INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

# Learning Framework for Design and Development of Cyber-Attack Detection and Cyber Security

**Priyanka Vaibhav Kulkarni**

**Department of Electronics, Dr. D. Y. Patil, Arts, Commerce & Science College, Pimpri, Pune, Maharashtra, India**

**DOI: https://doi.org/10.51583/IJLTEMAS.2025.1413SP027**

**Received: 26 June 2025; Accepted: 30 June 2025; Published: 24 October 2025**

**Abstract:** Cyber security means protecting information, devices, computers, computer resource, communication devices and information stored there in from unauthorized access, use, modification or destruction. Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Cyber security is a way of protecting the computers, network, and other devices from cyber criminals. Cybersecurity is the practice of protecting people, systems and data from cyber-attacks by using various technologies, processes and policies. At the enterprise level, cyber security is key to overall risk management strategy. Cybercrime is a crime which includes computer and network to execute a crime. For example, unauthorized access or modify data or application, intellectual property theft, writing or spreading computer viruses etc. Whenever we think about the cyber security the first thing that comes to our mind is cyber-crimes which are increasing immensely day by day. Cybercrime may put a person or a nation security in danger and it is not good for financial health. Cybercrime, especially through the internet, has grown because computers are used in every field like commerce, entertainment and government. This paper Approaches to prevent, detect, and respond to cyber attacks are also discussed. In the current world that is run by technology and network connections, it is crucial to know what cyber security is and to be able to use it effectively. This thesis aims to develop a cybersecurity threat detection or attack detection system.

**Keywords**: Cyber security, Cyber risk, cybercrime, Open data, Systematic review, computerized security,

## I. Introduction

Cyber security is a way of protecting the computers, network, and other devices from cybercriminals. Cyber security is concern with both physical security of the devices and information stored therein. (Taha, A.F,2018) cybercrime is committed by cybercriminals or hackers who want to make money.it is carried out by individuals or organizations. Some cybercriminals use advanced techniques and are highly technically skilled. Others are novice hackers. Cybercriminals prefer cybercafés to carry out their activities. In the past several years, many instances have been reported in India, where cybercafés are known to be used for terrorist communication. Cyber security protects IT systems from malicious attacks, allowing businesses to maintain their services and keep sensitive data safe. Without an effective cyber security strategy, organizations become easy targets for cybercriminals looking to infiltrate their systems, manipulating them for their own gain. Globalization, digitalization and smart technologies have escalated the propensity and severity of cybercrime. (Sudhakar, Jawaharlal Nehru University, 2022) Whilst it is an emerging field of research and industry, the importance of robust cyber security defense systems has been highlighted at the corporate, national and supranational levels. In addition, further information on datasets is attached to provide deeper insights and support stakeholders engaged in cyber risk control and cyber security. (Albalawi et al., 2022) Finally, this research paper highlights the need for open access to cyber-specific data, without price or permission barriers. Cyber security is essential in contemporary's networked planet to protect our mathematical methods, networks, and dossiers from unauthorized approach, criminal activity, and potential instabilities (IJARSCT, January 2024). For a society to efficiently put an end to or recover from cyber-attacks, all of the arrangements, society, and tools must agree. The tasks of finding, inspection, and remediation are three important freedom processes that can be increased by a united threat administration whole. The review of the main ideas and significance of cybersecurity in this introduction.

### Definition

Cybersecurity involves employing technologies, processes, and practices to safeguard information and ensure the confidentiality, integrity, and availability of digital assets. Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks, damage, or unauthorized access. Cybersecurity is the practice of protecting people, systems and data from cyber-attacks by using various technologies, processes and policies.

### Importance of Cybersecurity

Cybersecurity is the process of hampering unauthorized approach, misuse, and damage to computer arrangements, networks, dossier, and information. It involves a broad range of plans, forms, and procedures engaged to defend the confidentiality, approachability, and dependability of mathematical assets. Cybersecurity requires preventing, spotting, and fighting many connected to the internet dangers aforementioned hack attempts, malware contaminations, data breaches, and different cybercrimes.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

**Cyber Attacks**

A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach a computer system, network, or digital device with the intent to steal, expose, alter, disable, or destroy data, applications, or other assets. Cyber-attacks can be carried out by individuals, groups, or even nation-states, and they can target a wide range of victims, from individuals to large organizations. Cyber-attack (or cyber-attack) occurs when there is an unauthorized action against computer infrastructure that compromises the confidentiality, integrity, or availability of its content. Perpetrators of a cyber-attack can be criminals, hacktivists or states. They attempt to find weaknesses in a system, exploit them and create malware to carry out their goals, and deliver it to the targeted system. Once installed, the malware can have a variety of effects depending on its purpose. Detection of cyber-attacks is often absent or delayed, especially when the malware attempts to spy on the system while remaining undiscovered. A cyber-attack is any attempt by an individual or organization to use computers or digital systems to steal, alter, expose, disable, or destroy information, or to breach computer systems, networks, or infrastructures. Criminals use many methods and tools to locate the vulnerabilities of their victim. The victim can be an individual or an organization

**Criminals plan two types of attacks**

1. Passive attacks: passive attacks attempt to gain information about the target. It involves gaining data about a target without the knowledge of the target.
2. Active attacks: active attacks are usually used to alter the system. It may affect the integrity, authenticity and availability of data.

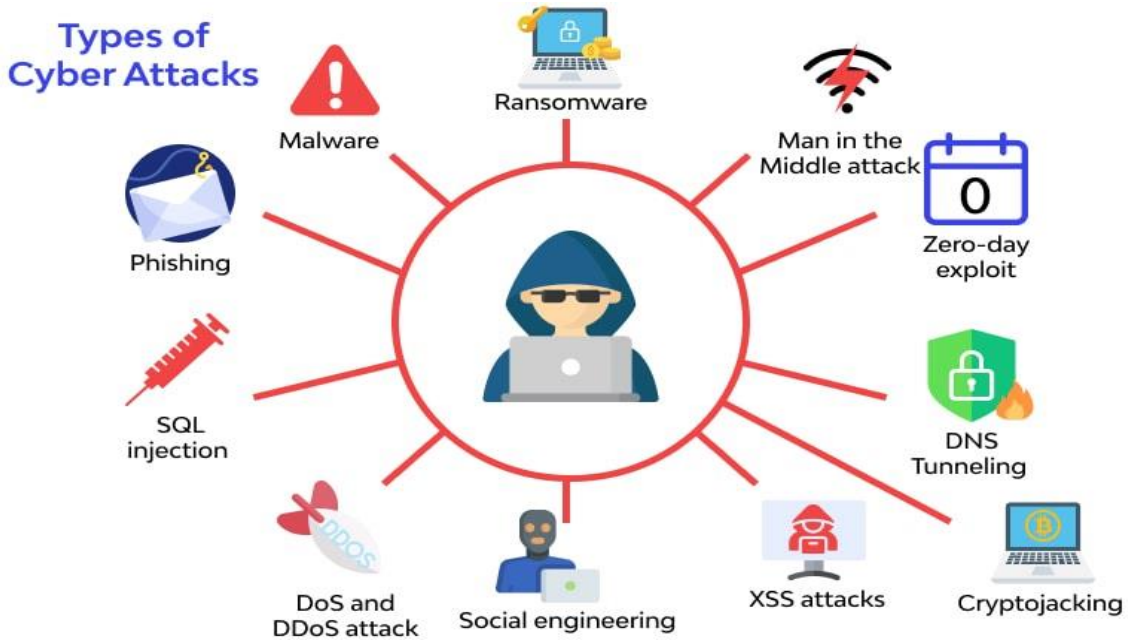


Fig.1: Types of Cyber Attacks

**Social Engineering**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

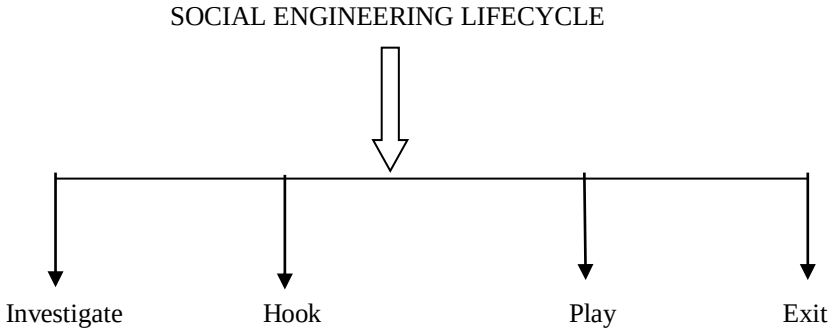


Fig.2: Lifecycle for Social Engineering

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

**Classification of social engineering**

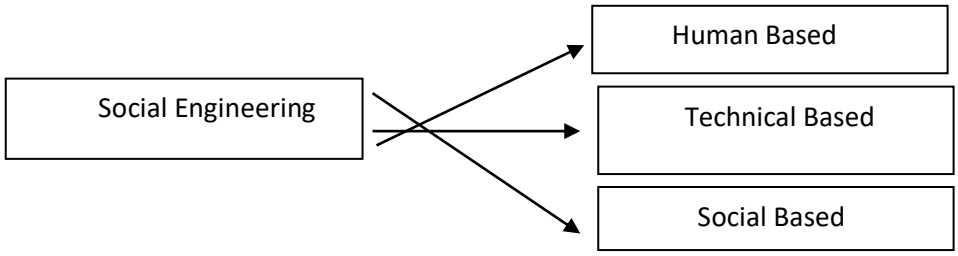


Fig.3: Classification of Social Engineering

**Following are some key types of social engineering attacks**

**Phishing:** This involves deceptive emails, messages, or websites designed to trick individuals into revealing personal information like passwords, credit card details, or other sensitive data. Variations include spear phishing (targeting specific individuals or organizations) and whaling (targeting high-level executives).

**Baiting:** Attackers lure victims with tempting offers or promises, such as free software or music, often containing malware. This could also involve leaving infected USB drives in public places.

**Tailgating (Piggybacking):** This involves gaining unauthorized access to a secure area by following someone who has legitimate access.

**Scare ware:** This technique uses fake alerts and warnings about viruses or other threats to scare victims into purchasing unnecessary or malicious software.

**Dumpster Diving:** Attackers search through discarded trash for sensitive documents or information that hasn't been properly disposed of.

**Quid Pro Quo:** Attackers offer a service or benefit in exchange for information, often posing as IT support to trick victims into revealing passwords or other data.

**Pretexting:** Attackers create a fabricated scenario or story to establish trust and manipulate victims into revealing information.

**Vishing (Voice Phishing):** A type of phishing attack that uses voice communication, often involving phone calls where attackers impersonate trusted individuals or organizations.

**Smishing (SMS Phishing):** A type of phishing attack that uses text messages to trick victims into revealing information or clicking malicious links.

**Reverse Social Engineering (RSE):** Attackers make themselves appear as a helpful resource to entice victims into seeking their assistance and then exploit that trust to obtain information.

**II. Block Diagram:**


Fig.4: Block Diagram of proposed system

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

**III. Block Diagram Description:**

A comprehensive learning framework for cyber-attack detection and cybersecurity should integrate multiple aspects, including threat modeling, risk assessment, security controls, and incident response. This framework should also incorporate machine learning and deep learning techniques for proactive threat detection and analysis. Furthermore, it should be adaptable to evolving threats and offer continuous improvement through feedback loops.

**Description of current security rules: -**

Current security rules encompass a wide range of practices and policies designed to protect information and systems. These rules are often based on the core principles of confidentiality, integrity, and availability (the CIA triad), and may also include authentication and non-repudiation. Key aspects include: establishing clear policies, implementing access controls, conducting regular security audits, and having incident response plans.

**Core Principles:**

**Confidentiality:**

Ensuring that sensitive information is only accessible to authorized individuals.

**Integrity:**

Maintaining the accuracy and completeness of data, preventing unauthorized modifications.

**Availability:**

Guaranteeing that authorized users have timely and reliable access to information and systems when needed.

**Description of required security guidelines: -**

Security guidelines outline the rules and procedures needed to protect information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. These guidelines encompass various aspects, including access control, data protection, incident response, and risk management.

**1. Confidentiality, Integrity, and Availability (CIA Triad):**

**2. Access Control:**

Defines who has access to what resources, based on roles and permissions.

Includes authentication (verifying identity) and authorization (granting access rights).

May involve multi-factor authentication, strong passwords, and regular access reviews.

**3. Data Protection:**

Covers data at rest (stored on devices) and in transit (moving across networks).

Includes encryption to protect sensitive information from unauthorized access.

Requires secure storage and disposal of data, following relevant regulations and policies.

**4. Incident Response:**

Outlines procedures for handling security incidents, such as data breaches or malware attacks.

Includes steps for detection, containment, eradication, recovery, and post-incident analysis.

Requires regular testing of incident response plans.

**5. Risk Management:**

Identifies potential threats and vulnerabilities to information and systems.

Assesses the likelihood and impact of these risks.

Implements security controls to mitigate identified risks.

**6. Security Policies:**

Formal documents that outline an organization's approach to information security.

May cover topics such as acceptable use, data handling, remote access, and physical security.

Should be regularly reviewed and updated to reflect changes in technology, threats, and regulations.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

**7. Compliance:**

Organizations must adhere to relevant laws, regulations, and industry standards.

Compliance may involve implementing specific security controls and reporting requirements.

**8. Security Awareness Training:**

Educates employees about security risks and best practices.

Helps employees understand their role in maintaining a secure environment.

May include training on topics such as phishing, malware, and social engineering.

**9. Network Security:**

Protecting the organization's network infrastructure from unauthorized access and attacks.

Includes firewalls, intrusion detection/prevention systems, and network segmentation.

Ensuring secure remote access to the network.

**10. Physical Security:**

Protecting physical assets, such as servers, workstations, and data centers.

Includes access controls, surveillance systems, and environmental controls.

**Make changes**

"Make changes" means to modify or alter something. It implies making something different from its current state, either through small adjustments or significant transformations.

**Evaluate the progress**

Evaluating progress involves assessing how well you or an entity is moving towards achieving predetermined goals or objectives. This process helps identify areas of success, areas needing improvement, and informs future strategies. It can be applied to personal goals, projects, or even broader programs.

**Risks**

**Risks** is an international, scholarly, peer-reviewed, open access journal for research and studies on insurance and financial risk management.

**IV. Conclusion:**

In conclusion, the proposed framework lays a solid foundation for building more secure digital infrastructures. It serves as a strategic blueprint for organizations aiming to strengthen their cyber security posture and effectively combat the ever-evolving landscape of cyber threats. Furthermore, the framework emphasizes a layered security strategy, addressing vulnerabilities across network, application, and user levels. The growing complexity and frequency of cyber threats necessitate the development of robust, adaptive, and intelligent frameworks for cyber-attack detection and cyber security. This framework, as presented, offers a comprehensive approach that integrates proactive threat identification, real-time monitoring, and dynamic response mechanisms. A comprehensive cyber security framework is crucial for effectively designing and developing systems that can detect and defend against cyber-attacks. a successful framework minimizes vulnerabilities, enables rapid response to incidents, and ensures the confidentiality, integrity, and availability of critical assets. A comprehensive learning framework for cyber-attack detection and security requires a multi-faceted approach that integrates robust defense strategies, advanced technologies, and proactive security practices.

**References**

1. Frank Cremer, Barry Sheehal, Stefan materne Article notes, "**Cyber risk and cybersecurity: a systematic review of data availability**".
2. ISSN (Online) 2581-9429 - International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal Volume 4, Issue 1, January 2024, "**Research Paper on Cyber Security Challenges and Threats".**
3. Taha, A. F. IEEE Trans. "**Risk mitigation for dynamic state estimation against cyber-attacks and unknown inputs"** Smart Grid 9(2), 886–899 (2018).
4. Albalawi, A.M.; Almaiah, M.A. J. Theor. "**Assessing and reviewing cyber-security threats, attacks, mitigation techniques in the IoT environment"**. Appl. Inf. Technol. 2022, 100, 2988–3011. [Google Scholar].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

5. Sridevi A, **"Development of Attack Resistant Cybersecurity Framework for Digital Health Systems",** Shodhganga: a reservoir of Indian theses @ INFLIBNET,2023.6. Sudhakar, Jawaharlal Nehru University, **"Cybersecurity threat detection using machine learning and deep learning**", Shodhganga: a reservoir of Indian theses @ INFLIBNET,2022.
6. **Das, Ishita,** "Outer Space and Cybersecurity Need for A New International Legal Framework"**- The National Academy of Legal Studies and Research (NALSAR) University of Law, Shodhganga: a reservoir of Indian theses @ INFLIBNET,2024.**
7. Suprabhath, Koduru Sriranga, Mahindra University**,** "Design and Development of Cyber Attack Detection and Mitigation Schemes for DC Microgrid Systems", Shodhganga: A reservoir of Indian theses @ INFLIBNET,2023.