Vol. 2 - No. 2
March 2025 E-ISSN: 2584-0657

Internet Security Threats and Defence Mechanisms (ISTDM)

Thejesh R[1], Vishnumurthi K[2], Rithick P[3], Muthamizhselvan R[4], Shreenandhini P[5]

[1,2,3,4] Computer Science and Engineering (Cyber Security)
Sree Sakthi Engineering College, Coimbatore, India
[5] Assistant Professor, Emerging Technology
Sree Sakthi Engineering College, Coimbatore, Tamil Nadu, India
***DOI**: https://doi.org/10.5281/zenodo.15641575*

Abstract

The rapid growth of internet usage has made cybersecurity a major concern for individuals, businesses, and governments. With more people and organizations relying on the internet for communication, banking, and data storage, the risk of cyber threats has increased. These threats can lead to data theft, financial losses, privacy breaches, and operational disruptions. To defend against these risks, organizations use firewalls, encryption, intrusion detection systems, and multi-factor authentication. New technologies like artificial intelligence (AI), blockchain, and Zero Trust Architecture (ZTA) are improving cyber security. AI helps detect unusual activity and prevent attacks, block chain ensures secure transactions, and ZTA ensures that no user or device is trusted by default. This study highlights the importance of strong cybersecurity measures, regular updates, user awareness, and proactive defense strategies to protect against evolving threats.

***Keywords**: Internet security, Threats, Defense mechanism, IOT, Cloud computing, Phishing attack, malware, Denial of service / Distributive Denial of service, Man-in-Middle Attack, SQL injection, Cross Scripting (XSS), Zero-Day Exploit, Insider Threats, Passwords Attack, Data Breaches, DNS Spoofing, Firewall, Antivirus and Anti-malware, IDS/IPS, Multi-Factor Authentication, Network Segment, AI in Cyber Security, Adopting Zero Trust Security, Blockchain for secure transition, Stronger Encryption and at a protection, Education user about Cyber security*

INTRODUCTION

In the fast-moving digital world, the spread of cloud computing and Internet of Things (IoT) has transformed data generation, processing, and usage. All these technologies are now at the core of industries from healthcare and smart cities to industrial automation and residential environments. But with their revolutionary advantages, they have brought a tangled web of security issues into view. As companies more and more implement cloud infrastructures for scalability and IoT environments for immediate responsiveness, the attack surface has grown exponentially, and the need for strong security measures has become more important than ever.

Cloud computing, which features its extensibility, on-demand capability, and shared resource models, is especially exposed with its multi-tenant infrastructure, virtualization layers, and reliance on pervasive networks

Typical threats encompass data breaches, unauthorized access, insider threats, and service interruptions such as Distributed Denial of Service (DDoS) attacks. Likewise, IoT systems, which consist of resource-limited devices and are based on diverse communication

protocols, are susceptible to physical tampering, identity spoofing, firmware tampering, and insecure data transmission.

These vulnerabilities are further compounded by the heterogeneity and volume of connected devices, usually without standardized security protocols.

Defence mechanisms for such ecosystems have come a long way. In cloud computing, security frameworks today include multi-layered architectures with intrusion detection systems (IDS), virtual machine isolation, role-based access controls, and encryption protocols that provide data confidentiality and integrity. For IoT, anomaly detection systems, intrusion prevention systems (IPS), lightweight cryptographic solutions, and secure key management schemes are the building blocks of upcoming protective architectures The incorporation of artificial intelligence (AI) has also enhanced the strength of cybersecurity systems. AI-based models improve threat detection efficacy, facilitate predictive analysis, and assist in adaptive security actions in real-time. Methods such as cloud security IDS using machine learning and AI-based anomaly detection in IoT networks hold great potential for countering advanced cyber threats.

All the while, though, there exist a number of challenges that persist. These consist of guaranteeing interoperability within heterogeneous devices, data privacy control across borders, real-time mitigation of threats where resources are not available, as well as theory-practice bridges in security architecture. The dynamism and the distributed nature of both cloud computing and IoT architectures call for never-ending innovation of defence mechanisms.

This case study critically discusses the common dangers and vulnerabilities endemic to cloud computing and IoT- based environments. It offers systematic examination of current defence mechanisms, analyses their efficiency, and points out areas where there are still gaps in existing implementations. Additionally, it offers holistic and visionary solutions that focus on strengthening the security position of these networked technologies. By illustrating threats versus counter measures and stressing interdisciplinary defence measures, this research offers a comprehensive perspective on Internet security in the era of hyper connectivity.

INTERNET SECURITY THREATS

In this session, let's discuss some important threats that most commonly occur on the Internet.

Phishing Attacks

Role

Phishing is perhaps the most ubiquitous social engineering threat for misleading users to divulge confidential information such as credentials or payment information. It is frequently the point of entry for broader attacks (e.g., ransom ware or data theft), particularly for cloud and email-based infrastructure.

Prevention Steps

- Implementing email filtering and anti- phishing solutions.
- Make users aware of suspicious-looking emails and URLs.

- Implement two-factor/multi-factor authentication (2FA/MFA).
- Use AI-powered behaviour-based monitoring of suspect login patterns.

Malware (Viruses, Worms, Trojans, Ransomware, Spyware)

Role

Malware can destroy systems, steal data, encrypt files (ransom ware), or monitor user behaviour. In IoT, malware usually infects unsecured devices to create bot nets or sabot age essential systems.

Prevention Steps

- Utilize proven antivirus/anti-malware programs.
- Periodically update and patch systems/devices.
- Segregate infected devices via network segmentation.
- Implement application white listing and block untrusted software installation.

Denial of Service (DoS) / Distributed Denial of Service (DDoS) Attacks

Role

DoS/DDoS attacks flood services, rendering them unavailable. In cloud, these attacks lead to expensived own time and service degradation. IoT devices are frequently compromised to carry out DDoS (e.g., Mirai botnet).

Prevention Steps

- Utilize DDoS protection services (e.g., Cloudflare, AWS Shield).
- Utilizerate limiting and traffic filtering.
- Inspect network traffic for suspicious spikes.
- Utilizered undant systems and scalable infra structure to soakup attacks.

Man-in-the-Middle (MitM) Attacks

Role

MitM attacks intercept messages to steal or modify data. Prevalent in insecure IoT device communication or data transit in cloud applications.

Prevention Steps

- Enforce HTTPS and SSL/TLS encryption.
- Utilize VPNs for secure remote access.
- Use strong mutual authentication (client- server).
- Do not use public Wi-Fi for sensitive transactions.

SQL Injection

Role

This attack exploits poorly sanitized database queries, enabling attackers to manipulate databases. Particularly risky in cloud-hosted web applications or platforms handling sensitive IoT device data.

Prevention Steps

- Use parameterized queries and prepared statements.
- Apply input validation and sanitization.

- Restrict database privileges to have minimal impact.
- Use Web Application Firewalls (WAFs).

Cross-Site Scripting (XSS)

Role

XSS adds malicious scripts to web pages being viewed by others, and it is commonly utilized to steal sessions or cookies. It's a significant threat in user-generated content cloud-based applications.

Prevention Steps

- Sanitize and escape the input of users.
- Utilize Content Security Policy (CSP).
- Validate data at both client and server sides.
- Use output encoding mechanisms.

Zero-Day Exploits

Role

Zero-days aim at unidentified or unpatched vulnerabilities. They are the top threats to both cloud infrastructure and IoT firmware and are usually taken advantage of ahead of a solution.

Prevention Steps

- Stayup to real-time threat feeds.
- Use behaviour-based intrusion detection (e.g., AI/ML).
- Enforce virtual patching via web proxies/firewalls.
- Have a quick-response security team for crash fixes.

Password Attacks (Brute Force, Dictionary Attacks, Credential Stuffing)

Role

These attacks crack or reuse passwords to gain unauthorized access. Weak/default passwords are particularly prevalent in IoT devices.

Prevention Steps

- Enforce password policies.
- Enable lockout account mechanisms.
- Implement MFA on all systems.
- Use CAPTCHA to block automated login attempts.

Insider Threats

Role

Insiders (contractors or employees) can in advertently or deliberately compromise systems. In cloud environments, they can abuse access rights or divulge information.

Prevention Steps

- Utilize Role-Based Access Control (RBAC).
- Monitor user activity with SIEM tools.

- Perform background checks and routine training.
- Implement the principle of least privilege (POLP).

Data Breaches

Role

Data breaches area case of unauthorized access and exfiltration of sensitive information. Misconfigured cloud storage and weak APIs are typical breach locations.

Prevention Steps

- Encrypt data at rest and intransit.
- Authenticate APIs properly.
- Regularly audit and scan for vulnerabilities.
- Back up data regularly and practice disaster recovery plans.

DNS Spoofing/Poisoning

Role

This attack manipulates DNS records to send users to malicious websites, allowing for credential theft or malware injection. Essential in IoT since devices depend on DNS for updates and commands.

Prevention Measures

- Utilize DNSSEC to authenticate DNS integrity.
- Inspect DNS traffic for suspicious activity.
- Clear DNS cache regularly and avoid recursion.
- Utilize endpoint protection with secure DNS resolvers.

This above mention threats are the commonly occur while the internet

INTERNET SECURITY DEFENSE MECHANISMS

In this session let as discuss about the some important defence mechanisms to prevent the internet threats

Firewalls Function

Serve as a shield for internal networks and external attacks by checking and blocking incoming/outgoing traffic according to defined rules. Firewalls represent the initial barrier against unauthorized entry, DoS/DDoS attacks, and dangerous payloads.

Antivirus and Anti- malware Software Function

Meant to identify, isolate, and eradicate malicious software such as viruses, worms, trojans, ransom ware, and spyware. Critical in endpoint protection, particularly in cloud deployments and edge IoT devices.

Encryption (SSL/TLS, AES, RSA) Function

Guarantees data in transit and at rest confidentiality and integrity. Shields against interception during communication (e.g., MitM attacks), and protects data storage in cloud systems. Ubiquitously applied in securing IoT transmissions and cloud-hosted applications.

Intrusion Detection and Prevention Systems (IDS/IPS) Function

IDS provides alerts upon signs of abnormality in network traffic. IPS proceeds to actually stop detected threats while they occur, in real time. They play a crucial part in the discovery and reduction of zero-day attacks, brute force attacks, as well as outliers in IoT or cloud networks.

Multi-Factor Authentication (MFA) Function

Adds a second (or more) level of identity authentication, in addition to a simple password. This significantly lowers the success rate of phishing, credential stuffing, and brute- force attacks—both common in cloud services and user-facing IoT apps.

Access Control and Role- Based Access Control (RBAC) Function

Restricts access to systems, data, or devices according to user roles or responsibilities. Reduces insider threats and assists in implementing the principle of least privilege. Commonly applied in enterprise cloud platforms and multi-user IoT systems.

Patch Management and Regular Updates Function

Remedies known vulnerabilities in operating systems, applications, firmware, and services. Regular updates protect against zero-day attacks, malware, and exploits on out-of-date software in IoT devices or cloud-based infrastructure.

Network Segmentation Function

Splits the network into several zones to isolate breaches and restrict lateral movement of attackers. Particularly effective in separating sensitive information or mission-critical IoT devices from the rest of the network.

Security Information and Event Management (SIEM) Function

Gathers, analyses, and correlates logs across systems to identify anomalies and trigger real-time alerts. Provides greater visibility across cloud and IoT infrastructures and enables quick incident response to sophisticated threats.

User Awareness and Education Training Function

Empowers users to recognize phishing, suspicious links, and social engineering tactics. Reduces the risk of human error, a major source of data breaches and credential theft in personal and enterprise settings.

Secure Coding Practices Function

Avoids attacks such as SQL injection, XSS, and buffer overflows during the development of software. Necessary for secure app development for the cloud, and firmware security for IoT devices.

VPNs (Virtual Private Networks) Function

Secures internet connections and conceals user IP addresses. Averts eavesdropping and MitM attacks, particularly when using public Wi-Fi or remote access applications typical of cloud computing and mobile IoT environments.

The above defence mechanisms are widely used to prevent the internet threats

PROPOSED SOLUTIONS INTERNET SECURITY THREATS AND DEFENCE MECHANISMS

In this session let's as discuss about the some proposed solution to give the extra layer of security to the internet security.

Adopting Zero Trust Security

Explanation

Zero Trust is a security framework that assumes no user or device should be automatically trusted, even if inside the network perimeter. Instead, access is granted based on continual verification of identity, device health, and user intent.

Real-World Implementation

Use case: A cloud-based enterprise environment.

How to implement

Micro-segmentation: Divide the network into granular zones so users can only access the resources they' reauthorized to.

MFA Everywhere: Require Multi-Factor Authentication for all internal and external logins.

Identity and Access Management (IAM): Enforce role-based access and real-time monitoring of login behaviours.

Device Verification: Only allow registered and secure devices to access sensitive applications (common in IoT ecosystems).

Using Artificial Intelligence (AI) for Cybersecurity

Explanation

AI and machine learning can detect patterns, anomalies, and evolving threats faster than human analysts. AI improves threat detection, response time, and even automates part of the defines lifecycle.

Real-World Implementation

Use case: AI-based Intrusion Detection System in cloud infrastructure.

How to Implement

Anomaly Detection: Train ML models to learn normal traffic patterns, and trigger alerts when deviations occur (e.g., a smart their most at suddenly sending gigabytes of data).

Threat Intelligence: Use AI to aggregate and analyse real-time threat feeds.

Automation: Automatically quarantine infected end points or deny risky login attempts.

Chatbots: Deploy AI-based virtual assistants for incident response triage.

Implementing Blockchain for Secure Transactions

Explanation

Blockchain technology ensures data integrity, transparency, and decentralization, making it ideal for secure transactions and record-keeping in IoT and cloud environments.

Real-World Implementation

Use case: Secure communication between IoT devices.

How to Implement

Smart Contracts: Use block chain to automate secure rules for device-to-device communication (e.g., a smart car only starts if its digital ID matches the owner's wallet).

Decentralized Identity Management: Securely verify and store digital identities across platforms.

Supply Chain Security: Track the entire lifecycle of a product (e.g., a medical device) on the block chain to ensure authenticity.

Regular Cybersecurity Checks and Response Planning

Explanation

Proactively identifying vulnerabilities and having a structured response plan helps minimize damage from cyber incidents. This includes regular penetration testing, vulnerability scans, and incident response simulations.

Real-World Implementation

Use case: Healthcare cloud platform managing patient data.

How to Implement

Routine Vulnerability Scans: Use tools like Nessus or Qualys to detect misconfigurations or outdated software.

Incident Response Plan (IRP): Create a documented playbook including team roles, contact protocols, and containment strategies.

Tabletop Exercises: Simulate attacks like ransomware or phishing and test how teams respond in real-time.

Audits: Perform regular compliance checks (e.g., HIPAA for healthcare, GDPR for Europe).

Stronger Encryption and Data Protection

Explanation

Encryption ensures data is unreadable to unauthorized users. This protects data at rest (stored) and data intrans it (moving between systems or devices).

Real-World Implementation

Use case: A smartcity platform handling sensor data.

How to Implement

TLS/SSL: Secure all communications between web services and devices with HTTPS.

End-to-End Encryption: Ensure only sender and recipient can read the message (e.g., messaging apps).

AES-256 or RSA: Use strong symmetric and asymmetric encryption standards for files and credentials.

Data Tokenization: Replace sensitive data with non-sensitive equivalents during storage or processing.

Educating Users about Cybersecurity

Explanation

Human error is responsible for a significant percentage of cyberattacks (e.g., phishing). Educating users improves awareness and reduces risky behaviour.

Real-World Implementation

Use case: A company using cloud email and document sharing platforms.

How to implement

Phishing Simulations: Regularly test employees with mock phishing emails and analyse responses.

Security Awareness Programs: Conduct mandatory training covering password hygiene, suspicious activity, and safe browsing.

Gamified Learning: Use platforms like KnowBe4 or Cyberhug to make cybersecurity training engaging.

Policy Handbook: Distribute a clear guide outlining best practices for BYOD, remote work, and password policies.

Intrusion Detection Systems (IDS)

Explanation

IDS monitors and analyses network or system activities for malicious actions. It's essential for real-time detection of threats before damage is done.

Real-World Implementation

Use case: Smart factory with IoT-enabled machinery.

How to implement

Host-based IDS(HIDS): Monitor individual endpoints for file changes, unauthorized access, or malware.

Network-based IDS (NIDS): Analyse traffic across the network to detect suspicious behaviour or known attack signatures.

AI-Enhanced IDS: Use machine learning models to detect zero-day anomalies.

Integration with SIEM: Feed IDS alerts into Security Information and Event Management systems for correlation and faster response.

SUMMARY TABLE

Proposed Solution	Role in Cybersecurity	Real-World Implementation Example
Zero Trust Security	Assumes every access request could be a threat. Verifies all users, devices, and applications.	Micro-segmentation, enforcing MFA, and device identity validation in cloud and IoT environments
Artificial Intelligence (AI)	Detects, learns, and responds to threats automatically. Enables proactive and intelligent defence.	Machine learning-based intrusion detection, predictive threat analytics, and autonomous response bots
Blockchain for Security	Provides immutable, decentralized records. Ensures data transparency and trust.	Using smart contracts for secure IoT communication and decentralized identity verification
Regular Cybersecurity Checks & Response Planning	Detects vulnerabilities early and prepares for incidents before they occur.	Scheduled penetration tests, creating an incident response plan, and running simulated cyberattacks.
Stronger Encryption & Data Protection	Ensures confidentiality, integrity, and availability of data at rest and in transit.	AES-256 file encryption, HTTPS communication, and tokenization of sensitive information
User Education	Reduces risk from human error, phishing, and social engineering attacks.	Phishing simulations, security training programs, and interactive cybersecurity learning modules.
Intrusion Detection Systems (IDS)	Monitors systems and networks to detect suspicious activities or intrusions.	Deploying host-based IDS on servers and network-based IDS in smart factories or cloud services.

RESULT ANALYSIS

Various cybersecurity solutions made effective through their implementation enhance safety from internet threats immensely. The following are the main areas that illustrate how different defence systems work based on current applications and research reports:

Reduction in Cyber Attacks with AI and Machine Learning

AI-powered security systems identify threats in real time, minimizing the possibility of malware infections and phishing attacks.

Research indicates that AI-driven intrusion detection systems have the potential to block between 90% of cyber attacks through the early detection of suspicious patterns.

Effect of Zero Trust Security

Companies implementing Zero Trust Architecture (ZTA) experienced a reduction in unauthorized access attacks by 40-50%.

Tight authentication and ongoing authentication assist in reducing insider threats and avoiding data breaches.

Blockchain for Secure Transactions

Financial institutions that employ blockchain technology experience a substantial reduction in fraud cases and enhanced security for online transactions.

Decentralized security eliminates data tampering, lessening the chances of cyber attacks on sensitive financial data.

Efficiency of Multi-Factor Authentication (MFA)

Businesses that employ MFA have seen an 80% decrease in unauthorized account access.

Login security is boosted through the application of biometric authentication, OTPs, and security tokens to counter password-related attacks.

Encryption for Data Protection

Encrypted channels of communication like end-to-end encryption in messaging applications have brought down cases of data interception by a great extent.

Those organizations implementing encryption policies see less data breaches than those that work on old-school password protection.

Employee Awareness and Training Results

Organizations have seen a reduction of 60% in phishing attack success rates when they actually train their employees.

Frequent training session senable users to identify suspicious emails, links, and web threats and minimize human mistakes causing security compromises.

LITERATURE REVIEW

Szymoniak et al., presents an in-depth analysis of the state of security and defence in the Internet of Things (IoT), with an emphasis on protocols and systems like Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and secure communication protocols.

Alijumah et al., discusses several types of threats facing cloud computing and defence measures to counter them. It points towards data breaches as a major concern because there has been an utter lack of understanding of cloud services and defence mechanisms by the management.

Gilbert discusses about the history of cybersecurity defence measures, more specifically the adoption of artificial intelligence (AI). It addresses the application of AI in threat detection, response, and vulnerability management, as well as the ethical and adversarial issues presented by AI.

REFERENCES

[1] https://www.dataguard.com/blog/cyber-risk-mitigation-strategies

[2] https://www.isaca.org/resources/news-and-trends/industry-news/2024/the-top-5-cybersecurity-threats-and-how-to-defend-against-them

[3] https://www.upguard.com/blog/reduce-cybersecurity-risk
[4] https://arkag30.medium.com/cyber-security-defence-mechanism-70f1e5097e3d
[5] https://www.mdpi.com/2076-3417/15/2/499
[6] https://www.cloudflare.com/en-in/learning/security/glossary/what-is-zero-trust/
[7] https://www.chainalysis.com/blog/blockchain-security/
[8] https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
[9] https://indjst.org/articles/intrusion-detection-using-idmal-algorithm-for-iot-devices
[10] https://onlinelibrary.wiley.com/doi/pdf/10.1155/2021/5533843