INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 3, March 2026 | ISSN: 2456-4184 | IJNRD.ORG

An Analysis To Minimize The Acute and Disruptive Impact Of Ethical Hacking Using Emerging Trends And Technology

Mrs. Chanda Prasad[1][PhD Scholar,
Dept. of CS/IT, Chanda.prasad49@gmail.com, AISECT University, India]
Prof. (Dr.) Binod Kumar [2][Professor, Dept. of CS/IT, binodkr75@gmail.com, AISECT University, India]

Abstract

This paper discusses acute and disruptive impact of ethical hacking done by ethical hackers using emerging tools and technology. Ethical hacking is the authorized, legal practice of probing systems, applications, and networks to uncover vulnerabilities before malicious hackers could exploit. Currently to deal with this is not just about identifying security vulnerabilities, we need to be prepared to deal with AI-attacks, securing cloud systems, and constantly changing compliance requirements. Just understanding the theory of ethical hacking will not be enough to protect the system is being hacked using emerging tools and technology. We should have practical skills, a willingness to keep learning, and someone to help steer us in right direction else will fail to minimize the acute, disruptive impact of ethical hacking on operational systems. Industry need to shift from, or augmenting, traditional "periodic, manual, intrusive" testing towards continuous, automated, and AI-driven methodologies. This paper goal is to provide deep security insights to ensue business continuity by using safe, non-disruptive testing techniques that simulate real-world attacks. It highlights AI-driven automation, cloud-native security, and quantum-resistant cryptography, transitioning from manual penetration testing to proactive, intelligent threat simulation. It discuss various ways to secure IoT/API infrastructures, AI-driven phishing defense and adopting zero-trust models to counter sophisticated, AI-enabled attacks.

Keyword: *Ethical-Hacking, Emerging-Technology, AI, IOT, API, Phishing, Cloud-System etc.*

1. Introduction

Now days, ethical hacking has spread to almost all fields of the life and especially to all paths of computer industry; the need to protect the important data of the same should be addressed with right technology[2][21]. Ethical hacking is the authorized, legal practice of probing systems, applications, and networks to uncover vulnerabilities before malicious hackers can exploit them. It is a rehearsal for real-world cyber-attacks[17][20].

Organizations hire ethical hackers to launch simulated attacks on their computer networks. During these attacks, the ethical hackers demonstrate how actual cybercriminals break into a network and the damage they could do once inside[5]. Organization's analysts use this information to eliminate vulnerabilities, strengthen security systems and protect sensitive data[1]. Thanks to the emerging technologies like cloud computing, the

Internet of Things, and blockchain, businesses have become more cost effective and efficient. However, these developments have also created new attack surfaces for malicious hackers. According to a recent report from security platform Bugcrowd, between May 2020 and August 2021, 80% of ethical hackers encountered a vulnerability they had not seen before[9]. Now, cyber security experts need to "think like a hacker" to keep pace with the ever-evolving threat landscape. To do so, they need cutting-edge ethical hacking technologies and up-to-date information on the latest hacking trends and techniques[18]. Emerging technologies have transformed industries to be more effective and collaborative, and increased dependencies on such platforms[7]. The downside is that, if these technologies are exploited/hacked, they can cause extensive harm to both organizations and people whose data has been compromised, and this is where the ethical concerns (i.e.,social contract) fits in[22].

This research paper outlines essential ethical hacking skills and offer advice for cyber security researchers interested in doing research in ethical hacking. It *deals with the ethical issues, and data privacy and security implications that arise as an outcome of unregulated and non-compliance integrations of these state-of-the-art technologies[8]. It explores Emerging technologies have featured prominently in the research on technology ethics, which is progressively concentrating on early-stage intervention in technological innovation. In investigates the diverse functions of ethical hacking within modern cyber security and integrates current research; it analyzes the progression of ethical hacking techniques, their use in identifying vulnerabilities and conducting penetration tests, and their influence on strengthening organizational security. Additionally, the paper discusses the ethical considerations, legal contexts and challenges that arises with ethical hacking. This review ultimately enhances the understanding of how ethical hacking can bolster cyber security defenses.*

2. Challenges

Nowadays, new cyberthreats are increasingly intricate and challenging to address Ethical hacking with emerging technologies (AI, IoT, Cloud) to introduce critical drawbacks, including high implementation costs, severe privacy risks and potential for data corruption or system downtime[2]. It creates legal ambiguity, requires constant, intense upskilling and poses the risk of AI-driven tools exhibiting bias or accountability gaps. Ethical hackers employ AI Driven technologies to thwart cyberattacks[11]. These technologies simulate sophisticated attack scenarios; analyze enormous databases, and spot anomalies. Ethical hackers uses AI to anticipate potential attack routes and assist in coming up with practical defenses. Emerging technologies like Cloud Computing, Autonomous Vehicles, Artificial Intelligence, Big Data and Machine Learning, and Cybersecurity have enormous potential[4]. These advancements raise ethical considerations related to data security and privacy that must be resolved before industries deployment. It has transformed industries to be

more effective and collaborative, and increased dependencies on such platforms. The downside is that, if these technologies are exploited/hacked, they can cause extensive harm to both organizations[10].

Another dimension involves ethical perspectives of different hat types (i.e., black hat, white hat, etc.[3][14]. Black hat hackers are cybercriminals having malicious intents looking for security vulnerabilities in an environment that can be exploited for stealing data/financial gain. White hat hackers are ethical hackers who has permission to perform threat intelligence and pen-testing for identifying and fixing security flaws/weaknesses. Gray hat hackers are equally skilled as black and white hackers, their intent is to look for security vulnerabilities without following the cyber code of ethics. They scan through software vulnerabilities without having the permissions/consent to do so. Red hat hackers are well-known for playing the offense strategy and re motivated by tracking down malicious threat actors for performing counter attacks and damaging their networks and devices. Red hat hackers are widely known for infiltrating the dark web and launching attacks against malicious/black hat hackers. Blue hat hackers are highly skilled cyber experts hired by enterprises for pen-testing the security posture and improving the cyber defense strategy of their digital environment. Though blue hat hackers are similar to white hats in terms of skillset, they differ based on services offered. Green hat hackers are professionals who wish to pursue careers in cyber hacking; they have limited understanding, experience, and technical knowledge in the domain and are usually found on domains/blogs for asking questions. Ethical hackers use the same techniques as malicious hackers—scanning, exploiting, and maintaining access—but with professional, ethical constraints. The five major ethical dilemmas currently faced by emerging technologies are (i) data privacy, (ii) risks associated with Artificial Intelligence, (iii) developing sustainable environments, (iv) health implications due to technology use, and (v) infodemic and data weaponization issues[16]. The other Key Drawbacks in Emerging Tech Ethical Hacking includes following:

- ***AI-Driven Vulnerabilities & Ethics:*** *Using AI for penetration testing lead to algorithmic bias, where the tool misinterprets data or focuses on incorrect vulnerabilities. There is also a major "dual-use dilemma" where AI tools designed for defense can be repurposed for malicious attacks.*

- ***Data Privacy and System Risks:*** *Advanced, automated or intrusive testing methods inadvertently expose, alter or destroy sensitive, critical information or damage user privacy.*

- ***High Cost and Resource Intensity:*** *Utilizing cutting-edge technology and hiring skilled, specialized or certified ethical hackers is expensive, often making it inaccessible for smaller organizations.*

- ***Legal and Compliance Ambiguity:*** *Technologies evolve faster than regulations, ethical hackers often operate in a legal gray area, leading to potential liability issues even when conducting authorized, professional tests.*

- ***Operational Disruption:*** *Testing in complex IoT or cloud environments may cause unintended disruption to business operations, leading to revenue loss.*

- ***Over-Reliance and False Security:*** *An over-dependence on automated, AI-driven hacking tools can create a false sense of security, causing companies to overlook necessary, traditional, in-depth security assessments.*

3. Proposed Solution

To minimizing the acute and disruptive impact of ethical hacking in current era requires transitioning from periodic, manual penetration testing to continuous, AI-driven, and "assume-breach" methodologies[6]. Below given measures can be used to minimize the disruptive impact of ethical hacking done using emerging trends.

1. *First measure is the shifting from "Continuous" & "Automated" Testing. Moving away from the annual, disruptive "big bang" penetration tests reduces the shock to IT systems. Under this measure falling below activities needed to carry out[12][19].*

   - ***Continuous Exposures:*** *Rather than of periodic scans, there is a need to continuously monitor for misconfigurations, privilege drift, and unusual behavior, allowing for faster, incremental, and less disruptive remediation.*

   - ***AI-Driven Scanning: PenTest++*** *or* ***DeepExploit*** *tool can be used to automate routine reconnaissance and vulnerability enumeration to reduce the time and manual efforts.*

   - ***AI Co-pilots:*** *It acts an assistant to ethical hackers, guiding them through testing steps, interpreting output, and suggesting non-disruptive, targeted actions.*

2. *Second deals with the implement of "Assume-Breach" & "Zero Trust" Models. These strategies focus on containment rather than just perimeter defense, limiting the "blast radius" of a test or attack[15].*

   - ***Zero-Trust Architecture:*** *Validates every access request (identity-based) and implementing micro-segmentation, ethical hackers can test specific segments without taking down the entire network.*

   - ***"Assume-Breach" Mindset:*** *Red teams act as if a hacker is already inside, focusing on lateral movement and privilege escalation, which allows for testing security controls in a controlled, granular manner.*

3. *Third deals with utilize the "Digital Twins" and Sandboxing.*
    - ***Digital Twins Cyber Exercises:*** *Increasingly using of virtual models of their IT environments to simulate high-stakes attacks in a risk-free environment, ensuring that a "what-if" scenario doesn't cause real-world downtime.*
    - ***Behavioral Analysis & Sandboxing:*** *Sandboxing for malware analysis and behavioral analysis tests systems behave under stress and allows ethical hackers to identify vulnerabilities without affecting production data.*
4. *Fourth deals with the Leverage AI for "Low-Noise" and "High-Precision"*
    - ***AI-Powered Threat Detection:*** *AI algorithms process vast datasets in real time, identifying anomalies and potential threats with high accuracy.*
    - ***"Invisible" Vulnerability Scanning:*** *Modern automated tools can analyze system configurations without generating high traffic, thus not triggering defensive systems or causing performance degradation (DoS).*
5. *Fifth one deals by Adopting "Purple Teaming" and Structured Reporting*
    - ***Purple Teaming:*** *"Red" (attackers) and "Blue" (defenders) teams work together for immediate feedback, knowledge transfer, and instant remediation of identified risks, reducing the duration of vulnerabilities.*
    - ***Context-Aware Reporting:*** *AI-enhanced platforms generate reports that provide business context, helping leadership prioritize patches that are critical to operational continuity.*
6. *Sixth measure is concerned with Strengthen "Human" Defenses (Awareness)*
    - ***Simulated Phishing & Social Engineering:*** *Using AI-powered simulation tools to train employees against advanced deepfake, voice-cloning, and phishing scams.*
    - ***Gamified Training:*** *Gamified, interactive training educate employees on recognizing and responding to threats, reducing human error and improving operational resilience.*
7. *Seventh is dealing by enforceing "Security-by-Design" & Supply Chain Oversight*
    - ***API and Third-Party Audits:*** *As organizations rely more on third-party integrations, continuous monitoring of shadow APIs and third-party security postures is crucial to stop attacks that bypass traditional perimeters.*

- ***Software Bill of Materials (SBOM):*** *Using SBOM to audit the software supply chain ensures all components are checked, reducing the likelihood of a major breach originating from a trusted vendor.*

In addition of above measures, some other ways are also mentioned below along with the potential cyber threats and how ethical hacking can alleviate them:-

1. ***AI powered cyber attacks:****–AI in hacks has greatly benefited criminals. AI driven Phishing techniques and viruses can change in real time. They are difficult to find. Attackers use AI to identify network vulnerabilities, produce deepfakes, and initiate extensive automated attacks.*

   Way to mitigate: *– Ethical hackers employ AI driven technologies to thwart cyberattacks. It supports threat detection and response. These technologies simulate sophisticated attack scenarios; analyze enormous databases and spot anomalies. AI is used by ethical hackers to anticipate potential attack routes and assist them in coming up with practical defenses.*

2. ***Supply Chain Attack:*** *– Supply chain threats still is a significant worry. Cybercriminals use suppliers and third-party vendors as a means of breaking into bigger companies. These advantage of links allow hackers to use a single point of entry to compromise systems.*

   Way to mitigate: *- Supply chain security requires ethical hackers. They evaluate the security of outside partners and providers. They evaluate the risk from outside sources. They then stop attacks on the supply chain. This entails implementing strong access restrictions, performing security assessments, and auditing vendor compliance.*

3. ***Ransomware as a service(RAAS)****:- Emergence of Ransomware-as-a-Service platforms has made ransomware more accessible to attackers. These services make it possible for even non-technical people to start assaults by offering ready-to-deploy ransomware kits. Expansion of RaaS led to a rise in ransomware attacks on governments, corporations, and healthcare institutions.*

   Way to mitigate it:- *Organizations may better prepare for and handle ransomware threats with the assistance of ethical hackers. They test backups and incident response methods by simulating ransomware scenarios. Additionally, ethical hackers assist in identifying and resolving vulnerabilities that RaaS operators may exploit.*

4. ***Quantum related threats****:- For cybersecurity, quantum computing presents both advantages and disadvantages. It poses a challenge to established encryption techniques even as it offers ground-breaking*

breakthroughs. Quantum technology is being used by cybercriminals to break encryption. As a result, many security protocols become outdated[19].

***Way to mitigate it**:- Ethical hackers are experimenting with quantum-resistant encryption as dangers from quantum computing grow. They collaborate with businesses to put post-quantum cryptography into practice. It guarantees data security against attacks allowed by quantum technology.*

5. ***IoT vulnerabilities**:- The IoT, or Internet of Things, is growing. In critical infrastructure, residences, and companies, there are billions of connected devices. IoT devices, however, frequently lack robust security. They become easy targets for cyberattacks because of this. Threats like device hacking, data breaches, and botnets are prevalent in 2025.*

***Way to mitigate it**:- By evaluating the security of linked devices, ethical hackers fix IoT vulnerabilities. They locate vulnerabilities in communication protocols, network settings, and device firmware. Their efforts help users and manufacturers increase security. IoT-based assaults are less likely as a result.*

4. Summary

This paper explores negative impact of ethical hacking done by using emerging tools and technology. It highlights the risk and dilemma involved with hiring the ethical hackers like Whit Hat, Balck Hat, Gray Hat and Red hat and then suggests measures to deal with them. It suhggests some additional ways specially to deal with hacking done in the current technological era, emerging technologies such as Cloud Computing, Autonomous Vehicles, Artificial Intelligence, Big Data and Machine Learning, and Cy-bersecurity have enormous potential. It deals with the ethical issues, and data privacy and security implications that arise as an outcome of unregulated and non-compliance integrations of these state-of-the-art technologies.

References:

[1] *Abhiraj, What are the Advantages and Disadvantages of Ethical Hacking in India?, Craw Cyber Security, 16 Aug 2025*

[2] *Abu Rayhan, The Role of Ethical Hacking in Modern Cybersecurity Practices, DOI:10.13140/RG.2.2.16619.55841, May 2024*

[3] *Bharti etl, White Hat Hacking: The Importance of Ethical Hacking in the Cyber-Security Industry IJFMR, E-ISSN: 2582-2160, Volume 7, Issue 3, May-June 2025.*

[4] *Christophe Gaie etl., Ethical hacking: at the heart of modern cybersecurity, May 14th, 2025*

[5] *Dr.P.Kannan etl, CYBER SECURITY AND ETHICAL HACKING, JETIR, ISSN-2349-5162, Volume 11, Issue 3, Mar 2024.*

[6] *Disha Bhosle, A Review Paper on Ethical Hacking, IJARSCT, ISSN (Online) 2581-9429, Vol. 3, Issue 1, August 2023*

[7] *Eder Rbeiro etl, Cyber Talks, Ethical Hacking: Emerging Technologies that Require Red Teamers, https://www.eccouncil.org/cybersecurity-exchange/, Oct 15, 2025*

[8] *Fatima Asif etl., Ethical Hacking and its role in Cybersecurity: AComprehensive Review, BS Data Science, Aug 2024*

[9] *Fiza Abdul Hafiz Qureshi etl, A Review Paper on Ethical Hacking, IJARSCT, ISSN (Online) 2581-9429, Volume 3, Issue 1, August 2023*

[10] *G Vishnuram etl, Ethical Hacking: Importance, Controversies and Scope in the Future, https://ieeexplore.ieee.org/document/9740860, International Conference 2022*

[11] *Hossana Maghiri etl, Ethical Implications of AI-Driven Ethical Hacking, Journal of cyber security, Oxford Academic, 14 Jul 2025*

[12] *Prashant Kumar Gavel etl, Ethical Hacking and Cyber Security against Cyber Attacks, https://ijtonline.com/, 21.06.2020.*

[13] *kavita choudhary, Advantages And Disadvantages Of Ethical Hacking, 13 May 2023*

[14] *Lubna Luxmi Dhirani etl., Ethical Dilemmas and Privacy Issues in Emerging Technologies, MDPI, Sensors 2023.*

[15] *Miss. Dhage T.S. etl, Ethical Hacking: A Proactive Approach to Cyber security, IJNRD ISSN: 2456-4184, Volume 10, Issue 11, November 2025*

[16] *Prabhat Kr Sahu etl, A REVIEW PAPER ON ETHICAL HACKING, International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 12, December 2020*

[17] *Ram Charitra Kurmi, Ethical Hacking and Cyber Security: A Comprehensive Overview, JETIR, ISSN-2349-5162, Volume 11, Issue 3, March 2024,*

[18] *Vitesh Sharma, Advantages and Disadvantages of Ethical Hacking, Jul 11, 2022*

[19] *www.amigocyber.com, Role of ethical hacking in the emerging trends of cyber threats, May 29, 2025*

[20] *www.geeksforgeeks.org, Introduction to Ethical Hacking, 12 Dec, 2025*

[21] *www.ibm.com, Security Intelligence, What is ethical hacking?, episode 22, February 2025*

[22] *Ying He etl, AI-based Ethical Hacking for Health Information Systems (HIS): a simulation study, Journal of Medical Internet Research on: August 07, 2022*