN, it has done so very reluctantly. Some of the clauses within this resolution have been criticised as an attempt to increase control over content and information in the guise of securing cyberspace [13].

Today, organizations rely heavily on cyber space to reach out to new customers and geographies, drive new business models and enhance operational efficiencies. However, given the increase in the number and sophistication of cyber threats and attacks, it's very critical for them to understand the risk involved and the counter measures required to derive the desired benefits of cyber space adoption. Though there has been tremendous increase in awareness, technology capabilities, market and vendor focus on cyber security, some key challenges still remains:

- Evolving risk and attacks – Cyber space has evolved as the backbone for the survival of entire organizations and even entire countries and is now the basic channel for covert warfare and focused attacks.
- Increase in complexity and evolving technology landscape – With the introduction of mobility, de-parameterization and cloud adoption, new threat vectors are constantly evolving.
- Dynamic business environment – IT security is still regarded as a cost centre and more effort is required for it to be perceived as a business need and work in collaboration with business.
- Point solution approach – Various security solutions provide good protection against a specific security problem; however, interoperability between the various solutions is still an issue.
- Significant effort and expertise – Significant effort and expertise is required in deployment, management and fine-tuning of cyber security solutions.

2.5 CYBER THREATS

Cyber threats can be disaggregated, based on the perpetrators and their motives, into our baskets: cyber espionage, cyber warfare, cyber terrorism, and cyber crime. Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware. DOSS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning. Identity theft is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day.

Cyber threat is a threat that percolates or infiltrates through the use of computers , internet or interconnected communication devices and could comprise of information stealth, cyber warfare, virus attacks, cyber terrorism, hacking attempts , phishing, singly or in combination. Some traditional Types of Cyber Threats as:

2.5.1 CYBER WARFARE

There is no agreed definition of cyber warfare but it has been noticed that states may be attacking the information systems of other countries for espionage and for disrupting their critical infrastructure. The cyberspace has been declared the fifth dimension of warfare after land, air, oceans and space, and reserved the right to take all actions in response, including military strikes, to respond to cyber attacks against it. The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries. The concept of cyber deterrence is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution.

2.5.2 CYBER CRIME

Cyber crime is a term that covers a broad scope of criminal activity using a computer. Some common examples of cyber crime include identity theft, financial fraud, web site defacements and cyber bullying. At an organizational level, cyber crime may involve the hacking of customer databases and theft of intellectual property. Many users think they can protect themselves, their accounts, and their PCs with just anti-spyware and anti-virus software.

Cyber criminals are becoming more sophisticated and they are targeting consumers as well as public and private organizations. Therefore, additional layers of defense are needed. The effects of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year. All citizens, consumers, and employees should be aware of cyber threats and the actions they can take to protect their own information, as well as the information within their organization.

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber crime being in billions of dollars worldwide. While other countries are reporting enormous losses to cyber crime, as well as threats to enterprises and critical information infrastructure (CII), there are hardly any such reports coming out of India other than those relating to cyber espionage. Though the report of the National Crime Records Bureau (NCRB) for 2012 reported an increase of 50% in cyber crime over the previous year, the numbers were quite small in absolute terms. Similarly, there are relatively few reports of Indian companies suffering cyber security breaches of the sort reported elsewhere. Companies attribute this to the primacy placed on information assurance in the outsourcing business. Industry bodies such as the National Association of Software and Services Companies (NASSCOM) also attribute this to the fact that they have been at the forefront of spreading information security awareness amongst their constituents, with initiatives such as the establishment of the Data Security Council of India (DSCI) and the National Skills Registry. That said, cyberspace is increasingly being used for various criminal activities and different types of cyber crimes, causing huge financial losses to both businesses and individuals. Organised crime mafia have been drawn to cyberspace, and this is being reflected in cyber crimes gradually shifting from random attacks to direct targeted attacks. Cyber criminals are using innovative social engineering techniques through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. While large enterprises are ploughing more resources into digital security, it is the small enterprises and individuals that are falling prey to cyber crime, as evinced by the increasing number of complaints on consumer complaint forums. The low levels of computer security are also apparent in recurring statistics that show that India is the third-largest generator of spam worldwide. A continuing trend for Internet users in India was that of the threat landscape being heavily infested with worms and viruses. The percentage of worms and viruses in India was significantly higher than the Asia-Pacific regional average.

According to CERT-In, India sees an average of 788 bot-infected computers per day. With regard to web-based attacks, India has seen a significant increase and has ranked seventh, with 3% of the world attacks, and second in the Asia-Pacific region.

2.5.3 CYBER TERRORISM

Cyberspace has been used as a conduit for planning terrorist attacks, for recruitment of sympathisers, or as a new arena for attacks in pursuit of the terrorists' political and social objectives. Terrorists have been known to have used cyberspace for communication, command and control, propaganda, recruitment, training, and funding purposes. While cyber hactivism cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of cyber terrorism both in terms of methods and end goals.

2.5.4 CYBER ESPIONAGE

Instances of cyber espionage are becoming quite common, with regular reports of thousands of megabytes of data and intellectual property worth millions being exfiltrated from the websites and NWs of both government and private enterprises. While government websites and NWs in India have been breached, the private sector claims that it has not been similarly affected. The multiplicity of malevolent actors, ranging from state-sponsored to hactivists, makes attribution difficult, governments currently can only establish measures and protocols to ensure confidentiality, integrity and availability (CIA) of data. Law enforcement and intelligence agencies have asked their governments for legal and operational backing in their efforts to secure sensitive networks and to go on the offensive against cyber spies and cyber criminals who are often acting in tandem with each other, and probably with state backing. Offence is not necessarily the best form of defence in the case of cyber security, as seen in the continued instances of servers of the various government departments being hacked and documents exfiltrated.

2.5.5 EMERGING TRENDS AND THREATS FOR 2013

Cyber threats in coming days are rapidly increase and day by day new threats are coming, so we need to aware of the some common cyber threats for coming times .Cyber security guys say, it will only get worse in 2013 through the cyber threats. Briefly explained some new trends of cyber threats [6]:

1. Targeted Attacks: While the threat landscape is still dominated by random, speculative attacks designed to steal personal information from anyone unlucky enough to fall victim to them, targeted attacks have become an established feature in the last two years. Such attacks are specifically tailored to penetrate a particular organization and are often focused on gathering sensitive data that has a monetary value in the 'dark market'. Targeted attacks can often be highly sophisticated. But many attacks start by 'hacking the human', i.e. by tricking employees into disclosing information that can be used to gain access to corporate resources. Any organization can become a victim. All organizations hold data that is of value to cybercriminals; and they may also be used as 'stepping-stones' to reach other companies.

2. More Hactivism : Last year's attacks included the DDoS attacks launched by Anonymous on government websites in Europe, following the government's announcement that it would support the Anti-Counterfeiting Trade Agreement(ACTA); the hacking of the official Formula one website in protest against the treatment of anti-government protesters in Bahrain; the hacking of various oil companies in protest against drilling in the Arctic; the attack on Saudi Aramco; and the hacking of the French Euromillions website in a protest against gambling. Society's increasing reliance on the Internet makes organizations of all kinds potentially vulnerable to attacks of this sort, so 'hactivism' looks set to continue into 2013 and beyond.

3. Cyber Espionage & Warfare: Stuxnet pioneered the use of highly sophisticated malware for targeted attacks on key production facilities. However, while such attacks are not common place, it's now clear that Stuxnet was not an isolated incident. We are now entering an era of cold 'cyber-war', where nations have the ability to fight each other unconstrained by the limitations of conventional real-world warfare. Looking ahead we can expect more countries to develop cyber weapons.

4. Big Brother Watching Even More: This will include using technology to monitor the activities of those suspected of criminal activities. This is not a new issue – consider the controversy surrounding 'Magic Lantern' and the 'Bundestrojan'. More recently, there has been debate around reports that a UK company offered the 'Finfisher' monitoring software to the previous Egyptian government and reports that the Indian government asked firms (including Apple, Nokia and RIM) for secret access to mobile devices. Clearly, the use of legal surveillance tools has wider implications for privacy and civil liberties. And as law enforcement agencies, and governments, try to get one step ahead of the criminals, it's likely that the use of such tools – and the debate surrounding their use – will continue.

5. Increase in Malware: The wide use of mobile devices, while offering huge benefits to a business, also increases the risk. Cloud data can be accessed from devices that may not be as

secure as traditional endpoint devices. When the same device is used for both personal and business tasks, that risk increases still further.

6. Privacy Rights Eroding: The value of personal data – to cybercriminals and legitimate businesses – will only grow in the future, and with it the potential threat to our privacy increases.

7. Cyber Extortion: This year we have seen growing numbers of ransomware Trojans designed to extort money from their victims, either by encrypting data on the disk or by blocking access to the system. Until fairly recently this type of cybercrime was confined largely to Russia and other former Soviet countries. But they have now become a worldwide phenomenon, although sometimes with slightly different modus operand. In Russia, for example, Trojans that block access to the system often claim to have identified unlicensed software on the victim's computer and ask for a payment. In Europe, where software piracy is less common, this approach is not as successful. Instead, they masquerade as popup messages from law enforcement agencies claiming to have found child pornography or other illegal content on the computer. This is accompanied by a demand to pay a fine. Such attacks are easy to develop and, as with phishing attacks, there seem to be no shortage of potential victims.

8. Apple under Attack: Attacks on the Mac OS has been growing steadily over the last two years; and it would be naive of anyone using a Mac to imagine that they could not become the victim of cyber crime. It's not only generalized attacks – such as the 700,000-strong Flashfake botnet – that pose a threat; we have also seen targeted attacks on specific groups, or individuals, known to use Macs. The threat to Macs is real and is likely kept growing.

9. Android, Even Worse: Mobile malware has exploded in the last 18 months. The lion's share of it targets Android-based devices – more than 90 per cent is aimed at this operating system. The appearance of the 'Find and Call' app earlier this year has shown that it's possible for undesirable apps to slip through the net. But it's likely that, for the time being at least, Android will remain the chief focus of cyber criminals. The key significance of the 'Find and Call' app lies in the issue of privacy, data leakage and the potential damage to a person's reputation. This application was designed to upload someone's phone book to a remote server and use it to send SMS spam.

10. Un-Patched Exploits in Java: One of the key methods used by cyber criminals to install malware on a computer is to exploit un-patched vulnerabilities in applications. This relies on the existence of vulnerabilities and the failure of individuals or businesses to patch their applications. Java vulnerabilities currently account for more than 50 per cent of attacks, while Adobe Reader accounts for a further 25 per cent. Cyber criminals will continue to exploit Java

in the year ahead. It's likely that Adobe Reader will also continue to be used by cyber criminals, but probably less so because the latest versions provide an automatic update mechanism.

11. Ransomware: Ransomware is a type of malware that is used for extortion. The attacker distributes malware that will take over a system by encrypting the contents or locking the system; the attacker then demands money from the victim in exchange for releasing the data and/or unlocking the system. Once payment is delivered, the attacker may or may not provide the data or access to the system. Even if access is restored, the integrity of the data is still in question. This type of malware and delivery mechanism will become more sophisticated in 2013.

12. Social Media: Use of social media sites has grown beyond just sharing personal information, such as vacation photos and messaging. These sites are being increasingly used for advertising, purchasing and gaming. For 2013, attackers will look to exploit this volume and variety of data being shared to credentials or other Personally Identifiable Information (PII), such as social security numbers.

13. Social Engineering: Social engineering tactics—including the use of rogue anti-virus to entice users into clicking on malicious links—will continue. Experts also anticipate that in 2013 we will also see a growth in fake registry cleanup, fake speed improvement software, and fake back-up software mimicking popular personal cloud services.

14. Advanced Persistent Threat: Advanced Persistent Threat (APT) refers to a long-term pattern of targeted hacking attacks using subversive and stealthy means to gain continual, persistent exfiltration of data. The entry point for these types of espionage activities is often the unsuspecting end-user or weak perimeter security. Whether focused on exploiting vulnerable networks or unsuspecting end-users, APT will remain a consistent threat to networks in 2013.

15. Spear Phishing Attacks: Spear-phishing is a targeted and personalized attack in which a specific organization or an individual is the target. Spear phishing is a deceptive communication, such as e-mail, text or tweet, targeting a specific individual, seeking to obtain unauthorized access to personal or sensitive data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators seeking financial gain, trade secrets or sensitive information. Spear phishing is often the nexus to cyber espionage/APT and will continue to increase this year. These attacks will utilize information about the user email addresses, which are similar to those of their acquaintances to entice the users to either divulge sensitive information or download a malicious file.

16. Mobile and Wireless attack (Wi-Fi and Bluetooth): They can be launched by pretending to be someone/something else such as Service Set Identifier (SSID) attacks, malicious association, MAC spoofing, man in the middle attack, Wired equivalent privacy , Wireless Application Protocol (WEP WAP) cracking etc or they can result in direct denial of service attacks such as insertion attack , encryption attack and jamming. The use of mobile devices will continue to grow in 2013, consequently, so too will the volume of attacks targeted to these devices. Every new smart phone, tablet or other mobile device provides another window for a potential cyber attack. Closely tied to the trend of more smart phones and tablets being deployed in the enterprise will be the influx of new apps for those devices. Location-based mobile apps and games all pose potential threats. The risks include access to information such as physical location or contacts lists, as well as the ability for the apps to download malware, such as key loggers or programs that eavesdrop on phone calls and text messages. Hackers are quickly learning how to harvest legitimate applications and repackage them with malicious code before selling/offering them on various channels to the unsuspecting user.

17. Search Engine Optimization (SEO) Poisoning: Cyber criminals will continue to take advantage of the 24-hour news cycle to target visitors searching on the most popular keywords or sites and infect users via sites designed to look like legitimate news services, Twitter feeds, Face book posts/emails, LinkedIn updates, YouTube video comments, and forum conversations.

18. Application Vulnerabilities: Many applications are deployed without adequate security controls. As more applications are developed and deployed across multiple platforms, cyber criminals will increasingly target these applications to gain access to data, due to vulnerabilities attendant in the applications.

19. Cloud Computing: The move to cloud computing will continue as organizations strive to save money and add flexibility to their operations. Due to the aggregate volume of data that is resident in the cloud computing environments, we anticipate that it will be a target that will attract cyber criminals. They will identify new methods to infiltrate these environments and gain access to data.

20. Increasing use of Apple Macintosh Computers: As the use of Apple Macintosh Computers increase, they may become larger targets for cyber criminals looking to take advantage of a growing pool of users and exploit potential vulnerabilities in the operating system.

21. SPAM: It is the flooding of internet with the same message in an attempt to force the message on the people who do not otherwise intend to receive such a mail.

22. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack: Dos or DDoS is an attempt to make the computer resource unavailable to its intended users.

23. Phishing and Pharming (Identity Theft and DNS attack): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Pharming can also be called as "Phishing without a lure". It is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.

24. Botnets: It is also known as a zombie army in which a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions to other computers on the Internet.

25. Instant Messaging (IM) attack such as spIM and Peer to Peer (P2P) attack: Spam over instant messaging (spIM) is an unsolicited e-mail that arrives on a personal computer screen in the form of an instant message. P2P programs are sharing computer resources such as files, CPU cycles and application hence it can be used to launch an attack on the system.

26. Root kits: They are software that is designed to hide or obscure the fact that the system has been compromised. Root kit enables an attacker to take control of the operating system by opening a backdoor to the system. They also act to evade the operating systems security scan and antivirus software giving the user a false sense of safety.

27. Web Application attack: These attacks exploit the vulnerabilities of poorly programmed web pages. Some of the most popular web application attacks primarily for PHP applications are Remote code execution, SQL injection, Format string vulnerabilities, cross site scripting (XSS) and user name enumeration.

28. Hacking with Google: Google hacking involves using advance operators in the Google search engine to locate specific strings of text within search results. Some of the more popular examples are finding specific versions of vulnerable Web applications.

CHAPTER: 3

PROPOSED "UNIFIED MODEL FOR INTEGRATED CYBER SECURITY (UMICS)" ANLYSIS

3.1 UMICS ANALYSIS

Different organizations have different expectations on the tasks and responsibilities of the previously developed cyber security model. The differences are generally concerning the management and supervision of the responsibilities. The key and primary role of the UMICS across the organization would be the same and include the following responsibilities:-

- Collecting and filtering computer network traffic,
- Analyzing the traffic for suspicious or unexpected behavior,
- Discovering system misuse and unauthorized system access,
- Reporting to the appropriate parties and working to prevent future attacks.
- Centrally monitoring the whole system

UMICS consult the output of an automated system that provide them with network data that have been automatically collected and filtered to focus the UMICS attention on data most likely to contain clues regarding attacks. These automated systems such as firewalls, border gateways, intrusion detection systems (IDSs), anti-virus systems and system administration tools produce log files and metadata that the UMICS can inspect to detect suspicious activities.

We classify the UMICS activities or functions into three generic groups: reactive, proactive, and security quality management.

- Reactive - Reactive activities are triggered by a preceding event or request such as a report of wide-spreading malicious code or an alert identified by an Intrusion Detection System (IDS) or network logging system. Looking to the past, reactive tasks include reviewing log files, correlating alerts in search of patterns, forensic investigation following an attack and identification of an attacker who has already penetrated the network.
- Proactive – These activities are undertaken in anticipation of attacks or events that have not yet manifested. Proactive tasks include identifying new exploits before they have been used against the defended network, predicting future hostile actions and tuning sensors to adjust for predicted attacks.
- Security quality management- These activities are information technology (IT) services that support information security, but that are not directly related to a specific security event; these include security training, product evaluation, and disaster recovery planning.

3.1.1 INTRUSION DETECTION SYSTEM (IDS) ALERTS

Usually a sign or an alert of a security breach gets the analyst to start with the incident handling process of a reactive nature. The Intrusion Detection Systems may have the automated incidence response in place for some kinds of attacks, but for others the onus is on the analyst to respond. Alerts from Intrusion Detection System (IDS) [8] [Figure: 3.1.1]:

- Antivirus software alerts
- Web server crashes.
- Users complaining of slow access to hosts on the Internet.
- The system administrator sees a filename with unusual characters.
- Users call the help desk to report a threatening e-mail message.
- The host records an auditing configuration change in its log.
- The application logs multiple failed login attempts from an unfamiliar remote system.
- The e-mail administrator sees a large number of bounced e-mails with suspicious content.
- The network administrator notices an unusual deviation from typical network traffic flows.
- Web server log entries that show the usage of a Web vulnerability scanner

- An announcement of a new exploit that targets a vulnerability of the organizations mail server
- A threat from a hactivism group stating that the group will attack the organization.

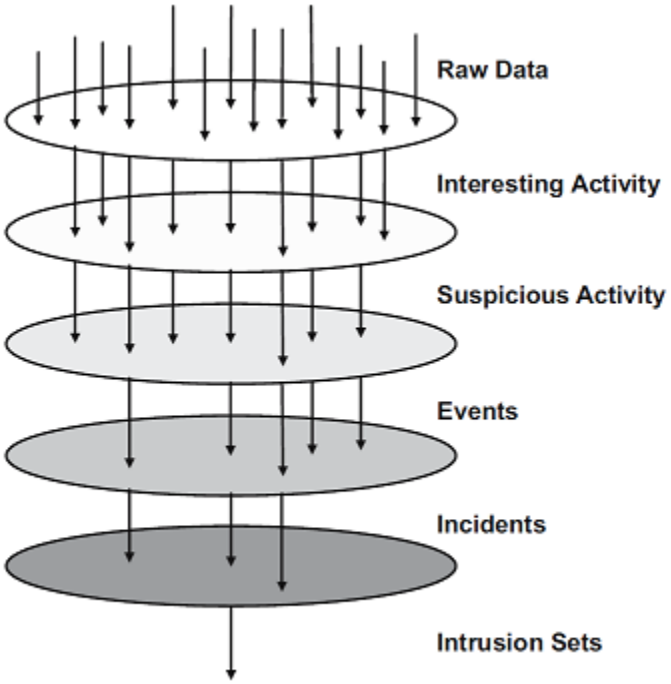

Figure: 3.1.1 Data Hierarchy as Data are Transformed into Security Situation Awareness

Cyber-attacks are becoming more advanced like sKyWiper (Flame) is one of the most sophisticated and complex malware ever found ,and Stuxnet was designed to exploit more than 4 zero-days vulnerabilities. More focused and targeted, especially at financial institutions, political, military establishments and intellectual property.

- Stuxnet includes a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems.
- RSA Advanced persistent attack which focuses on getting confidential data from internal servers.
- Zeus Botnet primarily focuses on financial frauds
- Attacks from Hacktivists like anonymous and lulzsec.

The cyber security UMICS get filtered raw data from the Intrusion Detection System (IDS). This data could be network packet traffic, net flow data or host-based log data. The IDS makes initial filtering decisions based on the pre-loaded attack signatures.

3.1.2 CYBER SECURITY TEAM MODEL ANALYSIS

Cyber security team model analysis is based on the group responsibilities. Intrusion sets are sets of related incidents. Intrusion sets commonly arise at the community level when Computer network data (CND) analysts can review incidents from different reporting organizations and group these incidents based upon shared features such as source and destination IP addresses, time, attack characteristics or attacker behavior. When a CND community suspects that separately reported incidents emanate from the same source or sponsor, the community groups the incidents into an intrusion set [Figure: 3.1.2]. Just as incidents are almost universally a formal analytic product, the designation of an intrusion set is an official decision point for the organizations. The community then increases attention and resources to detecting, understanding and responding to relevant activity. This process can include decisions about tuning data collection and IDS signatures to catch all new related data.

- Analysts generally work at IT support department or Cyber Security department. Duty analyst or administrators prioritize alerts; communicate with security analyst of the incidents.
- Analysts perform further investigations on the incidents.
- Any organization dealing with sensitive information employs a computer security analyst.

Incident response team structure models fall into one of three categories:

- Central Incident Response Team. A single incident response team handles incidents throughout the organization. This model is effective for small organizations.
  Distributed Incident Response Teams. The organization has multiple incident response teams, each responsible for handling incidents for a particular logical or physical segment of the organization. This model is effective for large organizations. However, the teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams.

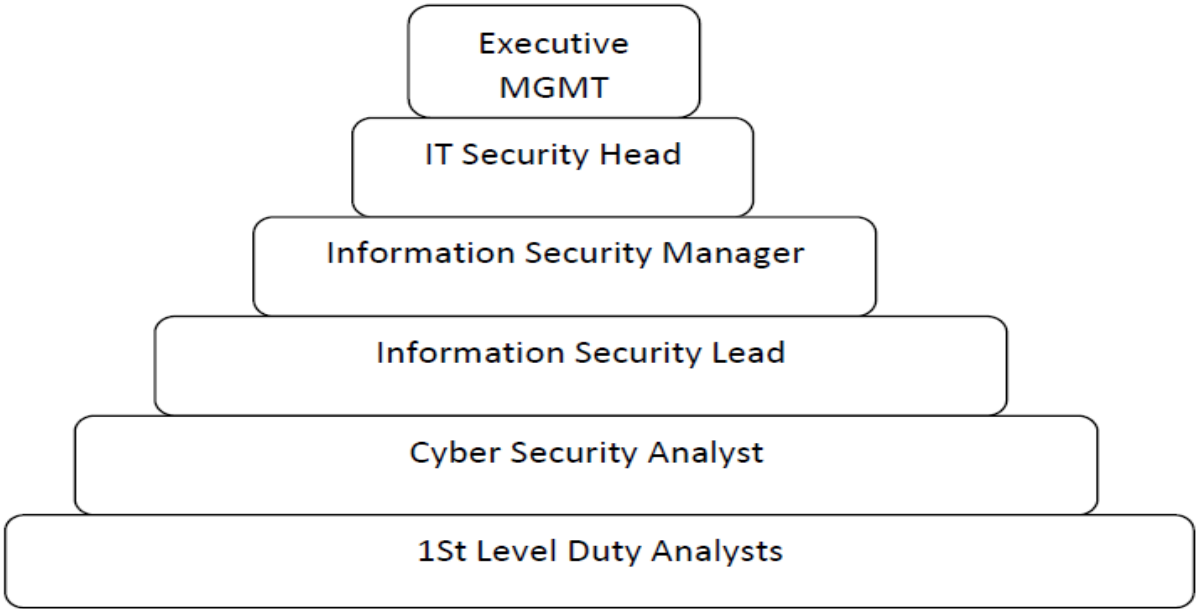

Figure: 3.1.2 Generic Hierarchy Team Models

- Coordinating Team. An incident response team provides guidance and advice to other teams without having authority over those teams

3.1.3 DEPENDENCIES WITHIN AN ORGANIZATION

Some Key factors are use in UMICS system those are relates each other and dependents of their functions [Figure: 3.1.3].

- Management
- Information Security
- Telecommunications
- IT Support
- Legal Department
- Public Affairs and Media relations
- Human resources
- Business Continuity Planning
- Physical Security and facilities management.

Figure: 3.1.3 Community Level Incident-Related Communications within a typical Organization

3.1.4 UMICS ANALYSIS TOOLS

Many of the tools are available to network security engineers and present specific pieces of information in textual form. The classified these resources into the four main categories:

(1) Global intrusion detection tools monitor and analyze network traffic data for suspicious patterns and generate alerts for patterns that are matched.
(2) Logs containing detailed information, coupled with the engineers expertise helps network security engineers to understand and assess the situation when an intrusion occurs. Typically, engineers filter through the data using textual commands in a computer "shell".
(3) Public information sources provide details of the latest intrusions and attacks. It should be kept up-to date.
(4) Code Samples - enable engineers to better understand an intrusion as well as help engineers to find vulnerabilities in the network that a given intrusion exposes.

Some of the most popular tools used by the cyber security analyst are as follow:-

1. **Snort :**
   - This lightweight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks.

- Through protocol analysis, content searching, and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior.
- Snort uses a flexible rule-based language to describe traffic that it should collect or pass, and a modular detection engine.

2. **OSSEC:**
   - Open Source Host-based Intrusion Detection System.
   - It performs log analysis, file integrity checking, policy monitoring, root kit detection, real-time alerting and active response.
   - It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows.
3. **BASE (Basic Analysis and Security Engine):**
   - It is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls, and network monitoring tools.
   - Its features include a query-builder and search interface for finding alerts matching different patterns, a packet viewer/decoder, and charts and statistics based on time, sensor, signature, protocol, IP address, etc
4. **Sguil :**
   - Its main component is an intuitive GUI that provides real-time events from Snort.
   - Facilitate the practice of Network Security Monitoring and event driven analysis of IDS alerts.
5. **BackLog:**
   - A Windows NT service to collect and process Event Log information.
6. **SNARE - System intrusion Analysis & Reporting Environment**
   - provides host-based intrusion detection for Linux, including graphical configuration, monitoring, and reporting tools:

3.1.5 CYBER SECURITY ANALYSTS RESPOND TO AN INCIDENT

The response to an incident can be automated by the IDS itself using “Honey Pots” and “Padded Cell Systems”, or it can be done by the cyber security analyst. In the latter case the response of a cyber security analyst to an incident may be as straightforward as blocking a source IP address, or as complex as “caging” or “fish bowling” an attacker inside the network to observe the attacker in action. Each of these methods is described below:-

Automated response:

Honey Pots: They are decoy systems filled with fabricated information designed to:

- Divert an attacker from accessing critical systems
- Collect information about the attackers activity,
- Encourage the attacker to stay on the system long enough for administrators to respond and get data on new trends and attack tools.
- Provide an environment that a legitimate user of the system would not access. Thus, any access to the honey pot is suspect.
- Honey Pot system also has sensitive monitors and event loggers that detect these accesses and collect information about the attackers' activities.

Manual response:

- **Padded Cell Systems**
  - A padded cell operates in tandem with traditional IDS. On detecting an attack the IDS seamlessly transfers the attackers to a special padded cell host which is a simulated environment where they can cause no harm.
  - Like the Honey Pot they are well-instrumented and offer unique opportunities to monitor the actions of an attacker.

- **Fish bowling**
  - Sometimes a target will be cut off from the outside world after an attack, and then reconnected with special access control measures taken to limit an intruder's maneuverability. This is called "fish bowling" a target.

3.2 UNIFIED APPROACH FOR CYBER SECURITY MONITORING AND MANAGEMENT SYSTEM

The unified approach for cyber security monitoring system is required in the current time, because this approach is a combination of all robust and reliable solutions of the integrated

cyber security techniques. Despite reasonable investment in security tools and technologies, several successful attacks have proved that something more needs to be done to effectively detect and manage the growing numbers of threats. One of the major causes is the lack of synergy between various functions and tools within the security domain itself and across layers including physical, network, user, data and application security. Hence, in order to evolve a successful response strategy for cyber security, it is important to look at all these layers holistically and leverage the information available at every layer to develop an overall threat and response model [11].

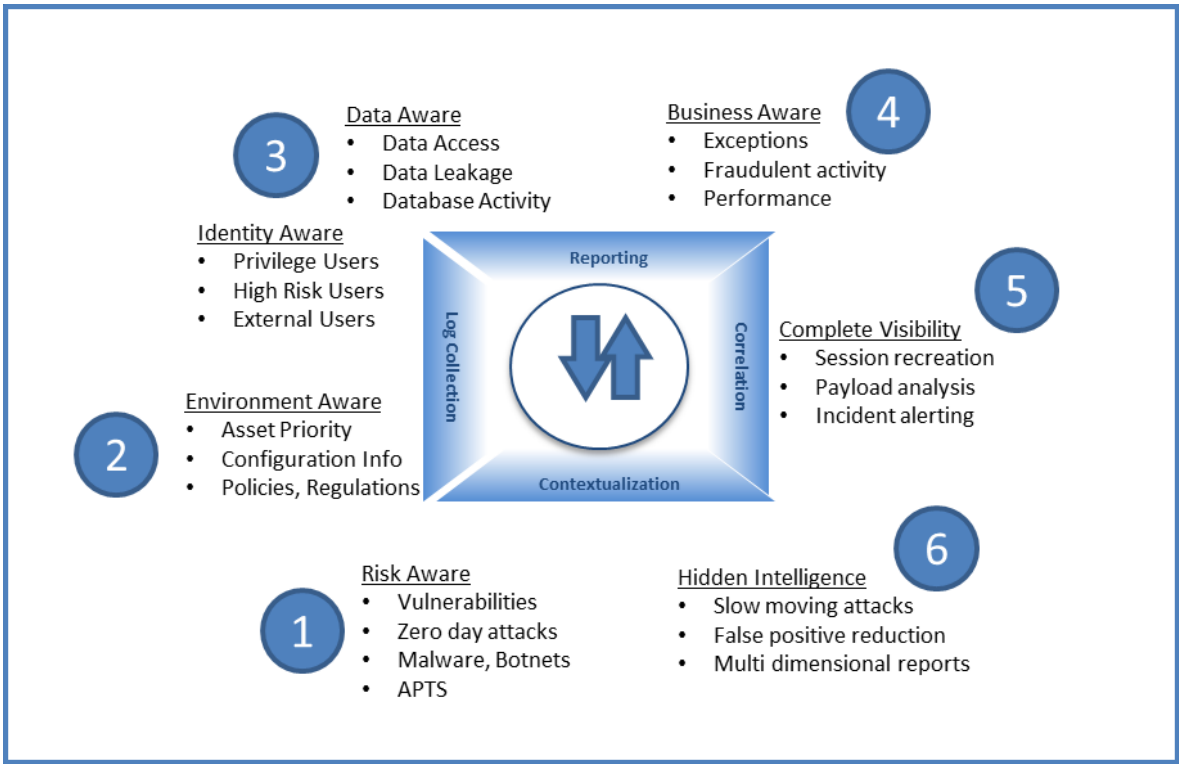

Figure: 3.2 Unified Approach to Cyber Security Monitoring System

In order to ensure a unified and holistic approach to cyber security, it's important to convert data available across various layers and across different functions/tools into real actionable intelligence. Some of the latest tools such as security information and event management (SIEM) have evolved on this premise and can serve as a basic building block for a unified framework [Figure:3.2].

The various critical steps are involved in building a unified cyber security monitoring and management frameworks as follow:

Step 1 - Risk Awareness

The most critical aspect of cyber security is to understand existing and emerging risks and threats to the business.

A risk based approach will not only ensure the optimum use of investments but will also provide clear and accurate visibility of current posture. Being risk aware broadly means:

- Visibility of the existing risks – leveraging vulnerability assessment, penetration testing, configuration audits, data, applications and identity handling policies and processes etc.
- Intelligence on emerging threats – leveraging threat intelligence related to emerging attacks, known sources and patterns of attacks, targeted attacks on the industry segments in which the organization is operating.

Risk assessment should form the basis of all ongoing and new investments. It is also important to design all the management and monitoring processes in accordance with the identified risk to ensure correct categorization, prioritization and response to any potential security threat.

Step 2: - Environment Awareness

Environment details serve as a fundamental element for the overall cyber security monitoring and management program. Asset information and software/application details from configuration management data base (CMDB), patch level details for patch management database, IP addressing schemes and network topology, business assets by priority, allowed software and applications, applicable policies and compliance regulations not only determine the level of security required and use cases but also help in responding quickly to any suspicious/confirmed incidents.

Step 3: - Identity and Data Awareness

The two most critical assets of any organization are its users and data. It's imperative for any cyber security framework to leverage and utilize the data and identity information to be able to protect against cyber threats.

- Identity and access management (IAM) solutions deployed in most organizations not only manage the entire lifecycle of users but can also provide information related to different categories of users including administrators, super users, contractors etc.
- Various data security solutions like data leakage protection (DLP) and database activity monitoring (DAM) can help track and monitor any unauthorized and suspicious use or leakage of data.

The integration of identity and data information in the framework will help to define the right level of data access levels, track and monitor privileged and disgruntled user activities, identify unauthorized entitlement changes and unauthorized data access/loss.

Step 4: - Business Awareness

Most of the current efforts in cyber security monitoring and management focus more on the infrastructure, host layers and security products. While these are critical elements, they exist solely to support business and business applications. It is important for the security team to understand the business context and build capabilities to detect and respond to any threats that can impact business applications. The traditional security tools do not have the integration and inspection capabilities for business contexts. In order to extract and use the information relevant to security, a separate intelligence engine is required. Such an engine should have the ability to look at transactions logs and audit logs to determine fraudulent activities and anomalous patterns and correlate this information with other layers to identify relevant threats and attacks.

Step 5: - Content Visibility

Security tools operate at different levels when it comes to the logging of actual content. While a SIEM solution typically works at the audit log level, an Intrusion Detection and Prevention Systems solution actually logs the entire packet detail at the network level. Many times, working only at the log level or isolated packet level does not provide the complete context for getting the desired level of visibility.

In order to build complete visibility across the network, details of actual data traversing the network can answer most of the requirements including identification of threats and

anomalous behavior, faster incident response and forensic and legal analysis. Such a solution has the ability to capture all the traffic traversing the network across the desired segments, create alerts on suspicious behaviours and recreate the complete session details to pin point the exact issue.

Step 6: Hidden Intelligence

Though SIEM tools and packet capturing tools have solved the issue of collecting and storing data for purposes of reporting, investigation etc, the amount of data generated in today's organizations can easily overload these tools and prevent any intelligence from being generated. Big Data platforms are evolving as very useful tools to address a lot of business intelligence and data mining applications and it is also possible to use these platforms for the purpose of security intelligence. Using Big Data platforms and tools, it is now possible to generate trends and carry out pattern analysis over a very large set of data, which can help in identification of slow moving attacks, building statistical machine learning models for predictive behavior analysis, identify any bottlenecks with regard to capacity, performance, availability etc.

Most importantly, for any cyber security solution to work, it must be managed effectively and evolve continuously. Deployment of point solution products and security technologies do not serve the purpose if they are not continuously updated and fine-tuned. Similarly, the overall cyber security framework should be capable of being upgraded and flexible enough to add new innovations, scale to meet new technology architecture like cloud, mobility and evolve to counter the latest emerging threats.

CHAPTER: 4

PROPOSED “UMICS” APPROACHES

4.1 UMICS APPROACHES OVERVIEW

The main objective of our work is to analysis, design and develop a unified model for integrated cyber security (UMICS) monitoring system that integrates a number of component techniques to collect time-series situation information, perform intrusion detection, keep track of event evolution, and characterize and identify security events so corresponding defense actions can be taken in a timely and effective manner. The integration of Cyber Panel technologies from the different areas into an advanced cyber defense systems Integrated Cyber Panel System .The Integrated Cyber Panel System is designed to provide cyber awareness and control for survivability. The system helps the operator defend the enclave against cyber attacks and maintain mission-required enclave functionality. The successful executions of many commercial, scientific, and military applications require timely, reliable, and accurate information flow in cyber space to support online transactions and remote operations. Developing effective security monitoring mechanisms to provide cyber situation awareness has become an increasingly important focus within the network research and management community. However, providing complete cyber situation awareness based on low-level information abstracted from raw sensor data is extremely challenging primarily because situation information is typically incomplete and imperfect, security events are constantly evolving over time, space, scale, and function, and the number and type of cyber attacks are practically immeasurable. It integrates technologies and concepts from the following integrated cyber security panel areas:

- Attack Sensing and Warnings
- Automated and Visual Alert Correlation
- Response Formulation and Evaluation
- Cyber Warfare Strategies and Tactics
- Database server
- Threat Evaluator

- Cyber Security Analysts
- Cyber Sensors
- Unified Threat Management (UTM)
- Next Generation –Intrusion Detection System(NG-IDS)
- Early Warning System
- Cyber Warfare (CW) Strategies
- Federated Cyber Defence System (FCDS)

Many infrastructure components have been developed to facilitate integration of these technologies including high-level models of the network and mission and common underlying communication tools. Cyber Panel technologies provide either awareness or response functionality. Situation awareness technologies include:

- Sensors that monitor for attack activities and system status.
- Correlators that provide alert filtering, clustering, prioritizing, and classifying.
- Situation selectors that correlate observations with mission knowledge to identify situations of interest.

Situation response technologies include response recommenders that evaluate alternatives and recommend responses in light of the mission and response managers and actuators that implement the responses. Many of these components rely extensively on a knowledge base that describes the network and mission being defended.

The technology of Cyber Security Monitoring (CSM) is based on observation, experience, and classification of attacks, vulnerabilities, and countermeasures. There exist a large number of commercial and government off-the-shelf tools and a significant amount of research and development efforts in CSM. A detection method falls into one of two categories using either statistical deviation or pattern matching. The proposed CSM system models security events in a graphical form of correlation networks and applies graph matching techniques for event identification.

We use sensors that are distributed in both networks and systems to collect time-series measurements of various event indicators. Each sensor makes a local threshold-based binary decision on the occurrence of an intrusion or security event and sends its decision together

with the raw event indicator measurements to a front-end data centre. Based on the local votes, the intrusion detector makes a global intrusion detection decision using a hard sensor fusion algorithm. When an alarm signal is raised, the correlation engine is invoked to construct an event indicator correlation matrix from time series raw situation measurements collected by sensors up to the current time step, which is then processed by the RMT based component to construct a correlation network of event indicators. Note that the inherent nature of a certain security event is captured in its correlation network that establishes the true relationships between all pairs of event indicators.

The graphical representation of the current security event is then compared to those of known events stored in a database to identify the event type based on network similarity measured by graph matching techniques. This security monitoring process is executed at a certain time interval in an adaptive manner. Sensor data are accumulated at more time steps as the event evolves, resulting in more robust and cognitive network representations and therefore more accurate event detection and identification. The system adaptively determines the duration as well as the amount of raw data that has to be collected and processed. We investigated an adaptive cyber security monitoring system that integrates a number of component techniques including intrusion detection based on decision fusion, correlation computation of event indicators, network representation of security events based on RMT, and event identification based on graph matching and network similarity measurement, in a unified framework.

The system of Integrated Cyber Security (ICS) protection should be invariant to a device through which a user gets an access to ICS. At the same time it is necessary to ensure a secure access to all resources in the cloud as a part of cyberspace. From this it follows that the security as a service may also be imposed to the cloud, giving customers a web interface to integrated cyber security system [1].

In order to meet the requirements for ICS security system the proposed model includes the set of modules on the client side and in the cloud. The process of threats analysis and detection imposed in the Security Cloud. On the user’s side there are tools of interaction with the cloud, as well as to monitor and protect integrity of the user's data and operational system. Using Internet browser to run security modules this model becomes platform-independent, as well as it does not depend on a device performance, which can be a smart phone or a tablet PC.

As a result a model of security system was proposed based on analysis of contemporary cyber threats and cloud technologies, thereby creating a safe virtual environment for a user. This model is invariant to OS platform and device performance, because of using security services in the cloud aimed to analyze and detect a cyber threat, as well as provides a range of services such as vaccination, certification and tokenization to ensure certain level of user's security. At the same time on the client side, users will be able to easily manage their safety profile through the Internet browser.

Cyber security UMICS model recreates the interaction and team collaboration found at cyber security departments in commercial and government organizations between the first responders and cyber security analysts. Cyber security techniques that protect our network from outside and inside cyber attacks are becoming more useful day by day, with the increase cyber threats and crimes.

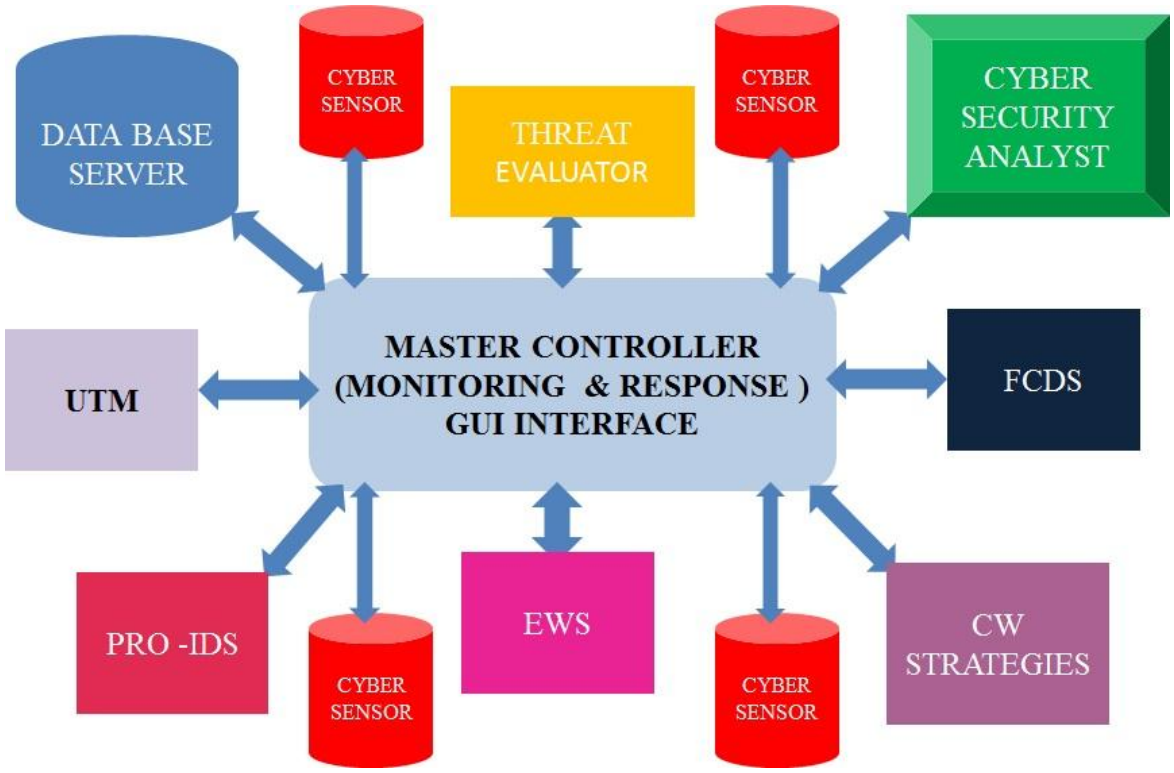

Figure: 4.1 Unified Model for Integrated Cyber Security (UMICS) Monitoring System

Some of the techniques are reviewed and analysis, which are very efficient, reliable, high accuracy, robust, and quick response. Major Cyber security techniques are integrated in UMICS system as shown [Figure: 4.1].

The major techniques and components of the UMICS model are:

1. Database server
2. Threat Evaluator
3. Cyber Security Analysts
4. Cyber Sensors
5. Unified Threat Management (UTM)
6. Next Generation –Intrusion Detection System(NG-IDS)
7. Early Warning System
8. Cyber Warfare (CW) Strategies
9. Federated Cyber Defence System (FCDS)

4.1.1 UMICS SIMULATOR OPERATION

The experimenter initiates the simulation exercise on the Master Controller and monitoring system. The Master Controller upon initiation, queries the SQL database server for an attack scenario along with its corresponding attack events. The attack events also contain false positives events that have no impact on the actual attack. Upon receiving the attack scenario and the corresponding events from the SQL database server, the Master controller sends the attack scenario retrieved to the participant's screen. The participants use the events provided to them and will try to match the symptoms to those events. If the participant is able to match the events to the symptoms, the participant publishes those events. On publishing an event, the event gets added to the suspicious events section on the common screen seen by all participants. The participant publishing an event as suspicious corresponding to his/her specialization could also recall the events, if the participant feels that the event has been added by mistake [7].

The other options available to the participant for the events are; mark an event as unimportant and to send an event to a particular participant. If a participant marks an event as unimportant, the event is removed from the participant's event log and gets added to the unimportant event section on the participants screen. The unimportant events can later be added to the participant's event log by using the "back" button corresponding to the event in the unimportant event section of the participants screen.

The option for a participant to send an event to other participant enables the participant to convey the message to the other participant that he/she has the events corresponding to the symptoms which need to be found and is published on the common screen by the other participant. This also increases collaboration between participants in trying to identify the potential attack and also provides a mechanism to record the interaction between participants. The participant receiving the event has the freedom to either accept the event or reject the event. On accepting the event the event gets added to the accepting participant's event log. On rejecting the event, the event is sent back to the event log of the participant sending the event. If a participant is unable to find an event corresponding to a particular symptom associated with his/her attack specialization, the participant publishes the symptom to "find" container on the common screen**.** Once any symptom is published by a participant, all the other participants will be able to view that as a symptom to be found. It is published on the common screen. The participant posting the symptom also has the authority to recall the symptom. Upon recall by the participant, the entry for the symptom will be removed from the common screen. During this stage, the interaction between the participants is also recorded in real-time to a log stored in the database server with the corresponding time stamp.

4.1.2 UMICS ATTACK ANALYSIS AND IDENTIFICATION STAGE

This is the precursor to the final stage of a scenario analysis simulation process. By this stage, the participants should have categorized all the events received from the Master Controller and threat Evaluator and other participants as either, unimportant events or suspicious events corresponding to their specialization. No event should remain in the participant's event log. Once all the events have been classified and categorized as unimportant, suspicious events – Malware, DoS or Phishing, all of the participants have to analyze the pattern of events and have to come to a common consensus on the type of attack. The participants then press the submit button corresponding to the attack on their respective GUI screens. It is possible that all the events presented might not correspond to an attack. They all may be normal events that occur in any organization. In that case all the participants have to click on the "not an attack" button.

The participants have reached a common consensus and have pressed either the submit button or "not an attack" button corresponding to the scenario on their respective GUI screens. Upon clicking the submit button, the type of attack identified and the events identified corresponding to the attack will be sent to the Master Controller and Evaluator for evaluation. The evaluator then analyses the results by comparing the stored information about the

scenario and its expected outcome with the current outcome and current events submitted by the participants. It also compares the time taken by the participants, with the time expected to identify the attack and calculates a score for the given scenario. The score, along with the attack identified and their corresponding events are sent to the database and logged to a separate file on the database server with the session identification. The Evaluator also sends the results to the participant's common controlling GUI screen.

4.2 DATABASE SERVER

The events corresponding to different kinds of scenarios like representing cyber attacks such as DoS, malware and phishing are stored onto the database on the server. In addition to the events associated with the scenarios, some false positive events, noise, and unimportant events are also stored in the database. The reason for having the false positives events is to ensure that the participants are able to separate the important events from noise as is the case in a real cyber attack scenario. The goal of the simulation is to create the need and opportunity for team interaction. They interact, by exchanging information both verbally and electronically, for making decisions individually and as a team. These interactions are continuously logged on to the database server in real time monitoring.

4.3 THREAT EVALUATOR

The threat evaluator primarily classified the classes of threats. When we identify the threat classes, then categorise the functionality of the threats and send the results to master controlling authority. The Master controller is a host computer with some specialized functions. The main purpose of the master controller is to query an attack scenario, the events associated with that particular attack scenario, along with some associated noise events from the database. The Master Controller distributes the events from the database to the eight cyber security host systems on a per role basis. Upon completion of a scenario analysis, the Master Controller logs the events along with the conclusion reached by the participants in the database, evaluates the conclusion reached by the participants, and then scores the participants by comparing the events identified, false positives and conclusion with the expected results corresponding to the attack.

4.4 CYBER SECURITY ANALYST

Cyber security analyst in the context of this simulation refers to the participants. Each participant is assigned a role name corresponding to his/her specialization. The cyber security analysts a major role in UMICS model, so we explained the functionality in previous chapter UMICS analysis. The role currently identified for three participants are as follows:

- Denial of Service (DoS) specialist
- Malware specialist
- Phishing specialist

4.5 CYBER SENSOR

Cyber Physical Systems (CPSs) are the integrations of abstract computations and physical processes, in which sensors, actuators, and embedded devices are networked to sense, monitor, and control the physical world. Different from traditional embedded systems, the CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. A typical example of CPSs is connecting objects embedded with sensors or actuators to the real-time decision-making system. Then the CPS reflects the decision to the physical world by a sequence of control processes. Although there are many applications that have been developed to integrate wireless sensor networks (WSNs) from different domains, the CPS is still hard to build because the physical world cannot be predicted and the theoretical assumptions on WSNs cannot be efficiently achieved in the real world applications. Consequently, designing a reliable and real-time CPS using sensor technologies becomes a big challenge. This special issue aims to bring together a variety of advanced technologies, theory, and applications in the area of CPSs using sensor technologies.

4.6 UNIFIED THREAT MANAGEMENT (UTM)

Unified threat management (UTM) is a comprehensive solution that has recently emerged in the Cyber security industry, and since 2004 it has gained widespread currency as a primary network gateway defense solution for organizations. UTMs represent all-in-one security appliances that carry a variety of security capabilities including firewall, VPN, gateway anti-virus, gateway anti-spam, intrusion prevention, content filtering, bandwidth management, application control, data leakage prevention(DLP) deep packet inspection(DPI) and

centralized reporting these are some basic features. The UTM has a customized OS holding all the security features at one place, which can lead to better integration and throughput than a collection of disparate devices [4].

The organizations of today demand an integrated approach to network security and productivity that combines the management of traditionally disparate point technologies. A single UTM appliance simplifies management of a company's security strategy, with just one device taking the place of multiple layers of hardware and software. Also from one single centralized console, all the security solutions can be monitored and configured. UTM is a means to provide centralized security with complete control over their globally distributed networks.

4.6.1 UNIFIED THREAT MANAGEMENT FUNCTIONS

Functions of Unified Threat Management

▪	Stateful Inspection Firewall
▪	VPN (SSL VPN & IPSec)
▪	Intrusion Prevention System
▪	Data Leakage Prevention (DLP)
▪	Anti-Virus & Anti-Spyware
▪	Anti-Spam
▪	Outbound Spam Protection
▪	Web Filtering
▪	Bandwidth Management

▪	Application Visibility & Control
▪	Web Application Firewall
▪	3G / 4G / Wi-MAX Connectivity
▪	IM Archiving & Controls
▪	Deep Packet Inspection(DPI)
▪	Multiple Link Management
▪	On-Appliance Reporting
▪	IPv6 Ready
▪	Wi-Fi Appliances

Table: 4.6.1 Functions of Unified Threat Management (UTM)

The biggest value with UTM platforms is simplicity and lower price given its “all-in-one” footprint. Some of the key benefits of UTMs include:

- Cost-effectiveness: By reducing the number of appliances, there is a lower up-front cost as well as lower management and support costs.
- Easy to configure and manage: By reducing the number of appliances, there is a lower up-front cost as well as lower management and support costs.
- Stop attacks at the Network Gateway: The additional layer of security that a gateway device provides simply makes sense. Gateway devices block network threats before they have the opportunity to enter your network attack individual desktop PCs or mail servers.

4.6.2 IDENTITY-BASED UNIFIED THREAT MANAGEMENT SYSTEM

Identity-based security solutions can secure your every move at work, at home and while you travel – from the network gateway to the endpoints. It binds security with your identity and works as your private security guard, even when you are away from work or at home. Its endpoint security protects your sensitive data by securing your endpoints, storage devices and controlling applications. Unified Threat Management appliances, available as hardware and virtual appliances, offer comprehensive security to small, medium and large enterprises through multiple security features integrated over a single platform. It is the first UTM that embeds user identity in the firewall rule matching criteria, offering instant visibility and proactive controls over security breaches and eliminating dependence on IP Addresses. UTM unique Layer 8 technology treats USER as the 8^{th} layer in the network stack. Also known as the Human layer, it penetrates through each of security modules, allowing organizations to create user identity-based security policies. This offers them complete visibility and control over user activities, showing who is doing what anywhere in the network and enables them to take network security decisions based on usernames and not just IP addresses. UTM identity-based security offers a high degree of granularity, making policy-setting an efficient process down to the user level that can be extended to any combination of group, job function or application. The IP-independent nature of UTM allows users to carry their own access rights and policies anywhere in the network, even in dynamic IP environments like DHCP and Wi-Fi. Layer 8 technology adds speed to the whole security set-up by offering administrators instant visibility into source of attacks, enabling them to identify attacker/victims by username and achieve immediate remediation to any security breach condition [Figure:4.6.2].

UTM is rapidly becoming a most important network security device in many enterprises, particularly in small-sized and mid-sized offices. Alone with the continuous development of

the computer network, more and more enterprises and governments treat their business on Intranet and Internet; network security shows itself as a serious problem in front of people Traditionally, customers used firewall as their first line of defence and protect the network from the clients end.

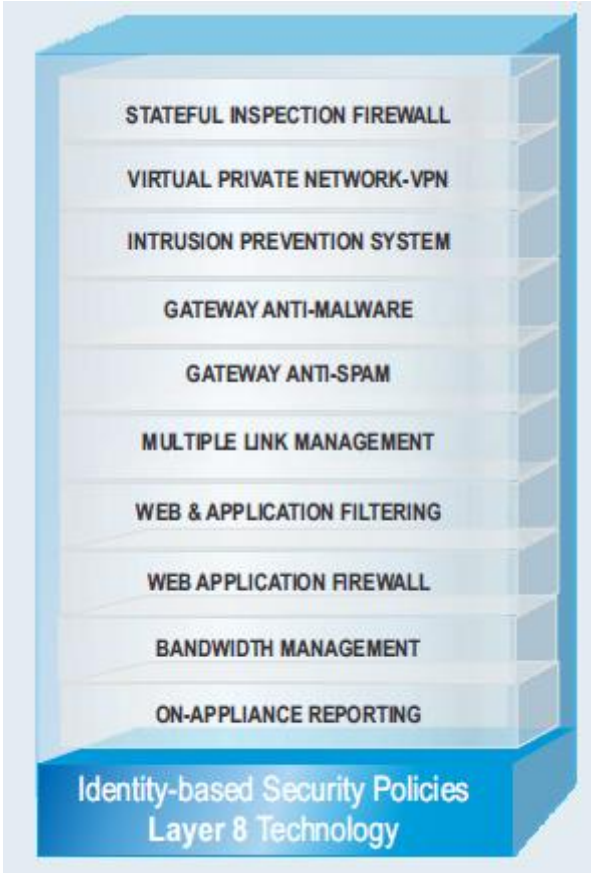

Figure: 4.6.2 Identity-Based Unified Threat Management

But with the more complicated network environment and mature attack means, the traditional firewall strategy cannot meet the demands of security. All those aggravate the work of network administrators and a little of negligence could result in great loss. To build united protection against complex and blended threats, multiple security features need to be integrated into unified security architecture, which results in a Unified Threat Management (UTM). UTM refers to a security appliance as a combination of hardware, software, and networking technologies whose primary function is to perform multiple security functions. The official definition of UTM is "Products that include multiple security features integrated into one box". To be included in this category, an appliance must be able to perform network firewalling, network intrusion detection and prevention and gateway anti-virus. All of the

capabilities in the appliance need not be used concurrently, but the functions must exist inherently in the appliance.

4.7 NEXT GENERATION- INTRUSION DETECTION SYSTEM (NG-IDS)

4.7.1 REQUIREMENTS FOR A NEXT-GENERATION IDS

The requirements for a Next-Generation IDS are discussed [21]. In detail, the IDS have to fulfill the following requirements:

1. Behavior-based analysis: Because of the increasing number of Zero Days, the growth of targeted attacks and the increasing percentage of encrypted communication, signatures are often not available in time or not possible at all. Even if the application of behavior-based methods is a challenge, sophisticated statistical methods can be used to detect attacks even in encrypted environments. Other reasons require behavior-based techniques. Because of limited computing resources and with regard to the endurance of the batteries, the application of signature-based techniques is not reasonable or even possible. Also in server systems, the necessary near real-time evaluation of patterns is limited not only by the amount of data to investigate but also by the sizes of the databases and millions of patterns.

2. Abdication of a learning phase: The use of behavior-based techniques often, requires a learning phase of the system in the productive, real-world environment. Because of the endangerment of the learning phase and the difficult task of creating clean labeled data, this phase must be omitted as far as possible. Unsupervised learning techniques can be used or the learning phase must be replaced by other techniques. It is important to understand that the abdication of the learning phase does not transform a behavior-based into a signature-based system: The detection is still fulfilled by the comparison of the measured state of the environment to the prediction of the model.

3. No payload evaluation: For a general applicability the system must be designed without the need of a payload evaluation as far as possible. Even more, the increasing use of encryption denies the use of payload data. Therefore, a Next-Generation IDS cannot rely on the availability of the packet payload.

4. Network-based evaluation and use of agents: Even if a host-based installation has several advantages with regard to the available information, the IDS require a network-centric design. On the one hand, distributed and sophisticated attacks against the whole network only can be recognized by a network-based installation, on the other side the management of numerous host-based system is error-prone, complex to manage and often poorly scalable in

large environments. Only if it is indispensable, host based agents should supplement the network-based core system.

5. Cross-evaluation and distribution: The upcoming threats and challenges require an exhaustive use of behavior-based techniques. Therefore, the related false alert rates have to be reduced. By examine ingress traffic and the correlation of anomaly detection alerts of administratively disjoint domains, the false alert rate can be reduced significantly and abnormal data and Zero Days can be detected.

6. Active and automated prevention: The system must be able to carry out a completely automated operation. On the one hand, the amounts of data, connections and speed of actions are already too high to be able to permit a reasonable manual interaction. On the other side, especially in the area of DLP, a beginning leakage of data must be stopped as early as possible. The loss of reputation after losing data will often be more expensive than the costs caused by a misleadingly activated interruption of a single connection, of course, the probability of a wrongly dropped connection must be very low.

4.7.2 ARCHITECTURE OF A NEXT-GENERATION IDS

To fulfill the requirements presented in previous section, architecture for a Next- Generation IDS is presented. An abstract view of the architecture is shown in [Figure: 4.7.2].

The system consists of three main parts, Early Warning, Intrusion and Extrusion Detection. The different parts can be implemented distributed and autonomous. A **EWS** has to be integrated comprehensive over the Internet. Event correlation, anomaly detection and inter domain cross correlation can be used to detect new threats. This knowledge can then be used to secure other, yet not affected sub networks in the Internet. The main purpose of the EWS is the detection and prevention of automated and undirected attacks. The **Intrusion Detection** is carried out as NG-IDS. Multiple detection techniques have to be combined. A behavior-based analysis of the network traffic is done to detect known as well as new, yet unknown threats. The needed model has to be built in an unsupervised fashion in such a way, that no endangered learning phase is needed. If the learning phase cannot be eliminated completely, in contrast to most existing systems, malicious instead of benign data can be used inductive anomaly detection. Cross-site correlation between systems and networks can be used to reduce the false alert rates of the anomaly detection efficiently. Statistical evaluation has to be done to cope with encrypted traffic.

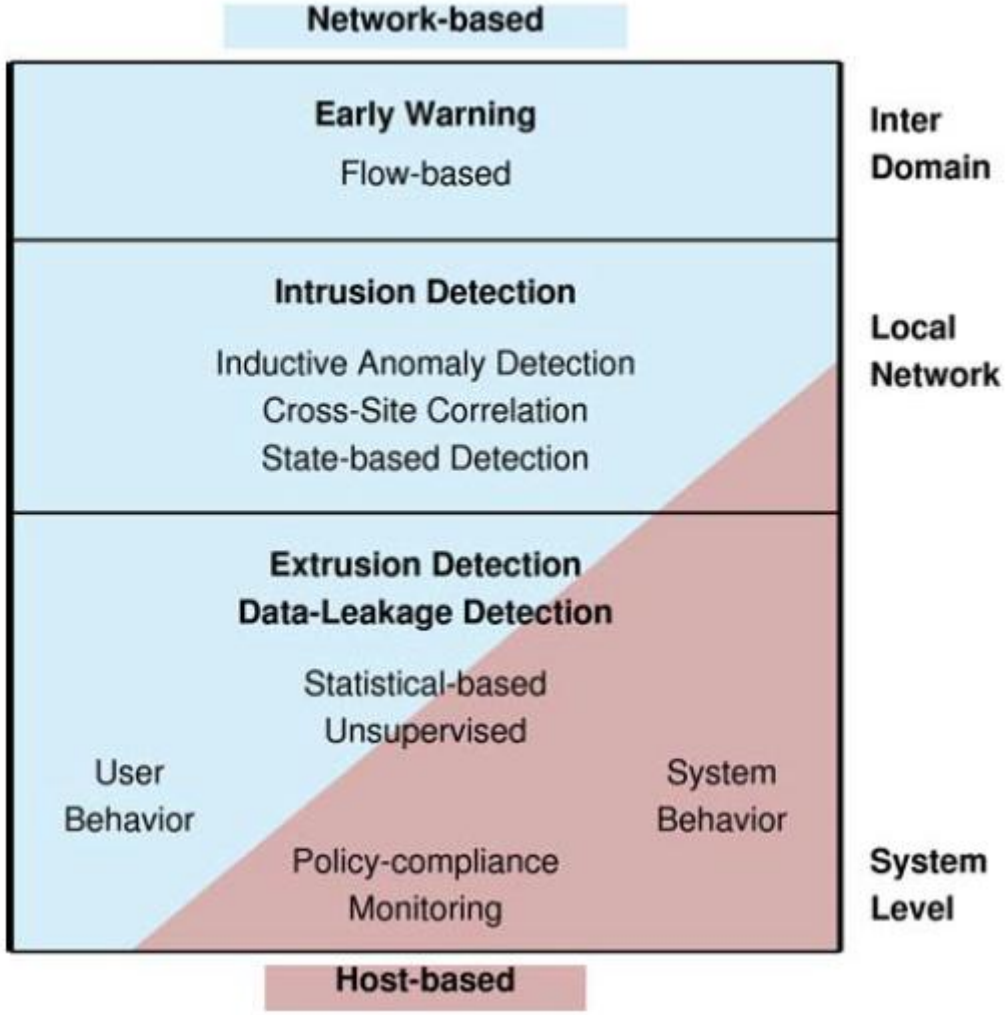

Figure: 4.7.2 Layers of a Next-Generation IDS

Additional, specialized host-based autonomous agents can be used to assist the evaluation. The agents with state-based detection techniques can be used to identify critical states in a SCADA network. The critical states are well-known in industrial systems; therefore an Intrusion Detection can be realized based on a critical state analysis. **Extrusion Detection** is the last component. It is also integrated into the NG-IDS, because due to the risk of insiders, manipulation and the administrative outlay with numerous hosts, host-based detection is not enough. Therefore, the user- and system-behavior is monitored by network-based sensors as well as host-based agents. With respect to the current research and developments, several open issues arise, especially in the area of Intrusion and Extrusion Detection in encrypted environments. Especially the claim of not using payload-related data to be able to cope with encrypted communication, targeted attacks and unknown threats is rarely address in current research.

There are three basic approaches to carry out Intrusion Detection in encrypted communication, namely:

- Protocol-based: Detection of misuse of the encryption protocol
- Intrusive: Modifications of the network infrastructure or the encryption protocol
- Non-Intrusive: Statistical analysis of encrypted traffic

The system developed by instruments shared libraries for cryptographic and application level protocols for conducting intrusion detection. Monitoring is integrated into the protocol handling. By that, attacks on the encryption protocol can be detected. Nevertheless, malicious activities hidden inside the encrypted channel could not be detected. The proposed NG-IDS for encrypted networks which is able to analyze the payload and simultaneously maintaining the confidentiality of the encrypted traffic. The network traffic is replicated and sent to the receiver and also to the Central IDS (CIDS). The protocol is set onto an underlying VPN and adds an additional layer. The system is able to do payload analysis and to keep the confidentiality, but it strongly depends on modifications of the protocols and infrastructure. Also, additional communications protected by e.g. SSH or TLS cannot be analyzed. Attacks are detected without decryption by the use of intrusion signatures which are generated from the frequency of accesses and specifications of the TCP traffic. Anyway, because of a high false alarm rate about 20 % in the best case, the system is not usable for a production environment. The system requires behavior profiles for the target servers and the exchanged information, which are often not available. Other work addressing IDSs in encrypted environments can be found, but to the best of our knowledge, all of it can be assigned to one of the three categories named before. Thus, all of these systems are not appropriate for the defined requirements due to the shortcomings already shown. An important point of all behavior-based systems are the false alert rates. For a comprehensive development of behavior-based techniques in productive environments, false alerts have to be minimized. The idea of a correlation of ingress traffic from different domains is relatively new and shows promising first results. Further investigations are necessary to improve the shown principles and make them usable for the defined requirements. In the recent area of DLP, most of the proposed systems are host-based and not able to operate only on a network-based installation. Extrusion and data leakage detection is a crucial part of a Next-Generation IDS. Therefore, these techniques have to be analyzed regarding the capability to be adapted to network-based systems.

4.8 EARLY WARNING SYSTEM (EWS)

4.8.1 FUTURE EARLY WARNING SYSTEM (EWS)

Early Warning System (EWS) is a main part of the future Cyber Defence. Special attention is given on the challenges associated to the generation of early warning systems for future attacks on the Internet of the Future. A next generation early warning system is securing the Internet of the future. Traditionally Internet providers are using Early Warning Systems (EWS) to protect themselves against and quickly react on certain Cyber Attacks. Due to a new level of cyber threats , we need an improved EWS architecture with the requirement not to be limited to the borders of different providers, based on traditional packet inspection, but to gather, analyze and correlate available network data flows to detect, analyze and react to threat patterns in near real time. This includes the development of completely new approaches such as the development of virtual sensors, sophisticated correlation of data, new reasoning models for network behavior analysis, learning algorithms as well as concepts to deal with scalability, dependability and resilience, especially in IPv6 networks [5].

4.8.2 IMPORTANCE OF EARLY WARNING SYSTEMS IN CYBER DEFENCE

The increasing importance of EWS is manifested in the enormous number of various research initiatives around the world. Trillions of devices, petabytes of data, gigabytes of transfer speed, payload of packets encrypted, IPv6 as well as the virtualization of services and data impose high requirements on developing a proactive action of the Internet of the Future. Key challenges in such a highly complex environment where data and services are also located somewhere in “clouds” are security, privacy and trust. Traditional network-based intrusion detection or intrusion prevention approaches cannot cope with such challenges. The need to protect the infrastructure of the Internet of the Future, as well as to manage such a security infrastructure has to have the highest priority [Figure: 4.8.2].

In the Internet of the Future, where (i) all devices communicate among each other, (ii) a seamless integration of networks enables the end user to see only one network, (iii) the data and services are located or are provided somewhere in the “cloud”, security, trust and privacy is needed. As traditional approaches are not sufficient any more, we need something completely new to proactively protect the infrastructure of the Internet of the Future and manage these security mechanisms in a consistent manner. More precisely, it is necessary to

address the following research issues; if we assume that the payload of packets will be encrypted because of privacy and security requirements, and also because of the huge amount of data flows, it is not possible to perform deep packet inspection.

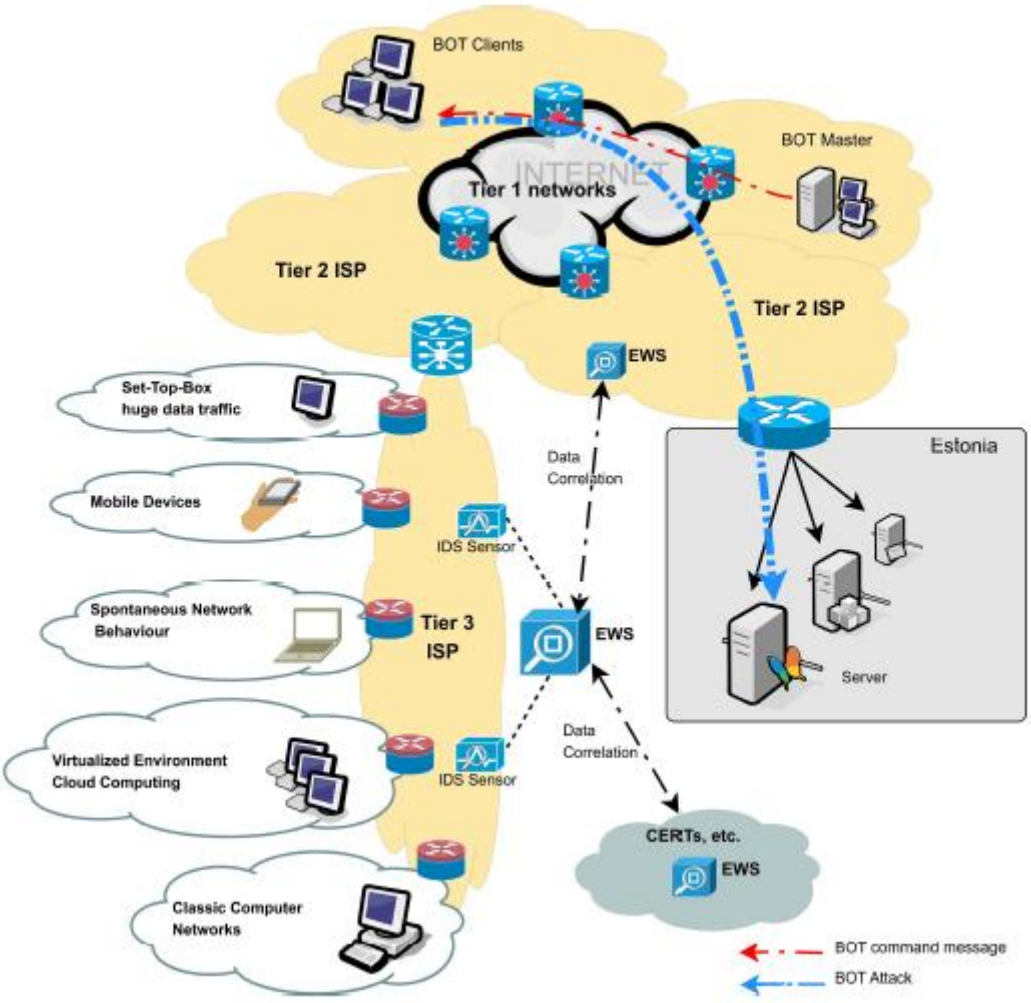

Figure: 4.8.2 Challenges for future EWS Technologies

The resulting objectives are therefore:

- An analysis and evaluation of available data, according to developed evaluation criteria and with respect to the relevance to detect a potential attack respectively a deviation of normal behavior. Hereby an analysis of passive and active measurement techniques and possibilities is necessary in addition to the relevance of the available data.
- Development and application of correlation techniques of various data sources, development and application of AI approaches.
- Development of methods for trend analysis in risk management.

- Modeling of network behavior, identification of the deviation from “normal” behavior.
- Determine EWS data sharing.
- Cooperative behavior, EWS have to be able to form binding commitments.

If we assume that data and services will be located, respectively provided in “clouds”, then the architecture of a EWS must address this virtualization aspect. Thus, virtualized security architecture is needed. Although virtualization is a mainstream technology nowadays, it seems that security issues are often an afterthought. Existing security models and practices cannot be directly applied to a vastly different environment. Furthermore, virtualization principles could change drastically the way we do security, that forces to rethink how to manage these security items.

4.8.3 THE OBJECTIVES OF EWS

1. Protect next-generation networks by developing a sophisticated next generation EWS.
2. Develop novel architectures, sophisticated models for network behavioral analysis and learning algorithms in order to build the next-generation EWS system, able to deal with specifics such as encrypted payload of packets, trillions of devices and petabytes of data as well as IPv6 networks.
3. Develop sophisticated correlation approaches to analyze, correlate and evaluate existing data flow information, and to reason about threat levels on basis of existing data; develop novel methods of detecting malware-driven network beaconing and command & control channels using both temporal and spatial flow attributes; develop concepts of fuzzy searching for resilient and adaptable malware detection at various sensing points in the network; investigate techniques for interpreting distributed sensor data for broader situational awareness.
4. Fundamentally improve the state-of-the-art in automated network threat blacklist derivation.
5. Develop approaches and models to define “normal” behavior and anomalies, threat levels, EWS data sharing; improve the automated assimilation of new security advisories and early warnings.
6. Improve the understanding of virtualization security; develop new security models based on the requirements.
7. Early warning systems especially focusing on security aspects of Internet of the Future.

4.8.4 THE FUTURE EARLY WARNING SYSTEM (EWS)

The inter-relationships and inter-dependencies between formerly stand-alone systems and networks are leading to complexities in the infrastructures of our society that have never been seen before. These complex systems and networks disseminate and process massive amounts of personal and business data, information and content in ways which are difficult to understand and control for users, in particular private citizens. In recent years we have witnessed a growing series of threats and attacks on the Internet and on applications and databases. Through denial of service attacks, viruses, phishing, spyware and other malware, criminals disrupt service provisioning and steal personal or confidential business data for financial gain or other purposes. Although we do not know how the Internet of the Future will look like, some characteristics can be identified:

- Layered, but augmented by a number of cross-cutting dependencies.
- Multitude in scale compared to the current Internet, billions of entities including things.
- Spontaneous and emerging behaviors and unanticipated new usages.
- Trust, privacy and security as key components.
- Pervasive digital environment, heterogeneous infrastructures, terminals and technologies.
- User-centricity and usability is critical.
- Enabling the “Internet of Services” and its new business models.
- Trust, privacy and security as key components, managed according a common security policy.

In respect to these characteristics the aim of our requirements is the development of an efficient cooperative Early Warning System for future networks. In the current environment of the Internet, multiple distributed and heterogeneous networks are connected at which no encryption is done or mostly only partial. Security-related cooperation between autonomous system providers is only done on a very marginal level. Anomaly detection, which is a very powerful instrument for intrusion detection, is only possible and available for sub networks, while current EWS are based on the analysis of log-files, flow-information or packet counting. Characteristics of the Future Internet will include a virtualized environment, IPv6

network, continuous payload encryption, an enormous number of devices and data as well as a highly distributed and pervasive environment. Therefore, most of the current components and management approaches are not applicable or sufficient any longer. To overcome these shortcomings, an efficient EWS has to be based on a network virtualization and will implement a EWS based on the use of virtual sensors, new reasoning models, new developed learning algorithms and a sophisticated correlation of data also taking into account security management aspects.

A long-overdue EWS will help the region to avoid deliberate or inadvertent outages, reduce the spread of new computer malware, and ensure continuity of services. Furthermore, the Future Internet has no centralized control hub and its complexity is not bounded by geographical, political, administrative or cultural borders. EWSs are present in various systems and are a crucial component of effective risk management in enterprises and for national homeland security systems. An Internet-wide EWS however is still missing. Because of the identified characteristics of the Internet of the Future, a EWS has to overcome the following issues that make the use of current State-of-the-Art Intrusion Detection Systems impossible or disadvantageous:

- **Applicability**: The persistent payload encryption blights Deep Packet Inspection.
- **Computational effort**: High bandwidth, numerous, highly dynamic connections and huge amounts of data would necessitate enormous amounts of computational power for deploying traditional systems and algorithms.
- **Energy consumption**: Mobile devices are becoming more and more important and the mobility will be one of the main characteristics of the Future Internet. Because of the increasing complexity of mobile applications, the processing capabilities of the mobile hardware and the endurance of the battery, it is neither possible nor desirable to set up sophisticated IDS on these devices. Therefore, the protection of the whole network from inside out is necessary and thus the intelligence has to be brought back to the network.
- **Novel threats: threats and attack possibilities evolving** from the highly dynamic environment with billions of devices cannot be handled by current systems, are not even known today.

4.8.5 TECHNICAL- SOCIO CYBER SECURITY WARNING SYSTEMS

This technique is more useful and robust, provided that it is implemented in all organizations and units. In 1988 when the first Computer Emergency Response Team (CERT) was established at the software engineering institute in Carnegie Mellon University and funded by the U.S. Department of Defense. "Critical Infrastructure Protection Act" implied the Presidential Commission on Critical Infrastructure Protection (PCCIP) created by the President of the U.S. One of the PCCIP recommendations was the establishment of "early warning and response capability" for protecting the critical nation infrastructure [2]. In 1999, the Federal Intrusion Detection Network (FIDNet) was implemented as an outcome.

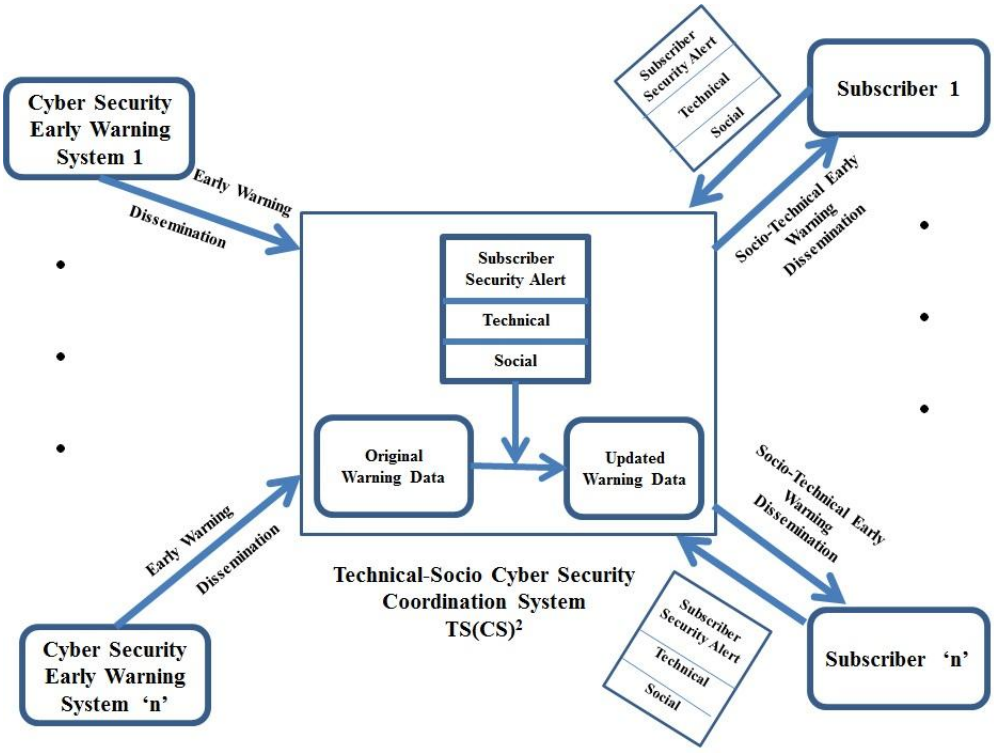

Figure: 4.8.5 The Technical Socio Cyber Security Coordination System TS (CS)^2

The International Multilateral Partnership against Cyber Threat (IMPACT) is currently the largest cyber security alliance in the world. IMPACT is also the framework for the ITU global cyber security agenda. ITU-IMPACT global response centre plays the role of almost real-time global cyber security warning system and it comprise of two parts: Network Early Warning System (NEWS) and Electronically Secure Collaborative Application Platform for Experts (ESCAPE). The idea of these collaborative features were inspired from the ITU-IMPACT global response centre NEWS and ESCAPE platforms which together provide collaborative

platform for domain experts and cyber security warning systems with the exception that they don't tackle the social aspect of cyber security [Figure: 4.8.5].

Cyber security is a global problem that requires collaboration and coordination between all countries. In order to address this vulnerability all nations should suggest a developing platform that eliminates the existing technical- socio gap between cyber security warning disseminators and end recipients.

A technical- socio cyber security coordination system TS $(CS)^2$ is collaboration between the cyber security warning system original data and updated warning data. As subscribers to the TS $(CS)^2$ platform, member organizations have to regularly feed the platform operators with the information about their security implementations at the different technical and social areas, policies, operations, practices and technical implementations. The TS $(CS)^2$ operators will collect this warning and analyze it from technical- socio perspective. The TS $(CS)^2$ platform will then disseminate a guided version of the warning to the subscriber. Guided warning will ensure those subscribes are effectively responding to security warnings [2].

4.9 CYBER WARFARE (CW) STRATEGIES

Cyber warfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and criple financial systems among many other possibilities. Inside Cyber Warfare, any country can wage cyber war on any other country, irrespective of resources, because most military forces are network-centric and connected to the Internet, which is not secure. For the same reason, non-governmental groups and individuals could also launch cyber warfare attacks. The most effective protection against cyber warfare attacks is securing information and networks. **Cyber warfare** refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. Any software-controlled system that can accept input can theoretically be infiltrated and attacked. This means all systems that accept input are vulnerable. Fundamentally, there are two ways to infiltrate cyber systems: physical and signal inputs. Expect every software-controlled system to be the objective of an attempted cyber infiltration.

Cyber attacks immediately follow physical attacks, Cyber attacks are increasing in volume, sophistication, and coordination, Cyber attackers are attracted to high-value targets, Many, if not most, targets would probably be commercial computer and communications systems, Organized Crime, Terrorist Groups.

4.9.1 CYBER WARFARE STRATEGIES

In this section we analyze the technique for protecting the network from the cyber threats which arises due to attacks on the network. The targeted attacks have significantly increased in cyberspace due to which there has been increased awareness and information about the targeted attacks. Targets of all targeted attacks can be divided into a specific organization and specific software or IT infrastructure. The type of attack on the former is directed at a specific organization and the aim of an attacker is to have unauthorized access to confidential intelligence such as operational secrets. The typical example of targeted attack is stuxnet. Stuxnet has raised the concerns for the security experts due to the following reasons: target choice, sophistication, and implications for future malware. The stuxnet is highly selective about its targets and specific conditions. The Security experts have estimated that the manpower required to develop stuxnet requires five to ten people working for six months to access to supervisory control and data acquisition (SCADA) systems. Stuxnet is the first real cyber weapon because it is aimed at a physical and military target [15].

4.9.2 CYBER FORCES MANPOWER

The cyber warriors should possess high level of technical knowledge, robust analytical skills, and an eminent understanding of cyber warfare. Cyber forces have to develop and manage them in the most effective way. They must understand military policy, cyber strategies and tactics. Cyber commander leads the cyber warriors and places them in the right place at the right time. Cyber intelligence collection enumerates system specification and exploits vulnerabilities of enemy's network and system by using scanning tools. A Cyber-attack technology includes hacking, sniffing, spoofing, hijacking, and DDoS etc. The Cyber defense technology consists of intrusion detection system, firewall, intrusion prevention system, and honey system etc [Figure: 4.9.2].

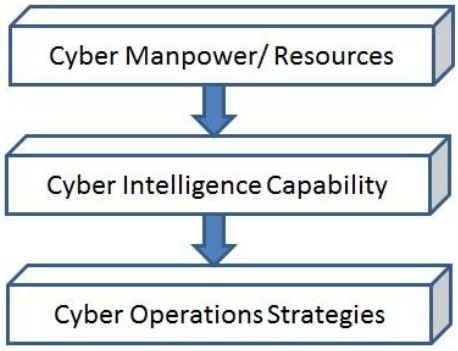

Figure: 4.9.2 Requirements for Cyber Forces Manpower

4.9.3 CYBER INTELLIGENCE CAPABILITY

The intelligence, surveillance, and reconnaissance (ISR) are the prior important factors to outbreak warfare, and mean the beginning of the battle. It is very important to conduct surveillance cyber-attacks and collect information about the aspects of cyber-attack. Global cyber defense system means early global response system. National cyber defense system monitors the intrusion of critical government infrastructure and SCADA. The military cyber defense system conducts surveillance about department of defence (DoD), Army, Navy, and Air force. Finally, personnel cyber defense system watches systems of officers, sergeants, soldiers, and civilian war workers. Cyber intelligence capability is useful in cyber response attacks for identifying information about the target systems. If we know precisely the information about our system, we can establish robust security measure in terms of response. The prepositional-cyber task order (pre-CTO) has defined the methods to disseminate components, subordinate units, capabilities and forces to targets for a specific missions for outbreak the war in short duration. It normally provides specific instructions to include fighter call signs, targets, weapons, and controlling agencies etc.

4.9.4 ORGANIZATIONS OF CYBER FORCES

In this section we show the organizations of cyber forces are mission or functional centric organizations unlike any other organizations. The department which continuously monitors cyber-attacks has to work for 24 hours, but the cyber-attacks response department has to solve in a few minutes or seconds as soon as cyber-attack occurs. Organizations of cyber forces should be organized in networked structure for sharing cyber-attacks information in real-time.

Control tower is also required for controlling and consistently managing the scattered organizations of cyber forces [15].

4.10 FEDERATED CYBER DEFENCE SYSTEM (FCDS)

In this section, we analyze and evaluate the techniques of cyber security and their results. The intrusion in the large cyber network under arbitrary attack is a critical process. There have been various schemes that had been proposed for intrusion detection problem. Some of them considered the Intrusion detection as the class of restless multi-armed bandit. This approach uses the whittle index policy which can be implemented without knowing the system parameters and is optimal over both finite and infinite time horizons [16]. The Intrusion Prevention System (IPS) which proactively combines the firewall techniques with the intrusion detection system. So that, it helps to analyze and identify the challenging issues to develop the intrusion prevention system. Thus the evaluation must show how to avoid anticipation. In order to develop adaptive intrusion detection system in cyber network infrastructures the classifier component of the framework should use a rule based approach in which the discovered patterns are represented in a simple "if-then" form. A domain expert can manipulate, delete, update, and add the extracted class association rules that are used for building the classifier model. Further, the system constantly monitors the performance of the classifier and updates the classifier according to the new patterns observed in the received data. An online adaptive cyber defence frameworks includes the following components: data pre-processing, rule mining algorithm, learning algorithm, prediction model, and a component that maintains the high accuracy of the classifier by using an incremental learning approach. Eventually, rule-based feature vectors are given to the support vector machines (SVM) algorithm and a classifier model is built [17]. The performance of the classifier is constantly monitored and the classifier is re-built if its quality drops under certain threshold.

FCDS is a system prototype designed for the improvement of federated network cyber security. Each domain of FCDS consists of the following elements: a number of sensors (S), a decision module (DM) and a number of reaction elements (RE) [14]. The Sensors forwards the information to the decision module with alarms when an event is observed in the network. Decision module performs reasoning analysis and makes decision if the observed action is an attack and produces appropriate rules applicable to reaction elements. Decision modules are deployed in autonomous networks which shares information about detected attacks and recommended reactions. It is assumed that information exchange between them is voluntary

as well as the use of recommended reactions depends on internal domain security policy and administrator decision. When set of domains are functioning together then those are able to produce a results not independently obtainable [Figure: 4.10.1].

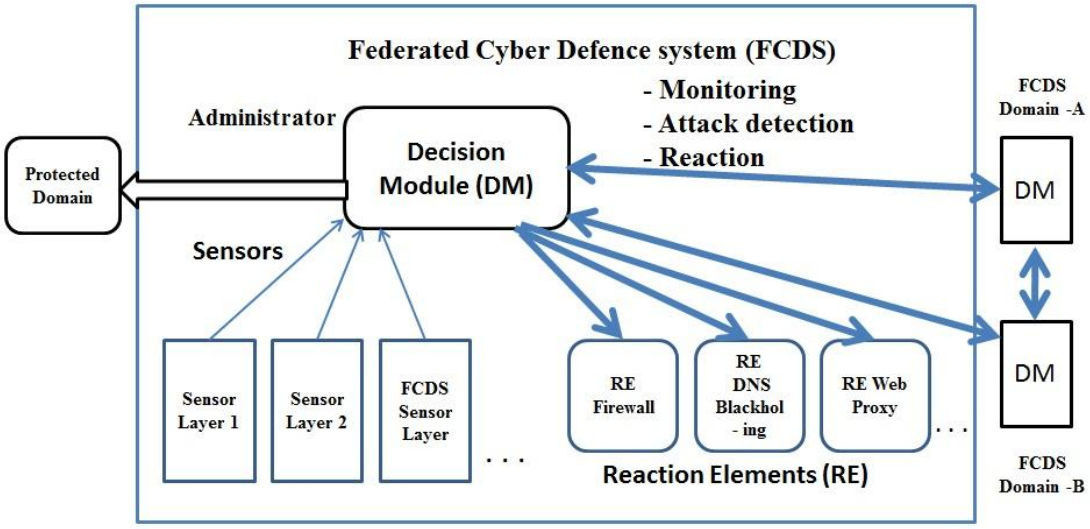

Figure: 4.10.1 Federated Cyber Defence System Architecture

Reliable and secure communication is required for sensor data collection, distribution and reaction element remote control. The dynamic physical world and complexity of cyber world present many challenges in CPS analysis and design, such as storage restriction, resource constrain, network bandwidth, and so on. The FCDS support the flexibility integration of loosely coupled services and components. The typical applications of CPS includes: intelligent transportation, precision agriculture, and medical cyber physical system [19].

CHAPTER: 5

CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

In this thesis we have reviewed, analyzed various latest research techniques for cyber security. In our study we find some efficient results of these techniques. In this thesis, we have presented an efficient and accurate cyber security model. This model can be creating a cyber threats free environment in cyber space using the various techniques and algorithms for both static and mobile networks. The main drawback of the existing cyber security model is there high computation cost and poor accuracy. The proposed model improves the performance of each cyber security techniques and integrated in a single platform for controlling and monitoring the whole cyber network. These theses studied how developed a UMICS system and implement the system in all organizations. During the thesis analysis, it found that the approaches in cyber security is different methods and approaches are used , so integration of all the useful technique is always a challenging work, but we try to best solutions for design a model UMICS. The thesis concluded that the cyber security strategy of a UMICS should have unique cyber security team performing tasks and filling roles that are appropriate for it and that these roles are not the same among all techniques.

We analyze and design a unified model for integrated cyber security (UMICS) framework for the future internet. This model can be subjected to better design and development. This model is unique, more powerful, reliable, robust, and efficient as compared to previously developed cyber security models. This model in fact, present drastic change in cyber security against the cyber threats. Countering focused and targeted attacks requires a focused cyber security strategy. Organizations need to take a proactive approach to ensure that they stay secure in cyber space and adopt a robust cyber security strategy which should be implemented through the UMICS. UMICS covers the best functions of cyber security like, risk driven, holistic, adaptable, efficient, collaborative etc.

The cyber security overview identifies the various general approaches and current issues and challenges in current cyber security environment. We categorize the cyber threats and evaluation of the future cyber threats. The UMICS analysis is more needful for developing a integrated system of cyber security. The cyber security monitoring and management system is a universal approach in cyber security, this approach more useful in developing a unified model for integrated cyber security (UMICS) system.

UMICS model integrated the various cyber security components and techniques; the collaboration of all the techniques is a major challenge in UMICS system. We identify a future early warning system (EWS). The next generation – intrusion detection techniques is required in this model. The NG-IDS techniques are develop according the future requirement of the cyber security.

The FCDS model enables information exchange between the cooperating domains and reaction against the cyber attacks. FCDS system enables the security measures improvement by using multi-sensor attack detection and joint reaction techniques. The cyber warfare tactics is robust and operational strategies in cyberspace superiority for cyber warfare this is efficient. Cyber psychological operation defines the propaganda and other planned activities affecting opinions, feelings, attitudes of all countries and groups for effectively achieving the purpose of national defence policy in cyberspace. The organization of cyber forces concentrates on mission or functional centric organizations which are different from other organizations. They represent technical-socio framework by implementing a pilot phase of the TS $(CS)^2$ platform. A technical-socio security expert will have to conduct a technical-socio security assessment for these organizations and feed results to the organization register stored in the platform.

The thesis reached this conclusion by studying the various cyber security techniques and the current theory on how develop a unified approach should solve the cyber threats problem. The analyses lead to the conclusion that a better approach starts by identifying differences between developed cyber security integrated models and developing cyber security models and how these differences impact strategies. UMICS is the universal approach to securing cyberspace. This thesis studied the cyber security situation by analyzing the cyber threat, cyber defense approaches and strategies.

5.2 **FUTURE WORK**

Cyber threats problem is common in every where our daily life or routine work. Cyber threat problems doesn't end or a single solutions, so we continue work in the field of cyber security. Cyber threats continue to haunt Internet users across the world & cyber-threats are the problems of today and the future. The Cold War may be over, but the cyber arms race has just begun. We must rapidly develop offensive and defensive cyber weapons capabilities as well as the military doctrine and regulations necessary to govern their use.

In the future, we are planning to further enhance the performance of our proposed UMICS cyber security model. We will try to include some more information about the cyber security techniques like optimization algorithms and include the proactive cyber threat detection techniques. We try to understand how to implement all the techniques in a single platform and how to integrate these techniques. We develop the algorithms according to the future requirement of the cyber security.

REFERENCES

[1] Adamov, A. ; Hahanov, V. (2011)," A security model of individual cyberspace", 9th East-West Design & Test Symposium (EWDTS), Page(s): 169 – 172.

[2] Al Sabbagh, B., Kowalski, S. (2012), "ST $(CS)^2$ Featuring socio-technical cyber security warning systems**"**, 2012 International Conference , Page(s): 312 – 316.

[3] Champion, M.A., Rajivan, P., Cooke, N.J., Jariwala, S. (2012), "Team-based cyber defense analysis", Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference , Page(s): 218 – 221.

[4] Chao, Yin ; Bingyao, Cao ; Jiaying, Ding ; Wei, Gu, (2009), "The Research and Implementation of UTM", Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference, Page(s): 389 – 392.

[5] Golling, M. ; Stelte, B., "2011" "Requirements for a Future EWS –Cyber Defence in the Internet of the Future" , Cyber Conflict (ICCC), 3rd International Conference , Page(s): 1 – 16.

[6] http://msisac.cisecurity.org/newsletters/, "Emerging Trends and Threats for 2013".

[7] http://muri-cybersituationalawareness.wikispaces.com /file/view/ ASU_Synthetic TaskEnvironment_Simulator.pdf/106279145/ASU_SyntheticTaskEnvironment_Simulator.pdf, "CYBER SECURITY SIMULATOR".

[8] http://muri-cybersituationalawareness.wikispaces.com/file/view/ASU_Cyber Security Analyst_Literature_Review.pdf , " Cyber Security & Cyber Security analysts".

[9] http://www.cert-in.org.in/

[10] http://www.cybersecurity.ox.ac.uk/

[11] http://www.happiestminds.com/unified-cyber-security-monitoring-and-management-framework , "Unified Cyber Security Monitoring and Management Framework".

[12] http://www.idsa.in/book/IndiasCyberSecurityChallenges, "India Cyber Security Challenges".

[13] http://www.itu.int/ITU-D/ cyb/ cybersecurity /docs/ ITUNationalCybersecurity Strategy Guide.pdf ,"THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE".

[14] Jasiul, B., Piotrowski, R., Berezinski, P.,Choras, M., Kozik, R., Brzostek J. (2012) ,"Federated Cyber Defence System Applied methods and techniques",

Communications and Information Systems Conference (MCC), 2012 Military , Page(s): 1 – 6.

[15] Jung-Ho Eom, Nam-Uk Kim, Sung-Hwan Kim, Tai-Myoung Chung (2012) , "Cyber military strategy for cyberspace superiority in cyber warfare", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference , Page(s): 295 – 299.

[16] Keqin Liu,Qing Zhao (2012), "Dynamic intrusion detection in resource-constrained cyber networks"**,** Information Theory Proceedings (ISIT),IEEE International Symposium , Page(s): 970 – 974.

[17] Kianmehr, K. (2012), "An incremental semi rule-based learning model for cyber security in cyber infrastructures "**,** Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), IEEE International Conference, Page(s): 123 - 128 .

[18] Lejun Fan, Yuanzhuo Wang, Xueqi Cheng, Jinming Li (2012) , "Analyzing Application Private Information Leaks with Privacy Petri Nets ", Computers and Communications (ISCC),IEEE Symposium , Page(s): 000370 – 000375.

[19] Liang Hu, Nannan Xie, Zhejun Kuang, Kuo Zhao (2012) , "Review of Cyber Physical System Architecture", 2012 15th IEEE International Symposium , Page(s): 25 – 30.

[20] RK Meena, Vinod Kumar (2013), "Cyber Security A Review", Cyber Times International Journal of Technology and Management,(Acceptance acknowledgement attached)

[21] Robert Koch, (2011), "Towards Next-Generation Intrusion Detection", Cyber Conflict (ICCC), 3rd International Conference , Page(s): 1 – 18.

[22] Shui Yu , Song Guo, Stojmenovic (2012), "Can we beat legitimate cyber behavior mimicking attacks from botnets ", INFOCOM, 2012 Proceedings IEEE , Page(s): 2851 - 2855 .

[23] Stiawan, D. , Abdullah, A.H. , Idris, M.Y. (2010), "The Trends of Intrusion Prevention System Network", Education Technology and Computer (ICETC), 2nd International Conference , Page(s): V4-217 - V4-221.

[24] Tinnel, L.S. ; Saydjari, O.S. ; Haines, J.W.(2003) " DARPA Information Survivability Conference and Exposition,", Volume: 2 ,Page(s): 32 – 34.

[25] White, G.B. , (2012), "A Grassroots Cyber Security Program to Protect the Nation", System Science (HICSS), 45th Hawaii International Conference , Page(s): 2330 – 2337.