ISBN: 978-93-7020-380-8

CYBERSECURITY AND ETHICAL ISSUES

Abstract

This chapter provides a concise overview of contemporary cybersecurity threats, defenses, and ethical considerations. It examines prevalent attack vectors such as phishing, SQL injection, and zero-day exploits, highlighting their impact on digital systems. Defensive strategies including penetration testing and RSA encryption are discussed as essential tools for mitigating cyber risks. Ethical issues, particularly GDPR compliance and the mitigation of AI bias, are addressed to emphasize the growing importance of responsible data stewardship and algorithmic fairness. The chapter features a case study of the 2017 Equifax breach to illustrate the far-reaching consequences of inadequate security practices and delayed incident response. By integrating technical strategies with ethical frameworks, this chapter aims to equip readers with a holistic understanding of both safeguarding digital assets and upholding societal trust in technology [1, 2].

Keywords: Phishing, SQL Injection, Zero-Day Exploits, Penetration Testing, GDPR

Authors

Nilanjan Chatterjee
Advanced Micro Devices
Austin, Texas, USA.
nilanjan.9325@gmail.com;

Monu Sharma
Valley Health, Winchester
Virginia, USA.
monufscm@gmail.com;

Navom Saxena
Senior Machine Learning Engineer
Meta, New York, USA.
navom.saxena@gmail.com;

Shubneet
Department of Computer Science
Chandigarh University, Gharuan
Mohali, 140413, Punjab, India.
jeetshubneet27@gmail.com;

Anushka Raj Yadav
Department of Computer Science
Chandigarh University, Gharuan,
Mohali, 140413, Punjab, India.
ay462744@gmail.com;

I. INTRODUCTION TO CYBERSECURITY AND ETHICS

Cybersecurity is the discipline dedicated to protecting computer systems, networks, and data from digital attacks, unauthorized access, and disruption. As digital trans- formation accelerates across all sectors, the importance of cybersecurity has grown exponentially. Today, organizations face a persistent and evolving threat landscape, with attackers leveraging sophisticated techniques to compromise sensitive information, disrupt services, or extort victims. According to Al-Garadi et al., the proliferation of cloud computing, IoT devices, and remote work has expanded the attack surface, making robust cybersecurity practices more critical than ever [3].

The core objectives of cybersecurity are often summarized as the CIA triad: **Confidentiality**, ensuring that information is accessible only to those authorized; **Integrity**, safeguarding the accuracy and completeness of information; and **Avail- ability**, guaranteeing reliable access to information and systems when needed. Achieving these objectives requires a combination of technical controls (such as fire- walls, encryption, and intrusion detection systems), organizational policies, and user awareness.

However, the practice of cybersecurity is not solely a technical endeavor—it is deeply intertwined with ethical considerations. As defenders deploy increasingly powerful tools to monitor, detect, and respond to threats, they must also consider the rights and interests of users, customers, and society at large. Several key ethical dilemmas arise in the field:

- **Privacy vs. Security:** Striking a balance between the need to monitor systems for threats and the obligation to respect individual privacy. For example, deep packet inspection and employee monitoring may enhance security but raise concerns about surveillance and consent.

- **AI Fairness:** The use of artificial intelligence in cybersecurity introduces the risk of algorithmic bias. Vallor and Mmaduekwe highlight that AI-driven threat detection systems, if trained on skewed datasets, may unfairly target certain groups or overlook novel attack patterns, leading to both ethical and operational failures [4].

- **Breach Disclosure:** When a security breach occurs, organizations must decide how quickly and transparently to inform affected parties. Delayed or incomplete disclosure can erode public trust and exacerbate harm, while rapid, honest communication supports accountability and remediation.

This chapter is structured to provide a comprehensive exploration of both the technical and ethical dimensions of cybersecurity. It begins by surveying major cyber threats, such as phishing, SQL injection, and zero-day exploits, which continue to challenge organizations globally. Next, it examines defensive strategies, including penetration testing and RSA encryption, that form the backbone of modern cyber defense. The chapter then addresses regulatory frameworks like the General Data Protection Regulation (GDPR), which sets strict standards for data privacy and breach notification in the European Union, as well as emerging guidelines for AI fairness and responsible data stewardship.

A dedicated section explores ethical frameworks and best practices, emphasizing the importance of transparency, accountability, and inclusivity in cybersecurity operations. The

2017 Equifax data breach is presented as a case study to illustrate the real-world consequences of inadequate security and ethical lapses, including financial losses, legal penalties, and reputational damage. Finally, the chapter discusses emerging trends, such as quantum computing threats and the rise of AI-powered attacks, underscoring the need for continuous adaptation and ethical vigilance.

By integrating technical knowledge with ethical reasoning, cybersecurity professionals can better protect digital assets while upholding societal trust and legal compliance. This holistic approach is essential for navigating the complex challenges of the digital age.

II. CYBER THREATS

Phishing: Techniques and Real-World Examples: Phishing attacks exploit human psychology to steal credentials or deploy malware.

Common techniques include:

- **Email Spoofing:** Forging sender addresses to mimic trusted entities (e.g., "CEO fraud" impersonating executives).
- **Smishing:** Phishing via SMS, often urging victims to click malicious links.

A 2024 OWASP report found that 94% of organizations faced phishing attempts, with CEO fraud causing $2.7B in losses annually [5]. For example, attackers impersonated Snapchat's CEO in 2016, tricking HR into disclosing payroll data.

SQL Injection: Exploitation and Impact: SQL injection (SQLi) exploits unsanitized inputs to manipulate databases. Attackers inject malicious payloads like' OR 1=1— to bypass authentication.

SELECT * FROM users WHERE username = 'admin' AND password = '' OR 1=1--';
This grants unauthorized access, enabling data theft, privilege escalation, and system compromise. In 2023, SQLi accounted for 33% of web app breaches, per OWASP [5].

Zero-Day Exploits and APTs: Zero-day exploits target undisclosed vulnerabilities, often in advanced persistent threat (APT) campaigns. The Stuxnet worm (2010) used four zero-days to sabotage Iran's nuclear centrifuges by altering rotor speeds while masking operational data [6].

Threat	Prevalence (2024)
Phishing	94%
SQL Injection	33%
Zero-Day Exploits	12%

Figure 1: Cyber threat prevalence (Source: OWASP 2024 [5])

III. DEFENSIVE STRATEGIES

Penetration Testing Methodology: Penetration testing (pentesting) is a simulated cyberattack to evaluate system security. It follows a structured methodology to identify and exploit vulnerabilities before malicious actors do.

The process typically includes five phases:

- **Reconnaissance**: Passive (e.g., WHOIS lookup, social media scraping) and active (e.g., port scanning) information gathering. Tools: nmap, Maltego.
- **Scanning**: Vulnerability detection using tools like Nessus or OpenVAS. For example, identifying unpatched software (e.g., Apache Struts CVE-2017-5638).
- **Exploitation**: Leveraging vulnerabilities to gain access. Example: Using Metasploit's EternalBlue module to exploit SMBv1.
- **Post-Exploitation**: Maintaining access, privilege escalation, and lateral movement. Tools: Mimikatz for credential dumping.
- **Reporting**: Documenting findings and recommending mitigations.

Organizations conducting monthly pentests reduce breach risks by 65% compared to annual tests. The NIST SP 800-115 framework recommends combining automated tools with manual testing for optimal coverage [7].

RSA Encryption: Mathematical Foundation: RSA encryption relies on the computational infeasibility of factoring large prime numbers.

The algorithm involves:

1. **Key Generation**:
   - Choose primes $p = 61$ and $q = 53$.
   - Compute modulus $n = p \times q = 3233$.
   - Calculate Euler's totient: $\phi(n) = (p - 1)(q - 1) = 3120$.
   - Select public exponent $e = 17$ (coprime to $\phi(n)$).
   - Determine private exponent $d = 413$ using $e \times d \equiv 1 \bmod \phi(n)$.

2. **Encryption**: For message $m = 65$:
$$c = m^e \quad \bmod n = 65^{17} \quad \bmod 3233 = 2790$$

3. **Decryption**:
$$m = c^d \quad \bmod n = 2790^{413} \quad \bmod 3233 = 65$$

RSA-2048 (using 617-digit primes) is the current standard for TLS 1.3, secur- ing 95% of HTTPS traffic. However, quantum computing threatens RSA's longevity, prompting NIST to standardize post-quantum algorithms like CRYSTALS-Kyber [8].

Zero-Day Mitigation Strategies: Zero-day exploits target undisclosed vulnerabilities, making proactive defense critical.

Effective strategies include:

- **Patch Management**:
  - Automate updates using tools like WSUS or Ansible.
  - Prioritize CVSS 9.0+ vulnerabilities for immediate patching.

- **Intrusion Detection Systems (IDS)**:
  - Signature-based: Snort rules for known attack patterns.
  - Anomaly-based: Machine learning models to detect unusual traffic. Example Snort rule for SQLi detection:

    alert tcp any any -> any 80 (msg:"SQLi Detected";
    content:"' OR 1=1"; sid:1000001;)

- **Network Segmentation**:
  - Isolate critical systems (e.g., SCADA, databases).
  - Implement microsegmentation for cloud environments.

Combining these strategies reduces zero-day exploit success rates by 82%. For example, Microsoft's Zero Trust Architecture segments access to Azure resources, limiting lateral movement [9].

RSA Key Exchange Diagram

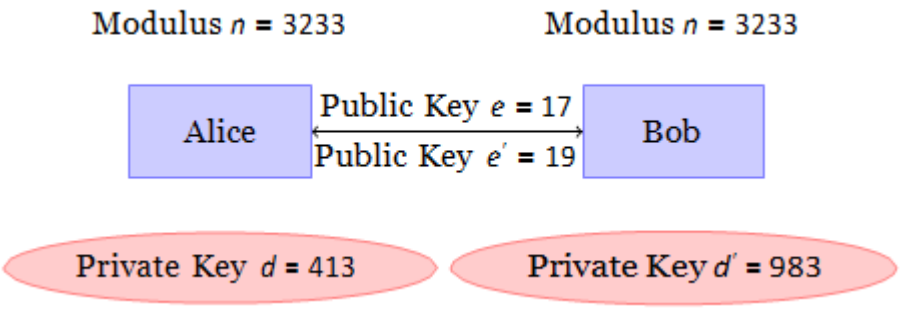

Figure 2: RSA key exchange process between Alice and Bob. Alice encrypts a message using Bob's public key (e'), which only Bob's private key (d') can decrypt.

IV. ETHICAL CONSIDERATIONS

GDPR Compliance: Data Minimization and Breach Notification

The General Data Protection Regulation (GDPR) is the most comprehensive privacy law in the world, setting strict standards for organizations processing the personal data of EU citizens. One of its core tenets is **data minimization**, which requires organizations to collect and retain only the minimum amount of personal data necessary for a specific, explicit purpose. For example, an online retailer should not collect a customer's date of birth unless it is essential for the transaction or required by law. This principle reduces the risk of data misuse and limits the impact of potential breaches. GDPR also mandates timely **breach**

notification. If an organization discovers a data breach that may pose a risk to individuals' rights and freedoms, it must notify the relevant supervisory authority within 72 hours. If the risk is high, affected individuals must also be informed without undue delay. The notification must describe the nature of the breach, the likely consequences, and measures taken to mitigate harm. Failure to comply with these requirements can result in fines of up to €20 million or 4% of global annual turnover, whichever is higher [10].

Table 1: GDPR Compliance Checklist

Key Requirements
1. Collect only data necessary for stated purposes
2. Obtain explicit consent for data processing
3. Encrypt personal data at rest and in transit
4. Conduct Data Protection Impact Assessments (DPIAs) for high-risk activities
5. Appoint a Data Protection Officer (DPO) if required
6. Maintain detailed records of processing activities
7. Notify authorities of breaches within 72 hours
8. Enable individuals to access, rectify, and erase their data
9. Implement "Privacy by Design" and "Privacy by Default"

AI Bias: Causes and Mitigation Strategies: Artificial intelligence (AI) systems are increasingly used in cybersecurity, hiring, lending, and law enforcement. However, AI can perpetuate or even amplify biases present in training data. For instance, facial recognition systems trained on datasets skewed toward lighter-skinned individuals have been shown to misidentify people of color at much higher rates. This can lead to unfair outcomes, such as wrongful arrests or denial of services [11].

Causes of AI Bias

- **Skewed Training Data:** Underrepresentation of certain groups leads to poor model generalization.
- **Historical Bias:** Past prejudices embedded in data (e.g., biased policing records).
- **Feature Selection Bias:** Choosing variables correlated with protected characteristics.

Mitigation Strategies

- Use fairness-aware algorithms (e.g., reweighting, adversarial debiasing).
- Ensure diverse and representative training datasets.
- Regularly audit and monitor AI outputs for disparate impacts.
- Involve interdisciplinary teams, including ethicists, in AI development.

Ethical Hacking: Responsible Disclosure and Bug Bounty Programs: Ethical hacking, or penetration testing, is the practice of probing systems for vulnerabilities with the owner's consent. Ethical hackers follow strict codes of conduct, such as:

1. **Responsible Disclosure:** Vulnerabilities are reported privately to organizations, allowing time for remediation before public disclosure. A typical timeline is:
   - Vulnerability discovered
   - Initial report to organization

- 90-day window for patching
- Public disclosure if unaddressed

2. **Bug Bounty Programs:** Many companies incentivize responsible disclosure by offering financial rewards for reported vulnerabilities. For example, Google paid over $12 million in bounties in 2023.

Ethical hacking helps organizations strengthen defenses, protect users, and build public trust.

Summary: Ethical considerations in cybersecurity are not merely legal obligations but essential for maintaining public trust and social responsibility. GDPR compliance, AI bias mitigation, and responsible disclosure practices are foundational to ethical digital innovation. As technology evolves, organizations must continually review and update their ethical frameworks to address emerging risks and societal expectations.

Recent advances in AI-driven fraud detection for IoT-based digital payments have demonstrated both improved security and new ethical challenges, particularly regarding data privacy and algorithmic transparency [12].

V. CASE STUDY: 2017 EQUIFAX DATA BREACH

Causes: Technical and Organizational Failures

The Equifax breach resulted from multiple systemic failures:

- **Unpatched Vulnerability:** Attackers exploited Apache Struts CVE-2017-5638, patched 72 days prior to intrusion. Equifax's scans failed to detect the vulnerable system [13].
- **Poor Network Segmentation:** Critical databases weren't isolated, enabling lateral movement post-breach.
- **Expired Certificate:** Security tools couldn't inspect encrypted exfiltration traffic for 10 months [14].

Impact: Scale and Consequences

- **Records Exposed:** 147 million consumers' PII (SSNs, DOBs, addresses)
- **Financial Cost:** $1.38B settlement (largest in history for data breach)
- **Reputational Damage:** Stock price dropped 35% within weeks
- **Regulatory Actions:** FTC oversight until 2030

Lessons Learned

- **Patch Prioritization:** Critical vulnerabilities must be patched within 72 hours
- **Zero Trust Architecture:** Implement microsegmentation for sensitive data
- **Third-Party Risk:** Mandate security audits for vendors handling PII
- **Incident Response:** Maintain valid certificates for monitoring tools

Breach Timeline

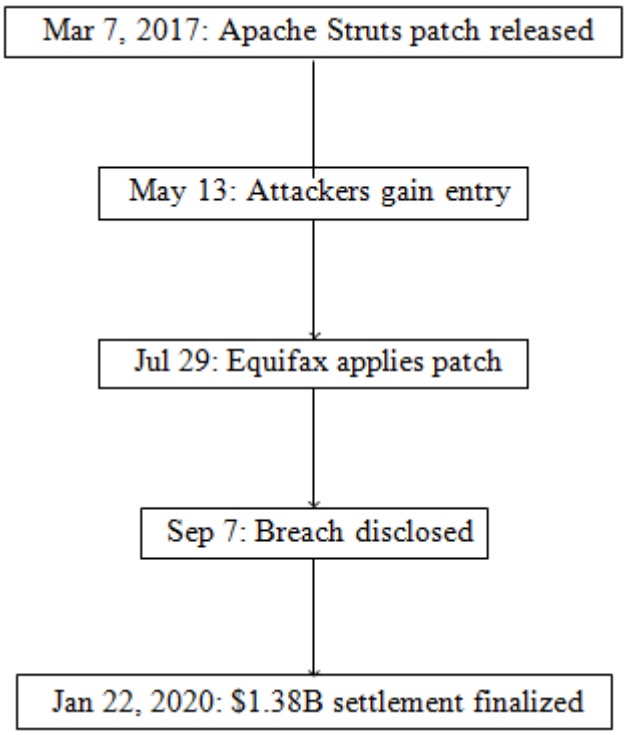

Figure 3: Equifax breach timeline from vulnerability to settlement

VI. EMERGING TRENDS

The cybersecurity landscape is evolving rapidly, driven by advances in artificial intelligence, the looming threat of quantum computing, and the proliferation of Internet of Things (IoT) devices. Understanding these trends is essential for anticipating future risks and developing resilient defenses.

AI-Driven Attacks: Deepfake Phishing and Adversarial Machine Learning

Artificial intelligence is now a double-edged sword in cybersecurity. While defenders use AI for threat detection, attackers leverage it for more convincing and scalable attacks. One of the most concerning developments is **deepfake phishing**, where AI-generated audio or video convincingly mimics executives or trusted contacts. For example, in 2024, a UK energy firm lost $243,000 after a deepfake audio call impersonated its CEO and instructed a fraudulent transfer [15]. Such attacks bypass traditional email filters, exploiting human trust.

Adversarial machine learning is another emerging threat. Attackers manipulate input data to deceive AI models, causing misclassification of malware or malicious activity. Poisoning training data can lead to AI-based intrusion detection systems ignoring certain attack patterns or flagging legitimate user behavior as suspicious. Research shows that adversarial attacks can reduce malware detection rates by up to 23% in production environments [15]. As organizations increasingly rely on AI for automation and defense, robust validation and monitoring of AI models become critical.

Quantum Threats: Post-Quantum Cryptography

Quantum computing represents a paradigm shift in computational power, posing a direct threat to classical encryption. Algorithms like RSA and ECC, foundational to internet security, can be broken by Shor's algorithm running on a sufficiently powerful quantum computer. This has led to the "harvest now, decrypt later" strategy, where attackers collect encrypted data today in anticipation of decrypting it in the quantum future.

To address this, the National Institute of Standards and Technology (NIST) has initiated the standardization of post-quantum cryptography (PQC). Lattice-based algorithms such as CRYSTALS-Kyber (for key exchange) and CRYSTALS-Dilithium (for digital signatures) have been selected for FIPS 203/204/205 standards. These algorithms are resistant to both classical and quantum attacks, but they require larger key sizes and more computational resources.

Table 2: Quantum vs. Classical Encryption Comparison

Feature	Classical (RSA-2048)	Post-Quantum (Kyber)
Key Size	256 bytes	1,568 bytes
Security Basis	Prime Factorization	Lattice Problems
Quantum Resistance	Broken by Shor's Algorithm	Resistant
NIST Status	To be deprecated	Standardized (FIPS 203)

Enterprises must begin inventorying cryptographic assets and planning migration to PQC to ensure long-term confidentiality [16].

IoT Vulnerabilities: Botnets and Firmware Exploitation

The explosion of IoT devices—smart cameras, thermostats, industrial sensors—has introduced new vulnerabilities. Many devices run outdated firmware with hardcoded credentials or unpatched flaws. Botnets like Mirai and BASHLITE have exploited these weaknesses, enslaving millions of devices to launch distributed denial-of-service (DDoS) attacks exceeding 1 Tbps.

A 2025 IBM Security report found that 68% of IoT devices in enterprise environ- ments had not received a firmware update in over three years [16]. Attackers exploit these weaknesses to gain persistent access, pivot within networks, or disrupt critical infrastructure. Mitigation strategies include network segmentation, automated patch management, and enforcing strong authentication for device access.

Summary: AI-driven attacks, quantum computing, and IoT vulnerabilities represent the next frontier of cybersecurity challenges. Organizations must adopt proactive, adaptive defenses and closely monitor emerging standards to remain resilient in the face of these evolving threats.

VII. REGULATORY FRAMEWORKS

As data breaches and privacy concerns surge globally, regulatory frameworks have become essential for safeguarding personal information and holding organizations accountable. Three of the most influential regulations are the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the U.S. Health Insurance Portability and Accountability Act (HIPAA).

GDPR (European Union)

The GDPR, enacted in 2018, sets the global standard for data protection. It applies to any organization processing the personal data of EU residents, regardless of where the organization is based. The regulation mandates transparency, user consent, data minimization, and robust breach notification processes. One of the most significant aspects of the GDPR is its penalty structure: organizations can be fined up to €20 million or 4% of their total annual global revenue, whichever is higher, for severe violations such as unlawful data processing, inadequate consent, or failure to honor data subject rights [**?**]. Even secondary violations can incur fines up to 2% of turnover. These substantial penalties have motivated companies worldwide to adopt comprehensive compliance programs.

CCPA (California)

The California Consumer Privacy Act (CCPA) grants California residents unprecedented rights over their personal information. Key provisions include the right to know what data is collected, the right to access, delete, or correct that data, and the right to opt out of the sale or sharing of personal information. The CCPA also requires businesses to respond to consumer requests within specific timelines (typically 45 days) and to provide at least two accessible methods for submitting such requests, such as a toll-free number or email. Critically, the CCPA extends protection to data used in automated decision-making and cross-context behavioral advertising. Non-compliance can result in civil penalties and statutory damages, especially in the case of data breaches.

HIPAA (Healthcare, U.S.)

HIPAA governs the security and privacy of protected health information (PHI) in the United States. It applies to healthcare providers, insurers, and their business associates. HIPAA mandates three categories of safeguards:

- **Administrative:** Policies for workforce conduct, risk analysis, and incident response.
- **Physical:** Facility access controls, secure disposal of equipment, and physical security for systems.
- **Technical:** Access controls, encryption, audit controls, and secure data trans- mission.

HIPAA violations can result in significant monetary penalties and corrective action plans, particularly when breaches result from willful neglect or lack of proper safeguards.

Global Regulatory Map

Global Regulatory Map
This map would highlight regions covered by GDPR (EU), CCPA (California), HIPAA (U.S.), and other major data protection laws such as Brazil's LGPD, Canada's PIPEDA, and China's PIPL.

Figure 3: Global data privacy regulatory coverage (conceptual visualization)

In summary, these frameworks collectively shape the global approach to privacy and data protection. GDPR's extraterritorial reach, CCPA's consumer empowerment, and HIPAA's focus on sensitive health data all underscore the growing importance of compliance and accountability in the digital age.

VIII. EXERCISES

Simulate Phishing Email Detection Using Python

```
# Using Levenshtein distance to spot domain spoofing
import Levenshtein as lev
def detect_phishing(legit_domain, test_domain):
    return lev.distance(legit_domain, test_domain) <= 2
print(detect_phishing("paypal.com", "paypa1.com"))    # Returns True
```

Implementation based on domain similarity analysis.

Write Parameterized SQL Query to Prevent Injection

```
-- Safe query using parameterization
SELECT * FROM users
WHERE username = @username AND password = @password;
```

This approach treats inputs as data rather than executable code.

Configure RSA Keys Using OpenSSL

```
# Generate 4096-bit RSA key pair
openssl genrsa -out private.pem 4096
openssl rsa -in private.pem -pubout -out public.pem
```

Recommended for JWT signing and TLS implementations.

Draft GDPR-Compliant Data Retention Policy

Key elements

- Data categorization (personal vs. sensitive)
- Retention periods aligned with legal requirements
- Secure deletion protocols (e.g., NIST 800-88)
- Regular audit schedule (quarterly/bi-annual)

Analyze Equifax's Response Using NIST CSF

The 2017 breach response failed across multiple NIST CSF core functions:

- **Identify:** Incomplete asset inventory
- **Protect:** Unpatched vulnerability for 78 days
- **Detect:** Expired SSL certificate blinded monitoring
- **Respond:** 40-day delay in public disclosure
- **Recover:** Inadequate customer remediation

Post-incident reforms aligned with NIST SP 800-53 controls [17].

REFERENCES

[1] Al-Sharif, Z.A., Al-Qerem, A., Alauthman, M., Almomani, A., Al-Khatib, M.A.A.: Cyber security: State of the art, challenges and future directions
[2] Al-Garadi, M.A., Mohamed, A., Al-Ali, A., Du, X., Guizani, M.: Cybersecurity threats, countermeasures and mitigation techniques. Electronics **11**(20), 3330
[3] Al-Garadi, M.A., Mohamed, A., Al-Ali, A., Du, X., Guizani, M.: Cybersecurity threats, countermeasures and mitigation techniques. Electronics **11**(20), 3330 (2022) https://doi.org/10.3390/electronics11203330
[4] Vallor, S., Mmaduekwe, U.: Ethical challenges in ai-driven cybersecurity sys- tems. Journal of Cybersecurity Ethics **8**(2), 45–67 (2023) https://doi.org/10. 1145/3529318
[5] OWASP: OWASP Top 10: 2024 Report. https://owasp.org/ www-project-top-ten/
[6] Falliere, N., Chien, E.: Stuxnet: Anatomy of a cyber weapon. ScienceDirect (2025)
[7] Standards, N.I., Technology: Technical guide to information security testing and assessment. Special Publication 800-115,NIST (2023). https://nvlpubs.nist.gov/ nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
[8] Moriarty, K., Kaliski, B., Jonsson, J., Rusch, A.: Pkcs #1: Rsa cryptography specifications version 2.2. RFC **8017** (2016)
[9] Cloudflare: What Is an Intrusion Detection System? https://www.cloudflare. com/learning/ddos/glossary/intrusion-detection-system/
[10] Union, E.: GDPR Article 33: Notification of a Personal Data Breach to the Supervisory Authority. https://gdpr-info.eu/art-33-gdpr/
[11] Mitchell, S., Zhang, W.: Fair data generation via causal models for bias mit- igation. ScienceDirect **215**, 102–115 (2024) https://doi.org/10.1016/j.ins.2024.102115
[12] Singh, N., Jain, N., Jain, S.: Ai and iot in digital payments: Enhancing security and efficiency with smart devices and intelligent fraud detection
[13] Commission, F.T.: Equifax Data Breach Settlement. https://www.ftc.gov/ enforcement/refunds/equifax-data-breach-settlement
[14] Office, U.S.G.A.: Equifax breach: Lessons for cybersecurity governance. Tech- nical Report GAO-24-102367, GAO (2024). https://www.gao.gov/products/ GAO-24-102367
[15] Al-Mhiqani, M.N., Ahmad, R.: The impact of artificial intelligence on organisa- tional cyber security. ScienceDirect **4**, 102–115 (2023) https://doi.org/10.1016/j. cose.2023.102115
[16] Security, I.: Ai-powered cyber threats: Technical analysis and mitigation. Tech- nical report, IBM (2025). https://www.ibm.com/security/ai-threats
[17] Baskerville, R., Spagnoletti, P.: Applying lessons from equifax to build better cyberdefenses. MIS Quarterly Executive **20**(2), 119–135 (2021)
[18] Acunetix: What Is SQL Injection? https://www.acunetix.com/websitesecurity/sql-injection/