*ISBN: 978-81-972400-5-8*

# 23. Cybersecurity Challenges in the Digital Era

**Sunita Jha**

Assistant Professor,
Arka Jain University.

***Abstract:***

*The rapid advancement of technology brought about unprecedented opportunities for innovation and connectivity, but it has also ushered in a new era of cyber threats and challenges. In this chapter, we will delve into the multifaceted landscape of cybersecurity challenges that have emerged in the digital age and explore strategies to mitigate their impact. In a world where the digital landscape evolves incessantly, the challenges outlined in this chapter are but a snapshot of the complex cybersecurity ecosystem. Adapting to these challenges demands a holistic approach, involving technological advancements, regulatory measures, user education, and collaborative efforts across industries and nations. Only through these collective actions can we strive to build a safer digital future.*

## 23.1 Introduction:

In today's hyper-connected digital landscape, cybersecurity challenges have taken center stage as businesses, governments, and individuals grapple with the evolving threat landscape. The exponential growth of technology has brought unprecedented opportunities, but it has also given rise to a myriad of vulnerabilities. This chapter delves into some of the most pressing cybersecurity challenges of our time. In the fast-paced digital era, where technology seamlessly intertwines with daily life, the realm of cybersecurity faces an array of intricate challenges. This chapter delves into the multifaceted landscape of cybersecurity challenges, exploring the evolving threats, vulnerabilities, and strategies required to safeguard our digital existence.

Cybersecurity has been growing rapidly since 2006 when cloud computing was introduced by most companies. Has a result more and more companies are spending more cash to improve their networks. There is no doubt that cyber has brought more problems with, however lack of training, unwarranted attacks, loss of property and human error have become a barrier that cannot be escaped within the cyber field. Cybersecurity refers to the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, and other cyber threats. It encompasses various technologies, processes, and practices designed to safeguard information and prevent disruption or damage to electronic systems. Key components of cybersecurity include network security, endpoint security, application security, data security, and identity management. As technology evolves, cybersecurity continues to be a critical concern for businesses, governments, and individuals to mitigate risks and protect against cyber threats. Cybersecurity means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today's world, cybersecurity is very important because of some security threats and cyber-attacks. For data protection, many companies develop software.

In the digital era, cybersecurity faces numerous challenges including evolving cyber threats, sophisticated hacking techniques, data breaches, inadequate security measures, IoT vulnerabilities, insider threats, and the growing complexity of IT environments. Additionally, ensuring privacy protection, compliance with regulations, and securing cloud-based infrastructure pose significant challenges for organizations and individuals alike. Cybersecurity plays a crucial role in safeguarding personal privacy by protecting individuals' personal information from unauthorized access. By implementing encryption, secure authentication methods, and data protection practices, cybersecurity ensures that personal data remains confidential and protected.

## 23.2 Cyber Crime:

Cybercrime refers to criminal activities carried out using computers or the internet. It includes various illegal activities such as hacking, phishing, identity theft, malware distribution, cyberstalking, and online fraud. Cybercriminals often exploit vulnerabilities in computer systems or use deceptive tactics to gain unauthorized access to sensitive information or commit financial crimes. It encompasses illegal activities conducted using computers or the internet, such as hacking, phishing, identity theft, malware distribution, cyberstalking, and online fraud. These activities exploit vulnerabilities in systems or use deceptive tactics to gain unauthorized access or commit crimes online.

## 23.3 What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. Cybersecurity challenges are the threats and vulnerabilities that organizations face in protecting their information and systems from these threats. It is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes. The field is significant due to the expanded reliance on computer systems, the Internet,[3] and wireless network standards such as Bluetooth and Wi-Fi. Also, due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

The following are the cybersecurity challenges faced in the digital era.

## A. Evolving Threat Landscape:

The digital era has ushered in a new era of threats. Traditional attacks like viruses and worms have given way to more sophisticated threats such as ransomware, advanced persistent threats (APTs), and zero-day vulnerabilities. Attackers constantly adapt their tactics, techniques, and procedures, making it imperative for organizations to stay ahead of the curve.

## B. Proliferation of IoT Devices:

The Internet of Things (IoT) has revolutionized industries, from smart homes to industrial automation. However, the proliferation of IoT devices has introduced a vast attack surface. Insecurely configured devices, lack of updates, and weak authentication mechanisms make them attractive targets for attackers aiming to breach networks or compromise privacy.

## C. Insider Threats:

While external threats are a major concern, insider threats pose a unique challenge. Malicious or negligent actions by employees, contractors, or partners can lead to data breaches or system disruptions. Balancing security measures with the need to maintain a collaborative and open environment is a complex endeavor.

## D. Cloud Security:

The shift to cloud computing offers scalability and flexibility, but it also raises security questions. Organizations must manage data stored across diverse cloud environments, ensuring proper encryption, access controls, and compliance. Shared responsibility models between cloud providers and customers further complicate the security landscape.

## E. Data Privacy and Compliance:

The digital era has prompted increased scrutiny of data privacy and protection. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose strict requirements on how personal data is handled. Balancing data utilization with privacy concerns remains a continuous challenge.

## F. Cyber Warfare and Nation-State Threats:

Geopolitical tensions have spilled into cyberspace, with nation-states engaging in cyber warfare. These threats can disrupt critical infrastructure, steal sensitive information, or even manipulate public opinion. Attribution is often difficult, blurring the lines between criminal activity and state-sponsored attacks.

## G. Skills Shortage:

As the complexity of cybersecurity challenges increases, there's a growing shortage of skilled professionals to counter these threats. Organizations struggle to find and retain qualified experts capable of understanding the evolving threat landscape and implementing effective defenses.

## H. User Awareness and Education:

Despite technological advancements, human error remains a significant factor in cybersecurity incidents. Phishing attacks, social engineering, and other manipulation tactics

target users who are often the weakest link in the security chain. Raising awareness and providing ongoing education are critical to reducing these risks.

## I. Phishing Attacks:

A phishing attack is a type of social engineering attack that targets users' login details and credit card information. In contrast to ransomware, here the information benefits the hacker. Gmail is a Google service that is used across the board for almost everything from business to personal purposes. Now, whenever you open your mail account, you might come across a spam folder that consists of emails that the platform recognizes as a threat to your data security. These spam emails consist of thousands of phishing attacks that your mailing partner recognizes and warns you about the potential cyber threat that it carries. Yet, some of the communications still make it to your inbox where you might fall into a trap. Officially, Google released a statement of how it blocks more than 100 million phishing emails on an everyday basis. It further emphasized how most of the communications were trying to impersonate government officials, authorities, agencies, or websites in order to sound more reliable to mail recipients.

## J. **Sophisticated Cyber Threats**:

The digital era has ushered in a new breed of cyber threats that are relentless and highly sophisticated. From nation-state actors to organized criminal groups, adversaries leverage cutting-edge techniques like zero-day exploits and advanced persistent threats to breach systems, compromise data, and disrupt critical infrastructure.

## K. Data Privacy and Compliance:

The colossal amount of data generated and exchanged daily underscores the importance of data privacy and compliance. Striking a delicate balance between data utilization and safeguarding individual privacy remains a formidable challenge. Stringent regulations like GDPR and CCPA compel organizations to adopt robust data protection measures or face substantial penalties.

## L. IoT and Connected Devices:

The proliferation of Internet of Things (IoT) devices has enriched our lives with convenience and automation. However, it has also opened avenues for cyberattacks. Inadequately secured IoT devices can serve as gateways for unauthorized access and potentially become part of botnets used in large-scale attacks.

## M. Ransomware and Extortion:

The rise of ransomware attacks epitomizes the financial motivations driving cybercriminals. Ransomware not only encrypts critical data but also threatens to leak it if the ransom is not paid. As organizations grapple with the dilemma of whether to comply with demands, the importance of robust backup strategies and incident response plans is underscored.

### N. Supply Chain Vulnerabilities:

In an interconnected digital ecosystem, the security of an organization is only as strong as its weakest link. Cybercriminals often target the supply chain to breach well-defended networks indirectly. Verifying the security posture of vendors and third-party partners becomes crucial to prevent a cascading compromise.

### O. Human Factor:

Despite technological advancements, human errors and social engineering attacks remain potent threats. Phishing, spear-phishing, and other manipulation tactics exploit psychological vulnerabilities to gain unauthorized access to systems or sensitive information. Comprehensive cybersecurity training and awareness programs are vital to mitigate this risk.

### P. Emerging Technologies and Security:

As emerging technologies like artificial intelligence, quantum computing, and 5G networks mature, they introduce both opportunities and risks. Adapting existing cybersecurity measures to secure these technologies and anticipating new threat vectors they might introduce pose unique challenges.

### Q. Global Collaboration and Legislation:

The borderless nature of cyberspace necessitates global collaboration to combat cyber threats effectively. Developing international norms and treaties for cybersecurity while respecting diverse legal systems and geopolitical interests remains a complex endeavor.

### R. Security vs. Convenience:

Striking a balance between robust security measures and user convenience is an ongoing challenge. Complex authentication processes can deter users, while lax security measures expose systems to breaches. Innovations like biometric authentication and adaptive security protocols aim to address this challenge.

### S. Cybersecurity Workforce Shortage:

The demand for skilled cybersecurity professionals far outpaces the available talent pool. Bridging this gap requires concerted efforts in education.

## 23.4 Importance of Cybersecurity in Digital Era:

Technology has become an integral part of our daily lives, and the importance of cybersecurity cannot be overstated. With the exponential growth of digital platforms and the increasing sophistication of cyber threats, individuals and organizations must prioritize their cybersecurity measures.

In this blog post, we will explore the significance of cybersecurity in the digital age and highlight the key reasons why it should be a top priority for everyone.

The digital age has revolutionized the way we live, work, and play. It's also created new opportunities for criminals to exploit vulnerabilities in our computer systems. That's why cyber security is more important than ever before. In this article, we'll explore the reasons why businesses need to invest in robust cyber security solutions. We'll also look at some of the steps you can take to protect your organization from attack. Cybersecurity provides protection against data breaches, safeguarding sensitive information, preserving trust with customers, mitigating financial losses from cyber-attacks, ensuring regulatory compliance, and fostering innovation by creating a secure environment for digital operations.

It enhances trust in digital transactions, protects critical infrastructure from cyber threats, preserves privacy and confidentiality, reduces the risk of financial losses from data breaches, ensures compliance with regulations, and promotes a safer online environment for individuals and businesses. It helps safeguard personal and sensitive information, prevents financial losses from cyber-attacks, preserves trust with customers and partners, ensures regulatory compliance, fosters innovation by creating a secure digital environment, and enhances overall organizational resilience against cyber threats.

In the digital era, cybersecurity is essential for protecting sensitive data, ensuring privacy, and maintaining trust in online transactions. It helps prevent identity theft, financial fraud, and cyber-attacks, thus safeguarding individuals and businesses from financial losses and reputational damage. Additionally, cybersecurity promotes innovation by creating a secure environment for digital advancements, enabling organizations to leverage technology without compromising security. Overall, cybersecurity in the digital era is crucial for building trust, preserving privacy, and fostering a resilient digital ecosystem.

**Protection against Cyber Threats:** Cyber threats such as malware, ransomware, phishing attacks, and data breaches are on the rise. These threats can lead to financial losses, reputation damage, and even legal implications. Implementing robust cybersecurity measures helps protect sensitive information, such as personal data, financial details, and intellectual property, from falling into the wrong hands.

**Safeguarding Personal Privacy:** In the digital age, privacy is at risk due to the vast amount of personal data shared online. Cybersecurity plays a crucial role in safeguarding personal privacy by protecting individuals' personal information from unauthorized access. By implementing encryption, secure authentication methods, and data protection practices, cybersecurity ensures that personal data remains confidential and protected.

**Protection for Businesses:** For businesses, cybersecurity is vital to protect their critical assets, maintain customer trust, and ensure uninterrupted operations. A cyber-attack can result in financial losses, disruption of services, and damage to a company's reputation. By investing in robust cybersecurity measures, businesses can protect their intellectual property, customer data, and financial transactions, ensuring the continuity of their operations.

**Prevention of Financial Losses:** Cyber-attacks can have severe financial implications for individuals and organizations. The costs associated with recovering from an attack, including investigating the breach, repairing systems, and compensating affected parties, can be significant. By implementing effective cybersecurity measures, the risk of financial losses due to cyber-attacks is reduced, saving individuals and businesses from potential financial hardships.

**Maintaining Trust and Reputation:** Trust is the foundation of any successful relationship, whether it is between individuals or businesses. In the digital age, where online interactions are prevalent, trust and reputation are even more critical. A single data breach or cyber-attack can erode trust and damage the reputation of individuals and organizations. By prioritizing cybersecurity, individuals and businesses demonstrate their commitment to protecting their stakeholders' interests, fostering trust, and maintaining a positive reputation.

**Compliance with Legal and Regulatory Requirements:** Many industries are subject to legal and regulatory requirements concerning data protection and cybersecurity. Non-compliance can result in severe penalties, legal consequences, and reputational damage. By implementing robust cybersecurity measures, organizations ensure compliance with these requirements, mitigating the risk of legal issues and demonstrating their commitment to responsible data handling.

**Preserving National Security:** Cybersecurity is not only crucial for individuals and businesses but also for the overall security of nations. Cyber-attacks can target critical infrastructure, government systems, and military networks, posing a significant threat to national security. By prioritizing cybersecurity, governments, and organizations can work together to protect their digital assets and defend against cyber threats, ensuring the stability and security of the nation.

## 23.5 Challenges of Cybersecurity in Digital Era:

## A. In the Digital Era, Cybersecurity Faces Numerous Challenges, Including:

- Evolving Threat Landscape: Cyber threats continue to evolve in sophistication and diversity, making it challenging for cybersecurity professionals to keep pace with emerging attack vectors such as ransomware, social engineering, and zero-day exploits.
- Insider Threats: Insider threats pose a significant risk to cybersecurity, as employees, contractors, or partners with access to sensitive information may intentionally or unintentionally compromise security through malicious actions, negligence, or human error.
- Proliferation of Connected Devices: The proliferation of IoT devices and interconnected systems expands the attack surface, creating new vulnerabilities and increasing the complexity of managing and securing networked environments.
- Cloud Security Concerns: As organizations migrate data and services to the cloud, ensuring the security of cloud-based infrastructure, applications, and data becomes paramount, requiring robust security controls and risk management practices.
- Shortage of Cybersecurity Talent: There is a global shortage of skilled cybersecurity professionals, making it challenging for organizations to recruit and retain qualified

personnel capable of addressing complex cybersecurity threats and implementing effective security measures.

- Compliance and Regulatory Complexity: Compliance with an ever-expanding array of cybersecurity regulations, standards, and industry requirements presents a significant challenge for organizations, requiring dedicated resources and expertise to ensure adherence and avoid non-compliance penalties.
- Budgetary Constraints: Limited cybersecurity budgets and resource constraints may hinder organizations' ability to invest in adequate security measures, leaving them vulnerable to cyber-attacks and unable to implement comprehensive cybersecurity strategies.
- Advanced Persistent Threats (APTs): Sophisticated APTs conducted by nation-state actors, cybercriminal groups, or organized cyber gangs pose a persistent and highly targeted threat to organizations, requiring advanced detection and response capabilities to mitigate their impact.

Addressing these challenges requires a proactive and multi-faceted approach, including investing in advanced security technologies, enhancing employee training and awareness, collaborating with industry peers and stakeholders, and continuously evaluating and improving cybersecurity practices to adapt to evolving threats.

## B. Some of the Key Challenges in Cybersecurity Also Includes:

**Sophisticated Cyber Threats:** Cybercriminals continually develop sophisticated techniques to exploit vulnerabilities in systems and networks, making it challenging to defend against evolving threats such as ransomware, phishing, and zero-day attacks.

**Shortage of Skilled Professionals:** There is a significant shortage of cybersecurity professionals with the expertise and experience needed to address complex security challenges. Recruiting and retaining skilled talent remains a persistent challenge for organizations.

**Complexity of IT Infrastructure:** Modern IT environments are increasingly complex, with hybrid cloud deployments, interconnected systems, and a proliferation of devices, all of which create additional security challenges in terms of visibility, management, and control.

**Insider Threats:** Insider threats, whether intentional or accidental, pose a significant risk to organizations. Malicious insiders, negligent employees, or compromised accounts can bypass traditional security measures and cause substantial damage.

**Compliance and Regulatory Requirements:** Meeting compliance mandates and regulatory requirements is a complex and resource-intensive task for organizations, especially in highly regulated industries. Achieving compliance while maintaining effective security practices can be a challenge.

**Rapid Technological Advancements:** The rapid pace of technological advancements, including IoT, AI, and 5G, introduces new security risks and challenges.

Ensuring the security of emerging technologies requires proactive measures and ongoing risk assessments.

**Budget Constraints:** Many organizations face budget constraints when it comes to cybersecurity investments. Limited resources may impact the ability to implement robust security measures and adequately address cybersecurity risks.

**Global Nature of Cyber Threats:** Cyber threats are not confined by geographical boundaries, and organizations must contend with threats originating from various locations around the world. Coordinating responses and sharing threat intelligence on a global scale presents challenges in itself.

Addressing these challenges requires a comprehensive approach that includes investing in advanced technologies, enhancing cybersecurity awareness and training, collaborating with industry peers and government agencies, and adopting proactive strategies to detect and respond to cyber threats effectively.

## 23.6 Why Cybersecurity is So Crucial in Digital Era?

Cybersecurity refers to the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, and other cyber threats. It encompasses various technologies, processes, and practices designed to safeguard information and prevent disruption or damage to electronic systems. Key components of cybersecurity include network security, endpoint security, application security, data security, and identity management. As technology evolves, cybersecurity continues to be a critical concern for businesses, governments, and individuals to mitigate risks and protect against cyber threats. Cybersecurity means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today's world, cybersecurity is very important because of some security threats and cyber-attacks. For data protection, many companies develop software.

In the digital era, cybersecurity faces numerous challenges including evolving cyber threats, sophisticated hacking techniques, data breaches, inadequate security measures, IoT vulnerabilities, insider threats, and the growing complexity of IT environments. Additionally, ensuring privacy protection, compliance with regulations, and securing cloud-based infrastructure pose significant challenges for organizations and individuals alike. Cybersecurity plays a crucial role in safeguarding personal privacy by protecting individuals' personal information from unauthorized access. By implementing encryption, secure authentication methods, and data protection practices, cybersecurity ensures that personal data remains confidential and protected.

## 23.7 Cyber Ethics:

Cyber ethics, also known as internet ethics or digital ethics, refers to the principles and values that guide appropriate behavior online. In today's interconnected world, where technology plays a central role in almost every aspect of our lives, understanding and adhering to cyber ethics is crucial.

Firstly, cyber ethics encompass respect for privacy and confidentiality. Users should understand the importance of safeguarding personal information and respect the privacy of others. This includes refraining from unauthorized access to others' accounts or sharing sensitive information without consent.

Secondly, integrity and honesty are fundamental in cyberspace. Users should refrain from spreading false information, engaging in online fraud or scams, or plagiarizing content. Maintaining honesty and integrity online contributes to a trustworthy and reliable digital environment.

Moreover, cyber ethics entail responsible use of technology. This includes practicing good digital citizenship by respecting intellectual property rights, adhering to copyright laws, and using technology for constructive purposes. Users should also be mindful of the impact of their online actions on others and society as a whole.

Additionally, cyber ethics involve promoting digital inclusivity and equality. Access to the internet and technology should be equitable, and efforts should be made to bridge the digital divide. Discrimination and harassment online should not be tolerated, and efforts should be made to create an inclusive and safe online environment for all users.

Furthermore, cybersecurity is an essential aspect of cyber ethics. Users should take measures to protect themselves and others from cyber threats, such as viruses, malware, and hacking attempts. This includes using strong passwords, keeping software up to date, and being cautious when sharing personal information online.

In conclusion, cyber ethics play a vital role in shaping responsible and ethical behavior in the digital age. By adhering to principles of privacy, integrity, responsibility, inclusivity, and cybersecurity, individuals can contribute to a safer, more respectful, and more equitable online community.

## 23.8 Conclusion:

Cybersecurity in the digital era is that it's an ongoing battle requiring constant vigilance, innovation, and collaboration. As technology evolves, so do cyber threats, necessitating adaptive defenses, robust policies, and public awareness to safeguard digital assets and privacy.

The digital era presents numerous challenges for cybersecurity, primarily due to the increasing complexity and interconnectivity of digital systems. One significant challenge is the constantly evolving nature of cyber threats, including malware, phishing attacks, and ransomware, which require constant vigilance and adaptation by cybersecurity professionals. Additionally, the proliferation of internet-connected devices in the Internet of Things (IoT) expands the attack surface, creating new vulnerabilities that can be exploited by hackers.

Another challenge is the shortage of skilled cybersecurity professionals to adequately defend against these threats.

The demand for cybersecurity expertise far outpaces the supply, leading to a talent gap that leaves many organizations vulnerable to attack. Furthermore, the rapid pace of technological advancement introduces new vulnerabilities before existing ones can be fully addressed, making it difficult for cybersecurity professionals to keep up.

Moreover, the interconnected nature of digital systems means that cybersecurity is not just a concern for individual organizations but also for society as a whole. A cyber-attack on critical infrastructure, such as power grids or financial systems, can have widespread and devastating consequences, making cybersecurity a national security issue.

Privacy concerns also come into play in the digital era, as the collection and analysis of vast amounts of personal data raise questions about data protection and individual rights. Ensuring the privacy and security of this data is essential for maintaining trust in digital systems and services.

Overall, the challenges of cybersecurity in the digital era require a multi-faceted approach that includes technological innovation, robust policies and regulations, investment in cybersecurity education and training, and collaboration between government, industry, and academia. Only by addressing these challenges collectively can we effectively safeguard digital systems and protect against cyber threats in the modern age.

## 23.9 References:


1. *Ashwini Seth, Sachin Shankar Bhosale (April 2021) Era of Cybersecurity.*
2. *Adnan Bukhari, Sonali Mayekar (May 2022) A survey on cybersecurity*
3. *Harshad Kadam (2021) Research paper on cloud computing.*
4. *https://sl-courses.iiitb.ac.in/advanced-executive-program-cyber-security?utm_source=google&utm_medium=cpc&utm_term=cyber%20security%20in%20networking&utm_content=19592622120-152760250794-660579058982&utm_device=m&utm_campaign=Search-TechCluster-Cyber-CCyber-PG-IIITB-IN-Main-AllDevice-IIITBDomain-adgroup-Cyber-Google-Suggested&gad=1&gclid=EAIaIQobChMIk6iGjabWgAMVORKDAx2QPA7xEAAYASAAEgLtx_D_BwE*
5. *https://www.skyflow.com/dataprivacyvault?kw=infosec&cpn=19907133572&kw=infosec&cpn=19907133572&utm_agid=147108193599&creative=654154985020&extension_id=&device=m&placement=&utm_term=infosec&utm_campaign=Australia+NZ+Japan-March30,2023&utm_source=google-ads&utm_medium=ppc&hsa_acc=6575335991&hsa_cam=19907133572&hsa_grp=147108193599&hsa_ad=654154985020&hsa_src=g&hsa_tgt=kwd-23326830&hsa_kw=infosec&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI2vH2nKbWgAMVDmd9Ch22jwPcEAAYAiAAEgIsWvD_BwE*
6. *https://edubirdie.com/examples/major-challenges-facing-cyber-security/*
7. *https://www.drishtiias.com/daily-updates/daily-news-editorials/rising-up-to-cyber-security-challenges*
8. *Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole*
9. *Computer Security Practices in Non-Profit Organizations – A Net Action Report by Audrie Krause.*

10. *A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.*
11. *International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in*
12. *Health Care Industry "by G. Nikhita Reddy, G. J. Ugander Reddy IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.*
13. *CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.*