INDIAN STREAMS RESEARCH JOURNAL
ISSN NO : 2230-7850
IMPACT FACTOR : 5.1651 (UIF)
VOLUME - 16 | ISSUE - 1 | FEBRUARY – 2026

RECENT TRENDS IN ARTIFICIAL INTELLIGENCE IN HEALTH CARE, INTERNET OF THINGS & CYBER SECURITY

Mr. S. Dinesh Kumar[1]
Research Scholar
Department of Computer and Information Science, Annamalai University, Annamalai Nagar, Chidambaram, Cuddalore District, Tamilnadu.

Dr. A. Saravanan[2]
Assistant Professor/ Programmer,
Department of Computer and Information Science, Annamalai University, Annamalai Nagar, Chidambaram, Cuddalore District, Tamil Nadu.

ABSTRACT

The rapid integration of Artificial Intelligence (AI), Internet of Things (IoT), and Cyber Security is reshaping the digital landscape. This article explores current trends, emerging models, challenges, and future research directions across these interlinked domains. With exponential data growth, intelligent automation, connected devices, and escalating threats, synergistic approaches are critical for resilience and innovation. The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) is rapidly transforming various industries and enabling innovative applications. In recent years, several trends have emerged in the application of AI in the IoT, including edge computing for real-time analysis, predictive maintenance, intelligent automation, smart homes and cities, and security. Edge computing enables IoT devices to perform real-time analysis and decision-making, while predictive maintenance allows for proactive maintenance and reduces downtime. Intelligent automation enhances the efficiency and effectiveness of IoT devices, while smart homes and cities enable IoT devices to adapt to the needs and preferences of their users. Security is becoming a more significant concern, and AI can be used to detect and prevent cyberattacks. Overall, the integration of AI with IoT has the potential to create a more intelligent and efficient world, and we can expect to see even more innovative applications emerge in the future.

KEYWORDS: *Artificial Intelligence (AI), Internet of Things (IoT), and Cyber Security, Intelligent automation enhances.*

1. INTRODUCTION

The convergence of AI, IoT, and Cyber Security marks a pivotal shift in computing and networking paradigms.

- AI offers machine cognition, prediction, and autonomous decision-making.
- IoT connects billions of devices, enabling real-time sensing and actuation.
- Cyber Security protects assets, data, and infrastructure from evolving threats.
- Collectively, they represent both opportunities and vulnerabilities in sectors like healthcare, industry (IIoT), smart cities, and finance.

2. ARTIFICIAL INTELLIGENCE: CURRENT TRENDS

2.1 AI Trends

Trend Description Impact.

Transformers & Large Language Models (LLMs) Self-attention mechanisms powering GPT-class models Better language understanding, reasoning. Explainable AI (XAI) Transparent models to interpret decisions Increased trust, compliance. Federated Learning Decentralized model training across devicesPrivacy-preserving learning AIoT AI integrated into IoT edge devices Low latency, real-time intelligence.

Applications of AI in Cybersecurity

1. *Password protection and authentication*

With AI in cybersecurity, organizations can better protect passwords and secure user accounts through authentication. Most websites include features that allow users to log in to purchase products or contact forms for people to input sensitive data. Extra security layers are necessary to keep their information secure and prevent it from getting into the hands of malicious actors.

AI tools, such as CAPTCHA, facial recognition, and fingerprint scanners enable organizations to automatically detect whether an attempt to log in to a service is genuine. These solutions help prevent cybercrime tactics like brute-force attacks and credential stuffing, which could put an organization’s entire network at risk.

2. Phishing detection and prevention control

Phishing remains one of the biggest cybersecurity threats facing businesses across all industries. AI within email security solutions enables companies to discover anomalies and indicators of malicious messages. It can analyze the content and context of emails to quickly find whether they are spam messages, part of phishing campaigns, or legitimate. For example, AI can quickly and easily identify signs of phishing, such as email spoofing, forged senders, and misspelled domain names.

ML algorithm techniques allow AI to learn from data to make analysis more accurate and evolve to address new threats. It also helps AI better understand how users communicate, their typical behavior, and textual patterns. This is crucial to preventing more advanced threats like spear phishing, which involves attackers attempting to impersonate high-profile individuals like company CEOs. AI can intercept suspicious activity to prevent a spear-phishing attack before it causes damage to corporate networks and systems.

3. Vulnerability management

As cyber criminals deploy more sophisticated methods and techniques, thousands of new vulnerabilities are discovered and reported every year. As a result, businesses struggle to manage the vast volume of new vulnerabilities they encounter every day, and their traditional systems cannot prevent these high-risk threats in real time.

AI-powered security solutions such as user and entity behavior analytics (UEBA) enable businesses to analyze the activity of devices, servers, and users, helping them identify anomalous or unusual behavior that could indicate a zero-day attack. AI in cybersecurity can protect businesses against vulnerabilities they are unaware of before they are officially reported and patched.

4. Network security

Network security involves the time-intensive processes of creating policies and understanding the network’s topography. When policies are in place, organizations can enact processes for identifying legitimate connections versus those that may require inspection for potentially malicious behavior. These policies can also help organizations implement and enforce a zero-trust approach to security.

However, creating and maintaining policies across multiple networks requires a significant amount of time and manual effort. Organizations often do not deploy the correct naming conventions for their applications and workloads. This means security teams may have to spend more time determining which workloads belong to specific applications. AI learns organizations' network traffic patterns over time, allowing it to recommend the right policies and workloads.

5. Behavioral analytics

With behavioral analytics, organizations can identify evolving threats and known vulnerabilities. Traditional security defenses rely on attack signatures and indicators of compromise (IOCs) to discover threats. However, with the thousands of new attacks that cyber criminals launch every year, this approach is not practical.

Organizations can implement behavioral analytics to enhance their threat-hunting processes. It uses AI models to develop profiles of the applications deployed on their networks and process vast volumes of device and user data. Incoming data can then be analyzed against those profiles to prevent potentially malicious activity.

2.2 Key Developments

Edge AI: Running inference near data sources to reduce latency and bandwidth.

Self-Supervised Learning: Models learn from unlabeled data, reducing dependency on costly annotations.

AI Governance: Ethical frameworks to prevent bias, ensure fairness and accountability.

3. INTERNET OF THINGS (IOT): EVOLUTION & TRENDS

3.1 IoT Market Growth

IoT devices are projected to exceed 30 billion connected devices by 2030 (industry research). This growth fuels automation across domains.

3.2 Architectural Trends

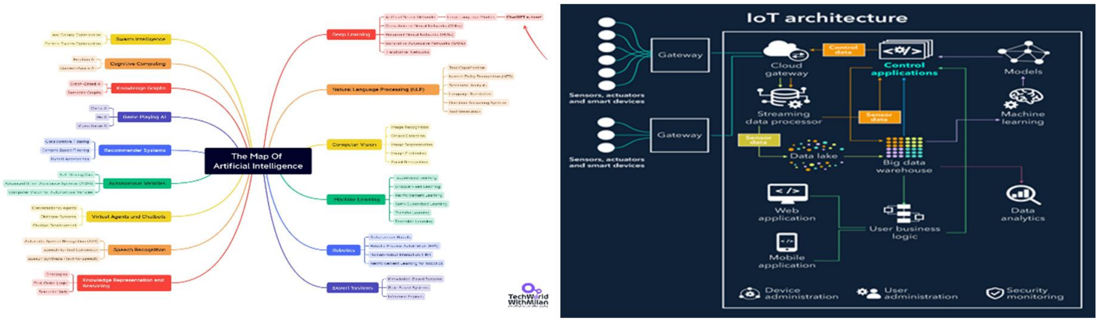

Figure 1: Typical IoT layered architecture from sensing to application.

3.3 Emerging IoT Technologies

5G & 6G Connectivity: Enables massive machine-type communication (mMTC) and ultra-reliable low-latency communication (URLLC).

Digital Twins: Virtual replicas of physical systems for simulation and optimization.

TinyML: Machine learning models optimized for microcontrollers.

4. CYBER SECURITY: TRENDS & CHALLENGES

4.1 Threat Landscape

With increased connectivity and automation:

- Ransomware attacks have surged.
- Supply chain vulnerabilities expose critical systems.
- Zero-day exploits target AI and IoT platforms.

4.2 Security Models

Figure 2: Cyber Security frameworks like Zero Trust and Defense in Depth.

4.3 Modern Security Trends

- Zero Trust Architecture (ZTA): Never trust, always verify users and devices.
- AI-based Threat Detection: Machine learning identifies anomalies in real-time.
- Security Orchestration, Automation and Response (SOAR): Reduces incident response time.

5. INTERSECTIONS: AI + IOT + CYBER SECURITY

The triad creates both innovation and risk.

5.1 AI for IoT Security

- AI enhances IoT safety through:
- Anomaly detection in device behavior.
- Predictive threat intelligence.
- Adaptive policies responding to threats dynamically.

5.2 IoT Data & Privacy

Challenges:

Massive telemetry data from IoT devices increases attack surface.
Privacy violation risks with personal or health information.

5.3 Secure Learning Systems

Federated learning with encrypted updates improves:

Model utility across devices.
Data confidentiality.

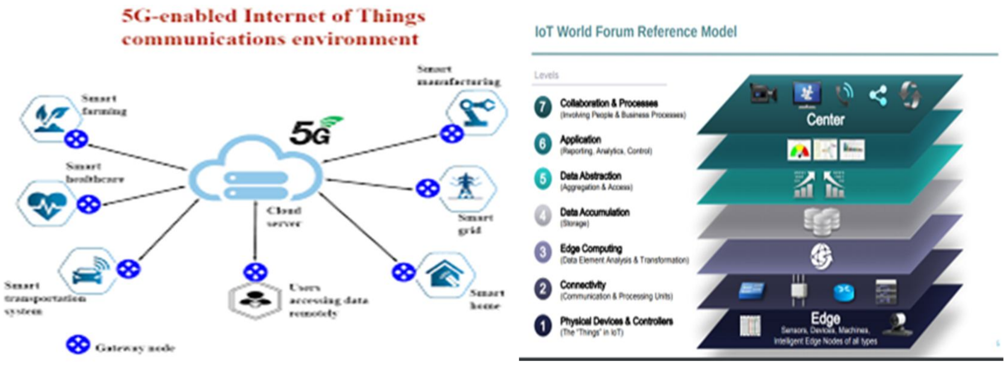
5G-enabled Internet of Things communications environment
Smart farming
Smart healthcare
Smart transportation system
5G
Cloud server
Users accessing data remotely
Smart manufacturing
Smart grid
Smart home
Gateway node
IoT World Forum Reference Model
Levels
7 Collaboration & Processes (Involving People & Business Processes)
6 Application (Reporting, Analytics, Control)
5 Data Abstraction (Aggregation & Access)
4 Data Accumulation (Storage)
3 Edge Computing (Data Element Analysis & Transformation)
2 Connectivity (Communication & Processing Units)
1 Physical Devices & Controllers (The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines, Intelligent Edge Nodes of all types

Figure 3: Hotspot intersections among AI, IoT & Cyber Security.

6. CASE STUDIES

6.1 Smart Healthcare

Wearable IoT sensors collect patient vitals.
AI predicts health anomalies.
Secure channels (TLS/SSL) and blockchain help protect patient data.

6.2 Smart Manufacturing (Industry 4.0)

IoT sensors optimize production.
AI ensures predictive maintenance.
Security monitoring prevents sabotage or data breaches.

7. CHALLENGES & OPEN ISSUES

- Area Key Challenges
- AI Model bias, explainability, energy consumption
- IoT Interoperability, firmware vulnerabilities
- Cyber Security Dynamic threat adaptation, talent shortage
- Integration Secure edge intelligence, scalable trust models

8. FUTURE DIRECTIONS

- **Quantum-Resilient Security:** Prepares cryptography for quantum attacks.
- **Self-Healing Systems:** AI that autonomously repairs vulnerabilities.
- **Regulatory Frameworks:** Stronger laws for data protection (GDPR, emerging AI acts).

9. CONCLUSION

The synergy of AI, IoT, and Cyber Security presents a powerful yet challenging frontier. Innovations in intelligent automation and interconnected devices deliver efficiency and value. However, robust security frameworks and ethical governance must evolve in parallel to safeguard digital ecosystems.

• REFERENCES & SUGGESTED READINGS

1. Goodfellow et al., Deep Learning (MIT Press) — foundational AI concepts.
2. Gartner IoT Forecast — device and connectivity projections.
3. NIST Cybersecurity Framework — industry best practices.
4. IEEE Transactions on Information Forensics and Security — research articles on AI & security.
5. Evans D. The Internet of Things: how the next evolution of the internet is changing everything. Cisco Internet Business Solutions Group: Cisco; 2011.
6. Lu Y, Xu LD. Internet of Things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. 2019;6(2):2103–15.
7. Farivar F, Haghighi MS, Jolfaei A, Alazab M. Artifcial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE Trans Ind Inf. 2020;16(4):2716–25. https://doi.org/10.1109/TII.2019.2956474.
8. Vorakulpipat C, Rattanalerdnusorn E, Thaenkaew P, Hai HD. Recent challenges, trends, and concerns related to IoT security: aan evolutionary study. In: 2018 20th international conference on advanced communication technology (ICACT), Chuncheon-si Gangwon-do, Korea (South); 2018. p. 405–10.
9. Linthicum D. App nirvana: when the internet of things meets the API economy. https://techbeacon.com/app-dev-testing/app-nirvana-wheninternet-things-meets-api-economy. Accessed 15 Nov 2019.
10. Lakhani A. The role of artifcial intelligence in IoT and OT security. https://www.csoonline.com/article/3317836/the-role-of-artificial-intelligen ce-in-iot-and-ot-security.html. Accessed 11 Feb 2020.
11. Roopak M, Yun Tian G, Chambers J. Models deep learning, for cyber security in IoT networks. In: IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA. 2019;2019:0452–7.
12. Radanliev P, De Roure D, Van Kleek M, Santos O, Ani U. Artifcial intelligence in cyber physical systems. AI & society. 2020; p. 1–14.
13. Cañedo J, Skjellum A. Using machine learning to secure IoT systems. In: 2016 14th annual conference on privacy, security and trust (PST), Auckland; 2016. p. 219–22, https://doi.org/10.1109/PST.2016.7906930.
14. Wang S, Qiao Z. Robust pervasive detection for adversarial samples of artifcial intelligence in IoT environments. IEEE Access. 2019;7:88693–704. https://doi.org/10.1109/ACCESS.2019.2919695.