

A STUDY ON NETWORK AND SECURITY MANAGEMENT IN IT COMPANY.

Submitted in partial fulfillment of the requirements for the award of

MASTER OF BUSINESS ADMINISTRATION

by

DHANUSH P

REGISTER NO: 42410085



**DEPARTMENT OF BUSINESS ADMINISTRATION
SCHOOL OF MANAGEMENT STUDIES**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade "A" by NAAC I 12B Status by UGC I Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

NOVEMBER 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

[DEEMED TO BE UNIVERSITY]

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **DHANUSH P 42410085** who carried out the Project Training "A STUDY ON NETWORK AND SECURITY MANAGEMENT IN IT COMPANY" under my supervision from September 2023 to November 2023.

DR.KRISHNAKUMARI

Internal Guide

External Guide

Dr. BHUVANESWARI .G, MBA., Ph.D

Dean – School of Management Studies

Submitted for Viva voce Examination held on_____

Internal Examiner

External Examiner

DECLARATION

I **DHANUSH P (42410085)** hereby declare that the Project Report entitled “**A STUDY ON NETWORK AND SECURITY MANAGEMENT IN IT COMPANY**” done by me under the guidance of DR.KRISHNAKUMARI is submitted in partial fulfilment of the requirements for the award of Master of Business Administration degree.

DATE:

PLACE:

DHANUSH P

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to the Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my sincere thanks to **Dr. G. Bhuvaneswari, MBA., Ph.D., Dean - School of Management Studies** and **Dr. A. Palani, M.Com., M.Phil., M.B.A., Ph.D., - Head - School of Management Studies** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **DR.KRISHNAKUMARI** for her valuable guidance, suggestions and constant encouragement which paved the way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **School of Management Studies** who were helpful in many ways for the completion of the Training.

DHANUSH P

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	
	LIST OF TABLES	
	LIST OF CHARTS	
1	INTRODUCTION	1
	1.1 Introduction	1
	1.2 Introduction of Security Management	1
	1.3 The Basic Principles of Network Security System	2
	1.4 The Establishment of Security System	2
	1.5 Security Policies of Computer Network System	3
	1.6 Management is the soul of security	5
	1.7 The analysis of security management standards	6
	1.8 Challenges of Network Security	7
	1.9 Network Security	8
2	REVIEW OF LITERATURE	12
3	RESEARCH METHODOLOGY	33
	3.1 Research Design	33
	3.2 Sample Design	33
	3.3 Sample Size	33
	3.4 Sampling Technique	34
	3.5 Data Collection	34
	3.6 Tools For Data Collection	34
	3.7 Statistical Tools	35
	3.8 Scope Of Study	35
	3.9 Limitation Of Study	36
	3.10 Hypothesis	36
4	DATA ANALYSIS AND INTERPRETATION	37
	4.1 Percentage Analysis	37
	4.2 Chi-Square Tests	50
	4.3 Correlation	52
5	FINDINGS, SUGGESTIONS AND CONCLUSION	53
	5.1 Findings of the study	53
	5.2 Suggestions & recommendations	54
	5.3 Conclusion	54
	REFERENCES	55
	ANNEXURE - Questionnaire	58

ABSTRACT

Network Security has the rapid development of network science and technology, people are dependent on the network and usage greatly improved, but the network to bring convenience, but it also brings a lot of network security issues, it has become a constraint computer network construction greatest limiting factor. This paper describes the impact of the computer network system security management of specific issues, according to the system requirements of practical application, in terms of the system operating environment, hardware systems, software systems, network systems and system data, such as design of the computer network system security policy and implementation are discussed. Through the computer network security threats faced by the system proposed safety management, regulations are important to ensure the development and implementation of computer network system security. Proposed computer network system security management strategies, we hope to enhance the computer network security have some help. With the rapid development of network science and technology, people are dependent on the network and usage greatly improved, but the network to bring convenience, but it also brings a lot of network security issues, it has become a constraint computer network construction greatest limiting factor. This paper describes the impact of the computer network system security management of specific issues, according to the system requirements of practical application, in terms of the system operating environment, hardware systems, software systems, network systems and system data, such as design of the computer network system security policy and implementation are discussed. Through the computer network security threats faced by the system proposed safety management, regulations are important to ensure the development and implementation of computer network system security. Proposed computer network system security management strategies, we hope to enhance the computer network security have some help.

LIST OF TABLES

TABLE NO.	PARTICULARS	PAGE NO.
4.1	Age of respondents	37
4.2	Gender of respondents	38
4.3	Education qualification of respondents	39
4.4	The computer system assets can only authorized parties	40
4.5	The computer security information in a computer system	41
4.6	The type of threats on the security of a computer system or network	42
4.7	The independent malicious program that need not any host program	43
4.8	The code that recognizes some special sequence of input	44
4.9	The code embedded in some legitimate program that is set to explode	45
4.10	The responsible for installing and maintaining security software on your computer	46
4.11	The web browser do you normally use	47
4.12	The use of Windows Update	48
4.13	The anti-virus software do you use	49

LIST OF CHARTS

CHARTS NO.	PARTICULARS	PAGE NO.
4.1	Age of respondents	37
4.2	Gender of respondents	38
4.3	Education qualification of respondents	39
4.4	The computer system assets can only authorized parties	40
4.5	The computer security information in a computer system	41
4.6	The type of threats on the security of a computer system or network	42
4.7	The independent malicious program that need not any host program	43
4.8	The code that recognizes some special sequence of input	44
4.9	The code embedded in some legitimate program that is set to explode	45
4.10	The responsible for installing and maintaining security software on your computer	46
4.11	The web browser do you normally use	47
4.12	The use of Windows Update	48
4.13	The anti-virus software do you use	49

CHAPTER-1

INTRODUCTION

1.1 Introduction

Network information security is a research field of many subjects including computer science, network technology, communication technology, cryptography, mathematics, information theory and so on. It is a complex and difficult work to protect the information security of the network, because information is spread in the open network. Under the joint efforts of network security experts and researchers, the evaluation system of network information security is established to ensure that the characteristics of network information can play a role in normal. Network information security assessment is based on the nature and meets the conditions of security. It is considered that the network information is safe when it meets confidentiality, integrity, availability, accountability, authentication, non-repudiation and authenticity of the network information in dynamic and static process desk. Later, computer security experts of the United States have added two natures, namely, practicability and possession, which make the network security evaluation more scientific and reasonable. The network information security model. The opponent or malicious code accesses the information through the communication channel from the client. Access will be subject to security checks such as a firewall and then will be confirmed by computer resources, data, processes, software and so on when they come into the interior and are authorized by trusted third party. All of this is to ensure the legitimate access and data security.

1.2 Theoretical Introduction of Security Management

Network security refers to the various components of the digital network system from accidental or malicious reasons destruction, alteration, and disclosure of, and mechanisms to ensure continuous digital network system normal operation, the ultimate aim is to achieve a digital network information processing and transmission process to maintain reliable confidentiality, integrity, availability and controllability. The development of the entire system is very complex, involving various computer and network technology, so that the various functions needed by campus computer network security management can be achieved, including network monitoring, equipment management, user management and fault management and so on. Network security features include: confidentiality. Ensure that the information on the digital network is not disclosed to unauthorized users or for its use; integrity. Prevent from digital libraries unauthorized users from tampering with, namely to ensure that information is not modified in the storage or transmission, is not destroyed and missing features; availability. Ensure digital information and information systems used by authorized users do to prevent computer viruses or other man-made factors causing the

network and the system can't operate properly and denial of service or used as a rival. Network system is secure against all kinds of threats to system security weaknesses in risk factors and systems from several aspects of the system design, equipment configuration, software application, system operating environment, take planning, control and a series of measures to prevent the system any form of damage, and after the destruction of the protection system can quickly resume normal operation. Therefore network authentication must be considered appropriate security means, which are authentication integrity, non-repudiation of the information, replay attacks and transport security, also be considered to avoid the user's identity forgery, tampering, repudiation, posing, etc. authentication is the first hurdle of network security system, logical structure of the safety system.

1.3 The Basic Principles of Network Security System

For the safety in compute and its network system requirements include: Make sure the file and transaction information is not tampered with, information to be protected; personal information confidential; various data material can have timely access and so on. The computer and network systems for use and access public services should be very convenient, and must be able to withstand a long uninterrupted run. The computer for public access and use is to provide readers with various public services, if the defect due to security measures, the inconvenience to the reader, or the reader does not need to provide timely press online search and other services, which will make service image libraries affected. When readers use the 's public computers, some personal information will remain on your computer, such as the local computer will record web browser to access records, the proxy server will record the readers visited website addresses, leaving the reader when using a public computer systems files will be saved. More information to protect the privacy of legitimate readers should bear the responsibility. Another new face is a legitimate question access to the computer and network systems. Since many libraries to provide access to Internet services to all readers, they must set up Internet access and filtering bad information and other issues. In addition, many libraries also offer services via the Internet to access the system and resources, the must use restrictions in accordance with the relevant agreements for such access is carefully controlled. Data transmission main purpose is to ensure the security of data transmission is not eavesdropping on the communication line, alteration and destruction, achieve this goal are the main technical data encryption and data integrity authentication techniques.

1.4 The Establishment of Security System

Computer network system according to the need of practical application, analyse the possibility of a variety of risk, and according to the degree of difficulty system and data recovery, combined with factors such as investment funds, design a scientific, rational,

careful and practicable the computer network security system . Secure network system is the computer network system security key. Operation and service of digital resources information management system needs to rely on a network, but the public and open Ethernet protocol, resulting in a lot of security risks. Hacker attacks on the computer network system, the virus destroyed the vast majority from the network. Therefore, the development and implementation of effective network security policy is to protect the computer network system security is very important part. Information Management System is the most important application system, its security is directly related to normal operations carried out an open. Already high between the campus network and the external Internet, enterprise-class firewall as a barrier to outside hackers is difficult to carry out effective attacks on the 's the computer system, but the's server if they are directly exposed to the campus network, campus network from malicious internal or mischievous attacks are difficult to prevent. Libraries should adopt VLAN (Virtual LAN) technology, the server area, office area, a public inquiry machine area, according to the different areas such as electronic reading devices logically divided into different independent LAN segments. In this way, both to ensure the secure server area, but also facilitate the management of network addresses, but also reduce the network load, effectively preventing large LAN network problems caused by the storm. Computer network security management is a systematic project, which requires the decision-making, management, technology layers effort with proceed from the safety aspects of institution building and technical means to enhance information security awareness education and training to enhance self-protection awareness, take comprehensive preventive measures, and continue to improve and perfect the security management measures. To upheld awareness of security, and gradually adopt a comprehensive and feasible security measures to reduce security risks to a minimum.

1.5 Security Policies of Computer Network System

Once the network system being hacked, infected with the virus, hundreds of thousands or even millions of bibliographic information collection and distribution of information, the museum self-built database data such as lost or destroyed, the loss will bring disastrous. The computer network technology to achieve network security management system to ensure the safety of the network system, reliable operation, mainly includes the following aspects. the security policies of computer network system Network Access Control can control the legitimate Internet users log on to the network server and access to network resources, control the time and manner permitted network user networks. Network users can access control can be divided into three steps: identification and verify the user name; identification and verify the user password; default user account limit checking. Permissions control network is a protective measure taken against the illegal operation network. Network users and user groups are given certain privileges, specify the network users and user groups which directories, subdirectories, files, and other network resources can be accessed. With the development of

computer and network technology, more and more rampant virus activity, therefore, maintain a good network system security, you need to choose a strong anti-virus, anti-virus capabilities and real-time monitoring capabilities of antivirus software . Computer network system should allow the user access to directories, files, and other network resources. Network users in the directory specified level permissions to all files and subdirectories are valid, the user can further specify access permissions for subdirectories and files in the directory of the. Access to directories and files in general are: the system administrator privileges, read access, write access, create permissions, delete and modify permissions, search permissions, access control permissions. Server is a very important role in terms of management. Security control server includes the server console can set a password to lock to prevent unauthorized users to modify, delete or destroy critical information network system resources; server login time limit can be set, to detect and shut down illegal visitors intervals and so on.

CONSTRUCTION OF NETWORK INFORMATION SECURITY SYSTEM

To ensure the security of network information requires a multi-discipline knowledge and a common component of multiple security units. Each security unit as an individual has the integrity, and each security unit is combined to form a security system. In 1989, National Institute of standards and technology (NIST) in Guidelines for the implementation of information resources protection of Special Publication SP500169put forward: "The success of information resources protection project depends on the strategy used, and it also depends on the management layer to protect the information in the automatic system. As a policy maker, it should set the tone and emphasize the important role of information security in the institution. The main responsibility for the development of the body is to develop information resources security strategy to achieve the following objectives: reduce the risk and be in compliance with laws and regulations; ensure the continuity of the organization's operations, information integrity and confidentiality. security management model refers to the existing model and describes the security control plan with three parts as follows:

- Management control: security content which is formulated and implemented by management. The content includes process management, network security plan, network life cycle, risk assessment, prevention and control mechanism, and access to legitimacy and so on.
- Operation control: security of network operation by internal staff. The content includes emergency measures, personnel safety training, physical equipment security, software and hardware system maintenance control and the network information integrity.
- Technical control: technical measures to ensure the security of network information. The content includes logic access control, identity recognition, digital authentication, firewall, active defence, intrusion detection and so on.

Security management model, as the Internet reference model OSI, is a system framework for the department to use as reference according to the need. Agencies refer to the model to develop their own security policies and measures and establish a security management system which suits for the specific network according to their specific security plan. In order to establish the security system, we should analyse the existing security control strategies and measures at first, find out other necessary security controls and form a security framework according to the requirements of safety management.

1.6 Management is the soul of security

In the network security, whether from the use of the management model or the three-layer network information security system, the most important thing is the consistent management. Management is various, including data management, security management, regulatory management, document management, software and hardware system management, maintenance management and so on. In the process of management, we must improve and modify the security policy and system, and apply it in practice, and continuously strengthen the security fortress. So management is the soul of network security. In the process of security, we must strengthen the sense of responsibility for all levels of personnel and increase their awareness and understanding of information security through regular training. The advice of network information security providers, users or information security experts should be adopted. Through full preparation for the needs analysis and risk assessment of safety system design, the cost will be lower, and the efficiency will be higher. Combining the actual situation of network information security management, the following methods need to be done:

- Develop correct safety awareness. Every one should be aware of their safety responsibilities and strengthen the training at regular time. Enterprises should regularly inform the network security situation.

- Establish the assessment system and the reward and punishment mechanism; strengthen supervision and inspection; protect the security system and measures to implement.

- Maintain the operation of the network in accordance with international standards, rules and regulations of the state and enterprises.

- For different levels of network, information and equipment, adopt different levels of security strategy.

Information security is an integral element of fiduciary duty that is considered a subset of IT governance . The purpose of information security is to protect an organization's valuable resources, such as information. In relevant standards and frameworks as well as in the literature the continuously increasing dependency of nearly all organizations on appropriate secure information processing was reported. Standards for the management of information

security and collections of best practice measures were developed and established. According to the most important and most widely accepted international initiatives for the development and operation of an ISMS are ISO 270xx, ITIL and COBIT, also relevant in aspects like information and security management, as well as cloud governance . Typical departments including risk management, legal, audit, compliance, privacy, business continuity, quality control, facilities, human resources, IT security, information security and physical security are all engaged in activities that have a bearing on, or are related to, security. Integration of these activities into a process framework for information security that makes explicit the interrelationships will enable a cost-effective security, but their activities tend to be viewed as silos. Over the last few years, cost benefit discussions have influenced information security practice. The value of information must justify protection costs. Adjustment and cost-effectiveness are key elements of a successful. Knowledge of the mission is needed to align the ISMS processes to the organization and their mission. Taking into account the importance of business alignment and cost-effectiveness for the successful operation of an ISMS, research contributions should address both problems by enabling a clear identification of necessary and appropriate ISMS processes as core elements of every ISMS. The problem is, that actually such a process framework for security management does not exist. This is still a problem because information security management is a complex issue and current research focuses on economics and cost benefit analysis of information security investment regarding single measures protecting information. The ISMS and the ISMS processes themselves are in focus of current research.

1.7 The analysis of security management standards

To answer the first research question, the objective of the analysis of security management standards can be summarized as follows:

- Analyze ISO 27001 standard statements on processes
- For the purpose of comparing it
- With respect to the degree of coverage and relationship with specific processes in ITIL and COBIT in favouring reuse
- From the viewpoint of process management and management in general
- In the context of organizations interested in planning, implementing and operating a process based information security management systems.

To reach this objective, multiple process reference models need to be harmonized. Baldassarre presented a strategy that guides the harmonization of multiple process reference models through a systematic stepwise approach, general enough to be applied to any reference models that are being taken into account. The harmonization strategy of Baldassarre is based on the process and the framework for supporting multi-model harmonization of. According to Baldassarre “In general, the harmonization framework defines as follows:

- (1) A guideline for determining the harmonization goals, based on the strategic plan and goals defined in the organization's mission;
- (2) A harmonization process for driving multi-model harmonization, with which to manage and lead the harmonization of models step by step;
- (3) A harmonization ontology, which presents the terms, concepts and relationships for supporting the harmonization models, and
- (4) A Set of Techniques and Methods, which facilitates the configuration and definition of the harmonization strategies. The harmonization strategy is the work product resulting from the implementation of the harmonization process.

A theoretical comparison process is used as the harmonization process, because mapping is one of the most widely used strategies for the harmonization of models. The purpose of this process is to perform a step-by-step comparison and a mapping of different models, aiming to guarantee the reliability and robustness of obtained results. For the theoretical comparison the ISO 27001 standard was considered as a starting model, as it is considered the most important standard for information security management. The outcome of the theoretical comparison process is a table (Result of Comparison) that maps the models and points out the relationships between them regarding the mentioned ISMS processes. An adaptation on the Models and Standards Similarity Study method was used for the analysis of the identified security management standards.

1.8 Challenges of Network Security

- With more features comes more vulnerabilities. These vulnerabilities serve as a challenge for network security.
- Not enough IT Security Management. Securing your computer from viruses and attacks requires lots of effort and time.
- The easy availability of the internet, attacks have become more common and are now more intense.
- Insecure Configurations another challenge to network security.
- Wrong configurations may sometimes prove to be treating and misleading privileged Access.
- For hackers, it is easy to target the privilege control than the whole network altogether.
- Abuse usage of the User accounts has been challenging.
- These securities sometimes prove time-consuming and take a lot of time to load tasks.

Benefits of Network Security:

There are different benefits of using security in your network:

Control over data access.

It is crucial to control your data. Not every user is allowed to access and make changes in the network and its data. You can limit access to your network. It prevents illegal access.

Reduced Risk.

The proper network security will help reduce attacks on your network. It will save you from viruses and malicious software that harm your computer.

Protect Sensitive Information.

With proper security and control, you can store your sensitive information in the right place. You can protect your crucial information and ensures the protection of data.

Protection Against Cyber Attacks.

With the easy availability of the internet, it becomes easy for hackers to attack your network and steal the data. You can protect your computer from cyber-attacks if network protection is appropriately enabled.

Centralized Updates.

These updates are essential in saving your computer from hardware and software viruses. The attackers can quickly attack the older version when the new version update is available.

Trust.

Helps build trust with the clients with proper security and safe data. Data security helps build trust and mutual consent between the client and the company. Security failures can harm a company's reputation.

1.9 Network Security

- As the name suggests, it is the method or attempts to secure the network through which we transmit data and use it in our day-to-day life.
- Network security is a set of terms and conditions along with configurations designed to protect the integrity of the network. It helps to protect the confidentiality of the network.
- It manages the accessibility of the networks using both software.
- Network security is the essential aspect and the method for all companies to protect themselves from cyber threats.

- Password protection is considered the most basic security method.

The vulnerabilities of computer systems that are protected are

- Locations.
- Data.
- Devices.
- Users.
- Applications.

1.10 Information security examples

There are many ways for information security. Threats come in many forms and from many directions. Threats can be malicious and well-planned incidents where the attack has been planned for a long time and is well executed. There are issues in programs and practices so that an unauthorized party gains access to information by accident (Väisänen, Trinberg, & Pissanidis, 2016). From all the possibilities, the first and foremost task for securing is to develop the used program to have sufficient security by default. It is only natural for developers to incorporate bugs and flaws in the programs, especially as they grow larger. This, however is not an excuse for not trying to produce the best possible result. Another critical issue is to have the policies set before starting to work on the tasks that are vulnerable. Should there be any issues in the task at hand, then there is a policy to adhere to. (Viestintävirasto, 2018.) Methods for the attackers are not scarce. There are multiple ways in technical areas and in less technical methods to gain access to information. In many cases, the attacks do not need to be elaborate highly complex and technical feats, but instead a simple forgetting to lock the computer or leaving notes of passwords will suffice. (Comp TIA, 2017.) Information security methods, or as Whitman and Mattord (2011) name them, measures are a category rather than a single entity. As stated in Section 2.2, they include exploits, used against vulnerabilities that are threats to an information system as a threat agent. There are several methods or means to information security. For attackers to gain access to assets, there are several threats to exploit the vulnerabilities. The owner or maintainer of the system needs to have a protection profile based on risks of incidents, having measures to protect subjects from being exposed. The attacks can be technical in nature, where the threat agent might consist of a man-in-the-middle attack. The attack can also be a human error, where the user has left the password to a system on a note, where the attacker might use and see it. (Whitman & Mattord, 2011.)

1.11 Information security policy

This section explains what an information security policy is. In short, it is a policy for managing information security. A policy is a set of rules for practices that are used and followed to ensure wanted outcome (Viestintävirasto, 2017c). In this instance, it is information security. Information security policy is used for ensuring standards in an organization or other party (Viestintävirasto, 2017c). Organizations tend to grow resulting in increase of people operating, requiring a set of rules to follow to mitigate decisions done individually that might not work in practice. Information security is easily forgotten to maintain when organizations change leading to issues that could be avoided. (Von Solms & Von Solms, 2018.)

There are several means to create and maintain information security policies. In some organizations, the policy is created separately for each section, in some instances it is one single document detailing all aspects. Since there are no identical organizations, many would benefit in having a policy specifically created for them. However, often organizations do use a more generic approach instead (Rees, Bandyopadhyay, & Spafford, 2003.) While there are benefits in all approaches, often the method of individual policy seems to be most beneficial, since it covers most of the organizations security aspects (Alshaikh, Maynard, Ahmad, & Chang, 2016). Often the creation of information security policy is governed by external influences, first and foremost the legislation.

Countries have their own national policy guidelines and laws regarding information security and organizations need to produce their policies accordingly. In Europe, countries have their own national laws that are guided by directives. Information security is governed European-wide by the GDPR-directive that 13 instructs on the creation and strictness on aspects of information security policy (European Union, 2016). As the main principle, the goal is to protect the citizens from organizations that do not comply with the regulation. However, from the organizations' perspective, the effects are different (Tankard, 2016). One factor in information security policy creation is the cultural factor, because different countries have different security cultures (Alkahtani, 2018). Inability to recognize cultural differences is sometimes great enough for the policy not to work properly (Alnatheer, Chan, & Nelson, 2012). Information security and the policies are essentially about managing information security.

Managing includes much more than preparing against active attackers. If the organization employs people, information security requires managing them (Kajtazi & Bulgurcu, 2013). Managing information security is having aware individuals, that are committed to the organization and to its policies (Lim, Chang, Maynard, & Ahmad, 2009).

There are several methods to enforce compliance and several attempts to create a framework for policy creation have been made. Regardless of the method, the most functional method seems to be raising awareness about information security (Scholl, 2018)

and even engaging users to participate actively (Alnatheer, Chan, & Nelson, 2012). Different nations have different rules and regulations regarding information security.

The National Institute of Standards and Technologies (NIST) provides a comprehensive framework for creating an information security policy (National Institute of Standards and Technology, 2018). While it is subject to mainly cover the needs and regulations of the United States of America, it has several valid aspects that are worth considering when creating a policy for an organization.

1.12 Security Objectives

Security Objectives are the targets the customer establishes for their security program. Without security objectives, they do not know what they are trying to accomplish for security and therefore will not reach any goals. Security Objectives are one of those areas requiring the customer's involvement, and so the assessment team cannot make up the information.

Security Objectives come from a combination of inputs, including:

- Customer Mission
- Regulatory Requirements
- Business Objectives
- Best Practices
- Industry Practices

Security Objectives need to be well-defined and made known throughout the organization. Ultimately, the security objectives should be tied to the business objectives of the organization.

CHAPTER-2

REVIEW OF LITERATURE

The literature review

This thesis is intended to be a review of existing studies of information security policies. The result will be an overview of aspects that concern information security policies. The aim is to find recent topics and types of research that have been used when studying information security policies. To achieve this, the processing of this thesis is begun by studying on how to do a literature review. As a base for this work, the guidelines were chosen from Kitchenham et al. (2007) as a starting point. Using these guidelines, a review protocol was created and used in this thesis.

A systematic literature review is a mean to identify, evaluate, and interpret research relevant to the research question or area of interest. The most common reasons for a systematic literature review are summarizing existing evidence, to identify gaps in current research or to provide a framework or background for new research (Kitchenham, et al., 2007). This thesis concentrates in reviewing and analysing literature regarding information security management, specifically on the information security policies.

With information security covering several aspects, this review can only provide an overview of how information security is achieved, or attempted, in organizations researched through information security policies. The process of systematic literature review begins with identifying the area of research, which in this case is information security policy. A plan for review is needed to create a framework which is followed. The plan defines the methods and steps used in the review, leading to the wanted outcome. In this chapter, the literature review process of this thesis is planned and detailed.

A.Calder, Information Security Based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing, 2009.

Information is the currency of the information age and in many cases is the most valuable asset possessed by an organisation. Information security management is the discipline that focuses on protecting and securing these assets against the threats of natural disasters, fraud and other criminal activity, user error and system failure. This Management Guide provides an overview of the two international information security standards, ISO/IEC 27001 and ISO 27002. These standards provide a basis for implementing information security controls to meet an organisation's own business requirements as well as a set of controls for business relationships with other parties. This Guide provides: An introduction and overview to both the standards The background to the current version of the standards Links to other standards, such as ISO 9001, BS25999 and ISO 20000 Links to frameworks such as CobiT and ITIL Above all, this handy book describes how ISO 27001 and ISO 27002 interact to guide

organizations in the development of best practice information security management systems.

T. R. Peltier, Information security fundamentals. CRC Press, 2013.

The authors of the present study proceed from the objective-subjective predetermination of any phenomena and processes of the external world. In this format, the study is based on general scientific methods: systematic analysis and generalization of normative and practical materials; formal and dialectical logic: analysis, synthesis, induction, deduction, hypotheses, analogies; and special methods of legal research: comparative-legal and historical-legal, system analysis and interpretation of legal norms. Based on the analysis, the following conclusions have been made: currently, the most important direction of the national economy development is the protection of vital human and social interests, the key element of which is information security. This study represents the development of a scientific overview of the modern ways to ensure information security in both applied and legal contexts. This article underlines and examines the problems and economic legal features of ensuring information security in Russia. These materials can be used both in preparation of other scientific research and in the development of guidance documents by the power structures.

H. Cavusoglu, H. Cavusoglu, J.-Y. Son, and I. Benbasat, "Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources," Inf. Manage., Jun. 2015.

To offer theoretical explanations of why differences exist in the level of information security control resources (ISCR) among organizations, we develop a research model by applying insights obtained from resource-based theory of the firm and institutional theory. The results, based on data collected through a survey of 241 organizations, generally support our research model. Institutional pressures and internal security needs assessment (ISNA) significantly explain the variation in organizational investment in ISCR.

S. Dzombeta, V. Stantchev, R. Colomo-Palacios, K. Brandis, and K. Haufe, "Governance of Cloud Computing Services for the Life Sciences," IT Prof., Jul. 2014.

The authors analyze legal regulation issues surrounding cloud computing in healthcare. As a result of the authors' expertise in cloud-based data processing for organizations in the areas of healthcare and life sciences, they propose an implementation roadmap. The roadmap is intended to provide guidance for organizations in the life sciences regarding the governance of health data processing and storage. This article is part of a special issue on life sciences computing.

International Organization for Standardisation and International Electrotechnical Commission, ISO/IEC 27001:2013. Geneva, 2013.

Information Security Management System (ISMS). ISMS-Processes, as basic elements of every ISMS, need to be aligned to the organization and its mission. As of today, a specific ISMS process framework does not exist. ISMS processes are not in focus of current research. This article aims to fill this research gap by presenting results of a process mapping study regarding ISMS processes in the most important and widely accepted international standards for Information Security Management. Authors propose a set of ISMS processes within an ISMS process framework which should be implemented at an individually appropriate maturity level.

H. Susanto¹², M.N. Almunawar, and Y. C. Tuan, "Information security management system standards: A comparative study of the big five," Int. J. Electr. Comput. Sci. IJECISIJENS,. 23-29, 2011.

It cannot be denied that nowadays information is a very important asset for any modern organization. Therefore protecting its security is very important and becoming a top priority for many organizations. Unfortunately there is no single formula that can guarantee 100% of information security. Therefore there is a need for a set of benchmarks or standards to ensure the best security practices are adopted and an adequate level of security is attained. In this paper, authors introduce various information security standards briefly and then provide a comparative study for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. The study will provide a picture of the position and specialization of each standard, adoption by countries and their usability levels.

M. Stoll An Information Security Model for Implementing the New ISO 27001 Handb. Res. Emerg. Dev. Data Priv.,, 216 (2014)

The importance of data privacy, information availability, and integrity is increasingly recognized. Sharpened legal requirements and increasing data leakages have further promoted data privacy. In order to implement the different requirements in an effective, efficient, and sustainable way, the authors integrate different governance frameworks to their holistic information security and data privacy model. More than 1.5 million organizations worldwide are implementing a standard-based management system. In order to promote the integration of different standards, the International Standard Organization (ISO) released a common structure. ISO/IEC 27001 for information security management was changed accordingly in October 2013. The holistic model full fills all requirements of the new version. Its implementation in several organizations and the study's results are described. In that way data privacy and security are part of all strategic, tactical, and operational business processes, promote corporate governance and living security, as well as the full fulfillment of all standard requirements.

T. Lucio-Nieto, R. Colomo-Palacios, P. Soto-Acosta, S. Popa, and A. Amescua-Seco, "Implementing an IT service information management framework: The case of COTEMAR," Int. J. Inf. Manag., Dec. 2012.

It is evident that organizations are demanding more efficient information management technologies in order to offer high quality services for both internal and external clients. Firms pursue the implementation of processes aligned to their strategic and operational objectives and, to achieve these goals, they usually introduce various frameworks and approaches to information technology service management, such as Information Technology Infrastructure Library (ITIL) or Control Objectives for Information.

L. Lema, J.-A. Calvo-Manzano, R. Colomo-Palacios, and M. Arcilla, "ITIL in small to medium-sized enterprises software companies: towards an implementation sequence," J. Softw. Evol. Process, Aug. 2015.

Information technology infrastructure library (ITIL) framework is a set of comprehensive publications providing descriptive guidance on the management of IT processes, functions, roles, and responsibilities related to IT service management. However, and in spite of its repercussion and popularity, the ITIL framework does not suggest an implementation order for their processes. This decision constitutes the first challenge that an organization must overcome when starting an ITIL implementation, the enterprise size being one of the leading factors to be considered in the decision-making process. In the scenario of small and medium enterprises dedicated to producing software, this paper is devoted to investigating which processes are the most selected to start the implementation of ITIL in these organizations. This is performed by means of two different instruments, first, a systematic literature review on the topic and second, a survey conducted among experts and practitioners. Results show in both cases that incident management process should be the first process when implementing ITIL framework. Copyright © 2015 John Wiley & Sons, Ltd.

V. Stantchev and L. Stantcheva, "Extending Traditional IT-Governance Knowledge Towards SOA and Cloud Governance," Int. J. Knowl. Soc. Res. IJKSR, , 2012.

Enterprises today often strive to keep up with the paces of technological development. A particular case in point is the IT function where traditional governance approaches are often questioned by technology trends. Examples for such trends in the last ten years are the service-oriented architecture (SOA) and cloud computing. The introduction of SOA in the enterprise was one of the key enablers for cloud computing. Therefore, it can serve as a natural fit for bringing traditional IT governance approaches forward to the challenges of cloud governance. This article presents an approach for extending IT governance mindsets to the areas of SOA and cloud governance. It allows an IT organisation the adaptation and the continuous usage of already established governance knowledge and models during the

adoption of cloud computing solutions. The authors also present an application case study where they demonstrate the feasibility of the approach in real-life scenarios in the context of an international telecommunication provider.

Information Systems Audit and Control Association, An Introduction to the Business Model for Information Security. Rolling Meadows, 2009.

With more than 35,000 members in more than 100 countries, the Information Systems Audit and Control Association (ISACA) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor (CISA) designation earned by more than 35,000 professionals since inception, and Certified Information Security Manager (CISM) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," Inf. Manage., 138-151, 2014.

Information security strategies employ principles and practices grounded in both the prevention and response paradigms. The prevention paradigm aims at managing predicted threats. Although the prevention paradigm may dominate in contemporary commercial organizations, the response paradigm (aimed at managing unpredicted threats) retains an important role in protecting information security in today's dynamic threat environment. This study provides an overarching security framework.

L. A. Gordon and M. P. Loeb, "The economics of information security investment " ACM Trans. Inf. Syst. Secure. TISSEC, 2002.

This article presents an economic model that determines the optimal amount to invest to protect a given set of information. The model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. It is shown that for a given potential loss, a firm should not necessarily focus its investments on information sets with the highest vulnerability. Since extremely vulnerable information sets may be inordinately expensive to protect, a firm may be better off concentrating its efforts on information sets with midrange vulnerabilities. The analysis further suggests that to maximize the expected benefit from investment to protect information, a firm should spend only a small fraction of the expected loss due to a security breach.

B. Von Solms, “Information Security governance: COBIT or ISO 17799 or both,” Comput. Secur, 2005.

This paper investigates the co-existence of and complementary use of COBIT and ISO 17799 as reference frameworks for Information Security governance. The investigation is based on a mapping between COBIT and ISO 17799 which became available in 2004, and provides a level of 'synchronization 'between these two frameworks.

S. Sahibudin, M. Sharifi, and M. Ayat, “Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations,” in Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, 2008

Several frameworks, tools and standards have been included in IT management systems, in organizations. However, on their own, they are not comprehensive enough to serve as efficient IT management system. This paper reviews two established frameworks, i.e. ITIL, COBIT and a standard, ISO/IEC 27002 focusing on their similarities and differences. It then proposes a comprehensive framework by integrating the three general framework and standards into an IT framework that could be used in every company.

C. Pardo, F.J. Pino, F. García, M. Piattini, and M. T. Baldassarre, “A process for driving the harmonization of models,” in Proceedings of the 11th International Conference on Product Focused Software, 2010

At present, there are several factors that may influence an organization in needing to work with more than one reference model. The following can be highlighted:

- (i) Market niches with specific models,
- (ii) Improvement of practices from legacy process models,
- (iii) Business positioning,
- (iv) Leveraged or merger corporates
- (v) Systematic search of the capability of the processes,
- (vi) Business growth, among others.

Currently, however, there is no detailed strategy to address the harmonization of reference models. So, the aim of this paper is to present a process that defines the elements necessary to support the harmonization of multiple reference models. This process allows us to guide the implementation of a harmonization project systematically. It also describes our experience of the application of the proposed process in one organization. These results show that the process and the harmonization techniques used to support the objectives of harmonization of ISO 27001 and ISO 20000 of the company involved were suitable.

D. Gentner, “Structure-mapping: A theoretical framework for analogy,”

CognSci, 1983.

A theory of analogy must describe how the meaning of an analogy is derived from the meanings of its parts. In the structure-mapping theory, the interpretation rules are characterized as implicit rules for mapping knowledge about a base domain into a target domain. Two important features of the theory are

(a) The rules depend only on syntactic properties of the knowledge representation, and not on the specific content of the domains; and

(b) The theoretical framework allows analogies to be distinguished cleanly.

W. Guo and S. B. Kraines, “Explicit scientific knowledge comparison based on semantic description matching,” Proc. Am. Soc. Inf. Sci. Technol., 2008.

Researchers begin new research by acquiring pre-existing explicit scientific knowledge that is potentially relevant to the research subject. In order to find some potentially relevant explicit scientific knowledge items, such as knowledge whose content is similar to the targeted research, a researcher must examine the semantics of each item. In this paper, after reviewing related work, an automated semantic description matching-based approach is presented for comparing items of explicit scientific knowledge. This approach obtains a matching score between semantic descriptions of two items of explicit scientific knowledge that indicates their similarity. Three dimensions are considered in this approach: matching granularity, similarity scale for instance classes, and logic similarity scale. In order to match two semantic descriptions, a six-step method is presented: creation of atomic queries, generalization of query classes, generalization of query properties, addition of rules, creation of instances implied by complex class definition, and semi-automatic pruning of matching results. Finally, some conclusions regarding the approach are presented together with plans for future work.

International Organization for Standardisation and International Electrotechnical Commission, ISO/IEC 27003:2010. Geneva, 2010.

Adjustment and cost-effectiveness are key elements of a successful Information Security Management System (ISMS). ISMS-Processes, as basic elements of every ISMS, need to be aligned to the organization and its mission. As of today, a specific ISMS process framework does not exist. ISMS processes are not in focus of current research. This article aims to fill this research gap by presenting results of a process mapping study regarding ISMS processes in the most important and widely accepted international standards for Information Security

Management. Authors propose a set of ISMS processes within an ISMS process framework which should be implemented at an individually appropriate maturity level.

C. Loebbecke and B. Thomas, “Developing and enforcing internal information systems standards: InduMaker's Standards Management Process,” Dev. Enforc. Intern. Inf. Syst. Stand. InduMaker's, 2016.

It is widely agreed that standards provide numerous benefits when available and enforced. Company-internal Information Systems (IS) management procedures and solutions, in the following coined IS ‘standards’, allow for harmonizing operations between company units, locations and even different service providers. However, many companies lack an organized process for defining and managing internal IS standards, which causes uncertainties and delays in decision making, planning, and design processes. In this case study of the globally operating InduMaker (anonymized company name), an established manufacturing supplier, we look into the company-internal management of IS standards. Theoretically grounded in the organizational and IS-focused literature on business process modelling and business process commoditization, we describe and investigate InduMaker’s newly developed Standard Management Process (SMP) for defining and managing company-internal business and IS standards, with which the multinational pursues offering clear answers to business and IT departments about existing IS standards, their degree of obligation, applicability, and scope at any time.

J. L. Cheng and W. McKinley, “Toward an integration of organization research and practice: A contingency study of bureaucratic control and performance in scientific settings,” Adm. Sci. Q., , 1983.

Three characteristics of utilizable research-practical relevance, applicability of findings, and specificity-were identified and used as a basis for assessing the usefulness of the results from this study. The focus of the study was the contingency effect of bureaucratic control on organizational performance, and the organizations studied were scientific research units in universities.

Information Systems Audit and Control Association, IT-Governance and Process Maturity. Rolling Meadows, 2008.

With more than 35,000 members in more than 100 countries, the Information Systems Audit and Control Association ISACA is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor (CISA) designation earned by more than 35,000 professionals

since inception, and Certified Information Security Manager (CIS) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

V. Stantchev and G. Tamm, “Reducing Information Asymmetry in Cloud Marketplaces,” Int. J. Hum. Cap. Inf. Technol. Prof. IJHCITP, 1-10, 2012.

Cloud Computing is emerging as a predominant paradigm for obtaining and providing computing functionality in the enterprise. Organizations that are planning to use cloud computing offerings struggle with the question “How do I choose the right offering?” Cloud offerings exhibit a variety of pricing models and different levels of service and functionality. In this article the authors define first Cloud Computing in the context of IT Governance. Then they set criteria to compare different offerings at the level of Software-as-a-Service (SaaS). This is an important precondition for the reduction of the verifiable information asymmetry and uncertainty in the cloud market. Besides deficiencies on the supply side, regarding configuration, display and communication of service bundles, the limited knowledge of potential buyers is main reason for the modest adoption. The authors apply strategies derived from information economics to reduce this asymmetry by integrating information substitutes in the service marketplace description, thereby transforming experience and credence qualities into search qualities.

Security threats to Internet: a Korean multi-industry investigation 2001

In recent years, a number of security problems with the Internet became apparent. New and current Internet users need to be aware of the likelihood of security incidents and the steps they should take to secure their sites. Before designing a secure system, it is advisable to identify the specific threats against which protection is required. The threats may be classified into interruption, interception, modification, and fabrication. The extents of these threats are examined across four industries in Korea — manufacturing, banking/financial, research institution/university, and distribution/service. Banking/financial firms generally perceive the four categories of threats more seriously than other industries. The companies in the manufacturing industry consider interruption to be the most serious. Research institutions/universities and distribution/service companies regard modification and interruption as critical threats. The appropriate security technique is recommended for each threat.

A survey of security issues in office computation and the application of secure computing models to office systems 1993.

With the proliferation of office information systems (OIS) into almost every area of industry and government, it is important to design systems that offer a guarantee of privacy and security to their users. The same solutions and research pertaining to traditional data-processing environments cannot, in most cases, be applied directly to the OIS environment. Many OIS do not provide the hardware/software controls necessary to protect information

from anyone who gains physical access to the system. Furthermore, users of an OIS cannot be expected to possess a clear understanding of the system, its operating characteristics, or even the implication of interconnecting component devices.

This paper examines the typical OIS environment with a view toward the provision of a secure operating architecture. Important security problems faced by OIS are enumerated and explained. We argue that the OIS environment presents a different problem to solve in a security sense from when working with a traditional non distributed system. Existing solutions found in large scale operating systems and networks cannot simply be scaled down and moved to an OIS, if for no other reason than the architecture's inability to support locks and multiple system states. An architecture of both software and hardware controls must be built for this new environment using concepts from large scale operating systems but recognizing the limitations and constraints of OIS. While we emphasize the security issues, we look at alternative technologies that can be combined to provide a solution.

Rutledge, L.S., Hoffman, L.J.: A survey of issues in computer network security. Comput. Secur. (1986)

Computer networks are proliferating rapidly for a number of reasons discussed in this paper. During this boom, relatively little attention has been paid to computer network security. This paper describes problems posed by network security and presents a survey of methods and technologies available today to enhance network security. Current methods are discussed, including information security strategy, computer security and its relation to network security, data communications security, and data encryption.

Koops, B.-J.: The Internet and Its Opportunities for Cybercrime, Transnational Criminology Manual, 1st edn., pp. 735–754, Herzog-Evans M. (ed.) (2010)

The Internet deserves special attention in criminology as well as criminal law and policy, because of several characteristics: it is global, instantaneous, intrinsically transborder, digital, and enables automated information processing. Because of these characteristics, the Internet provides special opportunities to commit cybercrimes: crimes in which computer networks are the target or a substantial tool.

Alguliyev, R., Imamverdiyev, Y., Sukhostat, L.: Cyber-physical systems and their security issues. Comput. Ind. 100, 212–223 (2018)

The creation of cyber-physical systems posed new challenges for people. Ensuring the information security of cyber-physical systems is one of the most complex problems in a wide range of defenses against cyber-attacks. The aim of this paper is to analyse and classify existing research papers on the security of cyber-physical systems. Philosophical issues of cyber-physical systems are raised. Their influence on the aspects of people's lives is investigated. The principle of cyber-physical system operation is described.

Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security—a Survey. IEEE Int. Things J. 4(6), 1802–1831 (2017)

With the exponential growth of cyber-physical systems (CPSs), new security challenges have emerged. Various vulnerabilities, threats, attacks, and controls have been introduced for the new generation of CPS. However, there lacks a systematic review of the CPS security literature. In particular, the heterogeneity of CPS components and the diversity of CPS systems have made it difficult to study the problem with one generalized model. In this paper, we study and systematize existing research on CPS security under a unified framework. The framework consists of three orthogonal coordinates:

- 1) From the security perspective, we follow the well-known taxonomy of threats, vulnerabilities, attacks and controls;
- 2) From the CPS components perspective, we focus on cyber, physical, and cyberphysical components; and
- 3) From the CPS systems perspective, we explore general CPS features as well as representative systems (e.g., smart grids, medical CPS, and smart cars).

The model can be both abstract to show general interactions of components in a CPS application, and specific to capture any details when needed. By doing so, we aim to build a model that is abstract enough to be applicable to various heterogeneous CPS applications; and to gain a modular view of the tightly coupled CPS components. Such abstract decoupling makes it possible to gain a systematic understanding of CPS security, and to highlight the potential sources of attacks and ways of protection. With this intensive literature review, we attempt to summarize the state-of-the-art on CPS security, provide researchers with a comprehensive list of references, and also encourage the audience to further explore this emerging field.

Aradau, C.: Security that matters: critical infrastructure and objects of protection. Secur. (2010)

Critical infrastructure protection is prominently concerned with objects that appear indispensable for the functioning of social and political life. However, the analysis of material objects in discussions of critical infrastructure protection has remained largely within the remit of managerial responses, which see matter as simply passive, a blank slate. In security studies, critical approaches have focused on social and cultural values, forms of life, technologies of risk or structures of neoliberal globalization. This article engages with the role of ‘things’ or of materiality for theories of securitization. Drawing on the materialist feminism of Karen Barad, it shows how critical infrastructure in Europe neither is an empty receptacle of discourse nor has ‘essential’ characteristics; rather, it emerges out of material-discursive practices. Understanding the securitization of critical infrastructure protection as

a process of materialization allows for a reconceptualization of how security matters and its effects.

Jordan, M.I., Mitchell, T.M.: Machine learning: trends, perspectives, and prospects. Sci. Am. Assoc. Advance. Sci. 349(6245):255–260 (2015)

Machine learning addresses the question of how to build computers that improve automatically through experience. It is one of today's most rapidly growing technical fields, lying at the intersection of computer science and statistics, and at the core of artificial intelligence and data science. Recent progress in machine learning has been driven both by the development of new learning algorithms and theory and by the ongoing explosion in the availability of online data and low-cost computation. The adoption of data-intensive machine-learning methods can be found throughout science, technology and commerce, leading to more evidence-based decision-making across many walks of life, including health care, manufacturing, education, financial modeling, policing, and marketing.

Kim, N.Y., Rathore, S., Ryu, J.H., Park, J.H., Park, J.H.: A survey on cyber physical system security for IoT: issues, challenges, threats, solutions. J. Inf. Process. Syst. 14(6), 1361–1384 (2018)

Recently, Cyber Physical System (CPS) is one of the core technologies for realizing Internet of Things (IoT). The CPS is a new paradigm that seeks to converge the physical and cyber worlds in which we live. However, the CPS suffers from certain CPS issues that could directly threaten our lives, while the CPS environment, including its various layers, is related to on-the-spot threats, making it necessary to study CPS security. Therefore, a survey-based in-depth understanding of the vulnerabilities, threats, and attacks is required of CPS security and privacy for IoT. In this paper, we analyze security issues, threats, and solutions for IoT-CPS, and evaluate the existing researches. The CPS raises a number challenges through current security markets and security issues. The study also addresses the CPS vulnerabilities and attacks and derives challenges. Finally, we recommend solutions for each system of CPS security threats, and discuss ways of resolving potential future issues.

Singh, A., Jain, A.: Study of cyber attacks on cyber-physical system. In: Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), (2018)

Cyber-Physical Systems are the combination of the cyber world and physical world components in order to increase the physical performance. The usages of cyber-physical systems (CPS) are increased, because of the more cyber and physical devices are connected to provide the state of the art technologies and thereafter cyber threats and attacks are also happened and reported exponentially. The Security issues and challenges of the CPS have become a global issue and appropriate mechanism for CPS is in urgent required. In this paper, an investigation about the relationship between the CPS and IoT, its definitions, and

some of its domains are discussed. Security challenges and issues are studied and discussed in the context of CPS. Various CPS vulnerabilities, cyber threats, and cyber-attacks on the cyber-physical system are presented in this paper. Finally, suggested security measures, methods, and security protocols for minimizing the cyber threat or attacks on the cyber-physical system.

Brown, G., Carlyle, M., Salmerón, J., Wood, K.: Defending critical infrastructure. *Interfaces* 36(6), 530–544 (2006)

We apply new bilevel and trilevel optimization models to make critical infrastructure more resilient against terrorist attacks. Each model features an intelligent attacker (terrorists) and a defender (us), information transparency, and sequential actions by attacker and defender. We illustrate with examples of the US Strategic Petroleum Reserve, the US Border Patrol at Yuma, Arizona, and an electrical transmission system. We conclude by reporting insights gained from the modeling experience and many “red-team” exercises. Each exercise gathers open-source data on a real-world infrastructure system, develops an appropriate bilevel or trilevel model, and uses these to identify vulnerabilities in the system or to plan an optimal defense.

Rajkumar, R., Lee, I., Sha, L., Stankovic, J.: Cyber-physical systems: the next computing revolution. In: *Proceedings of the 47th Design Automation Conference, DAC '10, ACM, New York, NY, USA, 2010*

Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Just as the internet transformed how humans interact with one another, cyber-physical systems will transform how we interact with the physical world around us. Many grand challenges await in the economically vital domains of transportation, health-care, manufacturing, agriculture, energy, defense, aerospace and buildings. The design, construction and verification of cyber-physical systems pose a multitude of technical challenges that must be addressed by a cross-disciplinary community of researchers and educators.

Singh, S., Yadav, N., Chuarasia, P.K.: A review on cyber physical system attacks: issues and challenges. In: *2020 International Conference on Communication and Signal Processing (ICCSP), IEEE (2020)*

Recent advancement of cyber physical systems open doors to various safety measures, threats, attacks and vulnerabilities are such major key challenges now days. The globally adoption of cyber physical systems basically forms a basis for cyber social attack in order to breakdown secure channel and control actions. Hence loopholes and vulnerabilities in trending cyber physical systems are targeted to make systems unstable and unsafe state.

The subsection of CPSs causes new critical issues for research and academics. However expeditious growth of CPS devices a question marks on security, integrity and confidentiality. The paradigm which forms basis for CPS are Smart phones, Defense System, Meteorology, Big data, Smart Technologies and Smart Vehicles. The purpose and analysis behind this paper to find out security issues and challenges of CPSs. Comparison of various cyber physical attacks and analysis on several parameters has been done. Key noted issues are results of cyber attacks, CPS attack traceability and the review on communication security architecture.

Miller, B., Rowe, D.: A survey of SCADA and critical infrastructure incidents. In: Proceedings of the 1st Annual Conference on Research in Information Technology, (2012)

In this paper, we analyze several cyber-security incidents involving critical infrastructure and SCADA systems. We classify these incidents based on Source Sector, Method of Operations, Impact, and Target Sector. Using this standardized taxonomy we can easily compare and contrast current and future SCADA incidents.

Bhattacharyya, D.K., Kalita, J.K.: Network Anomaly Detection: A Machine Learning Perspective. Chapman and Hall/CRC (2013)

With the rapid rise in the ubiquity and sophistication of Internet technology and the accompanying growth in the number of network attacks, network intrusion detection has become increasingly important. Anomaly-based network intrusion detection refers to finding exceptional or nonconforming patterns in network traffic data compared to normal behavior. Finding these anomalies has extensive applications in areas such as cyber security, credit card and insurance fraud detection, and military surveillance for enemy activities. Network Anomaly Detection: A Machine Learning Perspective presents machine learning techniques in depth to help you more effectively detect and counter network intrusion.

In this book, you'll learn about: Network anomalies and vulnerabilities at various layers The pros and cons of various machine learning techniques and algorithms A taxonomy of attacks based on their characteristics and behaviour Feature selection algorithms How to assess the accuracy, performance, completeness, timeliness, stability, interoperability, reliability, and other dynamic aspects of a network anomaly detection system Practical tools for launching attacks, capturing packet or flow traffic, extracting features, detecting attacks, and evaluating detection performance Important unresolved issues and research challenges that need to be overcome to provide better protection for networks Examining numerous attacks in detail, the authors look at the tools that intruders use and show how to use this knowledge to protect networks.

The book also provides material for hands-on development, so that you can code on a test bed to implement detection methods toward the development of your own intrusion

detection system. It offers a thorough introduction to the state of the art in network anomaly detection using machine learning approaches and systems.

Mitchell, T.M., et al.: Machine Learning (1997)

Every two years since 1997, an international colloquium on cognitive science is held in Donostia - San Sebastian, attracting the most important researchers in that field. This volume is a collection of the invited papers to the Sixth International Colloquium on Cognitive Science (ICCS-99), written from a multidisciplinary, cognitive perspective, and addressing various essential topics such as self-knowledge, intention, consciousness, language use, learning and discourse. This collection reflects not only the various interdisciplinary origins and standpoints of the participating researchers, but also the richness, fruitfulness, and exciting state of research in the field of cognitive science today. A must-read for anyone interested in philosophy, linguistics, psychology, and computer science, and in the perception of these topics from the perspective of cognitive science.

Mohri, M., Rostamizadeh, A., Talwalkar, A.: Foundations of Machine Learning. MIT Press (2018)

A new edition of a graduate-level machine learning textbook that focuses on the analysis and theory of algorithms. This book is a general introduction to machine learning that can serve as a textbook for graduate students and a reference for researchers. It covers fundamental modern topics in machine learning while providing the theoretical basis and conceptual tools needed for the discussion and justification of algorithms. It also describes several key aspects of the application of these algorithms. The authors aim to present novel theoretical tools and concepts while giving concise proofs even for relatively advanced topics. Foundations of Machine Learning is unique in its focus on the analysis and theory of algorithms.

The first four chapters lay the theoretical foundation for what follows; subsequent chapters are mostly self-contained. Topics covered include the Probably Approximately Correct (PAC) learning framework; generalization bounds based on Rademacher complexity and VC-dimension; Support Vector Machines (SVMs); kernel methods; boosting; on-line learning; multi-class classification; ranking; regression; algorithmic stability; dimensionality reduction; learning automata and languages; and reinforcement learning. Each chapter ends with a set of exercises. Appendixes provide additional material including concise probability review. This second edition offers three new chapters, on model selection, maximum entropy models, and conditional entropy models. New material in the appendixes includes a major section on Fenchel duality, expanded coverage of concentration inequalities, and an entirely new entry on information theory.

Caruana, R., Niculescu-Mizil, A.: An empirical comparison of supervised learning algorithms. In: Proceedings of the 23rd International Conference on Machine Learning, (2006)

A number of supervised learning methods have been introduced in the last decade. Unfortunately, the last comprehensive empirical evaluation of supervised learning was the Statlog Project in the early 90's. We present a large-scale empirical comparison between ten supervised learning methods: SVMs, neural nets, logistic regression, naive bayes, memory-based learning, random forests, decision trees, bagged trees, boosted trees, and boosted stumps. We also examine the effect that calibrating the models via Platt Scaling and Isotonic Regression has on their performance. An important aspect of our study is the use of a variety of performance criteria to evaluate the learning methods.

Dietterich, T.G., et al.: Ensemble learning. In: The Handbook of Brain Theory and Neural Networks, (2002)

The function is called a classifier, because it assigns class labels $\hat{Y}$ to input data points $\hat{X}$. Supervised learning can be applied to many problems including handwriting recognition, medical diagnosis, and part-of-speech tagging in language processing. Ordinary machine learning algorithms work by searching through a space of possible functions, called hypotheses, to find the one function, that is the best approximation to the unknown function. To determine which hypothesis is best, a learning algorithm can measure how well matches on the training data points, and it can also assess how consistent is with any available prior knowledge about the problem.

Polikar, R.: Ensemble learning. In: Ensemble Machine Learning, Springer (2012)

Over the last couple of decades, multiple classifier systems, also called ensemble systems have enjoyed growing attention within the computational intelligence and machine learning community. This attention has been well deserved, as ensemble systems have proven themselves to be very effective and extremely versatile in a broad spectrum of problem domains and real-world applications. Originally developed to reduce the variance—thereby improving the accuracy—of an automated decision-making system, ensemble systems have since been successfully used to address a variety of machine learning problems, such as feature selection, confidence estimation, missing feature, incremental learning, error correction, class-imbalanced data, learning concept drift from nonstationary distributions, among others. This chapter provides an overview of ensemble systems, their properties, and how they can be applied to such a wide spectrum of applications.

Sagi, O., Rokach, L.: Ensemble learning: a survey. Wiley Interdis. Rev. Data Min. Knowl. Discov. 8(4), e1249 (2018)

Ensemble methods are considered the state-of-the-art solution for many machine learning challenges. Such methods improve the predictive performance of a single model by training multiple models and combining their predictions. This paper introduces the concept of ensemble learning, reviews traditional, novel and state-of-the-art ensemble methods and discusses current challenges and trends in the field.

Kira, K., Rendell, L.A.: A practical approach to feature selection. In: Machine Learning Proceedings 1992, Elsevier (1992)

In real-world concept learning problems, the representation of data often uses many features, only a few of which may be related to the target concept. In this situation, feature selection is important both to speed up learning and to improve concept quality. A new feature selection algorithm Relief uses a statistical method and avoids heuristic search. Relief requires linear time in the number of given features and the number of training instances regardless of the target concept to be learned.

Guyon, I., Elisseeff, A.: An introduction to variable and feature selection. J. Mach. Learn. Res. 3(Mar):1157–1182 (2003)

Variable and feature selection have become the focus of much research in areas of application for which datasets with tens or hundreds of thousands of variables are available. These areas include text processing of internet documents, gene expression array analysis, and combinatorial chemistry. The objective of variable selection is three-fold: improving the prediction performance of the predictors, providing faster and more cost-effective predictors, and providing a better understanding of the underlying process that generated the data. The contributions of this special issue cover a wide range of aspects of such problems: providing a better definition of the objective function, feature construction, feature ranking, multivariate feature selection, efficient search methods, and feature validity assessment methods.

Li, J., Cheng, K., Wang, S., Morstatter, F., Trevino, R.P., Tang, J., Liu, H.: Feature selection: a data perspective. ACM Comput. Surv. (CSUR) 50(6), 1–45 (2017)

Feature selection, as a data preprocessing strategy, has been proven to be effective and efficient in preparing data (especially high-dimensional data) for various data-mining and machine-learning problems. The objectives of feature selection include building simpler and more comprehensible models, improving data-mining performance, and preparing clean, understandable data. The recent proliferation of big data has presented some substantial

challenges and opportunities to feature selection. In this survey, we provide a comprehensive and structured overview of recent advances in feature selection research.

Motivated by current challenges and opportunities in the era of big data, we revisit feature selection research from a data perspective and review representative feature selection algorithms for conventional data, structured data, heterogeneous data and streaming data. Methodologically, to emphasize the differences and similarities of most existing feature selection algorithms for conventional data, we categorize them into four main groups: similarity-based, information-theoretical-based, sparse-learning-based, and statistical-based methods. To facilitate and promote the research in this community, we also present an open source feature selection repository that consists of most of the popular feature selection algorithms. Also, we use it as an example to show how to evaluate feature selection algorithms. At the end of the survey, we present a discussion about some open problems and challenges that require more attention in future research.

E.: Discriminatory Analysis: Nonparametric Discrimination, Consistency Properties, vol. 1. USAF School of Aviation Medicine (1985)

The discrimination problem (two population case) may be defined as follows: a random variable Z , of observed value z , is distributed over some space (say, p -dimensional) either according to distribution F , or according to distribution G . The problem is to decide, on the basis of z , which of the two distributions Z has. The problem may be classified in various ways into subproblems. One pertinent method of classification is according to the amount of information assumed to be available about F and G .

Murphy, K.P., et al.: Naive Bayes classifiers. Univ. Br. Columbia 18(60) (2006)

We will focus our attention on probabilistic classifiers, ie, methods that return $p(y|x)$. (We will discuss the advantages of having probabilities below.) There are two main ways to do this. The first is to directly learn the function that computes the class posterior $p(y|x)$: this is called a discriminative model, since it discriminates between different classes given the input.

Cortes, C., Vapnik, V.: Support-vector networks. Machine Learn 20(3), 273–297 (1995)

The *support-vector network* is a new learning machine for two-group classification problems. The machine conceptually implements the following idea: input vectors are non-linearly mapped to a very high-dimension feature space. In this feature space a linear decision surface is constructed. Special properties of the decision surface ensures high generalization ability of the learning machine. The idea behind the support-vector network was previously implemented for the restricted case where the training data can be separated without errors. We here extend this result to non-separable training data.

High generalization ability of support-vector networks utilizing polynomial input transformations is demonstrated. We also compare the performance of the support-vector network to various classical learning algorithms that all took part in a benchmark study of Optical Character Recognition.

Breiman, L.: Random forests. *Machine Learn.* 45(1), 5–32 (2001)

Random forests are a combination of tree predictors such that each tree depends on the values of a random vector sampled independently and with the same distribution for all trees in the forest. The generalization error for forests converges a.s. to a limit as the number of trees in the forest becomes large. The generalization error of a forest of tree classifiers depends on the strength of the individual trees in the forest and the correlation between them. Using a random selection of features to split each node yields error rates that compare favourably to Ada boost (Y. Freund & R. Schapire, *Machine Learning: Proceedings of the Thirteenth International conference*, ***, 148–156), but are more robust with respect to noise. Internal estimates monitor error, strength, and correlation and these are used to show the response to increasing the number of features used in the splitting. Internal estimates are also used to measure variable importance. These ideas are also applicable to regression.

Geurts, P., Ernst, D., Wehenkel, L.: Extremely randomized trees. *Machine Learn.* 63(1), 3–42 (2006)

This paper proposes a new tree-based ensemble method for supervised classification and regression problems. It essentially consists of randomizing strongly both attribute and cut-point choice while splitting a tree node. In the extreme case, it builds totally randomized trees whose structures are independent of the output values of the learning sample. The strength of the randomization can be tuned to problem specifics by the appropriate choice of a parameter. We evaluate the robustness of the default choice of this parameter, and we also provide insight on how to adjust it in particular situations. Besides accuracy, the main strength of the resulting algorithm is computational efficiency. A bias variance analysis of the Extra-Trees algorithm is also provided as well as a geometrical and a kernel characterization of the models induced.

Freund, Y., Schapire, R., Abe, N.: A short introduction to boosting. *J.-Japan. Soc. Artif. Intell.* 14(771–780), 1612 (1999)

Boosting is a general method for improving the accuracy of any given learning algorithm. This short overview paper introduces the boosting algorithm AdaBoost, and explains the underlying theory of boosting, including an explanation of why boosting often does not suffer from overfitting as well as boosting's relationship to support-vector machines. Some examples of recent applications of boosting are also described.

Goh, J., Adepu, S., Junejo, K.N., Mathur, A.: A dataset to support research in the design of secure water treatment systems. In: International Conference on Critical Information Infrastructures Security, Springer (2016)

This paper presents a dataset to support research in the design of secure Cyber Physical Systems (CPS). The data collection process was implemented on a six-stage Secure Water Treatment (SWAT) test bed. SWAT represents a scaled down version of a real-world industrial water treatment plant producing 5 gallons per minute of water filtered via membrane based ultrafiltration and reverse osmosis units. This plant allowed data collection under two behavioral modes: normal and attacked. SWAT was run non-stop from its “empty” state to fully operational state for a total of 11-days. During this period, the first seven days the system operated normally i.e. without any attacks or faults. During the remaining days certain cyber and physical attacks were launched on SWAT while data collection continued. The dataset reported here contains the physical properties related to the plant and the water treatment process, as well as network traffic in the test bed. The data of both physical properties and network traffic contains attacks that were created and generated by our research team.

Morris, T., Gao, W.: Industrial control system traffic data sets for intrusion detection research. In: International Conference on Critical Infrastructure Protection. Springer (2014)

Supervisory control and data acquisition (SCADA) systems monitor and control physical processes associated with the critical infrastructure. Weaknesses in the application layer protocols, however, leave SCADA networks vulnerable to attack. In response, cyber security researchers have developed myriad intrusion detection systems. Researchers primarily rely on unique threat models and the corresponding network traffic data sets to train and validate their intrusion detection systems. This leads to a situation in which researchers cannot independently verify the results, cannot compare the effectiveness of different intrusion detection systems, and cannot adequately validate the ability of intrusion detection systems to detect various classes of attacks. Indeed, a common data set is needed that can be used by researchers to compare intrusion detection approaches and implementations. This paper describes four data sets, which include network traffic, process control and process measurement features from a set of 28 attacks against two laboratory-scale industrial control systems that use the MODBUS application layer protocol. The data sets, which are freely available, enable effective comparisons of intrusion detection solutions for SCADA systems.

Morris, T.H., Thornton, Z., Turnipseed, I.: Industrial control system simulation and data logging for intrusion detection system research. In: 7th Annual South eastern Cyber Security Summit, (2015)

Industrial control system intrusion detection is a popular topic of research for several years, and many intrusion detection systems (IDS) have been proposed in literature. IDS researchers lack a common framework to train and test proposed algorithms. This leads to an inability to properly compare proposed IDS and limits research progress. This paper documents 2 approaches to data sharing for the industrial control system IDS research community. First, a network traffic data log captured from a gas pipeline is presented. The gas pipeline data log was captured in a laboratory and includes artifacts of normal operation and cyber attacks. Second, an expandable virtual gas pipeline is presented which includes a human machine interface, programmable logic controller, Modbus/TCP communication, and a Simulink based gas pipeline model. The virtual gas pipeline provides the ability to model cyber-attacks and normal behavior. IDS solutions can overlay the virtual gas pipeline for training and testing.

Battiti, R.: Using mutual information for selecting features in supervised neural net learning. IEEE Trans. Neural Netw. 5(4), 537–550 (1994)

This paper investigates the application of the mutual information criterion to evaluate a set of candidate features and to select an informative subset to be used as input data for a neural network classifier. Because the mutual information measures arbitrary dependencies between random variables, it is suitable for assessing the "information content" of features in complex classification tasks, where methods based on linear relations (like the correlation) are prone to mistakes. The fact that the mutual information is independent of the coordinates chosen permits a robust estimation. Nonetheless, the use of the mutual information for tasks characterized by high input dimensionality requires suitable approximations because of the prohibitive demands on computation and samples. An algorithm is proposed that is based on a "greedy" selection of the features and that takes both the mutual information with respect to the output class and with respect to the already-selected features into account. Finally the results of a series of experiments are discussed.

CHAPTER-3

RESEARCH METHODOLOGY

RESEARCH

The term "Research Methodology" encompasses the systematic framework designed to assess the methods, tools, techniques, and procedures employed for data collection and analysis. The methodology employed encompasses diverse research techniques such as literature review, interviews, surveys, and other pertinent research methodologies, providing a comprehensive examination of both contemporary and historical data.

3.1 RESEARCH DESIGN

“A research design is the arrangement of conditions for collection and analysis data in a manner that aims to combine relevance to the researcher purpose with economy in procedure”.

It constitutes the blueprint for the collection, measurement and analysis of data. As such the design includes an outline of what the researcher will do from writing the hypothesis and its operational implication to the final analysis of data.

3.2 SAMPLE DESIGN

The sample design is a definite plan for obtaining a sample from a given population. It refers to the technique or procedure would adopt to selecting a items for the sample. Sample design may as well lay down to be included in the sample i.e. the size of the sample. Sample design is determined before data are collected. There are many sample design from which a researcher can choose. Some designs are relatively more precise and easier to apply than others.

TYPE OF UNIVERSE

The first step in developing any sample design is to clearly define the set of objects, technically called a universe to be studied.

3.3 SAMPLE SIZE

This refers to the number of items to be selected from the universe to constitute a sample. The sample size used in this study is 100 numbers;

3.4 SAMPLING TECHNIQUE

There is different type of sample design based on two factors viz. representation basis and element selection technique. On Representation basis the sample is classified into

- ❖ Probability sampling
- ❖ Non-probability sampling

The project is taken the Simple random sampling.

SIMPLE RANDOM SAMPLING

Probability sampling is also known as 'random sampling' or 'chance sampling'. Under this sampling design every item of the universe equal chance of inclusion in the sample.

3.5 DATA COLLECTION

There are two type of data collection

- Primary data
- Secondary data

Primary Data

In this project, the data is collected to know about the study of Network security management is the practice of managing the firewalls and policies to prevent and monitor access across the network. But separately managing each firewall and security tool creates several issues: The chances of human error are high, leading to vulnerabilities in the network.

Secondary Data

Secondary data was collected from Internet, books, journals, and Network security.

3.6 TOOLS FOR DATA COLLECTION

There are several methods of collecting primary data, particularly in surveys and descriptive researches. The tools used in this project are:-

QUESTIONNAIRE

A Questionnaire-cum-schedule was constructed with questions to obtain the necessary information for the research.

3.7 STATISTICAL TOOLS

❖ Percentage method

❖ Chi-square test

PERCENTAGE METHOD

This is one of the widely used methods to analyse the collected data. The percentage method is calculated by number of respondents divided by total number of respondents, which is multiplied by 100.

$$\text{Percentage analysis} = \frac{\text{No of Respondent}}{\text{Total no. of Respondents}} \times 100$$

Chi-Square Test

It is a useful measure of comparing experimentally obtained results with those expected theoretically and based on the hypothesis. Chi-square test involves comparison of expected frequency (E_i) with observed frequency (O_i) to determine whether difference between the two is greater than the tabulated value that might occur by chance.

Formula $\chi^2 = \sum (O - E)^2 / E$

Where, O = Observed Frequency, E = Expected frequency.

Uses

- It is used to check the goodness of fit among the variables.
- It is widely used to test the independence of attributes.

3.8 SCOPE OF STUDY

- The scope for cyber security in India is immense and continues to grow rapidly.
- The increasing digitization of various sectors and the rise in cyber threats, there is a significant demand for cyber security professionals and services in the country.
- As per today's industry infrastructure situation, all kinds of organizations first aim to prepare one good network security system to ensure the loss of any secure data.
- And in this specific place value of a network engineer will automatically gain as per organization requirements.
- Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.

- The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.
- Businesses will continue to need network engineers, but they'll be looking for candidates with new skills as networks increasingly shift to cloud architectures, security evolves, and how we interact with these tools changes.
- That's good news for network engineers because their jobs will remain in demand.

3.9 LIMITATION OF STUDY

- Addiction, time-waster, and causes distractions.
- Bullying, trolls, stalkers, and crime.
- Spam and advertising.
- Pornographic and violent images.
- Never being able to disconnect from work.
- Identity theft, hacking, viruses, and cheating.
- Affects focus and patience.
- Health issues and obesity.

3.10 HYPOTHESIS

HYPOTHESIS 1:

- H0: The choice of anti-virus software is independent of gender.
- H1: The choice of anti-virus software is not independent of gender.

HYPOTHESIS 2:

- H0: The occurrence of the code is independent of the type of malicious software.
- H1: The occurrence of the code is dependent on the type of malicious software.

CHAPTER-4

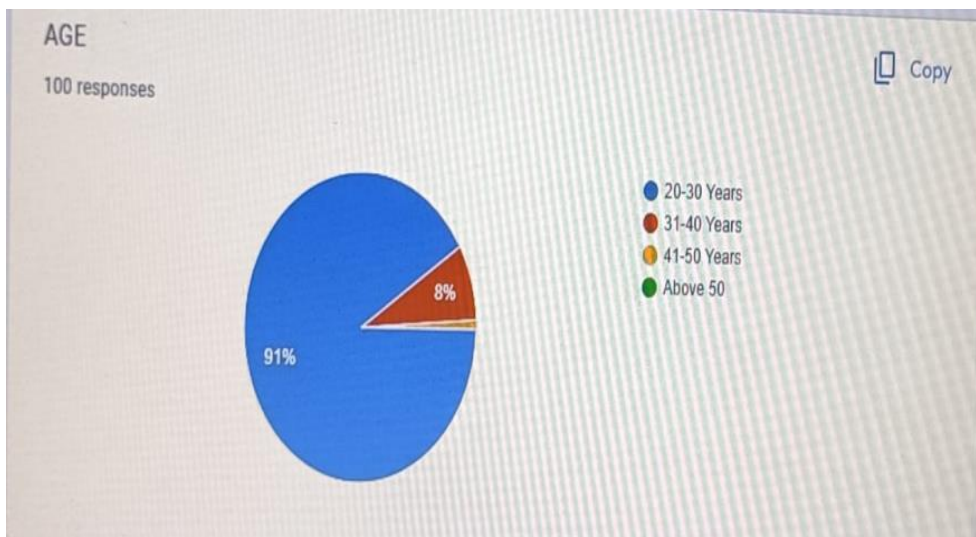
DATA ANALYSIS AND INTERPRETATION

PERCENTAGE ANALYSIS

4.1 Table indicating the age of respondents

S.no	Age	Percentage analysis
1.	20-30 Years	91%
2.	31-40 Years	8%
3.	41-50 Years	1%
4.	Above 50	
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents 20-30 ages of respondents are 91%, between 31-40 age of respondents are 8%, between 41- 50 age of respondents 1%, and above 50 ages of respondents are Nil.

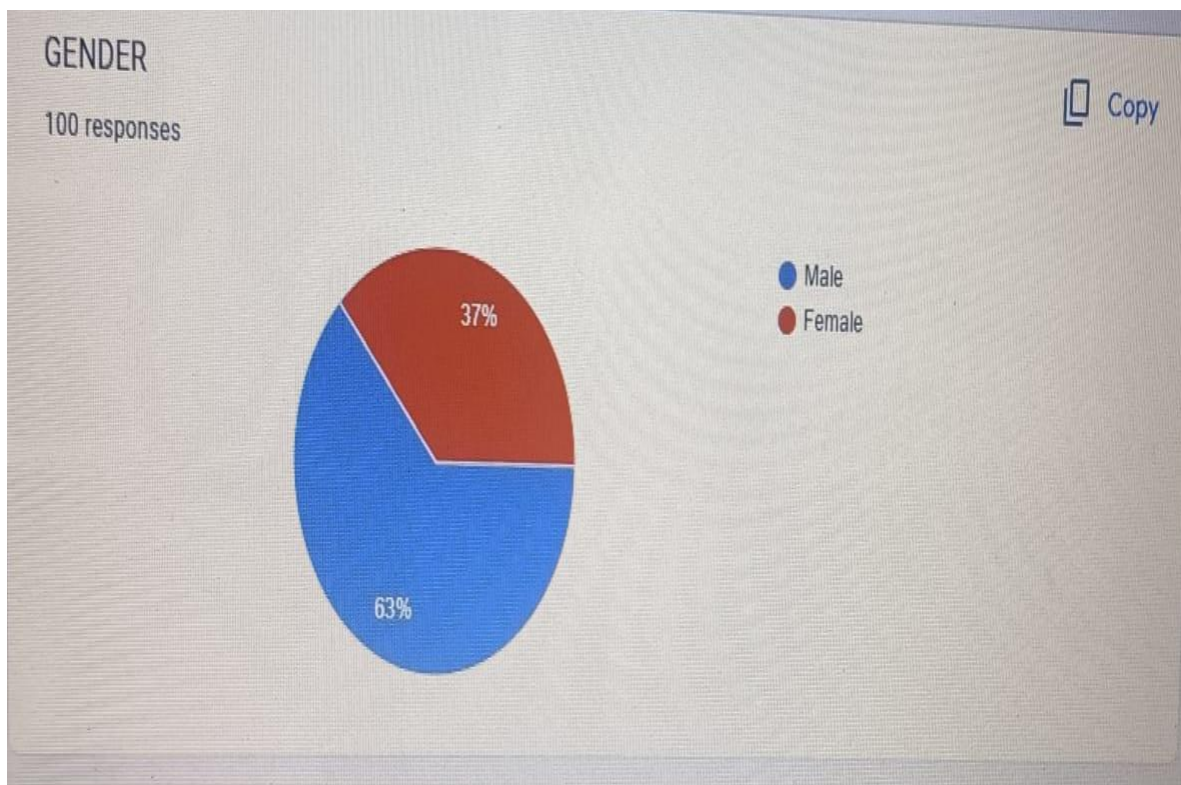
INFERENCE

➤ Majority 91 % of the respondents belong to the age group of 20-30 category.

4.2 Table indicating the gender of respondents

S.no	Gender	Percentage analysis
1.	Male	63%
2.	Female	37%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the gender of the respondents is male 63% and number of respondents in female are 37 %.

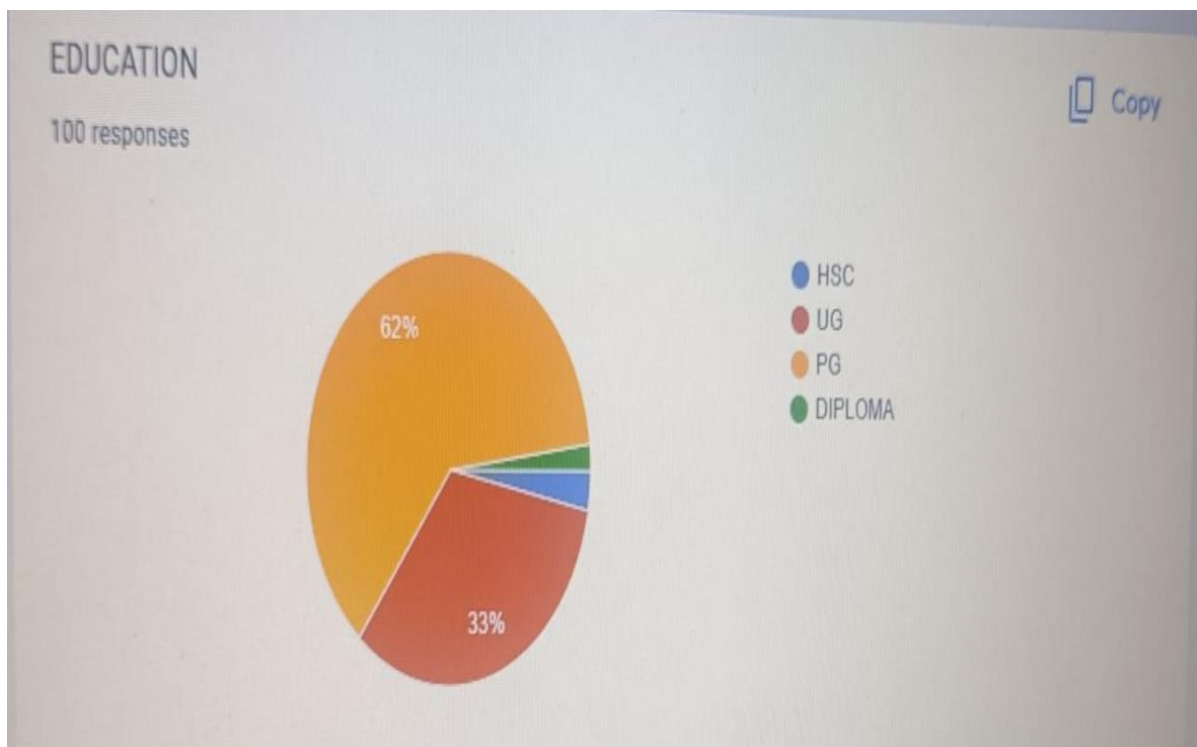
INFERENCE

➤ Majority 63% of the respondents are male.

4.3 Table indicating the education qualification of respondents

S.no	Education qualification	Percentage analysis
1.	HSC	4%
2.	UG	33%
3.	PG	62%
4.	DIPLOMA	1%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents HSC of respondents are 4% Under Graduate of respondents are 33%, and Post Graduate of respondents 62 %, Diploma of respondents are 1%.

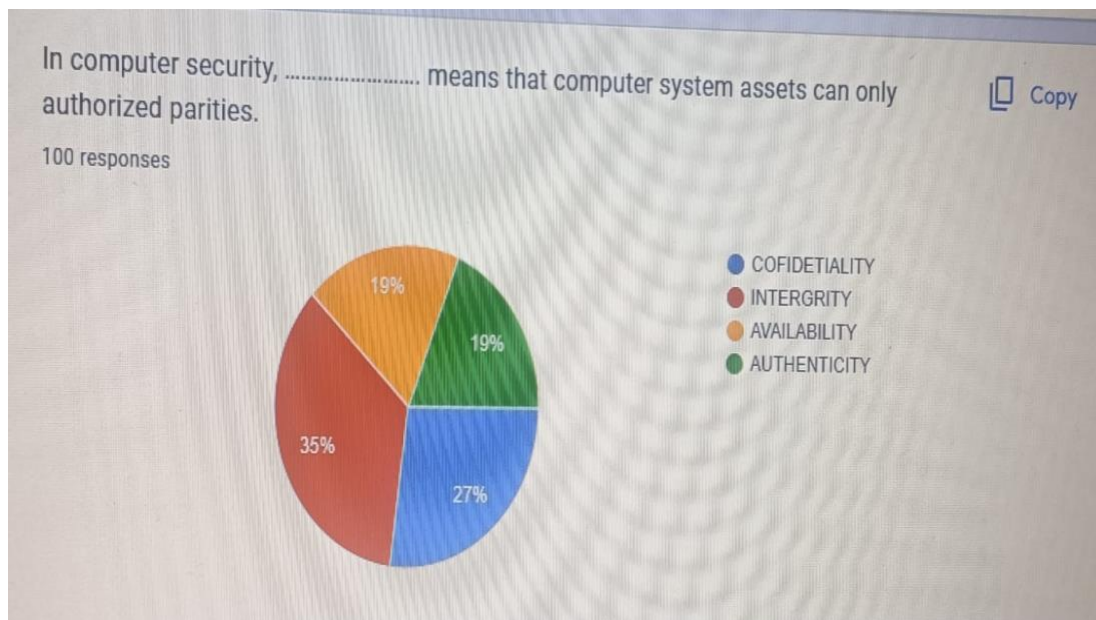
INFERENCE

➤ Majority 62% of the respondents belongs to PG educational qualification.

4.4 Table indicating the computer system assets can only authorized parities.

S.no	Attributes	Percentage analysis
1.	CONFIDENTIALITY	27%
2.	INTERGRITY	35%
3.	AVAILABILITY	19%
4.	AUTHENTICITY	19%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Confidentiality of respondents are 27%, Integrity of respondents are 35%, Availability of respondents 19%, and Authenticity of respondents are 19%.

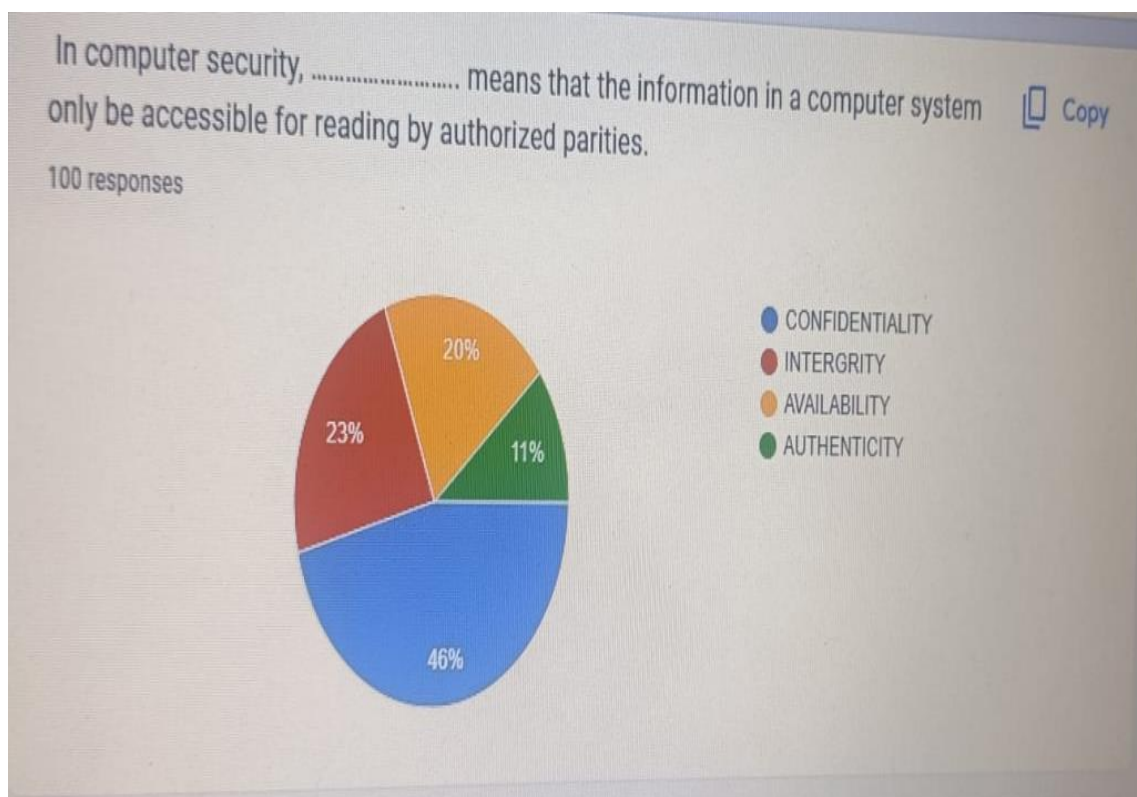
INFERENCE

➤ Majority 35% of the respondents belongs to Integrity.

4.5 Table indicating the computer security information in a computer system.

S.no	Attributes	Percentage analysis
1.	CONFIDENTIALITY	46%
2.	INTERGRITY	23%
3.	AVAILABILITY	20%
4.	AUTHENTICITY	11%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Confidentiality of respondents are 46% ,Intergrity of respondents are 23%, Availability of respondents 20 %, and Authenticity of respondents are 11%.

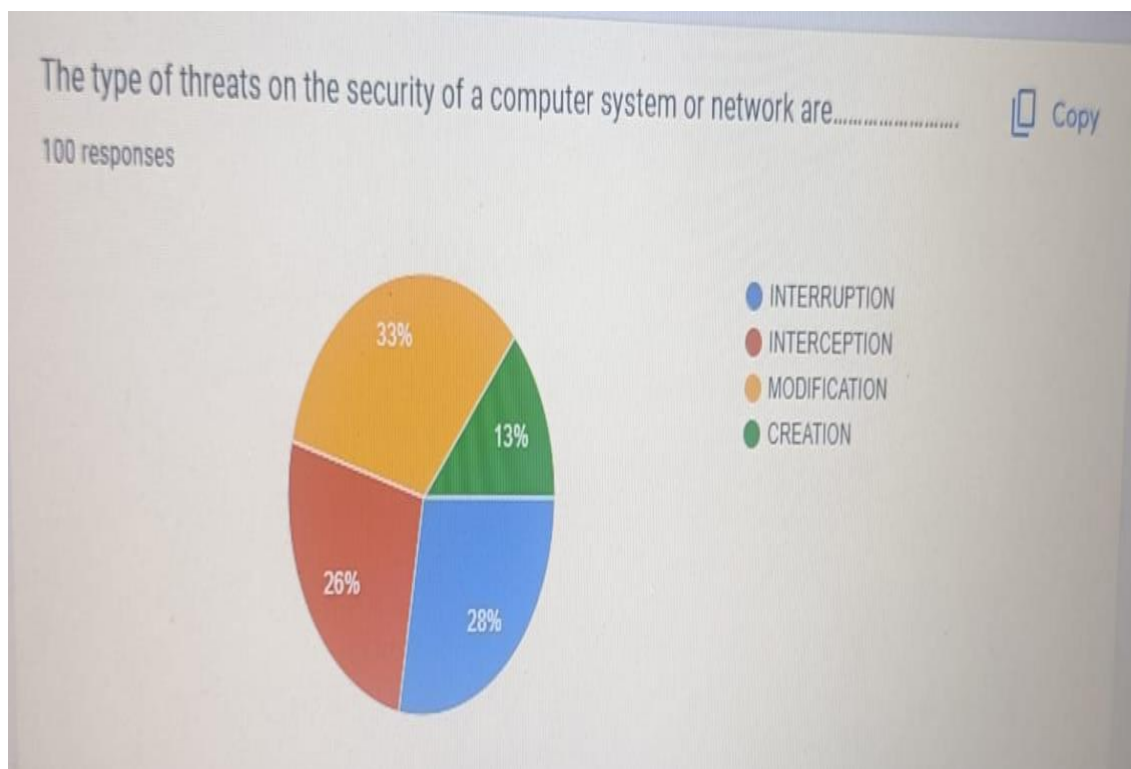
INFERENCE

➤ Majority 46% of the respondents belongs to Confidentially.

4.6 Table indicating the type of threats on the security of a computer system or network.

S.no	Attributes	Percentage analysis
1.	INTERRUPTION	28%
2.	INTERCEPTION	26%
3.	MODIFICATION	33%
4.	CREATION	13%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Interruption of respondents are 28% ,Interception of respondents are 26%, Modification of respondents 33 %, and Creation of respondents are 13%.

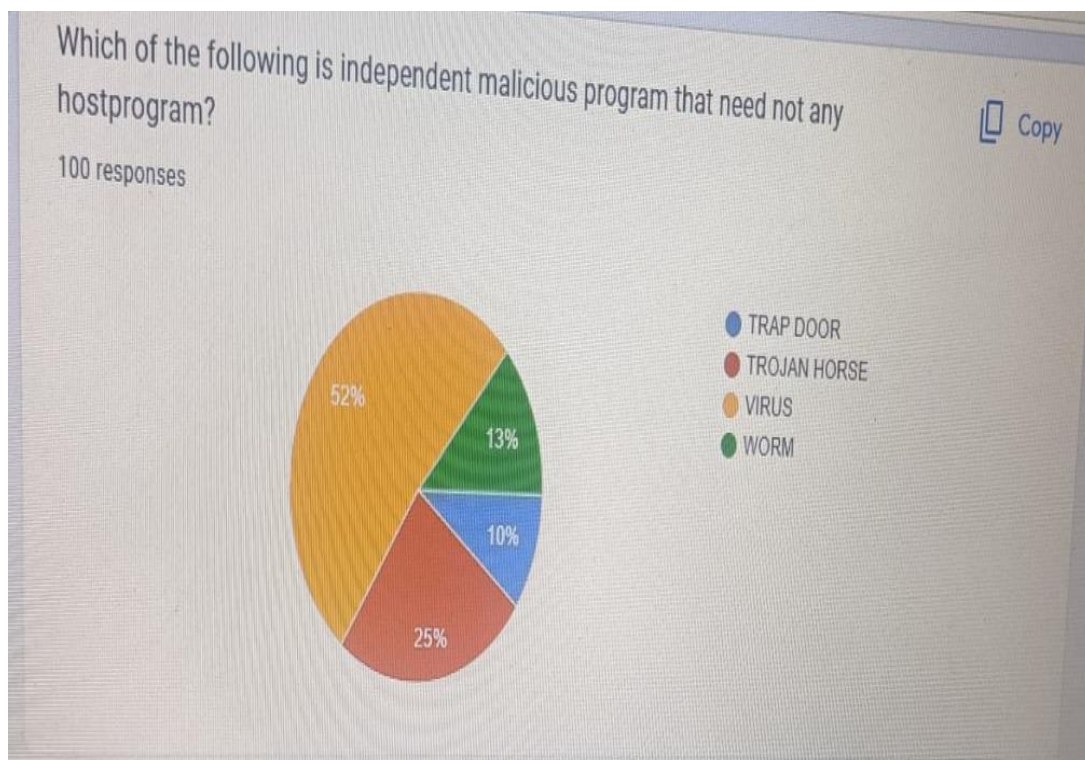
INFERENCE

➤ Majority 33% of the respondents belongs to Modification.

4.7 Table indicating the independent malicious program that need not any host program.

S.no	Attributes	Percentage analysis
1.	TRAP DOOR	10%
2.	TROJAN HORSE	25%
3.	VIRUS	52%
4.	WORM	13%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Trap door of respondents are 10% ,Trojan horse of respondents are 25%, Virus of respondents 52 %, and Worm of respondents are 13%.

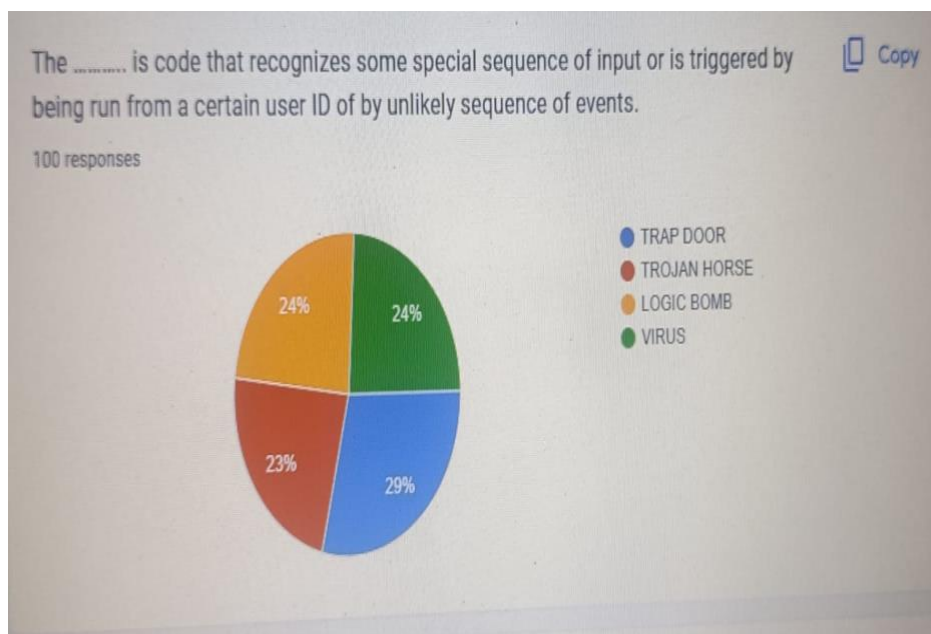
INFERENCE

➤ Majority 52% of the respondents belongs to Virus.

4.8 Table indicating the code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by unlikely sequence of events.

S.no	Attributes	Percentage analysis
1.	TRAP DOOR	29.3%
2.	TROJAN HORSE	23.2%
3.	LOGIC BOMB	24.2%
4.	VIRUS	23.3%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Trap door of respondents are 29.3% ,Trojan horse of respondents are 23.2%, Logic bomb of respondents 24.2 %, and Virus of respondents are 23.3%.

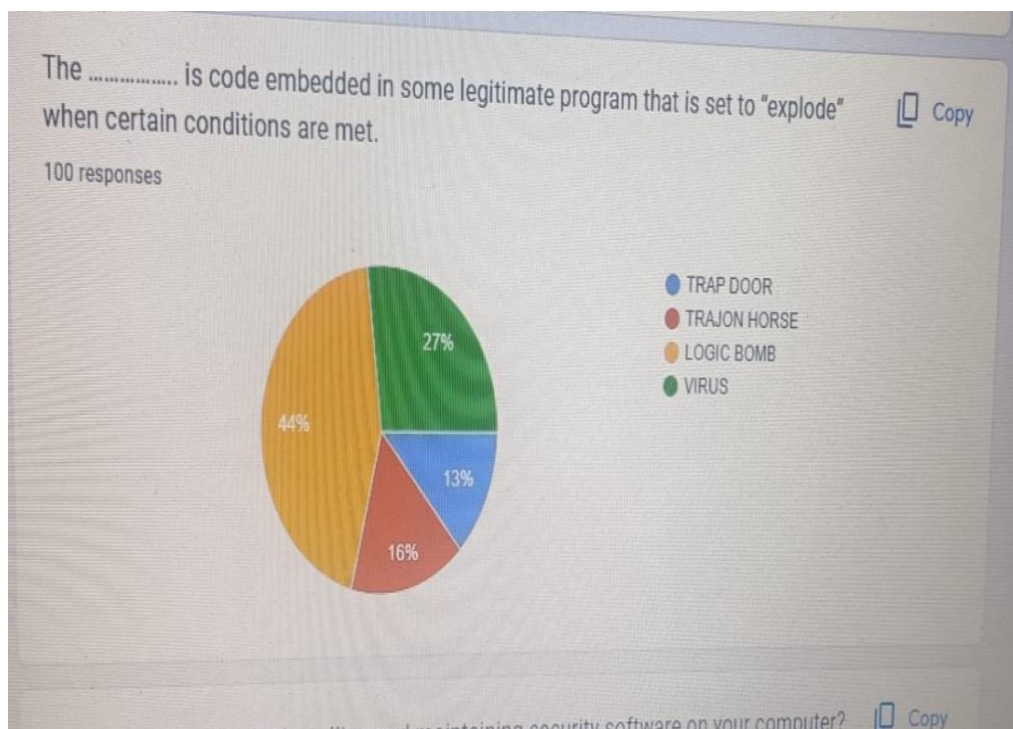
INFERENCE

➤ Majority 29.3% of the respondents belongs to Trap door.

4.9 Table indicating the code embedded in some legitimate program that is set to “explode”.

S.no	Attributes	Percentage analysis
1.	TRAP DOOR	13%
2.	TROJAN HORSE	16%
3.	LOGIC BOMB	44%
4.	VIRUS	27%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Trap door of respondents are 13% ,Trojan horse of respondents are 16%, Logic bomb of respondents 44 %, and Virus of respondents are 27%.

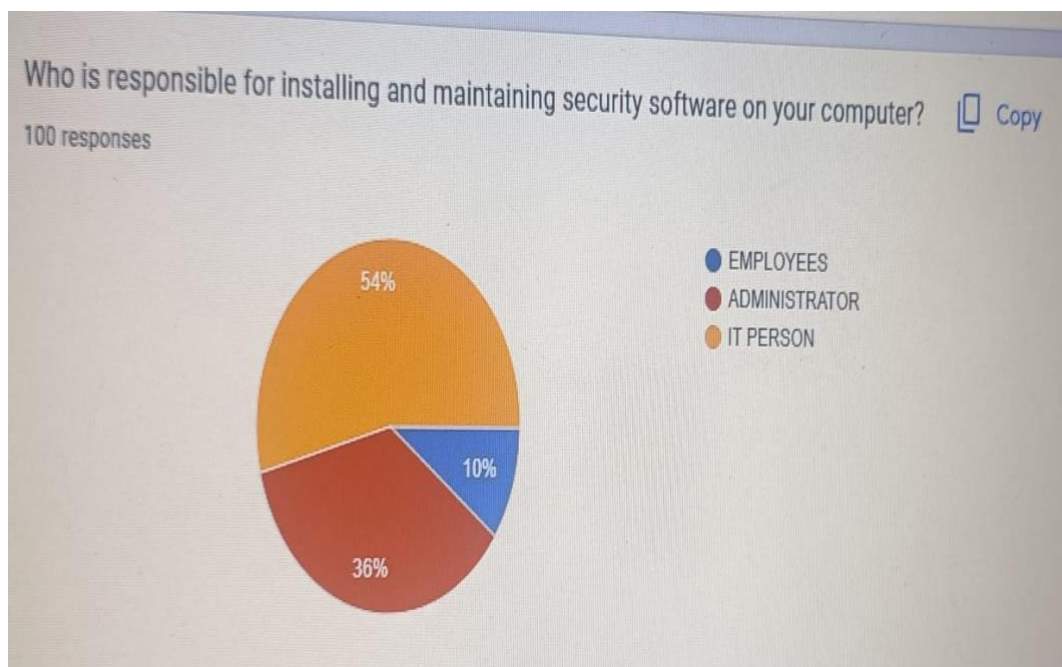
INFERENCE

➤ Majority 44% of the respondents belongs to Logic bomb.

4.10 Table indicating the responsible for installing and maintaining security software on your computer.

S.no	Attributes	Percentage analysis
1.	EMPLOYEES	10%
2.	ADMINISTRATOR	36%
3.	IT PERSON	54%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Employees of respondents are 10%, Administrator of respondents are 36%, and IT Persons of respondents 54 %.

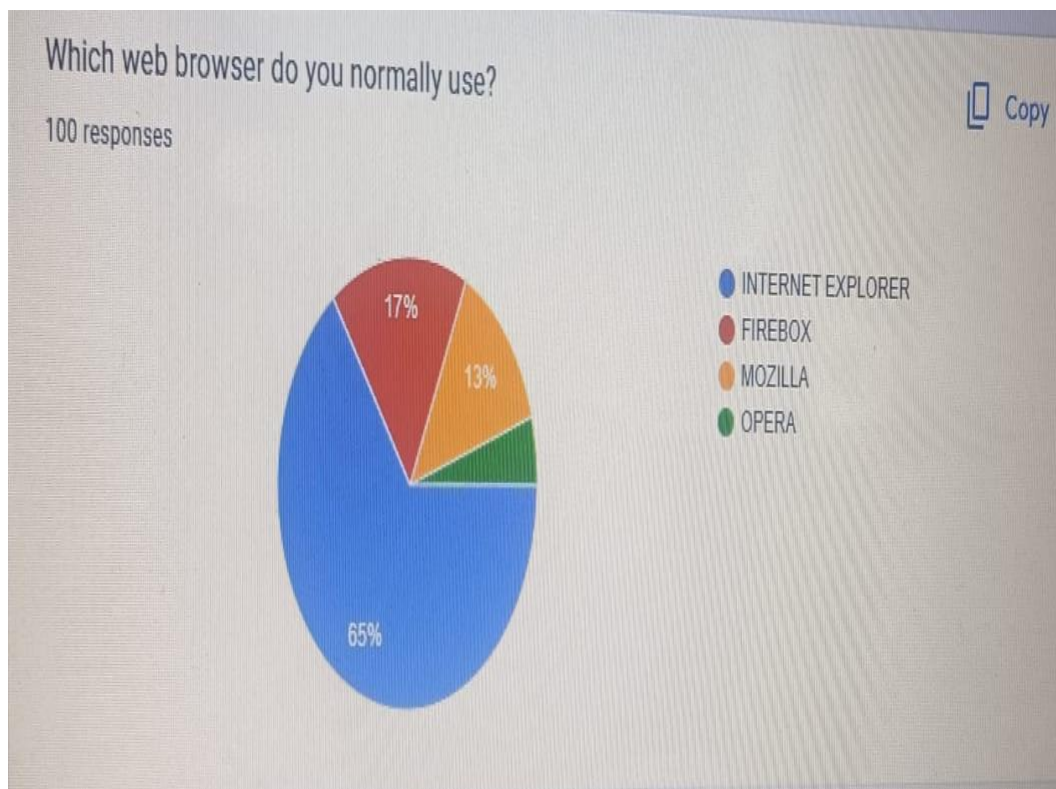
INFERENCE

➤ Majority 54% of the respondents belongs to IT Persons.

4.11 Table indicating the web browser do you normally use.

S.no	Attributes	Percentage analysis
1.	INTERNET EXPLORER	65%
2.	FIREBOX	17%
3.	MOZILLA	13%
4.	OPERA	5%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Internet Explorer of respondents are 65% ,Firebox of respondents are 17%, Mozilla of respondents 13 %, and Opera of respondents are 5%.

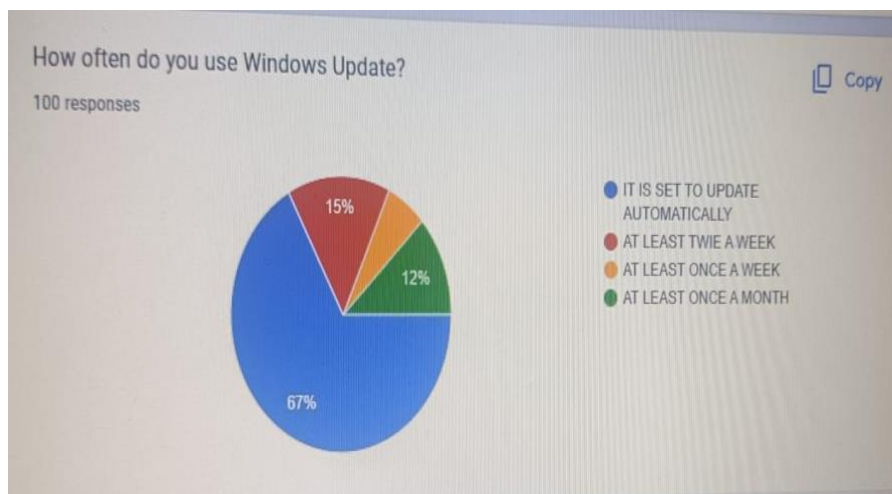
INFERENCE

➤ Majority 65% of the respondents belongs to Internet Explorer.

4.12 Table indicating the use of Windows Update.

S.no	Attributes	Percentage analysis
1.	IT IS SET TO UPDATE AUTOMATICALLY	67%
2.	AT LEAST TWIE A WEEK	15%
3.	AT LEAST ONCE A WEEK	6%
4.	AT LEAST ONCE A MONTH	12%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents It is to update Automatically of respondents are 67%, At least twice a week of respondents are 15%, At least once a week of respondents 6 %, and At least once a month of respondents are 12%.

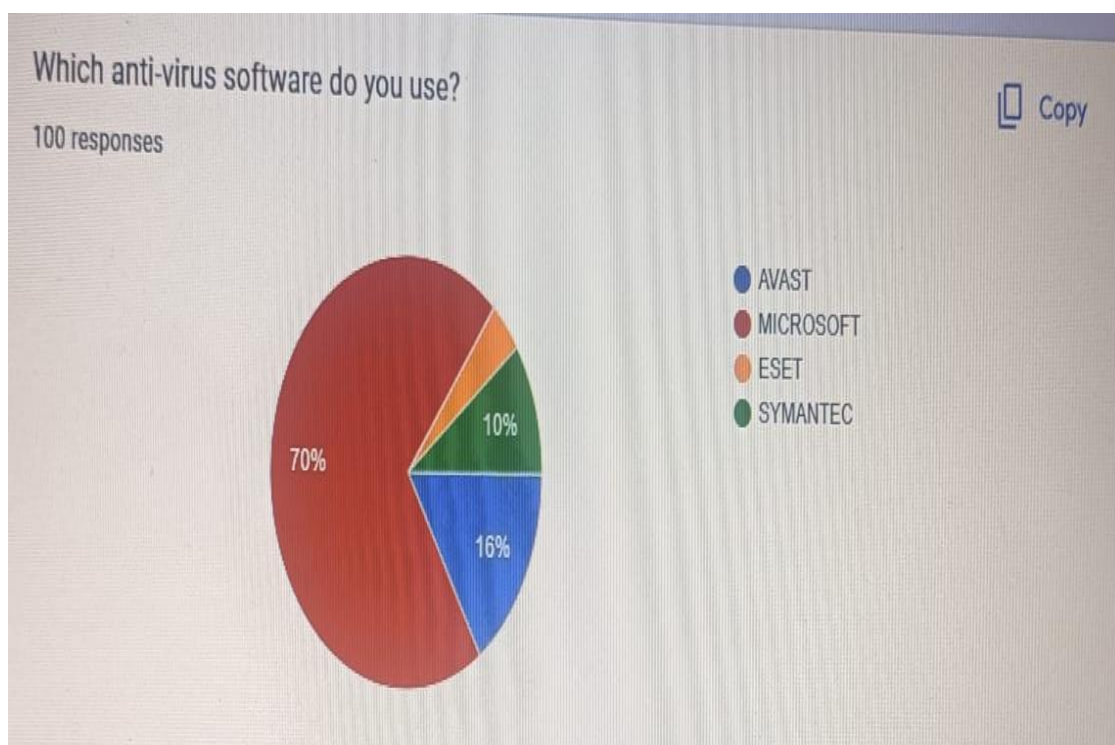
INFERENCE

➤ Majority 67% of the respondents belongs to It is to update Automatically.

4.13 Table indicating the anti-virus software do you use.

S.no	Attributes	Percentage analysis
1.	AVAST	16%
2.	MICROSOFT	70%
3.	ESET	4%
4.	SYMANTEC	10%
TOTAL		100

CHART:



Interpretation

From the above table it is interpreted that the number of respondents Avast of respondents are 16%, Microsoft of respondents are 70%, Eset of respondents 4%, and Symantec of respondents are 10%.

INFERENCE

➤ Majority 70% of the respondents belongs to Microsoft.

4.2 Chi-Square Tests

HYPOTHESIS 1:

- H0: The choice of anti-virus software is independent of gender.
- H1: The choice of anti-virus software is not independent of gender.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percentage	N	Percentage	N	Percentage
GENDER*Which antivirus software do you use?	100	100.0%	0	0.0%	100	100.0%

GENDER * Which anti-virus software do you use? Cross tabulation

	Which anti-virus software do you use?					Total	
		AVAST	ESET	MICROSOFT	SYMANTEC		
GENDER Female	Count	1	9	2	22	3	37
	Expected Count	.4	5.9	1.1	25.9	3.7	37.0
Male	Count	0	7	1	48	7	63
	Expected Count	.6	10.1	1.9	44.1	6.3	63.0
Total	Count	1	16	3	70	10	100
	Expected Count	1.0	16.0	3.0	70.0	10.0	100.0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.521a	4	.163
Likelihood Ratio	6.677	4	.154
N of Valid Cases	100		

a.5 cells (50.0%) have expected count less than 5. The minimum expected count is 37.

INTERPRETATION

The p value is 0.163 which is greater than the significance value (0.05) hence null hypothesis H0 is accepted. And H1 is accepted.

INFERENCE

There is significant association between gender and the preferred methods or principles employed for waste management.

4.3 Correlation:

HYPOTHESIS 2:

- H0: The occurrence of the code is independent of the type of malicious software.
- H1: The occurrence of the code is dependent on the type of malicious software.

		The is code that recognizes some special sequence of input or is triggered by being run from a certain user ID of by unlikely sequence of events.	The is code embedded in some legitimate program that is set to “explode” when certain conditions are met.
The is Code that recognizes some special sequence of input or is triggered by being run from a certain user ID of by unlikely sequence of events.	Pearson Correlation Sig. (2-tailed) N	1	.100
			.322
		100	100
The is code embedded in some legitimate program that is set to “explode” when certain conditions are met.	Pearson Correlation Sig. (2-tailed) N	.100	1
		.322	
		100	100

INTERPRETATION

The p value is -0.100 which is less than the significance value (0.05) hence alternative hypothesis H1 is accepted. Therefore the average monthly waste generated by projects is not within the range malicious software.

CHAPTER -5

FINDINGS, SUGGESTIONS AND CONCLUSION

FINDINGS

- Majority 91 % of the respondents belong to the age group of 20-30 category.
- Majority 63% of the respondents are male.
- Majority 62.6% of the respondents belongs to PG educational qualification.
- Majority 35.4% of the respondents belongs to Intergrity.
- Majority 46% of the respondents belongs to Confidentially.
- Majority 33.3% of the respondents belongs to Modification.
- Majority 52% of the respondents belongs to Virus.
- Majority 29.3% of the respondents belongs to Trap door.
- Majority 44% of the respondents belongs to Logic bomb.
- Majority 54% of the respondents belongs to IT Persons.
- Majority 65% of the respondents belongs to Internet Explorer.
- Majority 67% of the respondents belongs to It is to update Automatically.
- Majority 70.7% of the respondents belongs to Microsoft.

SUGGESTIONS

Should perform risk analysis regularly, use intrusion detection tools, analyses logs, be conscious of security breaches and take appropriate action because security is as strong as the weakest link.

- Should deploy security solutions depending on the risks involved.
- Should not depend on a single defence but should use multi-layered security.
- Should restrict network access by using firewall, prevent listener access, encrypt network traffic, make the operating system restrictive etc.
- Should install only the products that are of use.
- Should create an organization wide network security policy.
- Should clearly define goals, organization's position on each issue and expected level of privacy and responsibilities in network security policy.
- Should perform periodic network security audits and take action on audit results.
- Should arrange user awareness programs regularly for internal as well as external users.
- Should keep an up to date document of the policy.
- Should have a well-defined disaster recovery plan ready.
- Should make the network security policy easily accessible to all members of the Library and Information Centres.

CONCLUSION

- In conclusion, effective network and security management are paramount for ensuring the robustness and integrity of IT infrastructure within a company.
- This study has underscored the significance of proactive measures, such as regular vulnerability assessments and robust access controls, to mitigate potential risks.
- Additionally, the findings emphasize the need for continuous monitoring and adaptation to evolving threats.
- Implementing a comprehensive network and security management strategy not only safeguards sensitive data but also bolsters the overall resilience of an IT company in the face of a dynamic and challenging digital landscape.
- As technology advances, prioritizing these measures becomes indispensable to foster a secure and reliable IT environment.

REFERENCES

- Halsall, F. (2001) Multimedia Communications, Addison Wesley.
- ITU-T X.509 (2000) Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks , International Telecommunication Union.
- King, T. and Newson, D. (1999) Data Network Engineering, Kluwer.
- Peterson, L. L. and Davie, B. S. (1996) Computer Networks: A Systems Approach, Morgan Kaufmann.
- RFC 2401 (1998) Security Architecture for the Internet Protocol, Kent, S., Atkinson, R.
- Schneier, B. (1996) Applied Cryptography, 2nd edn, Wiley.
- Stallings, W (1999) Cryptography and Network Security, Prentice Hall.
- Stallings, W (2001) SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, 3rd end, Addison Wesley.
- Anderson, R. (2001) Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley.
- BS 7799-2 (2002) Information Security Management Systems – Specification with Guidance for Use, British Standards Institution.
- Ellis, J. and Speed, T. (2001) The Internet Security Guidebook, Academic Press.
- ISO/IEC 17799 (2000) Information Technology – Code of Practice for Information Security Management, International Organization for Standardization.
- Tanenbaum, A. S. (1996) Computer Networks, 3rd edn, Prentice Hall.
- Xiang Heng & Fu Peng. 2005. Information Security Management, Chongqing: Chongqing University Press.
- Zhang Yunzhuang & Liu Jifeng. 2013. The opportunities and challenges for information security in the era of big data: An example of open information and intelligence. National Defense Science & Technology.
- Pan Minghui, Principle and Application of Network In-formation Security Engineering, Beijing: Tsinghua Uni-versity press.
- Viktor Mayer-Schonberger & Kenneth Cukier. 2013. Big Data: A Revolution that Will Transform How We Live, Work and Think. Boston: Houghton Mifflin Harcourt.
- Introduction to industrial control networks, IEEE Com-munications Surveys and Tutorials, 2012.
- NIST Manufacturing Engineering. 2008. NIST Programs of the Manufacturing Engineering Laboratory.
- Zhang Xuefeng. 2014. Introduction to Information Secu-rity, Beijing: People's Posts and Telecommunications Press.
- Information processing systems; Open Systems Inter-connection; basis reference model; Part 2: Security ar-chitecture.
- Malek & Harmantzis F. 2004. Security Management of Web Services, Network Operations and Management Symposium, pp.175-189
- Charlie Kaufman. 1995. Network Security. PTR Pren-ticeHa.

- Cheswick B & Bllovin S. 1994. Firewall and Internet Security. Addison-Wesley.
- Xiao Junmo. 2003. Network Information Security. Bei-jing: China Machine Press, pp.222-256.
- Lemke, William A. Readshaw & Neil I. 2014. Coordi-nated network security management, International Busi-ness Machines Corporation.

- ❖ <http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf>
- ❖ <http://www.usenix.org/publications/login/1998-8/tcpdump.html>
- ❖ <http://java.sun.com/docs/books/tutorial/networking/sockets/definition.html>
- ❖ http://en.wikipedia.org/wiki/Application_Layer
- ❖ http://en.wikipedia.org/wiki/Message_transfer_agent
- ❖ <http://www.webopedia.com/TERM/H/hacker.html>

ANNEXURE – QUESTIONNAIRE
A STUDY ON NETWORK AND SECURITY MANAGEMENT
IN IT COMPANY.

1. Name

2. Age Groups

a.20-30 b. 31-40 c.41-50 d. above 50

3. Gender

a.Male b. Female

4. EMAIL

5. Education

a. HSC b.UG c.PG d. DIPLOMA

6. In computer security means that computer system assets can only authorized parities.

a. COFIDETIALITY b. INTERGRITY c. AVAILABILITY d. AUTHENTICITY

7. In computer security means that the information in a computer system only be accessible for reading by authorized parities.

a. COFIDETIALITY b. INTERGRITY c. AVAILABILITY d. AUTHENTICITY

8. The type of threats on the security of a computer system or network are.....

a. INTERRUPTION b. INTERCEPTION c. MODIFICATION d. CREATION

9. Which of the following is independent malicious program that need not any host program?

a. TRAP DOOR b. TROJAN HORSE c. VIRUS d. WORM

10. The is code that recognizes some special sequence of input or is triggered by being run from a certain user ID of by unlikely sequence of events.

a. TRAP DOOR b. TROJAN HORSE c. LOGIC BOMB d. VIRUS

11. The is code embedded in some legitimate program that is set to “explode” when certain conditions are met.

a. TRAP DOOR b. TROJAN HORSE c. LOGIC BOMB d. VIRUS

12. Who is responsible for installing and maintaining security software on your computer?

a. EMPLOYEES b. ADMINISTRATOR c. IT PERSON

13. Which web browser do you normally use?

a. INTERNET EXPLORER b. FIREBOX c. MOZILLA d. OPERA

14. How often do you use Windows Update?

a. IT IS SET TO UPDATE AUTOMATICALLY b. AT LEAST TWIE A WEEK

c. AT LEAST ONCE A WEEK d. AT LEAST ONCE A MONTH

15. Which anti-virus software do you use?

a. AVAST b. MICROSOFT c. ESET d. SYMANTEC