

Cybersecurity Law, Policy and Ethics

Prepared by **Dr. Kamal Alieyan**

Lecture 05

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Cybersecurity Ethics: Cyberspace and Other Applications (2)



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture Objective

- Target more aspect of cybersecurity ethics.
- The cybersecurity is an advancing field and makes its presence felt in various other domains and applications, we will highlight ethics in those domains and applications.

Lecture topics

- **3.1 CYBERSECURITY ETHICS: A DETAILED STUDY (DOMINS)**
- **3.2 CYBERSECURITY ETHICS IN APPLICATIONS**

Lecture topics

- 3.1 CYBERSECURITY ETHICS: A DETAILED STUDY (DOMAINS)
- 3.2 CYBERSECURITY ETHICS IN APPLICATIONS

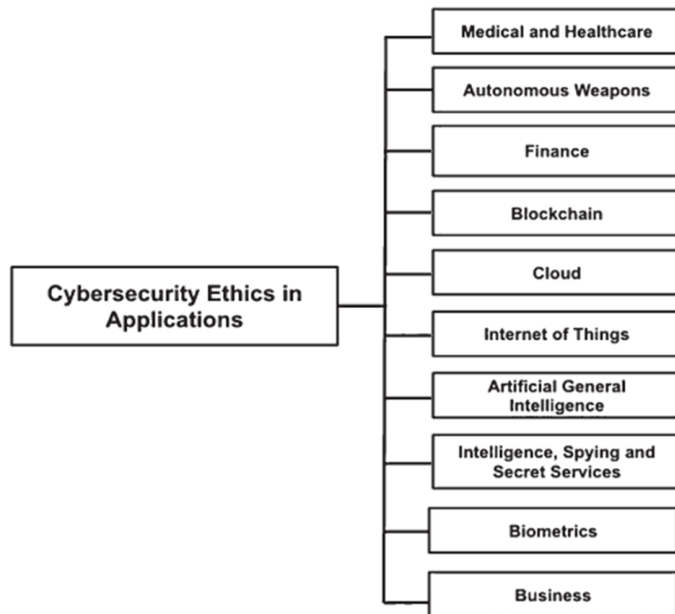


FIGURE 3.2 Cybersecurity ethics in applications.

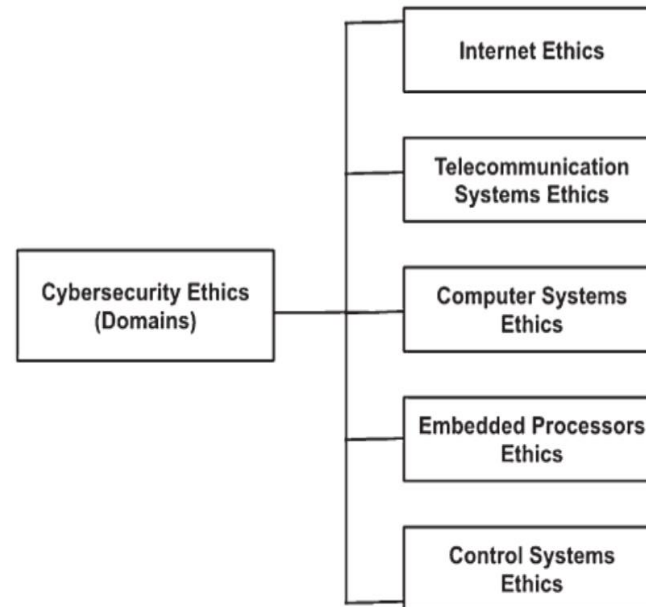


FIGURE 3.1 Cybersecurity ethics (domains).

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

- **Cyberspace** incorporates the Internet, telecommunication systems, computer systems, embedded processors, and control systems.
- Each of these domains have specific functionalities and operates in various ways.
- Thus each of these have their own ethics and standards.
- Each of these components are responsible for establishing cyberspace and their applications traverse the globe.
- Therefore, a detailed study on ethics for these components is of great significance.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

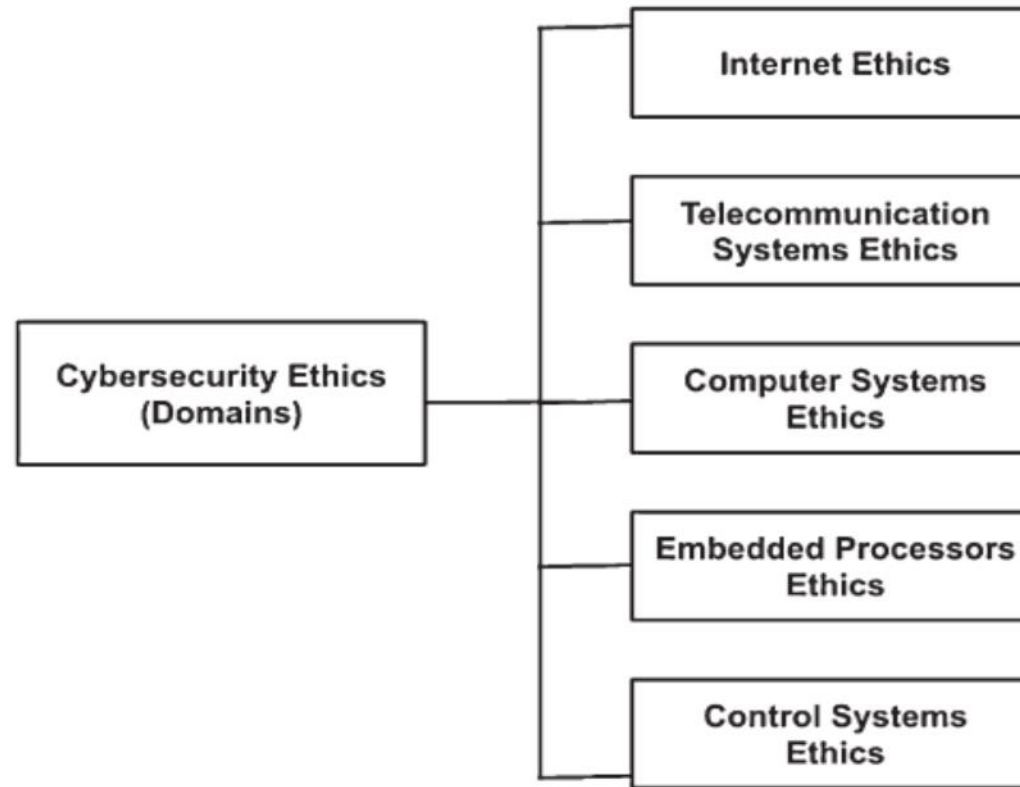


FIGURE 3.1 Cybersecurity ethics (domains).

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- One of the most remarkable and active components of cyberspace is the Internet.
- In fact, the majority of the communication among devices and users takes place over the Internet.
- Since the Internet harbors millions of users and devices, exchange of information over the platform must be performed in an ethical way.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- Definition of the Internet:
 - ☐ The Internet might be characterized as a method for interfacing a computer to any other computer anywhere in the world by means of dedicated routers and servers.
 - ☐ At the point when two computers are associated over the Internet, they can send and receive a wide range of information like text, design, voice, video, and computer program.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- Many times ethics over the Internet referred as Internet Etiquette or Netiquette.
- As Etiquette corresponds to the code of polite behavior in society, netiquette concerned with code of good behavior on Internet.
- Netiquette takes into account various aspects of the Internet, like email, social media, and web forums. Also, online chat, website comments.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- There are no specific netiquette rules or guidelines, however the overall idea is to respect others online:
 1. Remember the Human
 2. Following the Same Standard of Behavior online as in Real life
 3. Knowing that You are in Cyberspace
 4. Appreciating the Other Peoples Time and Bandwidths
 5. Making your self Good online
 6. Sharing Expert knowledge
 7. Helping Keep Flame Wars Under Control
 8. Respecting Other People's Privacy
 9. Not Abusing Power
 10. Be Forgiving of Other People's Mistakes
- Good netiquette is useful for everyone in Cyberspace, and it ensures a healthy environment.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- Definition of Telecommunications:

- ☐ Telecommunications is referred to as the transmission of information. This information may be in the form of signs, signals, messages, words, writings, images, and sounds.
- ☐ The information is usually transmitted through means of a wire, radio, optical or other electromagnetic systems.
- ☐ Telecommunication occurs when there is an interchange of information between communication parties which includes the use of technology.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- A telecommunications system operates as a cluster of nodes and links to facilitate telecommunication.
- Telecommunication incorporates **three important aspects**, namely information, communication, and technology, and they are related to one another.
- **Information** is produced due to an interpretation process. Usually, a receiver interprets data during a specific time-space based on the total amount of knowledge and experience of the receiver.
- **Communication** may be defined as the interaction between elements and the repercussion of the effect that the performance of one element has on the performance of another element.
- **Technology** is a field of knowledge and skills that includes design, construction, and use of created artifacts, and the theoretical science of technology itself.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- When technology-based environments are considered, and the complexity that emerges in the cross between humans, between technology and humans, and between information, communication, and technology, a cultural focus emerges where human attitudes, values, and behavior sets the conditions for communication and interaction.
- Inside the ethical circle of information, the issue of suitable or right conduct related to information, creation of information, and transfer of information is considered primarily.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- In a changing technological infrastructure, ethical considerations have an effect on the outcome of human communication.
- Common norms and rules must be respected to enable humans to live and act together in Cyberspace.
- Rules or norms can be both explicit and implicit.
- Society depends on technology. This dependence brings to the fore ethical considerations of its design, use, and implementation.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- One way of dealing with ethics when designing ICT environments is through a framework for ethical guidance in development projects and the design of information systems.
- The framework includes a method with four steps:
 - Identify the different needs that can be associated with the situation;
 - Identify where conflicts may occur;
 - Solve the problems that can cause conflicts;
 - Let the common needs to be included in a requirement catalog and perform a requirement analysis for the situation to be designed.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

- All the operations in Cyberspace take place due to the interaction of computer systems over the network.
- Definition of Computer Systems
 - ☐ Computer systems are shaped by an arrangement of interconnected systems that share a central storage system.
 - ☐ It also supports various peripheral devices like printers, scanners, and routers.
 - ☐ Every system associated with the system can work autonomously, however, it can communicate with other external devices and computers.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

- Cyberspace continues to grow as more and more computer systems are added.
- More computer systems mean increased usage as well as more communication among users.
- Therefore, it is mandatory to take care of ethical considerations in Cyberspace with respect to computer systems.
- Some ethical considerations are as follows:
 1. **Contributing to Society and Human Well Being:** While designing or implementing systems, it is mandatory that computer experts guarantee that the results of their endeavors will be utilized in socially mindful manners, will address social issues, and will stay away from destructive impacts to wellbeing and welfare.
 2. **Avoiding Harm to Others:** The use of computing technology should not harm users, the general public, employees, employers. Harmful actions incorporate intentional destruction or modification of files and programs. This may have severe consequences in the form of serious loss of resources and unnecessary expenditure of human resources (HR).

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

3. **Being Honest and Trustworthy:** Honesty and trust go hand in hand. For an organization to function effectively, trust is very important. Honest computing professionals do not make intentionally bogus or tricky cases about a system or system design. Rather, they give complete honesty of all appropriate system constraints and issues.
4. **Being Fair and Taking Action Not to Discriminate:** Discrimination between different groups of people may be the result of use or misuse of information and technology. All individuals are entitled to equivalent opportunity to participate in, or take advantage of, the utilization of computer resources irrespective of their race, sex, religion, age, disability, national origin, or other such comparative elements. These standards, however, do not legitimize unapproved access and utilization of computer resources. Further, they do not give an adequate motivation to infringement of some other ethical objectives of this code.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

5. **Honoring Property Rights Including Copyrights and Patents:** Violating copyrights, patents, trade secrets, and the terms of license agreements is prohibited by law in most circumstances. The violations are contrary to professional behavior even if the software is not so protected. Copies of software must be made and distributed only with proper authorization. Unauthorized duplication of materials must be discouraged.
6. **Giving Proper Credit for Intellectual Property (IP):** Computing experts must ensure the integrity of protected innovation. Hence it is not ethical to assume acknowledgment for other's ideas or work, even in situations where the work has not been unequivocally ensured by copyright, patent, and so on.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

7. **Respecting the Privacy of Others:** This principle is significant for electronic communications, including electronic mail. It denies strategies that capture or monitor electronic client information, including messages, without the consent of clients or approval identified with system activity and support. Client information must be treated with strictest secrecy, aside from in situations where it is proof for the infringement of law or authoritative guidelines. In such cases, the nature or contents of the sensitive information must be disclosed only to proper authorities under the right circumstances.
8. **Honoring Confidentiality:** Honesty and confidentiality are interconnected. It is necessary to honor confidentiality. Computer professionals must regard all commitments of secrecy to employers, customers, and clients except if released from such commitments by necessities of the law or different standards of this code.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- An embedded system may be thought of as a combination of computer hardware and software, which is either fixed in capability or programmable, designed for a specific function or functions within a larger system.
- Embedded system hardware can be microprocessor- or microcontroller-based.
- Definition of Embedded Processor:
 - ☐ An embedded processor is primarily a microprocessor designed into a system that is responsible for controlling electrical and mechanical functions.
 - ☐ An embedded processor can be programmed specifically for the specific operations.
 - ☐ It may support many different CPU (central processing unit) architectures.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- Since embedded processors are deep-seated in critical hardware, such systems can be remarkably tricky to safeguard. Hence cybersecurity and cyber resiliency must be considered toward the start of the plan and design process.
- Embedded processors are known to be powerless against cyber-attacks because of a few reasons, which may go from the electronic system's capacity to withstand cyber threats to the side effects of processor pipeline designs to empower cyber-attacks.
- In addition, fixes may bring about inadvertent impacts, including expanding power utilization and influencing processing or timing, all of which can constrain hardware performance. Therefore, ethical considerations must be kept in mind while designing such embedded processors.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- This is important since each person involved in the working of an embedded system acts assuming that the other team members have done their job properly, e.g., a captain sails a ship accepting the originator/designer/maker have planned, created, responsibility and that the ship control works perfectly, etc.
- It is the ethical obligation of all team members to release their obligations with the most noteworthy honesty and meticulousness.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- Each individual included must adhere to the most elevated moral norms to forestall the odd practices inside his/her obligation:
 1. **Communicating Information Responsibly:** When there are many team members, there is a collective obligation that requires the architects/engineers/makers, clients, and software writers to interface capably, particularly without ambiguity, to guarantee the safe operations of the embedded processors. Protocols with respect to communication must be created for this reason, and correspondence must be kept up in any event until the activity of the processors is steady.
 2. **Attributing Responsibility to Software:** Embedded systems must be accompanied by suitable (self) regulatory mechanisms that will guarantee their moral conduct.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

- **Definition 3.5: Control Systems**

- ☐ A control system is made of a set of mechanical or electronic devices that controls other devices or systems using control loops.
 - ☐ It consists of many elements that may be combined together to form a system for producing desired outputs.
- Control systems are an integral part of the automation industry.
 - Different control loops that regulate these processes may be in the form of industrial control systems (ICS).
 - Supervisory control and data acquisition (SCADA) and distributed control systems (DCS) are some examples of control systems.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

- The advancement of Control systems has significantly increased the cyber-attack surfaces.
- The challenges may be in forms like increasing cyber threats, lack of visibility and control, difficulty in securing control layer protocols and unsecured networks.
- Therefore, addressing the issues from an ethical point of view is mandatory:

1. Machine Design Ethics:

- Machine ethics are to be considered from the earliest starting point of the research work and the meaning of the necessities, past classical safety studies.
- For each stage of the machine design process, it is advised to realize a risk assessment and to implement redundant technological barriers to contain possible machine ethical risks.
- It is important to consider how the designed control system could be misused by error or rendered harmful (hijacked) using cyber-attack technologies, for example.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

- 2. Human-Centered Approach:** Researchers must design the control system using a human-centered approach rather than a techno-centered one. This will guarantee utilizing the possible capacity of people when confronting the unexpected while at the same time confining automatic and deliberate abuses of the control system.
- 3. Design Process:** It is encouraged to define a ventured design process, containing distinctive approval stages. Although it is a classical design way, adding exaggerated tests at each of the steps could be yet another approach. This approach would be beneficial for testing the robustness of the designed elements facing exaggerated risks, before the final targeted implementation of the control systems.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

4. **Safety, Responsibility, and Liability:**

- Safety aspects should be one of the primary concerns such that control systems and humans can work together without accidents.
- Since control systems increasingly operate in close proximity to humans, safety is very important. Control systems are not only large and complex, but also intelligent and self-learning.
- But it is equivalently important to understand that these systems may fail, and neither the systems nor humans can be blamed for it.
- Besides, it is much harder to locate the underlying reason and attribute liability.
- It is equally hard to find who is accountable for the failures and malfunctions. Therefore, these questions need to be addressed from an ethical point of view.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

5. Privacy Concerns:

- Control Systems require immense measures of information to work successfully, and this poses several privacy questions.
- For instance, in order to build smart home security systems, smart home systems need to keep track of the times when residents are away. This information may be private, but valuable for burglars. Robots spying on the working habits of their human co-workers may be yet another privacy concern since they may manipulate humans to work harder.
- The ethics behind reviewing medical professional secrecy concerning the health data stored on connected parts of medico-technical systems also raises many privacy concerns and questions.
- Thus, collecting data on an individual's lifestyle and physical parameters may contribute towards improving their health, but it is not ethical to take advantage of the data shared on medico-technical systems.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

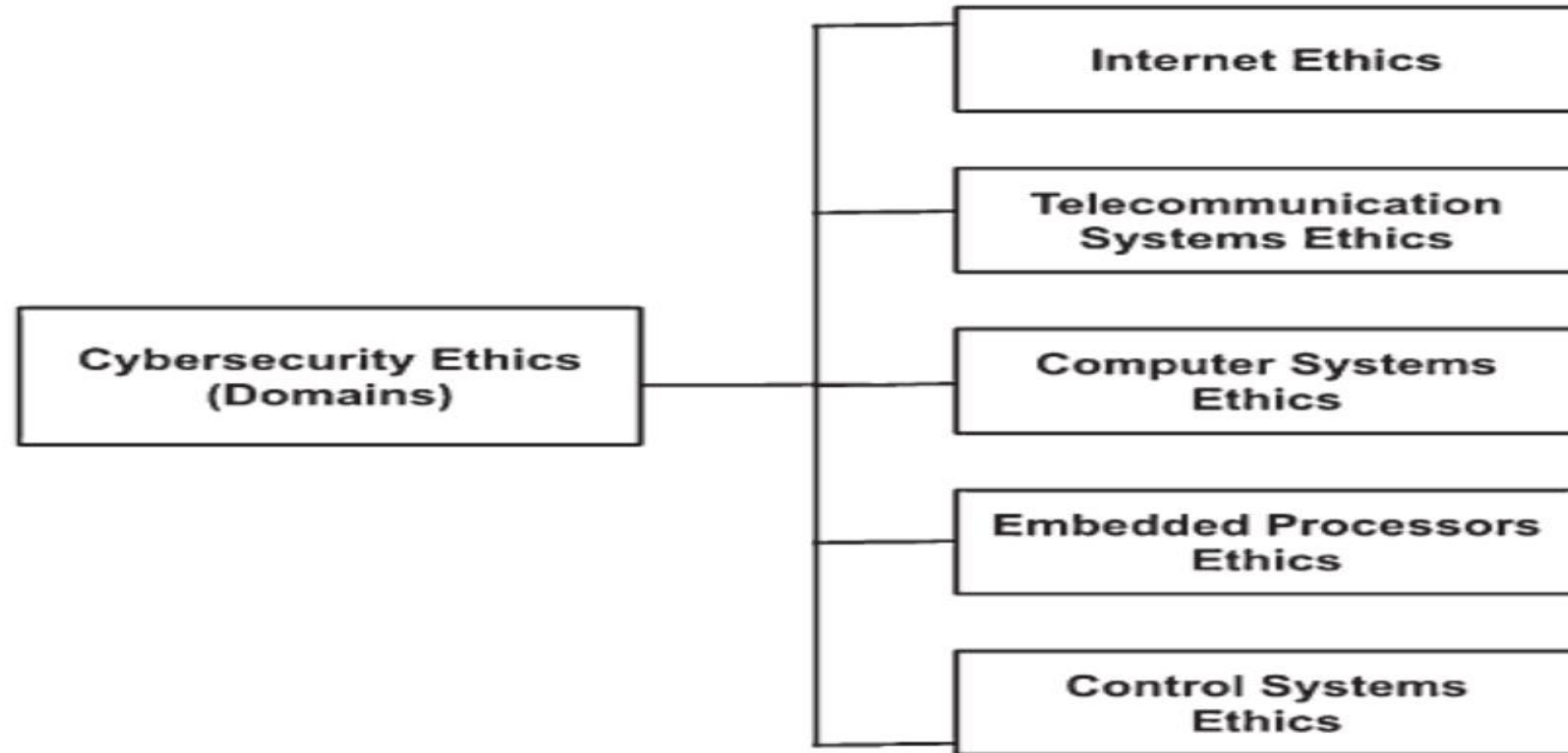


FIGURE 3.1 Cybersecurity ethics (domains).

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

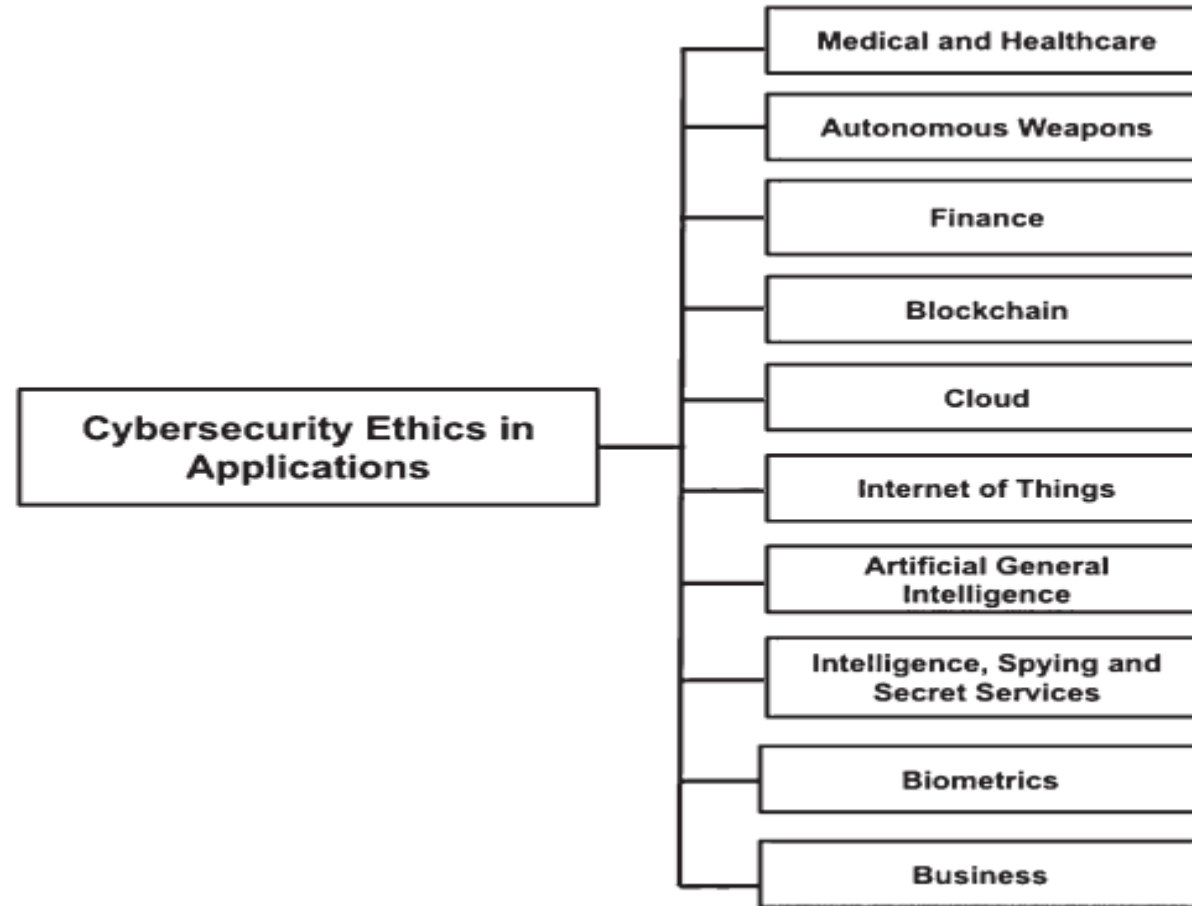


FIGURE 3.2 Cybersecurity ethics in applications.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

- Healthcare cybersecurity is a challenging issue in the healthcare industry.
- **Electronic Health Records (EHRs)**, include a plethora of sensitive information about patients' health and medical histories.
- Due to this, the hospital network security is a potential target for hackers.
- Through EHRs, it is very easy to share essential information among physicians and other healthcare professionals, and insurance companies.
- A cybercriminal's dream is to easily obtain files that contain an individual's social security number, address, email address, credit card data, and even medical history.
- Healthcare organizations are vulnerable to cyberattacks, mainly because their security is often much more relaxed than other organizations.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

- The healthcare industry is vulnerable to cyber-attacks due to the following reasons:
 1. High Prize
 2. Ransomware
 3. Major Vulnerabilities-Employees and Encryption
 4. Counteracting Attack Attempts



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

- The healthcare industry is vulnerable to cyber-attacks due to the following reasons:
 1. **High Prize:** Healthcare records fetch for a high price since they incorporate sensitive details like credit card data, email addresses, social security numbers, medical history records, and employment information. Cybercriminals use the data to launch spear-phishing attacks, commit fraud and steal medical identities.
 2. **Ransomware:** Cybercriminals rely on ransomware to make even more money off of the healthcare organization itself. Hackers mostly demand the money to be paid in bitcoin currency, and some have even demanded a ransom as they vandalize the systems and gain control of entire hospital computer systems.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

- The healthcare industry is vulnerable to cyber-attacks due to the following reasons:

3. Major Vulnerabilities-Employees and Encryption:

One of the greatest cyber threats to a healthcare organization is its own employees. Over half of the data breaches came from people within the organization. Another major threat is the lack of encryption as the healthcare sector has one of the lowest overall rates of data encryption.

4. Counteracting Attack Attempts: Due to the rapid changeover to EHRs, and the fact that healthcare organizations increasingly face sophisticated digital changes, the need for cybersecurity protocol grows more each day. Patients with compromised records usually have no choices in these circumstances. Numerous medicinal services associations have wound up paying the government fines, and settling in civil suits. Smaller organizations lacking experts and staff to prevent these attacks are extremely vulnerable. Therefore, it is important to train all staff members on proper information technology (IT) protocols. If a user can identify a phishing attack, attacks can be avoided.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

- Since the data in the medical industry is very sensitive, it is mandatory that information is protected using a combination of ethical as well as a best practices approach.

3.2.1.1 CASE 1: IDENTIFYING COMMON HEALTHCARE SECURITY THREATS

When looking at potential threats, one must consider:

1. **Staff or Insider Threats:** Healthcare employees have easy access to patient files and medical records.
2. **Malware and Phishing Attempts**
3. **Vendors:** One of the common mistakes that healthcare providers do is work with vendors without estimating the accompanying risk. Let us take an example of a hospital that hires a cleaning company. The employees may gain access to computers.
4. **Unsecured Mobile Devices:** Many healthcare facilities that allow mobile logins do not require the devices to meet security standards.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

3.2.1.1 CASE 1: IDENTIFYING COMMON HEALTHCARE SECURITY THREATS

When looking at potential threats, one must consider:

5. **Lost and Stolen Mobile Devices**
6. **Online Medical Devices**
7. **Unrestricted Access to Computers**
8. **Inadequate Disposal of Old Hardware**

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

3.2.1.2 CASE 2: ADDRESSING DATA SECURITY ISSUES IN HEALTHCARE

A few critical ways an organization and its employees can prevent cyber threats include:

1. **Educating Employees:** It is necessary to make employees understand their role in cybersecurity and its influence on patients' lives. This creates an atmosphere that values and respects security. Regular briefing sessions and frequent communication on the state of the organization's security may ensure cyber safety of an organization. Further, staff training sessions and regular cybersecurity meetings could promote cybersecurity awareness among employees.
2. **Establishing Procedures**
3. **Require Software Updates**
4. **Set Strict Personal Device Regulations**

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

3.2.1.3 CASE 3: DEALING WITH SECURITY BREACH IN A HEALTHCARE ORGANIZATION

In case of a patient information being violated the following steps may be considered:

1. **Reporting the Breach**
2. **Sharing the Information**
3. **Reexamining the Network**

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

3.2.1.4 CASE 4: MINIMIZING SECURITY THREATS IN A HEALTHCARE ORGANIZATION

- To limit security dangers in a healthcare association it is pivotal for information to be encoded with the goal that outsiders cannot get to data during transmission or when information is stored:
 1. **Understanding the Network Map:** Using innovation that gives a review of the gadgets and capacity on the system is critical.
 2. **Updating the Software:** It is equally important to ensure that all software and operating systems information are up to date.
 3. **Virtual Private Network (VPN) Encryption**

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

3.2.1.4 CASE 4: MINIMIZING SECURITY THREATS IN A HEALTHCARE ORGANIZATION

4. Conducting Regular Audits
5. Setting Strict Access
6. Thinking Like a Hacker
7. Using Professional Services

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

3.2.1.5 CASE 5: IMPROVING DATA SECURITY IN HEALTHCARE ORGANIZATIONS

For considering data security, the following may be considered:

1. **Considering All Phases:** Although cybercrimes are a significant threat, records theft may happen at any stage in the recordkeeping process. Therefore, it is crucial to develop technical, administrative, and physical safeguards, so as to ensure protection against
2. **Using the Crosswalk:** It is intriguing to take note of that the health insurance portability and accountability act (HIPAA) cyber-security crosswalk, connects each HIPAA security rule to a related NIST cybersecurity classification.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.1 CYBERSECURITY ETHICS IN MEDICAL AND HEALTHCARE INDUSTRY

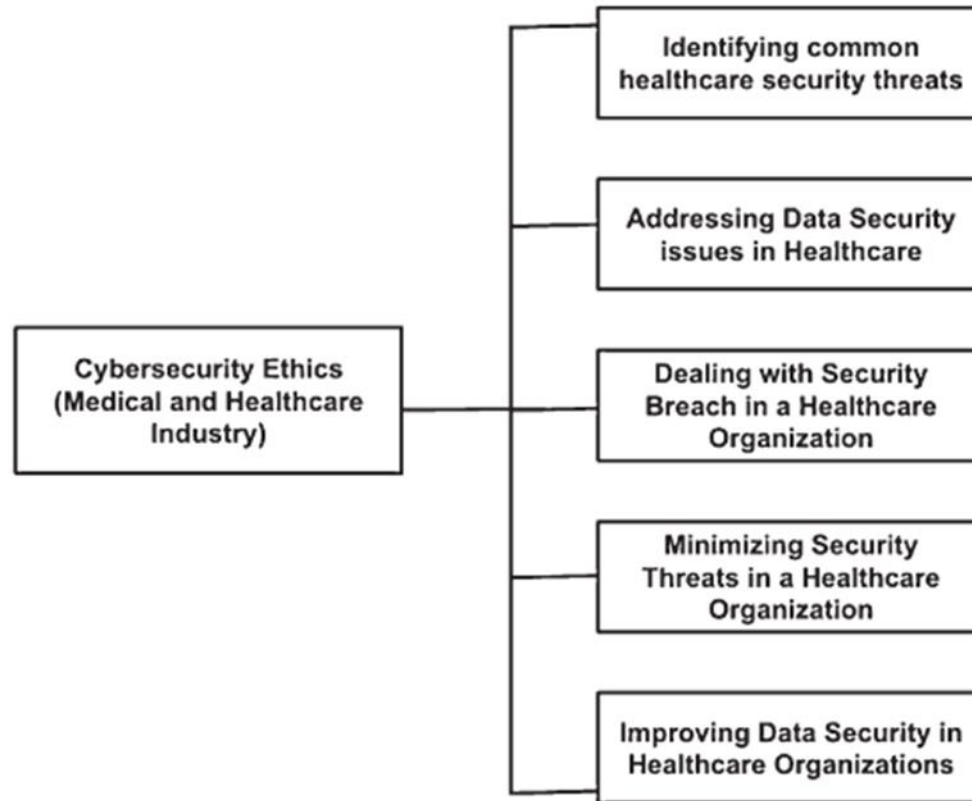


FIGURE 3.3 Cybersecurity ethics in medical and healthcare industry.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.2 CYBERSECURITY ETHICS IN AUTONOMOUS WEAPONS

- **Definition of Autonomous Weapon Systems:**

Autonomous weapons systems (AWS) are characterized by the U.S. Department of Defense (DoD) as a weapon system that, when actuated, is equipped for choosing and engaging targets without any more intercession by a human administrator.

- The rise of cybersecurity could see cyber warfare. Cyber Warfare alludes to the utilization of computer technology and innovation for disrupting the operations of a state or association. This is done by the intentionally assaulting information systems for key or military purposes. Cyberwarfare incorporates techniques, tactics, and procedures which may be involved in a cyberwar. Autonomous weapons could play a major role in cyber warfare.
- The AWS proposes the chance of dispensing with the human administrator from the war zone which raises **several ethical questions**.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.2 CYBERSECURITY ETHICS IN AUTONOMOUS WEAPONS

- The questions refer to moral decision-making by human beings involving an intuitive, non-algorithmic capacity that may not be captured by even the most sophisticated of computers.
- Some of the questions are as follows :
 - Is the intuitive moral perceptiveness on the part of human beings ethically desirable?
 - Is the automaticity of a series of actions capable of making individual actions in the series easier to justify, as arguably is the case with the execution of threats in a mutually assured destruction scenario?
 - Should the legitimate exercise of deadly force should always require meaningful human control?
 - What could be the nature and degree of a human oversight over an AWS?



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.2 CYBERSECURITY ETHICS IN AUTONOMOUS WEAPONS

- The questions refer to moral decision-making by human beings involving an intuitive, non-algorithmic capacity that may not be captured by even the most sophisticated of computers.
- Some of the questions are as follows :
 - Should the definition center around the system's capacities for self-governing target selection and engagement, or on the human administrator's utilization of such abilities?
 - Should the human administrator's pre-commitment expectation have a conclusive bearing on the system's definition as an AWS?
 - What are the suggestions for legal liability?
 - Who should bear the legitimate risk for choices AWS makes?



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.2 CYBERSECURITY ETHICS IN AUTONOMOUS WEAPONS

- Therefore, five principles for ethical use of autonomous weapons are as follows:
- **Responsibility:** There is a need for human beings to exercise appropriate levels of judgment and be responsible for developing, deploying, and using AI.
- **Equitability:** The military must take action to avoid unintended bias that may inadvertently cause harm.
- **Traceability**
- **Reliability:** Reliable behavior of AI is critical. The military does not need an AI application that behaves abnormally. Rather, they require reliable techniques and tools that perform as they are expected to. Therefore, these systems must be tested thoroughly to understand its effects and side effects before using it to carry out any operations.
- **Governability:** This standard tends to the biggest fear of automation of war and weaponry. A few scientists accept that the systems may become sophisticated and become unmanageable.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.2 CYBERSECURITY ETHICS IN AUTONOMOUS WEAPONS

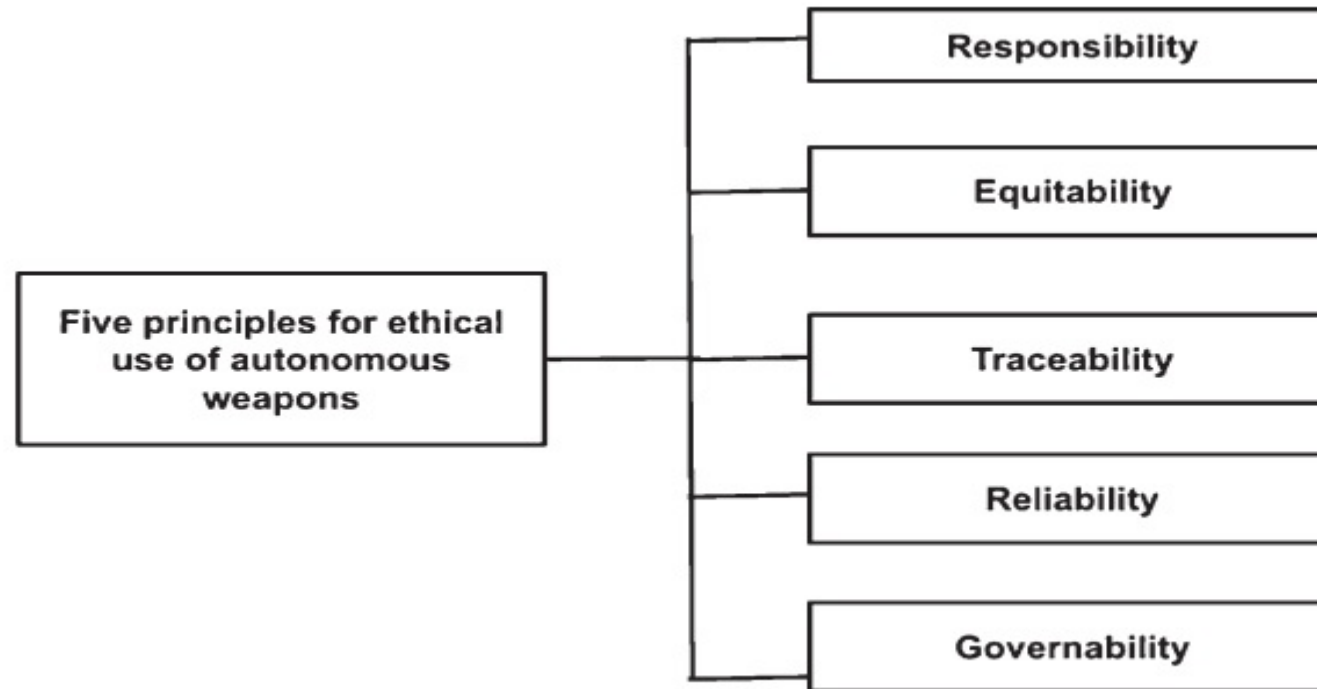


FIGURE 3.4 Five principles for ethical use of autonomous weapons.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.3 CYBERSECURITY ETHICS IN FINANCE

- Financial institutions incorporate wealth management firms, investment brokers, and credit unions. These are very attractive to cyber-attackers as they host a variety of sensitive data like bank account numbers, social security numbers, etc.
- Attacking financial institutions may lead to loss of sensitive data, which may in turn have a devastating effect on the institution's reputation.
- Therefore, significant amounts of time and money to repair may be required. While banks have strict regulations and guidelines regarding security, not all these institutions fall under the same rules and regulations.
- **Most security breaches** are due to human errors. If one of the employees clicks on a malicious link in an email or allows an attacker to change the client's address without proper verification, it may lead to system compromise.
- Therefore, all organizations must promote cyber-security awareness and make security best practices mandatory for their employees.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.3 CYBERSECURITY ETHICS IN FINANCE

- Banks and financial institutions can ensure cybersecurity by combining best practices as well as cyberethics.
- Several key security questions arise for a financial firm, which may not be handled completely in a technical manner. There are some moral contemplations that must be considered for such questions.
- Financial institutions must consider some key security questions for securing their organization:
 - Is there an integrated information security strategy that underpins IT risk management?
 - Is the association elevating careful risk evaluations to secure client data?
 - Are representatives being kept updated on the strategy changes, new data security risks, and best practices?
 - Is the association teaching its customers about data security risks and best practices?
 - Is the organization effectively managing and monitoring system configurations?
 - How is the organization staying abreast of the latest threat and vulnerability information?



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.3 CYBERSECURITY ETHICS IN FINANCE

- The following questions can be answered using various techniques described as follows:

1. Establishing a Formal Security and Ethical Framework: Currently, several core security frameworks assist financial institutions in managing cyber risk more effectively. These include:

- I. The NIST cybersecurity framework (CSF) incorporates best practices in five significant domains of information security, i.e., identify, protect, detect, respond, and recover.
- II. The Federal Financial Institutions Examination Council (FFIEC) IT examination handbook presents a comprehensive list of security guidelines.

2. Arming the Employees with Knowledge

3. Performing Continuous Threat Monitoring

4. Assessing and Managing Vulnerabilities

5. Creating a Strong Cybersecurity Culture, Starting at the Top

6. Devising Comprehensive Incident Response (IR) Plans

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.4 CYBERSECURITY ETHICS IN BLOCKCHAIN

- **Blockchains** are digital records of transactions. It gets its name from the structure, in which individual records, also called blocks, are linked together to form a single list, which is called a chain.
- Blockchains can be used for recording cryptocurrency-based transactions, like Bitcoin.
- Transactions that are added to the Blockchain must be validated through multiple computers on the Internet.
- These systems are configured to monitor specific types of blockchain transactions and form a peer-to-peer network. Before adding a transaction to a block, it must be ensured that the systems work together to validate the transaction.
- This makes blockchain technology inherently secure. Since data is distributed, blockchain technology removes any single point of failure.
- Blockchain technology is also based on cryptographic proofs and game theory consensus mechanisms, which is why it is impossible to hack.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.4 CYBERSECURITY ETHICS IN BLOCKCHAIN

- Although blockchain technology boasts of several safety features, it does not mean that security issues are non-existent.
- Although Blockchains are robust, they are not immune to security issues.
- Some of the security issues related to blockchain technology are as follows:

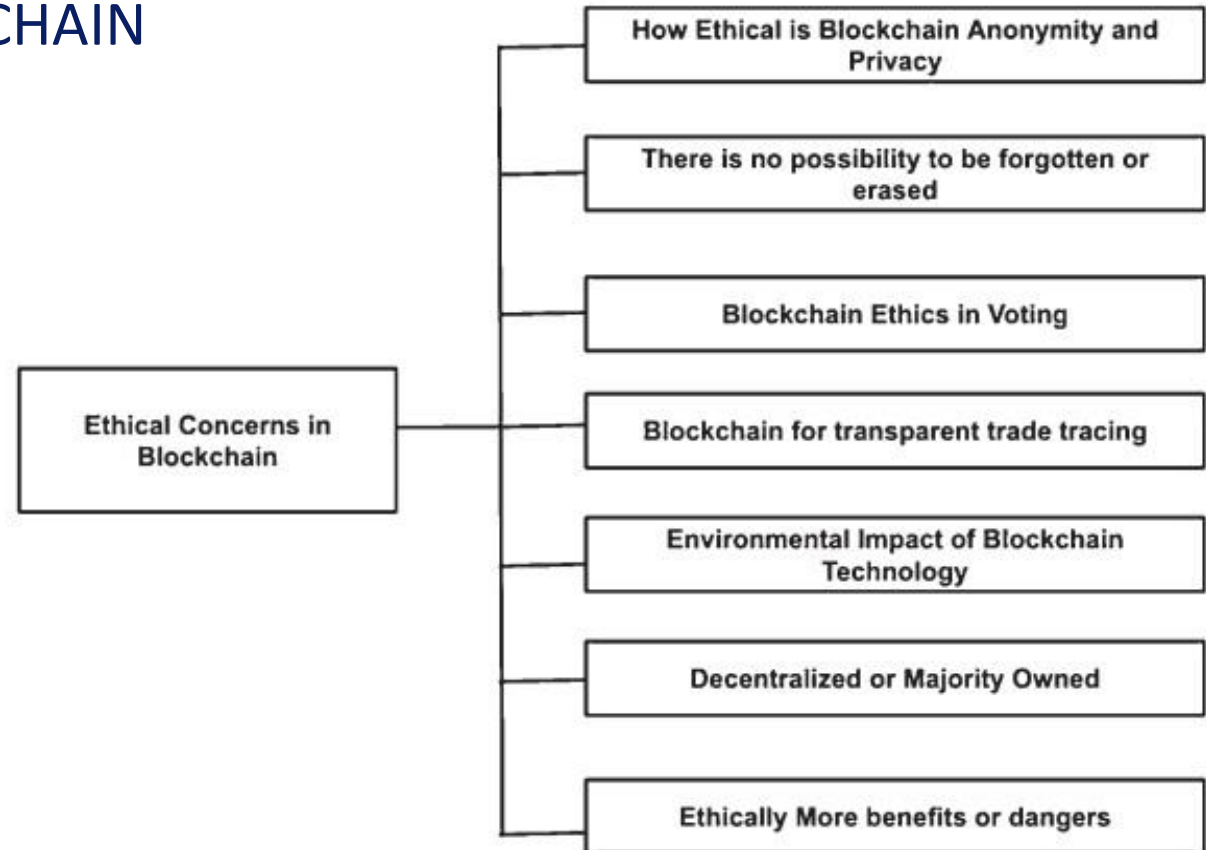


FIGURE 3.6 Ethical concerns in Blockchain.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.5 CYBERSECURITY ETHICS IN CLOUD

- **Cloud computing** the delivery of computing services which include storage, software, servers, analytics, networking databases, and intelligence over the Internet.
- It offers quicker advancement, adaptable assets, and economies of scale.
- The domain of cloud computing is expanding rapidly and used by a great many individuals and organizations.
- The **features of cloud computing** are resource/storage virtualization, scalability, and elasticity, efficiency of resource sharing, usage optimization/optimized by usage, ease of usage, fast information sharing, delivery, and control, accessibility, and anonymity.
- An ethical analysis start with the moving of control from technology users to the third parties servicing the cloud due to re-appropriating and offshoring of information and communication technology (ICT) usefulness to the cloud.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.5 CYBERSECURITY ETHICS IN CLOUD

- Since there are different levels of functionality for different providers, it is connected to provide a specific service to an end-user.
- Some ethical issues in cloud computing are as follows:

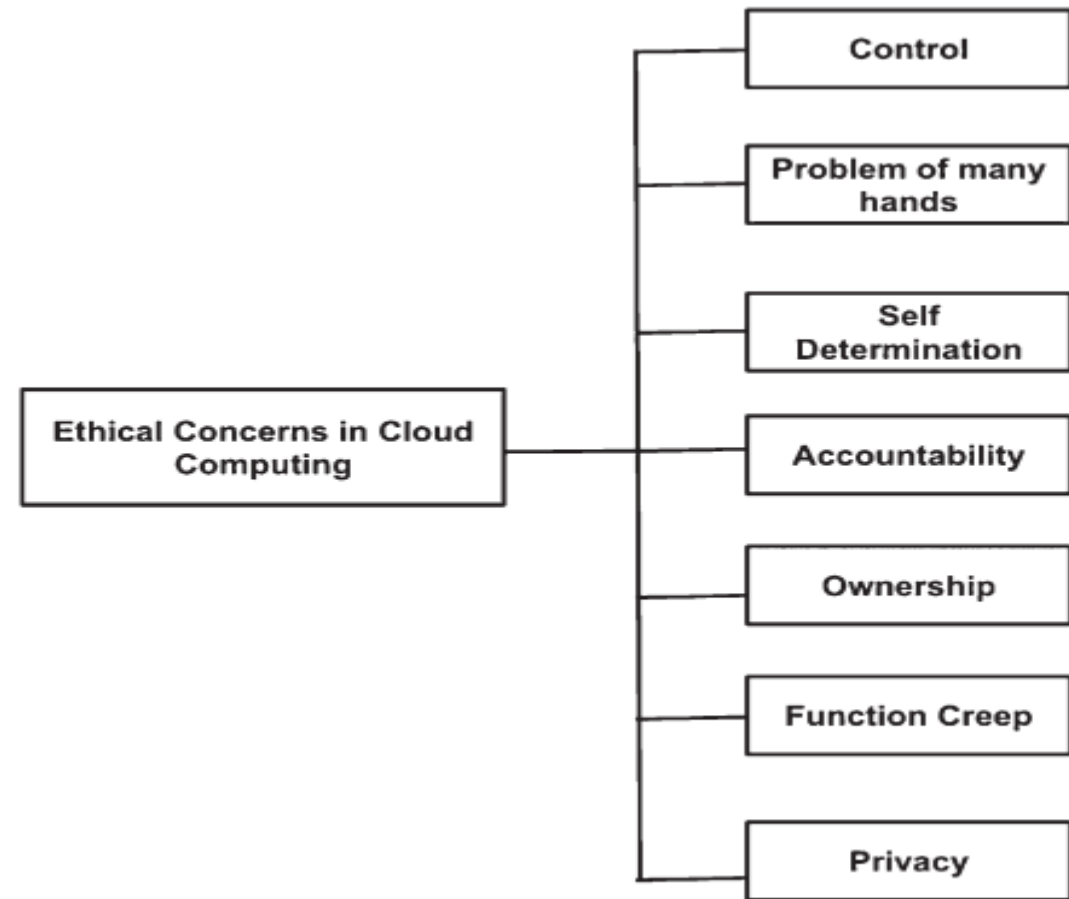


FIGURE 3.7 Ethical concerns in cloud computing.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.6 CYBERSECURITY ETHICS IN INTERNET OF THINGS (IOT)

- The **Internet of things (IoT)** the ever-growing network of physical objects over the Internet, identified by an internet protocol (IP) address.
- IoT guarantees web network, and the correspondence that happens between these items and other Internet-empowered devices and frameworks.
- Over the network, the physical devices connect to other physical devices, using wireless communication and offering contextual service.
- The combination of these technologies raises a number of ethical questions.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.6 CYBERSECURITY ETHICS IN INTERNET OF THINGS (IOT)

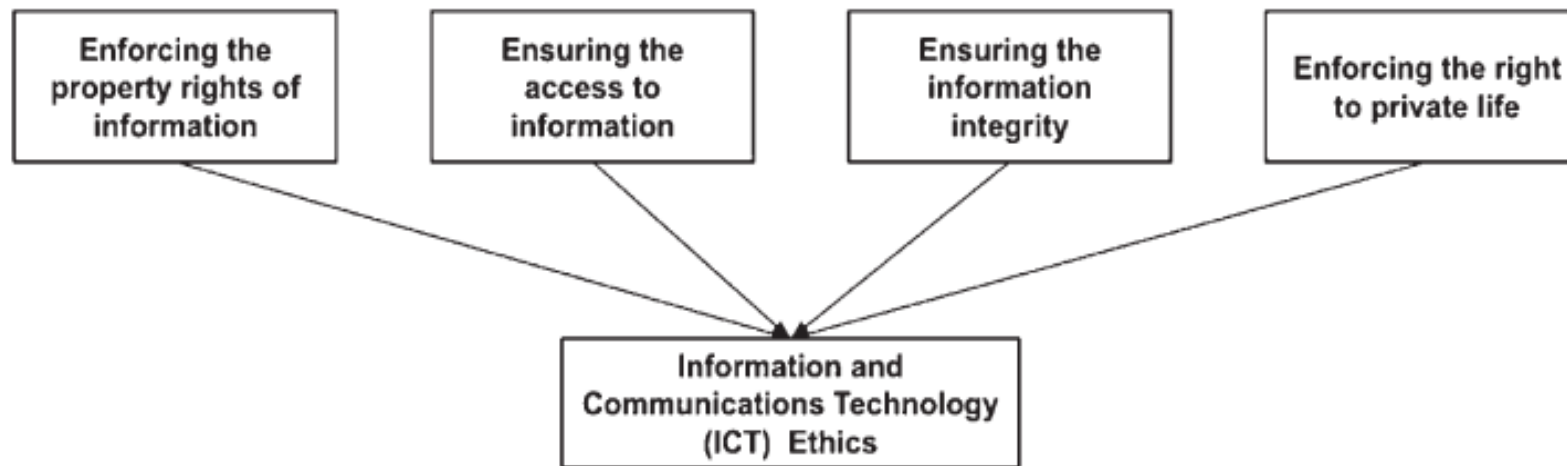


FIGURE 3.8 Information and communication technology (ICT) ethics.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

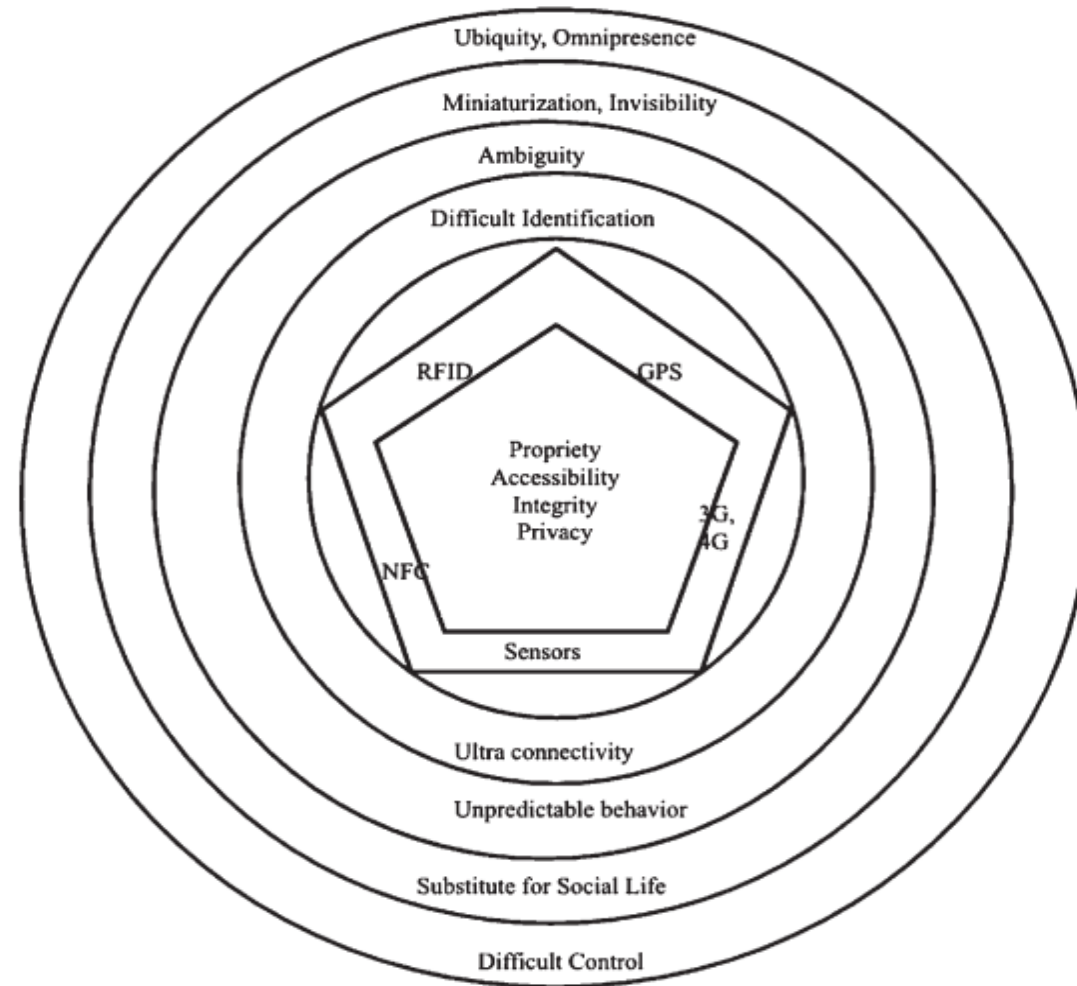


FIGURE 3.9 Ethics for Internet of things.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.9 CYBERSECURITY ETHICS IN BIOMETRICS

- Over the last few decades, continuous development of computer technology has led to reduction of prices and the improvement of performance, and increase in practical and social applications like biometrics technology.
- The field of biometrics innovation is fundamentally utilized in the fields of exchange installment, visa, border access control, and access control.
- Be that as it may, technological advancements require a ceaseless examinations on the moral issues that may emerge, and biometrics is no special case.
- Therefore, it is necessary to consider the ethical issues that may crop up from the use cases and applications of biometrics.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.9 CYBERSECURITY ETHICS IN BIOMETRICS

- There is a need to explore ways to deal with these ethical issues:

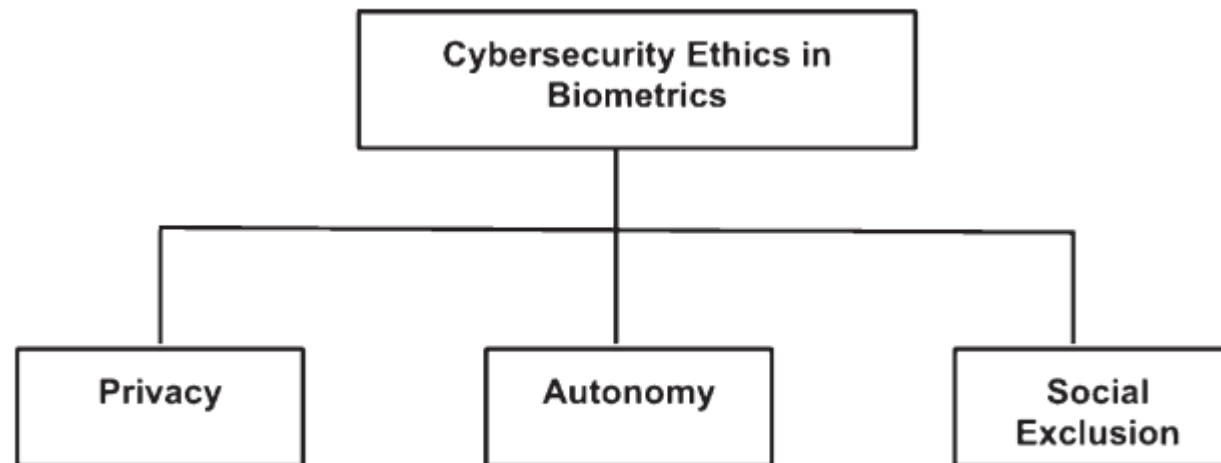


FIGURE 3.12 Cybersecurity ethics (challenges) in biometrics.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.10 CYBERSECURITY ISSUES IN BUSINESS

- Business world has been impacted majorly over the last few decades by globalization and digitization.
- This has not only altered the ethical issues but also their gravity, as evidenced by the widening of problems and complaints.
- As business management is becoming more complex, a multitude of ethical issues appears simultaneously. Therefore, an in-depth understanding of ethical problems is required.
- Although the business world is largely dominated by technological advancement, all recent developments in business management, call for considering ethical issues. Addressing these issues may lead to strengthened business perspectives.
- There are issues related to cyberethics that have profoundly strengthened after the development and popularization of social media.



3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.10 CYBERSECURITY ISSUES IN BUSINESS

- Managers and management personnel are always under ethical pressure and stress from different stakeholders like owners, government entities, employees, customers, suppliers, competitors, and other managers.
- The trust, integrity, and honesty of management and companies are under permanent stress. There are several levels on which business managers may face ethical issues.
- Some of the levels are personnel, organizations, trade, society, and the globe.
- Ethical issues may also arise with managers, customers, suppliers, employees, companies, and government entities.
- Therefore, it is possible that many layers of ethical issues can crop up, however, **ethics in the business world is based on integrity and trust.**
- If integrity and honesty of a management/ company become doubtful or its trust is shaken, the ethical issues are strengthened and need attention.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.10 CYBERSECURITY ISSUES IN BUSINESS

- Ethical issues may also arise due to conflicts of interests, poor management of employees and people, diversity, and cross-culture composition of working teams, ineffective communication, ethical conduct on social media, workplace safety issues and ignoring legal liabilities.
- Hence, the moral issues in the business world and current administration are rising as a huge problem.
- **Business ethical issues** and their **practices** in different organizations have gained very high importance currently because these are now readily exposed on social media.
- Not agreeing with business ethics may affect the businesses negatively, and may also lead to losing reputation, popularity of companies, and losing in revenue.

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

3.2.10 CYBERSECURITY ISSUES IN BUSINESS

- Some of the cybersecurity ethical issues faced by the businesses are as follows:

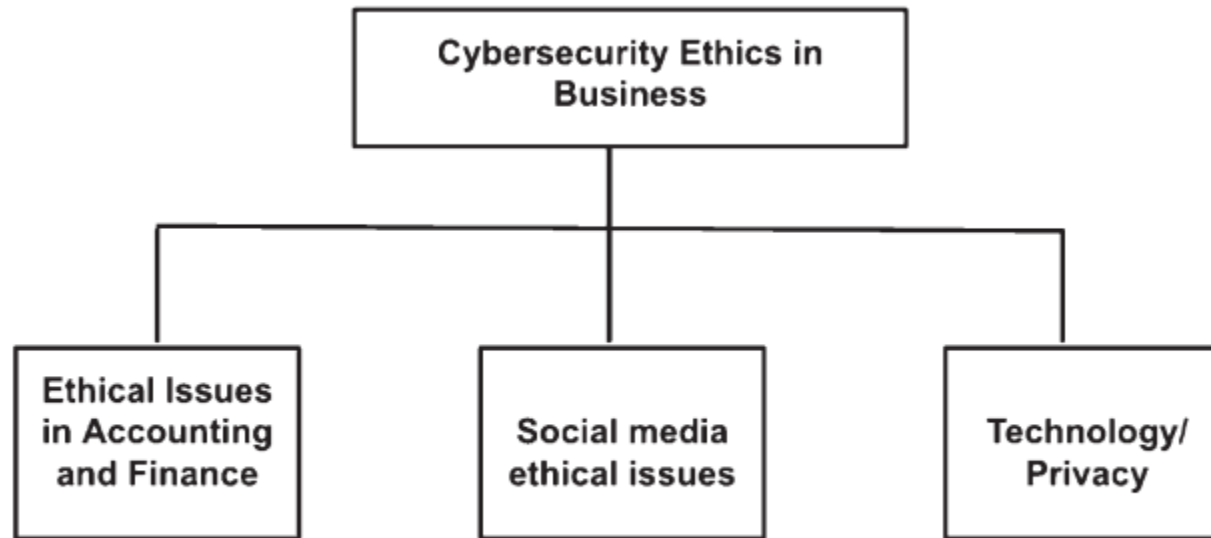


FIGURE 3.13 Cybersecurity ethics in business.

THANK YOU

