IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STUDY ON CYBER THREATS AND CYBER SECURITY AND THEIR TRENDS

KOUSALYA SENTHIL KUMAR

JANAGAR K M

DEPT OF COMPUTER SCIENCE ENGINEERING(U.G)

SRM IST VDP

1.ABSTRACT : Currently, a significant portion of global economic, commercial, cultural, social, and governmental activities occur in the digital realm. This includes interactions at all levels . The increasing prevalence of cyber-attacks and the risks associated with wireless communication technologies have become pressing concerns for private companies and governmental organizations worldwide. Given the world's heavy reliance on electronic technology, safeguarding data from cyber threats is becoming a very important concern .

The usual aim of the cyber attacks is to set in financial losses inn the organization,

although in some instances, these attacks may serve military or political purposes. The damages resulting from such attacks include PC viruses, breaches of sensitive information, data distribution service (DDS) disruptions, and various assault vectors. To mitigate these risks, organizations deploy diverse solutions aimed at preventing or minimizing the impact of cyber-attacks. Cybersecurity involves real-time monitoring of the latest IT developments.

Researchers globally have proposed numerous methods to prevent cyber-attacks or mitigate their effects, with some approaches already in operational use and others still in the research phase. This study aims to conduct a comprehensive survey and review of standard advancements in the field of cyber security. It seeks to explore the challenges, weaknesses, and strengths of these proposed methods. The study delves into various descendant cyber-attacks, providing detailed consideration of emerging threats.

The discussion encompasses standard security frameworks, tracing the history and early-generation cyber-security methods. Additionally, the study explores emerging trends and recent developments in cyber security, highlighting evolving threats and challenges.

KEYWORDS : Cyber threats , trends and frequency , mitigation methods

2.INTRODUCTION

For over two decades, the Internet has become an integral part of global communication, influencing the lives of people worldwide. Its innovations and affordability have led to a significant increase in internet accessibility, resulting in approximately 3 billion users globally[1]. The internet has not only created a vast global network generating billions of dollars annually for the global economy[2] but has also become the primary space for economic, commercial, cultural, social, and governmental activities.

Cyberspace, with a majority of crucial information being transferred or formed within this space. Media activities, financial transactions, and a substantial portion of citizens' time and activities are conducted in cyberspace. The income from cyberspace businesses contributes significantly to a country's Gross Domestic Product (GDP), and cyberspace indicators play a crucial role in measuring a nation's development.

The low entry cost, anonymity, uncertain geographical threats, and lack of public transparency in cyberspace have attracted a diverse range of actors, including governments, organized groups, terrorists, and individuals[3]. This has given rise to threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage, setting them apart from traditional national security threats.

Analysts have contemplated the potential consequences of cyber-attacks for over a decade, envisioning scenarios of severe physical or economic damage. The inadequate and proper definition of cyber attack makes the understanding and analysis of attack difficult [4]. The absence of such a definition not only hampers legal clarity but also leads to diverse interpretations and practices, resulting in contradictory legal conclusions.

Apart from the absence of a proper definition to cyber attacks the absence of the classification and the types of cyber attacks makes it difficult to comprehend. Establishing a clear understanding of cyber-attacks is crucial for navigating the legal landscape, identifying their consequences, and providing informed legal analysis[5]. The study concludes by emphasizing the need for an acceptable definition as a foundational step in comprehending and addressing the multifaceted nature of cyber-attacks.

3.FUNDAMENTALCONCEPTS :

Cyber-attacks extend beyond the conventional scope of information operations, encompassing a broader context. Information operations involve the strategic integration and security measures. These coordinated efforts, coupled with specialized support and relevant capabilities, aim to infiltrate, disrupt, incapacitate, or manipulate human decision-making processes within national institutions[6]. The anatomy of a cyber-attack is illustrated in Fig. 1.

According to the US National Military Strategy for cyberspace operations, computer network operations comprise three main components: attack, defense, and utilization enabling. Unlike network attacks and defense, utilization enabling operations focus more on information collection and analysis rather than network disruption. These operations may serve as a precursor to an actual attack and can be employed for the dissemination of information and propaganda. Within the realm of computer network exploitation enabling operations, the objective may involve the theft of crucial computer data[7]. In this context, tools such as Trap Sniffers and Doors play a crucial role in cyber surveillance. Trap Doors provide external users with unauthorized access to software without the computer user's knowledge, while Sniffers serve as tools for illicitly capturing usernames and passwords.[8]

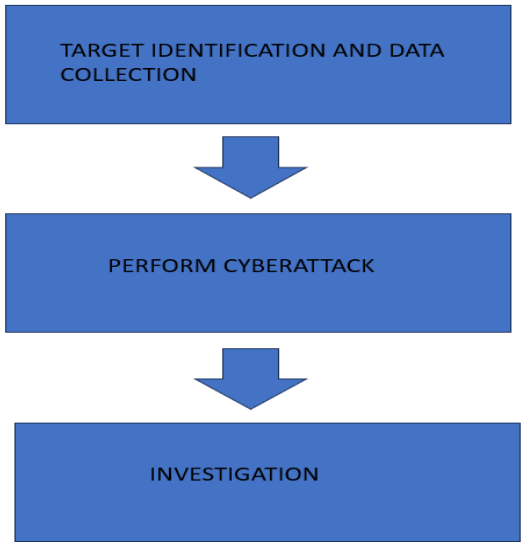


Fig .1. Anatomy of cyber attacks

4.THREATS IN CYBER SPACE

The cyberspace creates a vast environment for the availability of information through websites and internet sources. Countries worldwide have become heavily reliant on cyberspace for communication and control of the physical world to an extent that separation from it is practically impossible[9]. Consequently, the security responsibilities are increasingly influenced by the dynamics of cyberspace.

The danger of web application attacks, where cybercriminals try to steal data or spread harmful

code, is still very real. These criminals often use compromised legitimate web servers to distribute their malicious code. Data theft attacks, which often make headlines, are a significant concern. It's crucial to focus more on protecting web servers and applications because they are prime targets for cybercriminals looking to steal data.

In recent times, businesses of all sizes are gradually shifting to cloud services, meaning the world is increasingly embracing the cloud. However, this emerging trend poses a significant challenge for cybersecurity because data traffic can bypass traditional inspection points. Cloud has the policies and controls that expands to try and prevent the loss of valuable information. Athough there are expanding application of the cloud yet the threat for the loss of data still persists and thus the concerns for the same still exists and grows .Fig 3 shows the different sources of cyber threats .

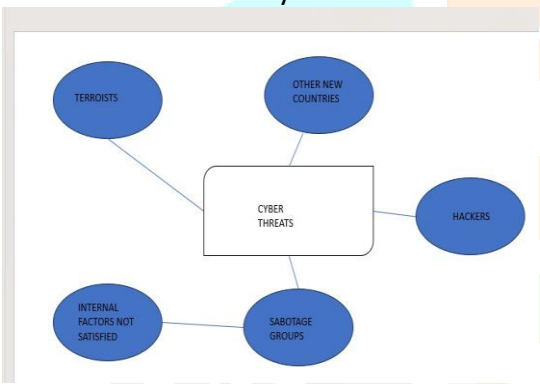


Fig 2 .Sources of cyber threats

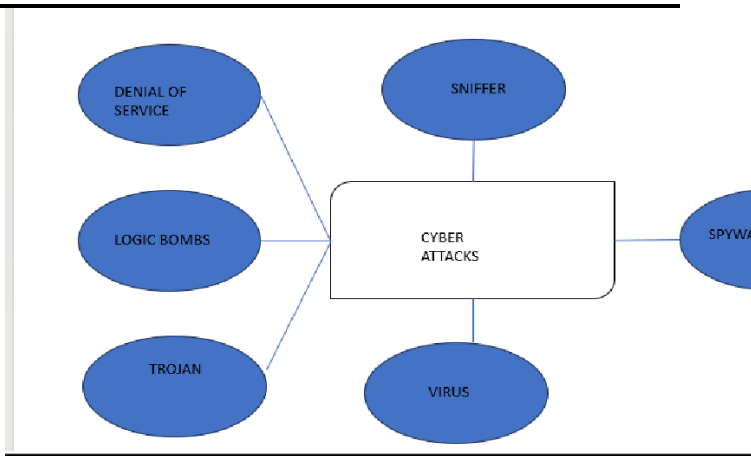


Fig 3. Main cyber attack types

The increasing evolution of computing contributes to the dynamic nature of cyberspace, with each change creating new vulnerabilities and responses. [10].

Fig . 3. Shows various cyber attacks and its common types Various groups, driven by financial motives or political agendas, contribute to the escalating cyber threats. Some infiltrate networks to make money, while others, known as "hacktivists," carry out politically motivated attacks on popular websites or email hosts. Internal dissatisfied agents within organizations emerge as a significant source of cybercrime, often not requiring extensive knowledge of cyber-attacks due to their insider access.[11].Additionally, terrorists pose a threat, aiming to disrupt, disable or exploit the available resources which further weakens the economy and trust among people.

5.TRENDS IN CYBERSECURITY

In today's interconnected world, mobile networks play a vital role in connecting people globally. However, the security of these mobile networks is a significant concern.Despitetheuseoffirewallsandsecuritymeasures,vulnerabilitiesexistas people access these networks through various devices like tablets, phones, and PCs, each requiring additional security beyond what the applications provide. It's crucial to be mindful of the security challenges associated with mobile networks, which are particularly susceptible to cybercrimes, necessitating careful attention to their security.

IPv6, the new Internet protocol replacing IPv4, introduces fundamental changes and is essential for expanding available IPaddresses.EnsuringthesecurityofIPv6 goes beyond merely adapting capabilities from IPv4. [12] Switching to IPv6 promptly is recommended to mitigate the risks associated with cybercrimes.

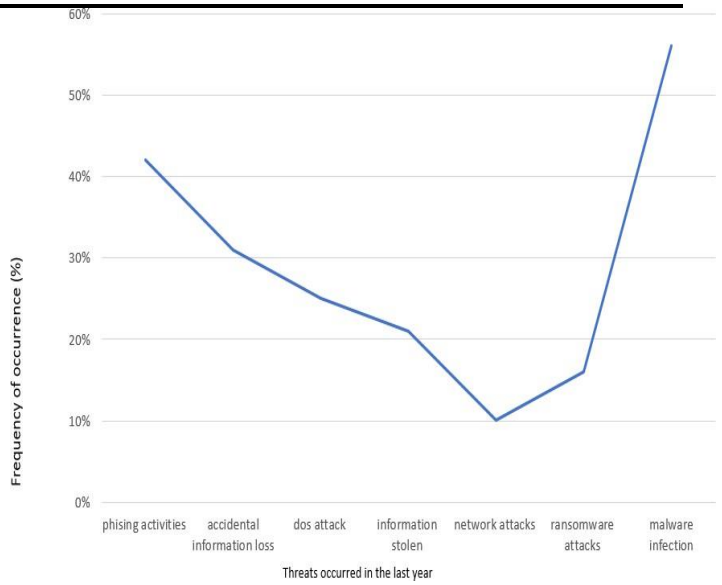
Encryption, process of encoding messages to prevent unauthorized access,isa crucial aspect of cybersecurity. While it safeguards data privacy and integrity, increasing its use poses challenges in cybersecurity. Encryption is employed not only to protect data at rest but also during transmission over networks like the Internet and mobile communication systems . Encrypting the code becomes essential for detecting any potential leakage of information.

In summary, these trends highlight the evolving landscape of cybersecurity. Mobile networks,the transition to IPv6,and the growing use of encryption are all significant factors shaping the future of cybersecurity, with a constant need for vigilant adaptation to emerging threats

.6.METHODOLOGY

The danger of web application attacks, where cybercriminals try to steal data or spread harmful code, is still very real. These criminals often use compromised legitimatewebserverstodistributetheirmaliciousco de.Datatheftattacks,which often make headlines, are a significant concern[13]. It's crucial to focus more on protecting web servers and applications because they are prime targets for cybercriminals looking to steal data.

In recent times, businesses of all sizes are gradually shifting to cloud services, meaning the world is increasingly embracing the cloud. However, this emerging trend poses a significant challenge for cybersecurity because data traffic can by pass traditional inspection points. Cloud has the policies and controls that expands to try and prevent the loss of valuable information. Athough there are expandingapplicationofthecloudyetthethreatfort helossofdatastillpersists and thus the concerns for the same still exists and grows .



GRAPH.1.GRAPHONTHEFREQUENCYOFDIFFEREN TTHREATSOCCURREDINLAST YEAR

6.1GRAPH EXPLANATION

Theabovegraphsexplainsthedifferentkindofthreatsencounteredoverthepast year.Themostfrequentlyoccurredthreatsincludethemalwareattacks,phishing attacks, compromises in the network , information theft the external sources , ransomware attacks and accidental loss of information .

Themostcommonfrequentlyoccurredthreatsincludethemalwareinfectionlike the viruses , trojan etc,

Thenextfrequentattacksarethesuccessfulphishing attacksthatisthefraudulent attempts by the hackers and attackers into stealing the users personal and sensitive information like the password and thefinancial details .

Theotheractivitiesaretheaccidentallossofinformationorthetheftofthe informationfromanexternalsourceorsellingtheinformationbytheinside employees .

The other activities are the DoS attacks that is the disrupting of the normal functioning of the network by flooding it with illegitimate traffic and making it inaccessible by the legitimate users. The other include the ransomware attacks that is stepping into the organizations system to illegally access data

they come from a trusted and reliable origin and haven't been altered.Anti-virussoftwareondevicestypicallyhandlesthisauthentication, making a reliable antivirus program essential for protecting devices from potential threats.

7.CYBERSECURITY TECHNIQUES

let's breakdown the key cyber security techniques:

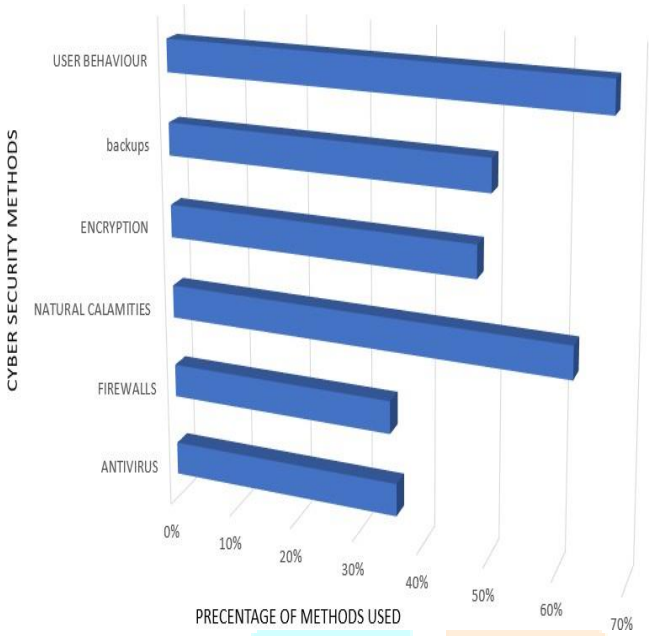
- The use of usernames and passwords is a foundational method for safe guarding information.It's often the initial step in cybersecurity, controlling who can access specific data or systems.

- Beforedownloadinganydocuments,it'scrucialtoauthenticatetheirsource to ensure

- Software programs like malwares scan thefile and documents lookingfor any malicious activities or viruses . this includes dealing with trojan , worms , viruses collectively called malware
- Firewalls,whether software or hardware,act as aprotectivebarrieragainst hackers, viruses, and worms attempting to access a computer from the internet. They scrutinise all incoming and outgoing messages, blocking those that don't meet security requirements. Detection and prevention of malware is done using firewalls .
- Anti-virus software is a computer program designed to detect, prevent, and take action against malicious software like viruses andworms.These programs often feature an auto-update function, allowing them to download profiles of new viruses and promptly check for them. Reliable antivirus software are required for every computer thatprovidealayerof defence against cyberthreats .
- In todays growing technological world where everything revolves around the internet , the role of cybersecurity is very significant . As our social interactions increase in the digital realm, protecting personal information becomes a paramount concern for companies.Social media,while fostering connectivity,also becomes a contribution to threats .
- Thewidespread adoption of using internet basedsites and social networking sites among individuals have led to rise in the threat of cyber attacks . With almost everyone using social networking sites daily, they have become prime targets for cybercriminals seeking to hack all the valuable information . Given the ease with which people share theirpersonal information online, companies have to swiftly identifythethreatsandrespondtothesame effectivelywiththeproperresponse to identify and remove the breaches

The challenge for businesses lies in the ability of individuals to share information with a vast audience.While companies cannot afford to cease using social media due to its vital role in publicity, they must implement solutions that promptly notify them of potential threats, allowing for quick intervention before significant damage occurs.

Despite the risks associated with socialmedia ,companies should recognize its importance and implement strategies to analyze information within social conversations. This entails the deployment of appropriate security solutions, including the formulation of policies and the use of relevant technologies, to effectively mitigate risks and safeguard against potential cyber threats.



GRAPH2.GRAPH ON THE PERCENTAGE OF DIFFERENT CYBER SECURITY METHODS

7.1GRAPHEXPLANATION

- The above graph shows the widely used cyber security methods . from the graph it is evident that the common methods used to keep the cyber threats away include tracking the user behavior and identifying and reporting any change or unusual behavior , tracking and downloading backups and restoring data to prevent data loss , encryption of the data while working the data through website or internet applications , using fire walls and installing antivirus software .
- From the graph the most widely opted method for protection against cyber threats include tracking and monitoring user behavior .
- Then the encryption and the frequent backup methods are widely used. Finally the antivirus software installation and malwares are used .

8.CYBER ETHICS

In essence ,cyber ethics can be seen as the internet's code of conduct. Adhering to these principles ensures responsible and safe internet use. Here are a few key cyber ethics:

- Utilize the internet for constructive communication and interaction. Email and instantmessagingfacilitatestayingconnectedwith friends,family,andcolleagues, fostering the exchange of ideas and information globally.

- Refrain from being a cyberbully. Avoid name-calling, spreading false information,sharingembarrassingcontent,oren gaginginanybehavioraimedat causing harm to others.

- Recognizetheinternetasavastrepositoryofinfo rmationoneveryconceivable topic. Using this information in a legal and ethical manner is imperative.

- Avoidunauthorizedaccesstoothers'account sandrefrainfromattemptingto send malware to corrupt their systems.

- Exercisecautionbynotsharingpersonalinformation,asitcanbemisusedby others, leading to potential troubles.

- Maintainauthenticitywhileonline,avoidingpretenseandrefrainingfrom creating fake accounts, which can lead to trouble for both parties involved.

- downloadonlycopyrightedgamesandvideosifitispermissibleandalignswith copyright laws.

In essence, these cyber ethics mirror the principles of proper conduct that we learn from an early age, now applied in the cyber realm. By practicing these guidelines,individuals can contribute to a safer and more responsible use of the internet.

9.MITIGATIONMETHODS

It is very crucial in devising a plan that mitigates all the cyber threats one such very important step in the above is to develop a effective security policy . the security policy must provide clear instructions along with the blueprint of the behaviouroftheemployeestoguardagainstanypotentialthreats.itisimportant to provide correct information totheauthorised users and keep the unauthorised users away . the key steps are identifying and accessing the users authorisation. Keeping a check on the vulnerabilities and taking appropriate methods to detect and remove them . enabling email and website security .

Improvements have been made in providing security like providing multi factor authentication but passwords are still only been widely used . improvements in the biometric recognition is also helpful in providing security against threats . risk modelling is onesuch methods used by the organisations to provide overall security to the scheme involved.it helps in accessing risks and estimates their impact for the organisations to work on .

RISK FACTOR ANANLYSIS METHOD

RiskAssessment:

IdentifyingAssets:thisinvolvesidentifyingandcategorisingalltheavailable digital assets

ThreatAnalysis:thisincludesevaluatingthethethreatslikemalware,dosattacks to understand their impact.

VulnerabilityAssessment:thisinvolvesidentifyingthevulnerabilitiesinthesystem that can be breached by the hackers or attackers .

RiskMitigation:

Thisincludes :

- providingSecurityControls
- properresponseplanning
- frequentmonitoring
- trainingtheemployeestomanagethethreats

RiskQuantification:

ProbabilityAnalysis:thisincludesidentifyingtheprobabilityofthethreatsthat can occur based on the past data and the measures used currently .

Impact Analysis:this includes identifying and assessing the impact of an attacker to the organisation and losses that can come up with it that includes the loss of data , the financial losses , the reputation ,etc.

RiskMetrics:Introducingtheriskmetrictoquantifytheeffectoftheriskbasedon the matrices and scores .

Byadoptingacomprehensiveriskmodellingapproach,organisationscanbetter understand their cyber risk landscape, prioritise their defences, and respond effectively to potential threats, thereby enhancing their cybersecurity posture.

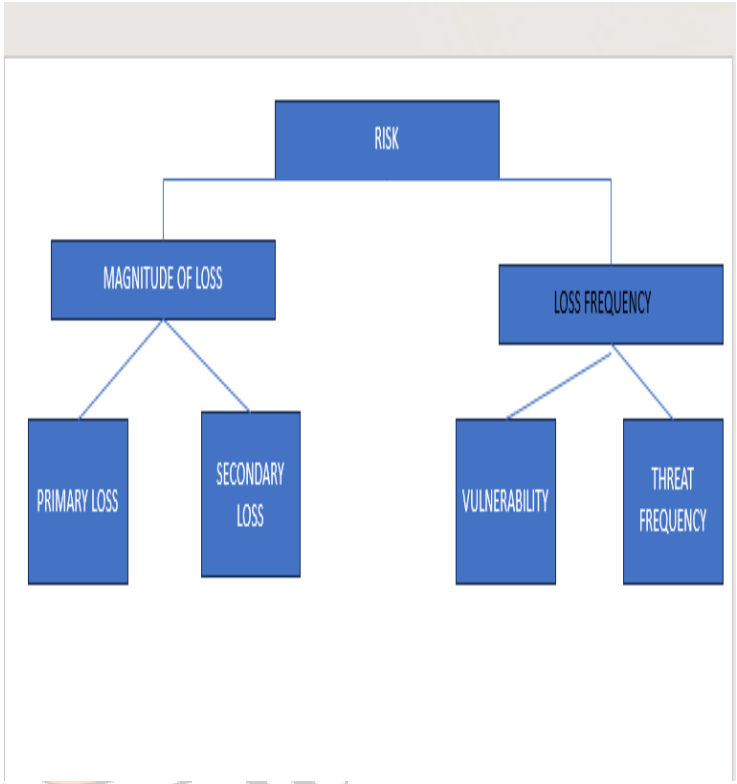


FIGURE.4.FLOW CHART ON RISK MITIGATION METHOD

10.CONCLUSION:

Cyberspace and its associated technologies have emerged as crucial sources of power. The all new and different characteristics of cyberspace like low entry barriers, , vulnerability, and no known symmetry , have given rise to power dispersion. While governments have traditionally held the reins of power, a diverse set of actors, such as private companies, organized terrorist and criminal groups, and individuals, now play significant roles in this landscape, though governments remain pivotal. However, this evolving dynamic doesn't diminish the importance of governments in ensuring national security.

Computer security is an expansive subject that is gaining increasing significance as our world becomes more interconnected. Networks play a crucial role in facilitating critical transactions, making the security of these systems paramount. With each passing year, cybercrime takes on new forms and information security becomes more challenging.

The constant emergence of technologies , coupled with the discovery of new cyber tools and threats, poses a continual challenge for organizations. It's not just about securing the existing infrastructure; there's a growing need for new platforms and intelligence to address evolving cyber threats effectively.

While there isn't a foolproof solution for cybercrimes, it's essential to make earnest efforts to minimize them. This is crucial for ensuring a safe and secure future in the ever-expanding realm of cyberspace. As the digital landscape evolves, the collective endeavor should be to stay vigilant and adapt security measures to safeguard against the dynamic nature of cyber threats.

11.REFERENCES:

1.Tan, S., et al., 2021. Attack detection design for dc microgrid using eigenvalue assignment approach.

2.Judge, M.A., et al., 2021. Price-based demand response for household load management with interval uncertainty.

3.Akhavan-Hejazi, H., Mohsenian-Rad, H., 2018. Power systems big data analytics: An assessment of paradigm shift barriers and prospects,.

4.Amir, M., Givargis, T., 2020. Pareto optimal design space exploration of cyber–physical systems. Internet Things 12.

5. Cyber attacks research methods by Edar T.M .

6.Mitigation and future methods on cyber security by Khan . S

7.Zhang , protecting sensitive informations and valuable informations.

8.Z., Anwar, Z., 2020. SCERM—A novel framework for automated management - cyber threat response activities.,

9. Gayathri : cyber threat intelligence management

.

10.gayathri .k : mitigation methods using blockchain .

11. Li , cyber space and their threats .

12.Zhan, confidentiality and availability of sensitive over a network and threats

13.Sarker, effectiveness of cyberlearning .

14. Minz, science involved in cyber security .

15. Furnel, effects of cyber security breaches