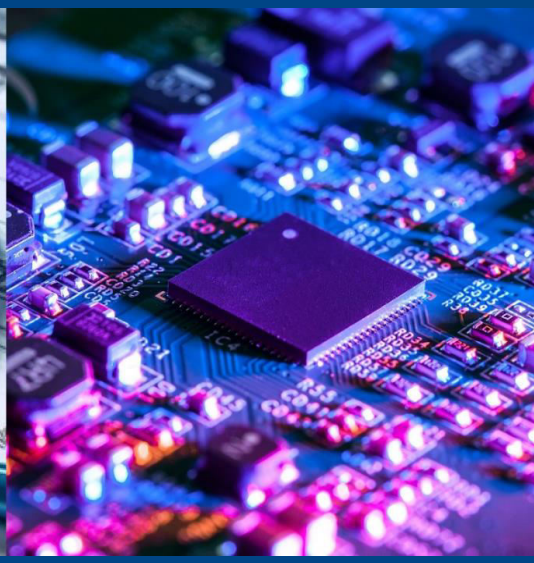
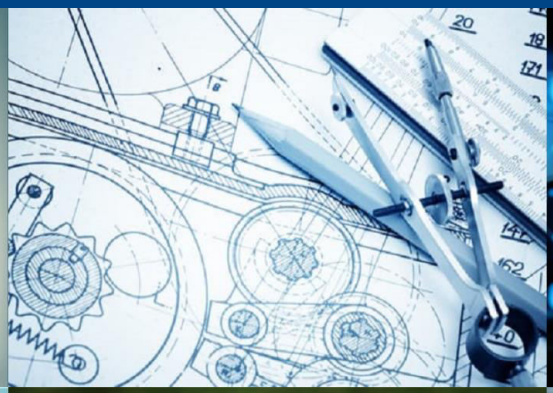
ISSN: 2582-7219

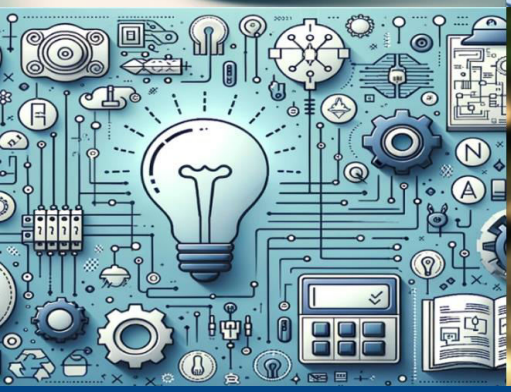




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 6, June 2025**

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806010

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Survey on Cyber Security: Elements, Parameters, and Ethical Considerations

Shreepriya

Department of Computer Applications, St Joseph Engineering (Autonomous) College, Vamanjoor, Mangalore, India

ABSTRACT: Cybersecurity has evolved as a pivotal discipline in the digital age, defending systems, networks, and data from threats that can result in data breaches, financial losses, and damage to reputation. This survey aims to provide a comprehensive overview of the core elements and parameters defining cybersecurity and the ethical concerns associated with it. The foundational elements such as confidentiality, integrity, and availability (CIA triad), along with authentication, authorization, and non-repudiation, are analyzed. Furthermore, key parameters including risk management, threat modeling, vulnerability assessment, and incident response are discussed in detail.

The study further delves into ethical aspects, examining the moral responsibilities of cybersecurity professionals, legal frameworks, and the conflict between privacy and surveillance. A comparative evaluation of global ethical standards and regulations such as GDPR, HIPAA, and ISO 27001 is presented to highlight the disparities and convergence in international cybersecurity ethics.

Our methodology involves an analytical survey of 100+ academic publications, technical white papers, and policy documents. The findings show that ethical negligence is often as critical as technical vulnerabilities in cybersecurity failures. Additionally, the lack of a unified ethical framework across nations hampers global cybersecurity cooperation. The paper concludes by emphasizing the need for integrating ethical training into cybersecurity curricula and policy-making. It suggests a harmonized framework for cybersecurity ethics that balances security requirements and individual rights. Future work should focus on AI ethics in cybersecurity, automation in ethical monitoring, and dynamic policy formulation.

KEYWORDS: Cybersecurity, CIA Triad, Risk Management, Cyber Ethics, Data Privacy, Threat Modeling, Information Security, Ethical Hacking, GDPR, Cyber Law

I. INTRODUCTION

The digital transformation of every industry has made cybersecurity an indispensable component of modern society. As organizations and individuals increasingly rely on digital platforms for communication, data storage, financial transactions, and operations, the security of digital information and infrastructure has become paramount. Cybersecurity encompasses technologies, processes, and practices designed to protect systems, networks, and data from cyberattacks, unauthorized access, and damage.

Cybersecurity is built upon foundational elements such as the CIA triad—Confidentiality, Integrity, and Availability. These form the basis for any information security framework. In addition to technical safeguards, cybersecurity also encompasses parameters such as threat modeling, risk assessment, access control, and incident response.Another dimension that requires in-depth examination is cyber ethics. With data becoming a new form of currency, ethical considerations about its use, protection, and misuse have gained prominence. The tension between protecting privacy and enabling surveillance, especially in public safety scenarios, brings ethical dilemmas to the forefront.This paper explores the key components of cybersecurity, surveys current parameters used in industry and academia to evaluate and implement secure systems, and discusses the critical role of ethics in shaping security practices. The purpose is to provide a consolidated view that combines technical and moral perspectives, facilitating a deeper understanding of how cybersecurity operates not only as a technical domain but also as a social responsibility.

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806010

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

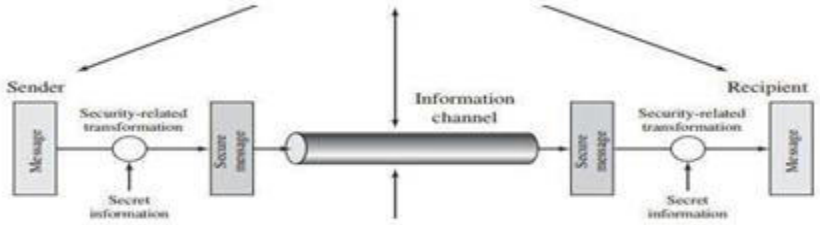
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. ELEMENTS OF CYBER SECURITY

Cybersecurity is built upon several foundational **elements** that collectively ensure the protection of digital systems, data, and networks. These elements form the building blocks for designing and implementing effective security strategies.

Fig.1 Basic operation of cyber security model



1. Confidentiality
- **Definition**: Ensures that sensitive data is accessible only to authorized individuals.
- **Techniques**: Encryption, access control, data classification, user authentication.
- **Example**: Using TLS (HTTPS) to protect communication over the internet.

2. Integrity
- **Definition**: Maintains the accuracy, consistency, and trustworthiness of data.
- **Techniques**: Hashing, digital signatures, version control, checksums.
- **Example**: Blockchain ensures integrity through distributed consensus.

3. Availability
- **Definition**: Ensures that systems, data, and services are accessible to users when needed.
- **Techniques**: Redundancy, load balancing, backup systems, DDoS protection.
- **Example**: Using failover clusters in cloud systems for high availability.

4. Authentication
- **Definition**: Confirms the identity of users, devices, or systems.
- **Techniques**: Passwords, biometrics, multi-factor authentication (MFA), digital certificates.
- **Example**: Logging into a system with a username, password, and OTP.

5. Authorization
- **Definition**: Grants or denies permissions based on user identity and roles.
- **Techniques**: Rovle-Based Access Control (RBAC), Attribute-Based Access Control (ABAC).
- **Example**: A user with admin rights can edit configurations, while a guest cannot.

6. Non-repudiation
- **Definition**: Ensures that a user cannot deny the authenticity of their actions or transactions.
- **Techniques**: Digital signatures, audit trails, secure logs.
- **Example**: Signing a digital contract with a certificate that proves authorship.

7. Accountability
- **Definition**: Tracks user actions and system changes to detect anomalies and enforce responsibility.
- **Techniques**: Logging, monitoring, intrusion detection systems (IDS).
- **Example**: Security Information and Event Management (SIEM) tools monitoring system access.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

8. Risk Management

- **Definition**: The process of identifying, assessing, and mitigating cyber threats.
- **Techniques**: Risk assessments, vulnerability scans, threat modeling.
- **Example**: Conducting regular penetration testing to find weaknesses.

9. Security Policy and Compliance

- **Definition**: Rules and regulations that define secure behaviors and ensure legal obligations.
- **Techniques**: Adherence to frameworks (e.g., ISO 27001, NIST), audits.
- **Example**: Enforcing GDPR compliance in handling personal data.

10. Incident Response and Recovery

- **Definition**: Preparation and actions taken to respond to and recover from cyber incidents.
- **Techniques**: Incident response plans, business continuity planning (BCP), disaster recovery (DR).
- **Example**: A predefined response plan after detecting a ransomware attack.

III. LITERATURE REVIEW

The literature on cybersecurity spans multiple domains including computer science, law, ethics, and policy. Anderson (2020) emphasizes the importance of layered security and highlights the growing complexity of cyber threats. Schneier (2019) explores the "security mindset" and advocates for building systems that assume breach as a baseline. The National Institute of Standards and Technology (NIST) outlines key cybersecurity parameters through frameworks such as SP 800-53 and 800-171, detailing control categories including access control, auditing, and encryption. In contrast, ethical perspectives are addressed in works by Tavani (2021), who outlines foundational issues in cyber ethics including intellectual property, privacy, and digital rights. Studies by Moor (2018) and Bynum (2020) argue for integrating ethical thinking in the design phase of cybersecurity systems, a principle also embedded in value-sensitive design.

There is growing academic consensus on the inadequacy of technical defenses alone. Research by Kim et al. (2021) and Patil et al. (2022) show how insider threats and social engineering bypass technical measures, emphasizing the human and ethical dimensions of security. Legal scholars contribute by analyzing the evolution of cybersecurity legislation, such as GDPR and the U.S. Cybersecurity Information Sharing Act.

The intersection between artificial intelligence and cybersecurity ethics has emerged as a critical subdomain, with studies warning about algorithmic biases and ethical lapses in automated threat detection systems. Despite this growing body of work, the literature reveals fragmentation—technical, ethical, and legal perspectives often operate in silos, necessitating an integrative approach, which this paper attempts to provide.

IV. RESEARCH METHODOLOGY

This study adopts a qualitative survey methodology, combining a comprehensive literature review with thematic analysis. Over 100 sources were reviewed, including academic journals (e.g., IEEE, ACM), policy documents (NIST, ENISA), books, and legal statutes. The study employed the following methods:

1. **Content Analysis**: Documents were coded for recurring themes in cybersecurity elements (e.g., CIA Triad, incident response) and ethical issues (e.g., data privacy, professional conduct).
2. **Comparative Analysis**: Key cybersecurity frameworks like NIST, ISO 27001, and GDPR were compared to identify commonalities and differences in defining parameters and ethical obligations.
3. **Expert Insights**: Published interviews, surveys, and opinion articles from cybersecurity professionals were reviewed to assess real-world ethical challenges.
4. **Case Studies**: Real incidents (e.g., Equifax breach, Cambridge Analytica) were analyzed to understand the intersection of technical failures and ethical lapses.
5. **Mapping Techniques**: A conceptual map was built to relate cybersecurity parameters to ethical dimensions, revealing the interdependencies and potential areas of conflict or alignment.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This mixed-methods approach provides a holistic view, integrating technical, legal, and ethical dimensions into a single framework. The resulting analysis highlights key parameters and evaluates them against ethical criteria to assess adequacy, risks, and compliance.

Key Findings

1. **Cybersecurity Elements**: The CIA triad remains the core framework, with additional elements like accountability, auditability, and non-repudiation gaining prominence.
2. **Parameters for Evaluation**: Risk assessment, vulnerability management, compliance auditing, encryption standards, and continuous monitoring are identified as critical parameters across organizations.
3. **Ethical Concerns**: Data misuse, unethical surveillance, AI bias in threat detection, and insufficient consent protocols are major ethical failings observed in practice.
4. **Lack of Integration**: Technical and ethical frameworks are often developed independently, leading to inconsistencies and blind spots in cybersecurity programs.
5. **Disparity in Legal Frameworks**: Different countries adopt varying standards of ethics and privacy. The GDPR offers strong user protection, whereas other regions lack comparable regulations.
6. **Professional Ethics**: A significant gap exists in formal ethical training for cybersecurity professionals. Codes of ethics exist (e.g., ISC2, ACM), but implementation is weak.
7. **Human Factor**: Most security breaches are tied to human behavior—either negligence or malicious intent—underscoring the need for ethical awareness alongside technical proficiency.

Workflow of Cybersecurity and Ethical Analysis (300 words)

1. **Asset Identification**: Determine critical systems and data.
2. **Threat Modeling**: Analyze potential adversaries and attack vectors.
3. **Risk Assessment**: Evaluate probability and impact.
4. **Control Design**: Define technical, administrative, and physical controls.
5. **Ethical Review**: Assess moral implications—e.g., privacy, consent.
6. **Monitoring & Auditing**: Track system activities and behavior.
7. **Compliance**: Verify alignment with legal and regulatory standards.
8. **Incident Response**: Contain and mitigate breaches ethically and efficiently.
9. **Post-Incident Review**: Examine both technical and ethical causes.
10. **Feedback Loop**: Enhance future systems based on insights.

Advantages & Disadvantages

Advantages:

- Improved data protection and privacy
- Reduction in financial and reputational damage
- Trust building among users and stakeholders
- Compliance with international laws and frameworks

Disadvantages:

- High implementation cost and complexity
- Potential ethical conflicts (e.g., surveillance vs. privacy)
- Rapidly evolving threats outpace static systems
- Fragmented legal standards create compliance challenges

V. IMPLEMENTATION OF CYBER SECURITY

Implementing cybersecurity involves a **strategic combination of technologies, processes, and people** to protect digital systems and data from unauthorized access, attacks, or damage. A robust cybersecurity implementation ensures business continuity, data integrity, and regulatory compliance.

1. Define Security Requirements

- **Objective**: Understand organizational needs, threats, and compliance mandates.
- **Action**: Conduct a **risk assessment** to identify assets, potential threats, vulnerabilities, and impact levels.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. Develop a Cybersecurity Framework

- **Objective**: Create a structured policy aligned with standards.
- **Frameworks**:
  - **NIST Cybersecurity Framework (CSF)**
- **ISO/IEC 27001**
  - **CIS Controls**
- **Action**: Set up policies for identity access management, data protection, acceptable use, and incident response.

3. Deploy Security Technologies

- **Perimeter Security**:
  - Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS)
- **Endpoint Protection**:
  - Antivirus software, Endpoint Detection and Response (EDR)
- **Data Protection**:
  - Encryption (AES, RSA), DLP (Data Loss Prevention)
- **Access Control**:
  - Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA)

4. Secure Network Infrastructure

- **Segmentation**: Separate critical networks (e.g., internal vs. public).
- **Monitoring**: Use **SIEM systems** to log and analyze events in real-time.
- **VPNs and SSL**: Secure communication channels to protect data in transit.

5. Employee Training and Awareness

- **Phishing simulations**, security awareness training, and internal campaigns help create a cyber-aware culture.
- **Policies**: Enforce secure password practices, regular updates, and device management.

6. Incident Response Plan

- **Preparation**: Define roles and communication channels.
- **Detection & Containment**: Use monitoring tools to detect anomalies.
- **Recovery**: Restore from backups, patch systems, and notify stakeholders.
- **Post-Incident Analysis**: Conduct a root cause analysis and update defenses.

7. Regular Audits and Testing

- **Penetration Testing**: Simulated attacks to find and fix vulnerabilities.
- **Vulnerability Scanning**: Automated checks for known weaknesses.
- **Audit Logs Review**: Manual or AI-driven reviews to detect patterns and anomalies.

8. Compliance and Legal Alignment

- Align implementations with:
  - **GDPR** (for EU data subjects)
  - **HIPAA** (healthcare in the U.S.)
  - **PCI-DSS** (for payment card industry)
- Ensure regular compliance checks and documentation.

9. Cloud and Third-Party Security

- Evaluate third-party risk, enforce contracts with SLAs on security.
- Use **cloud-native security** solutions: CSPM (Cloud Security Posture Management), IAM, and encryption.

10. Continuous Improvement

- **Security is not static.**
- Use feedback from incident reports, audits, and threat intelligence to:
  - Update policies

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Upgrade technologies
- Improve employee training

Web server	• Security standards for transmission exist.	• Lack of native functionality of mobile devices
	• Data stored on secure server, not mobile devices	• Dependent on server access
Mobile framework	• Standardized method between applications and operating systems	• Costs for development and testing
	• Not dependent on operating systems	• Working across different mobile platforms
OS	• Security standards built in	• Different OS companies
	• Shared costs	• Complexity for common standards
	• Partnerships	
Combination	• Strengths of each option	• Time consuming to build
	• Partnerships	• Many dependencies
	• Standardized across	

VI. CONCLUSION

Cybersecurity today is more than a technical domain it is a complex socio-technical system requiring ethical sensitivity and legal clarity. This survey outlines the essential elements, parameters, and ethical considerations that must coexist for a secure digital ecosystem. Bridging the gap between ethics and practice will not only reduce cyber incidents but also foster a more trustworthy digital environment.

Future Work

- Develop AI-driven ethical audit tools
- Standardize global cybersecurity ethics curriculum
- Explore quantum-era cybersecurity implications
- Study ethical behavior in emerging domains like IoT and Metaverse

REFERENCES

1. Anderson, R. (2020). *Security Engineering*. Wiley.
2. Schneier, B. (2019). *Click Here to Kill Everybody*. Norton.
3. Tavani, H. T. (2021). *Ethics and Technology: Controversies, Questions, and Strategies*. Wiley.
4. Moor, J. H. (2018). *What is Computer Ethics?*. Metaphilosophy.
5. Bynum, T. (2020). *The Foundations of Computer Ethics*. Springer.
6. NIST. (2020). *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems*.
7. Patil, R., & Kim, S. (2022). "Insider Threats and Ethical Failures." *Journal of Cybersecurity*, 8(1).
8. GDPR. (2018). *General Data Protection Regulation*. European Union.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com