Deep Science Publishing, 2025
https://doi.org/10.70593/978-93-7185-625-6_7

Chapter 7: Security and Privacy Challenges in AI-IoT-Cloud Convergence Architectures

7.1. Introduction

The continuous advancements in Artificial Intelligence (AI) and the Internet of Things (IoT) allow the intelligent and efficient integration of connected devices and services. The integration of AI into the IoT system architecture enhances the operational management of IoT services and devices. Also, it supports other horizontal services, Â as intrusion detection, authentication, addressing schemes, and security enhancement. Employing AI technologies at the IoT layer is limited due to data, computing, and storage-resource constraints.

Cloud computing platforms function as a central data repository and offer abundant resources from the infrastructure layer. Network capacity can also be added on demand for wider connectivity and faster response times. The integration of AI, IoT, and cloud computing facilitates a broad range of emerging applications capable of supporting both horizontal and vertical services for the Internet of Everything (IoE). Access to massive data from IoT services and devices also supports advanced training of the AI system through cloud-based resource sharing. However, the AI-IoT-cloud integration also raises security and privacy concerns related to data protection, owing to the dependence on centralized cloud resources for processing.

7.1.1. Purpose and Scope of the Study

The rapid convergence of artificial intelligence (AI), the Internet of Things (IoT), and cloud computing provides considerable benefits for users and numerous opportunities for society and the economy. While AI-IoT-cloud systems will remain valuable, their protection represents a continuous challenge because of the complexity and heterogeneity of these systems and the aforementioned opportunities for the users and the economy. This paper describes security and privacy concerns related to AI-IoT-cloud

systems and summarizes current technological solutions. It also outlines directions for future research.

These three components are critical for future cybersecurity efforts. The emerging framework presented in this paper offers a comprehensive overview of the latest AI-IoT-cloud security trends and discusses key research problems for future cybersecurity development. As data generation and processing from IoT devices surpasses the capabilities of cloud platforms, integrating AI at the network edge through edge computing offers numerous advantages. This integration of AI, IoT, and cloud technologies forms the AI-IoT-cloud convergence framework, which enables distributed data processing that is unmatched by cloud-only solutions.

7.2. Overview of AI-IoT-Cloud Convergence

Over the past six years, the evolution of three pillars—Artificial Intelligence (AI), Internet of Things (IoT), and Cloud Computing—has individually garnered tremendous attention in the domain of Intelligent Systems. AI has significantly advanced due to the availability of extensive datasets, forsaking earlier constraints stemming from limited information. In parallel, IoT has revolutionized the traditional Internet, facilitating rapidly evolving connections among smart devices. Cloud Computing has become ubiquitous, offering the backbone for intelligent data storage and processing. Despite their successes, the true potential of these pillars remains untapped: IoT's full capabilities are unrealized without the benefits of AI and Cloud Computing, likewise true of AI and Cloud capabilities without IoT-generated data.

The intrinsic dependencies among these three important areas have been conceptually recognized for some time, with initial efforts documenting the role of Cloud Computing in AI and IoT domains. Detailed descriptions of integrating AI and Cloud have been presented, underscoring the symbiotic relationship between the two. However, it is only recently that a holistic approach emphasizing the convergence of AI, IoT, and Cloud has emerged, positioning Cloud Computing as the foundation for future AI developments using data from IoT networks. Advancements in Cloud, IoT, and AI are expected to produce an intelligent system so powerful that it will complement and enhance human intelligence[1-3].

7.2.1. Key Concepts and Frameworks in AI-IoT-Cloud Integration

The integration of Artificial Intelligence, Internet of Things, and Cloud computing transforms the technology landscape. Research overviews integration frameworks, including three frameworks for AI-IoT integration, key enablers and intelligence levels

within the IoT-IoT integration framework, and insights from an industry perspective on the combined use of AI, IoT, and cloud computing—namely the Artificial Intelligence of Things (AIoT). A general architecture for enabling AI within an IoT network identifies five key layers: perception, network, data processing, service, and security. Research identifies the suitability of the 5G network for the AIoT framework, and a multi-dimensional architecture for AIoT integration encompasses components for sensing and spectrum management, data processing and transmission, and AI network application.

Based on a systematic literature review, a three-layer AIoT framework links AI cloud services to IoT layers through four types of AI technologies: learning, goal-orientation, knowledge, and reasoning. AI-IoT integration is evaluated against four performance goals: user privacy, service security, edge resource management, and service scheduling. A conceptual framework for AI-IoT integration within an Industry 4.0 context relates features of AI, IoT, edge computing, 5G, and industrial applications. Although these frameworks do not specifically address an AI-IoT-cloud concept, they are well-positioned to enable the integration of cloud computing towards security and privacy assurance.

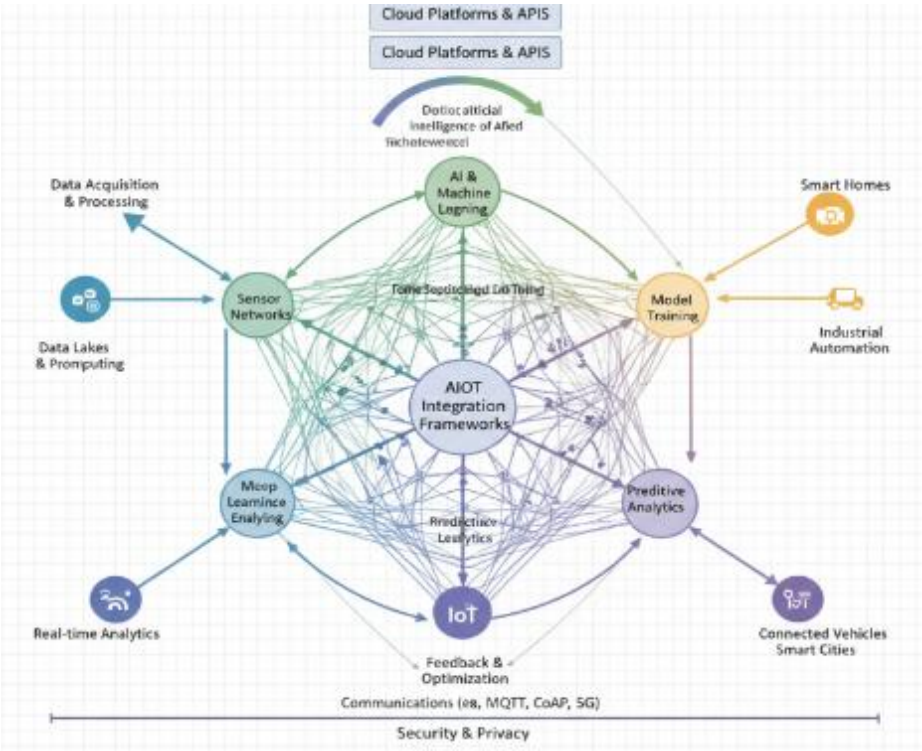

Fig 7 . 1 : The Artificial Intelligence of Things (AIoT) Integration Frameworks

7.3. Security Challenges in AI-IoT-Cloud Systems

At every level of the AI-IoT-Cloud architecture, the security risks and challenges are enormous. At the AI layer, deep learning itself acts like a black box that can be vulnerable to adversarial attacks designed to fool deep learning models via small perturbations or completely new synthetically created samples that look like real data to humans but are deceptive to the underlying deep model. Data poisoning attacks at the AI level can create serious risks to systems that rely on human-annotated data for training, an aspect that is becoming more evident with the proliferation of open-sourced foundation models trained on webscraped data with little understanding or control of the data provenance. Moving down to the IoT layer, some of these connected IoT devices operate real-time physical processes, and hence, integrity is of foremost concern, so that if these devices are hacked, the integrity of the physical processes is not compromised. The real-time operation of these systems also requires very high availability with minimal latency, and hence, the system has to be designed for such operation. For IoT devices that are deployed in a remote location, a lack of configurability or updates can create serious risks to the system over their lifecycle. On the other hand, some of these capabilities, such as programmability or reconfigurability, can be leveraged to insert malicious hardware Trojans, especially during the manufacturing of these devices, an aspect that raises an important consideration for supply chain security. Another very important concern at the IoT layer is privacy. Many of these IoT devices are capturing information from the user within the privacy perimeter of the user, and the system has to safeguard such information and not use or allow such private information to be sold to other entities.

At the level of the cloud services, the security provided by these services is, in fact, a use case for the AI-IoT-Cloud architecture itself [2,4,5]. These services provide attack detection and forensics capabilities for the huge volume of telemetry data that is generated by the cloud edge. The services themselves leverage techniques from artificial intelligence and data analytics, as well as an understanding of the behavior of the underlying cloud infrastructure to perform attack detection and forensics. At the level of the networking connectivity connecting the cloud and the IoT devices, ensuring security and privacy of the communications remains an important consideration, with approaches such as quantum key distribution being explored as potential solutions. A recent approach emerging is to allow all devices to have their inventory that includes a cryptographic binding between their identity and their physical properties. Using hardware attestation, the network can verify that the inventory has not been tampered with and, based on the hardware properties of the device, implement fine-grained access control on the network, allowing only the desired functions on the device to access a specific part of the network, based on a zero-trust philosophy of network security.

7.3.1. Threat Landscape

Security and privacy challenges in the AI-IoT-cloud convergence are agents of a very diverse threat landscape. A running list of threats is presented to provide a view of attacks and malicious activities for which the convergence must be resilient.

The classic cyberattack examples in IoT are the man-in-the-middle, replay, impersonation, or Denial-of-Service (DoS). Intrusions in an IoT system can be addressed through the traditional proxy, firewall, Demilitarized Zone (DMZ), or Intrusion Detection System (IDS). The Open Web Application Security Project (OWASP), meanwhile, has published the top ten security threats for IoT. Apart from such known threats that have long been mitigated, the convergence creates novel vulnerabilities arising from interlinked operations of the AI, IoT, and Cloud.

7.3.2. Vulnerability Assessment

A comprehensive evaluation of the latest IoT-cybersecurity and related security standards, guidelines, good practices, and reports from international organizations reveals that the continuous assessment of vulnerabilities is stressed, is paramount, and must be conducted by the organization. Vulnerability assessment is a critical aspect of the proposed security frameworks, standards, and guidelines of IoT, ICS, WAS, etc., and must be included in the ongoing security strategy. Many organisations still use a manual approach to security assessment, report generation, remediation, and report distribution. However, there is a simple way to automate the security testing procedures. This methodology encompasses a group of phases that include information gathering, penetration testing, vulnerability assessment, penetration report generation, and report distribution among the stakeholders.

In particular, the vulnerability-assessment phase is considered, with a detailed description presented [1,3,5]. The concept of an automated assessment mechanism for IoT, as proposed in the cited study, serves as a starting point. In addition, a meta-automation strategy is introduced to simultaneously execute multiple Automated Security Assessment Distribution Framework (ASADF) workflows by testing several networks or devices across different organisations. Both the IoT Cybersecurity Assessment Framework and the Conceptual Meta-Formalization of the Automated Security Assessment Distribution Framework are formalized. It should be noted that the meta-automation procedure can be applied to any workflow for various IoT cybersecurity-related activities, especially when applied to Operating Technology, Industrial Control Systems, Wireless Automation Systems, and Cloud and Wi-Fi environments.

7.3.3. Attack Vectors

Before selecting a specific architecture for an AI-IoT-cloud application, it is essential to understand the nature of the data streams and the resulting analysis that subsequent streams undergo. This analysis typically occurs at different levels, making managed services focus on various stages of the stream, depending on the required services. In an AI-IoT-cloud architecture, where data transitions between managed services and different layers of the architecture, each of these boundaries represents a potential point of exploitation. Table 2 presents the vulnerabilities and attack vectors associated with the various security boundaries in the layered architecture that supports AI-IoT-cloud workloads.

These vulnerabilities and attack vectors serve as preliminary indicators of data and analytics sensitivity, guiding the choice of the most appropriate architecture. The figure further plots contrasting dimensions of processing locations and data movement, revealing that decisions in one dimension can complement choices in another. For example, reducing data movement inside a supervised algorithm can be achieved by employing a hierarchical approach that also localizes sensitive data close to the devices.

Description of Layer 0 Vulnerabilities and Attack Vectors. Besides devices with little or no computing capabilities, there are also weakest links in the layered architecture: authentication servers. If the authentication server is compromised, attackers can generate valid authentication tokens for a particular service or system area. In this way, honeypots can be prepared to lure people into a specific area or to enable safe penetration testing.

7.4. Privacy Concerns in Data Handling

Privacy is a paramount concern in the implementation of convergence architectures, especially when wireless technologies form part of the infrastructure. Large amounts of data are collected, processed, and transmitted. Beyond personal information, this data includes movement and behavior patterns of users, which are particularly delicate when concerning sensitive groups such as children, seniors with disabilities, or other vulnerable populations [6-8]. Consequently, any breaches in security could have severe privacy implications, with individuals potentially being harmed as a result of data theft.

Several fundamental assets are considered critical for ensuring the security of AIoT-Cloud convergence architectures. Privacy remains a key asset, as private information of the data owners is at risk of being leaked by eavesdroppers during different stages: data transmission from the user's environment to IoT artifact nodes, from these nodes to cloud services, and finally, within the AI application services themselves, especially during the training of deep learning models applied to these data. The high sensitivity of the data

generated within the convergence architecture renders any compromise of the privacy asset particularly dangerous for the individuals involved.

7.4.1. Data Collection Practices

Aware of emerging regulations on the horizon, AIoT manufacturers are beginning to rethink their data collection practices and deciding—at the beginning of the design and manufacturing process—whether their AIoT product should be collecting sensitive or private data at all. Some AIoT devices, such as smart home speakers, are incapable of providing sensible services without collecting sensitive data, and manufacturers can only try to improve protections on that data. Other devices, such as a smart speaker housed in an auto mechanic's shop, might be better off not collecting sensitive data in the first place, even if doing so makes the device a little less "smart."

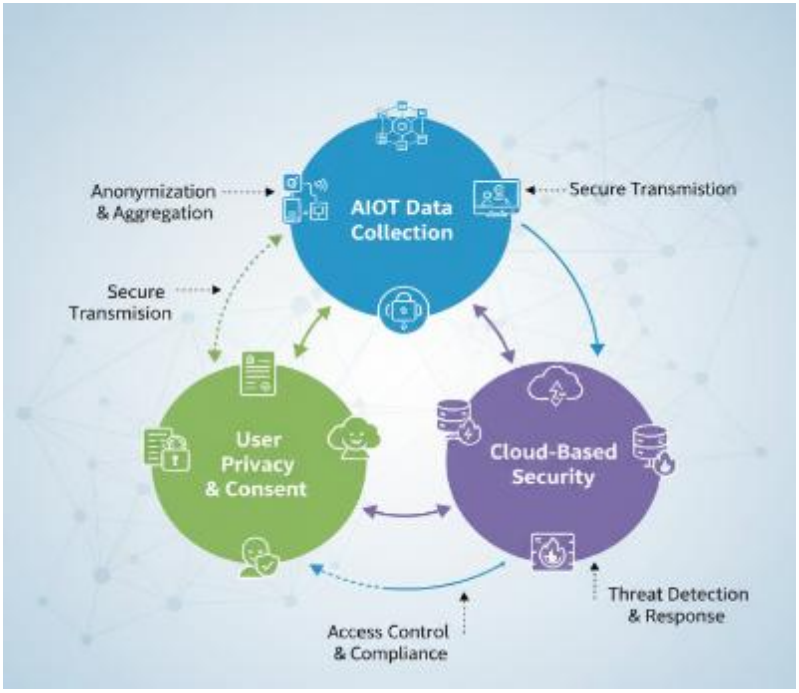

Fig 7 . 2 : AIoT Data Collection, Privacy, and Cloud-Based Security

Regardless of the device's function and the nature of the data it collects, some researchers recommend that devices collect as little raw data as possible, thereby reducing their associated security and privacy risks. For instance, malware detection capabilities can be provided to smartphones by the cloud rather than through a local on-device malware detection system. Using the cloud's much greater processing power, the on-phone system can be simplified by focusing on collecting and sending data to detect malware. Such data might include recent phone calls and text messages, recently

installed apps, and package names of sensitive permissions. By then performing the malware detection function in the cloud, there is no longer a need for an onboard malware detection system, thereby reducing raw data levels on the phone.

7.4.2. User Consent and Control

Most of the literature related to surveillance assumes the consent of the public in public spaces. However, the general public lacks control over how such data is used and shared. It then raises the issue of privacy and intrusion. According to the Cambridge Dictionary, it is an "act of intentionally interfering in a situation in a way that is annoying or upsetting other people" (https://dictionary.cambridge.org/grammar/british-grammar/interference-or-intromission).

To address these concerns, it is especially prudent to keep humans in the loop. Researchers underline the importance of keeping humans in the loop by enabling user control. The main users and stakeholders would include companies, administrators, and security personnel of private and government buildings or streets. At the same time, the uninvolved public, such as customers and passersby, could opt out from being documented by a surveillance system.

7.4.3. Data Anonymization Techniques

The extraction of useful information from uploaded data without compromising privacy has gained significant attention. According to the China Internet Network Information Center's 50th Statistical Report on Internet Development, privacy protection ranks fourth among Chinese netizens' urgent needs. Before data is uploaded, it must be encrypted and anonymized to prevent privacy disclosure and address data security vulnerabilities. Privacy-preserving data collection enhances the accuracy of data collection in an untrusted network environment and can be executed with low computational demands. Privacy-preserving aggregation aims to reduce the computational and communication burden on data collectors, improving efficiency.

The Lagrangian relaxation algorithm increases privacy time series data release, with the FastTF method offering secure and swift mobile traffic data release through efficient aggregation. An improved generative model, accommodating all deformation fields, reduces the dimensionality of input features and employs a deep convolutional architecture for more accurate gravity inversion estimations. A privacy-aware data collection scheme allows data collectors to obtain accumulated utility under differential privacy constraints, bounding individual privacy disclosure risks. An end-to-end encrypted data collection scheme extends FastPriFi to asynchronously handle dynamic

group membership by adopting Lagrange Coded Computing. Privacy-preserving data aggregation based on Fog computing reduces communication costs for data aggregators and prevents exposure of power usage or payment information during Security and Privacy in AI-IoT-Cloud Convergence Architecture.

7.5. Regulatory Frameworks and Compliance

Cross-domain data-driven services enable new interactions between objects, such as connected cars and human users in their environment, through leveraging data gathered from multiple verticals. In such cases, requirements guidelines such as the automotive safety standard ISO 26262 and functional safety concepts need to be considered. Cross-domain services also commonly introduce storage and processing services that utilize multi-tenant Public clouds such as Amazon Web Services (in particular Amazon S3 and Amazon Glacier). This means that regulatory frameworks, such as the European General Data Protection Regulation, must be considered.

Privacy and confidentiality rules must be maintained; that users' privacy, geographic and jurisdiction concerns are not violated; and that data cannot be accessed and controlled by parties that do not have such rights. It is worth noting that many utilities are currently provided from within the cloud by the Public Cloud vendors themselves, and thus every customer could be vulnerable if they experience a breach of a shared cloud utility or infrastructure.

7.5.1. GDPR and Its Implications

The General Data Protection Regulation (GDPR) was adopted by the European Parliament in April 2016 and became enforceable on May 25, 2018. It applies to all companies processing the personal data of individuals residing in the European Union, regardless of the company’s location. The primary goals of the GDPR are to ensure data protection and privacy for citizens and residents of the European Union and to address the export of personal data outside the EU. Non-compliance can result in severe fines amounting to millions of euros.

The GDPR grants several rights to consumers regarding their data processing. Consumers have the right to access, correct, or delete their data and to control its usage by consenting or revoking consent under specified circumstances. Organizations handling large quantities of personal data of EU citizens must designate a Data Protection Officer (DPO). Additionally, data controllers are required to notify data protection authorities and data subjects about data breaches within 72 hours of becoming aware of the breach.

7.5.2. CCPA Overview

The California Consumer Protection Act provides rights to Californian consumers that include the ability to learn what personal data companies have collected from them, request the deletion of some of the collected data, and opt out of the sale of their information to third parties. These provisions provide an appreciable safeguard to consumers in California regarding how their private information can be collected, stored, and utilized by organizations. Although the CCPA was specifically designed for residents of California, its reach extends to any company (anywhere in the world) that collects, processes, shares, trades, markets, or sells personal data of California citizens. Consequently, CCPA has the potential to impact a very significant portion of enterprise AI-IoT-Cloud business operations.

7.5.3. International Regulations

Security challenges in AI-IoT-Cloud convergence architectures are a complex and multifaceted subject. The discussion considers the size and distributed nature of the infrastructure, the specific roles of the cloud, AI, and IoT components, and the critically important potential impact of successful attackers. The mitigation challenges are playing out on multiple fronts, from the components at work in the converged infrastructure, to the defining characteristics of the converged AI-IoT-Cloud environment, to the shared global infrastructure on which the underlying ICT technologies depend. Privacy concerns are considered from two perspectives: the overarching privacy-related challenges and the GDPR-related aspects of international regulations. Finally, privacy-protecting approaches and directions for future research are examined.

The breadth and depth of the security challenges are clearly illustrated by considering the wide range of threat types that must be addressed. Taking a supply-chain perspective for the converged infrastructure, key challenges include ensuring that the components, software, and firmware are legitimate and trustworthy. For the operational environment, the diverse attack vectors pose significant risks, for example, through IoT devices (botnets, malware, protocols, configuration and password management, device management, vulnerabilities, sniffing), AI models and containers, open APIs, VM instance sprawl, SDN, system data, investigations, and logs. The consequences of being attacked span multiple levels in the AI-IoT-Cloud environment: data, model, service, application, platform, and coalition. Finally, attacks that affect the global ICT infrastructure may have unanticipated repercussions for the AI-IoT-Cloud infrastructure, with technologies such as the Domain Name System being especially vulnerable.

7.6. Technological Solutions for Security

Technological solutions that address the security and privacy challenges in the AI-IoT-Cloud Convergence Architecture must be carefully considered. Key objectives include the secure sharing of data and models for enhancing performance and the integration of intelligence. Blockchain technology, a decentralized ledger, assures data immutability and transparency by publicly recording all transactions. Two key properties are non-repudiation, ensuring a user cannot deny actions on the ledger, and traceability, enabling the tracing of transactions and users involved.

Smart contracts serve as a mutual agreement between involved parties, deploying self-executing code with defined execution conditions on the ledger. The immutability property of the transaction plays a vital role in security enhancement. For instance, integrating blockchain in deep learning frameworks mitigates model poisoning attacks by recording model hashes on the ledger.

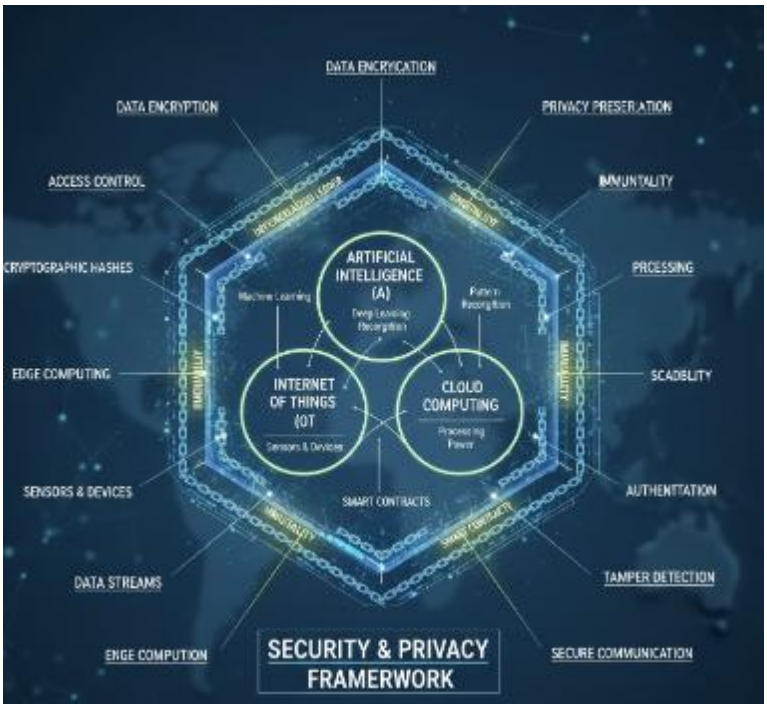

Fig 7 . 3 : Blockchain for Security and Privacy in AI-IoT-Cloud Convergence

7.6.1. Encryption Methods

Encryption plays a crucial role not only in cybersecurity but also in securing Internet of Things (IoT) devices. The lack of robust security in most public-key-encrypted approaches can be tackled by making the key nonrepudiable and leveraging blockchain

technology. In the realm of cloud communications, a practical solution to active man-in-the-middle attacks involves encrypting and securing user device data within the cloud before transmission. Employing cipher-text policy attribute-based encryption (CP-ABE) allows only those users with the specified attributes held by the authority to decrypt the ciphertext, effectively mitigating such attacks.

These concepts also extend to machine learning approaches. By obfuscating feedforward neural networks or encrypting their activations and weights, the neural networks themselves become vulnerable to attacks, necessitating the application of fully homomorphic encryption (FHE) to protect these elements [5-7].

7.6.2. Access Control Mechanisms

Access control is a fundamental feature in enterprise security that ensures that only authorized users and processes can access the organization's resources. Access control models are mechanisms that implement access control policies to guarantee the security of assets. Various models support different organizational needs and offer unique advantages and disadvantages.

The simplest access control model is Discretionary Access Control (DAC), which manages access permissions based on identity. Users can change objects and assign permissions to other users, with a central administrator overseeing all objects. Another approach, Rule-Based Access Control (RBAC), grants permissions to users and roles based on a set of rules implemented by the administrator. Lastly, Role-Based Access Control (RBAC) merges aspects of the previous models, enabling permissions and roles to be assigned to users with administrative regulation.

7.6.3. Intrusion Detection Systems

Intrusion Detection Systems Intrusion detection systems (IDSs) monitor and analyze the events taking place in a computer or network and are mostly specified for the detection of time-critical adverse events. Intrusion detection techniques follow two main approaches:

Signature-based detection: It detects known attacks using rules derived from the signatures of known threats. The key advantage of signature-based detection is the low false-alarm rate. However, it cannot detect new or unknown attacks.

Anomaly-based detection: It detects attacks by creating a profile of normal system or network behavior. Anomalies are detected when the activity of the system deviates from the normal profile. Anomaly-based detection can detect new and unknown attacks, but

it suffers from a high rate of false alarms. Based on data sources and deployment methods, intrusion detection can be classified as follows:

Host-based intrusion detection systems (HIDSs): These are deployed on individual hosts and monitor host logs, processes, and file system changes as the data sources for intrusion detection.

Network-based intrusion detection systems (NIDSs): These use networks as data sources. NIDSs analyze the network traffic for potential attacks against the resources inside the network. Many IDSs hybridize the above methods to build hybrid intrusion detection systems (HIDS).

7.7. Future Directions in AI-IoT-Cloud Security

One promising innovation that addresses many of the security and privacy challenges in the AI-IoT-Cloud convergence is federated learning. Instead of sending sensitive data to a centralized cloud, federated learning trains a machine learning model using data from all organizations without the need for sharing or transferring any data or allowing other organizations direct access to raw data. Advanced cryptographic measures ensure that the training data of one organization remains unidentifiable to others throughout the training process.

While still in its infancy, federated learning holds immense promise for AI security and privacy and for the solution of security and privacy threat vectors arising in the AI-IoT-Cloud convergence. As an increasingly attractive research direction, it addresses many of the concerns associated with offloading sensitive data and training to a centralized cloud. Despite its current nascency, federated learning ensures that the training data of participating organizations remains private and unidentifiable throughout the training process. Enhancements to the architecture are feasible and desirable, provided that the organization participating in training needs access to only the model stored in the cloud, and neither the raw training data nor the associated gradients need to be uploaded.

7.7.1. Emerging Technologies

The combined application of Internet of Things (IoT), cloud computing, and Artificial Intelligence (AI) technologies will lead to fully connected Internet of Everything (IoE) platforms that integrate all the fundamental components of the ecosystem. This integration covers people and devices at one end of the platform and advanced applications and services at the other, seamlessly converging and collaborating across a fully connected ecosystem. The IoE is envisioned to support the increased levels of smartness for human–machine and machine–machine interactions. The driving force

behind these three technologies stems from their inherent capabilities and features. Broad application of the IoT is driven by the need to sense and detect everything of interest, positioning the cloud as the technology that provides the support infrastructure with infinite resources, with the ability to elastically accommodate variations in the load on an on-demand basis. This resource core supports emerging AI services, and in the future, it is proposed as an integral part of the IoE support infrastructure. Predictive analytics is a significant capability within AI services because it can forecast possible faults and deviations, enabling timely preventive measures.

7.7.2. Trends in Cybersecurity

Artificial intelligence (AI) is a branch of computer science focusing on developing systems capable of intelligent behaviour. Its applications extend to expert systems, natural language processing, speech and voice recognition, machine vision, robotics, automatic control, and decision management systems. Machine learning (ML) enables computers to learn from data, while deep learning (DL) is a subset of ML, consisting of multilayer artificial neural networks that simulate brain behaviour to solve complex computational problems. These advanced technologies have become integral to cybersecurity solutions, automating repetitive tasks and rapidly analysing activities within networks and systems [7-9]. They also support the development and evolution of security management, compliance, vulnerability and risk management, adaptive security, and cyber-disruption detection, diagnosis, response, and prediction.

Machine learning is playing a decisive role in controlling the coronavirus pandemic. Scientists use ML to detect the outbreak's next location, track the virus in real-time with the help of data analytics, and help identify the primary as well as secondary symptoms. The emerging capabilities of ML are assisting health professionals and governments by forecasting the pandemic's surge. AI-ML is helping in research and development related to the discovery of promising drugs for the coronavirus. ML can also help include the prediction of viruses and their possible mutations.

7.7.3. Research Gaps and Opportunities

AI-IoT-Cloud convergence systems combine two evolving paradigms, IoT and AI, and provide a flexible IoT system with intelligence. Nevertheless, these systems become attractive to many malicious users because they repeatedly connect numerous devices, servers, or applications in a single system and exchange data. Therefore, proposed AI-IoT-Cloud security and privacy issues are mainly divided into two: intrusion detection removal and cryptography. The former is researched through ML techniques, which determine the type of attack, and subsequently prevent the AI-IoT-Cloud services from

intrusion. The latter analyzes the security and privacy because of the sensitive user data exchange of the AI-IoT-Cloud system. As a result, cryptographic techniques with ML are studied. However, research in this area is still in its infancy.

The constantly growing number of cybersecurity dangers, including malware such as attackers and crackers, is uncannily comparable to Michael Faraday's linear transmission, which is inextricably linked to the exponential increase in the scale of Internet of Things (IoT) devices. Everyone has seen a spike in DDoS attack growth since the utilization of IoT devices went out of control, albeit for a rather brief period. For researchers in cybersecurity, the field of AI, especially deep AI architecture, presents itself as a fresh and promising field of study. This work focuses on traffic analysis and the early prediction of malware on the network by developing a deep learning model for the early recognition of malware that may be forthcoming on the network. It is based on a dataset of public traffic records.

7.8. Conclusion

The security and privacy challenges of AI-IoT-Cloud converged architectures are highlighted, together with several potential solutions. The state of the art for network-enabled security and privacy solutions is presented in order to showcase the different approaches taken through the integration of AI into Cloud computing and IoT networking domains.

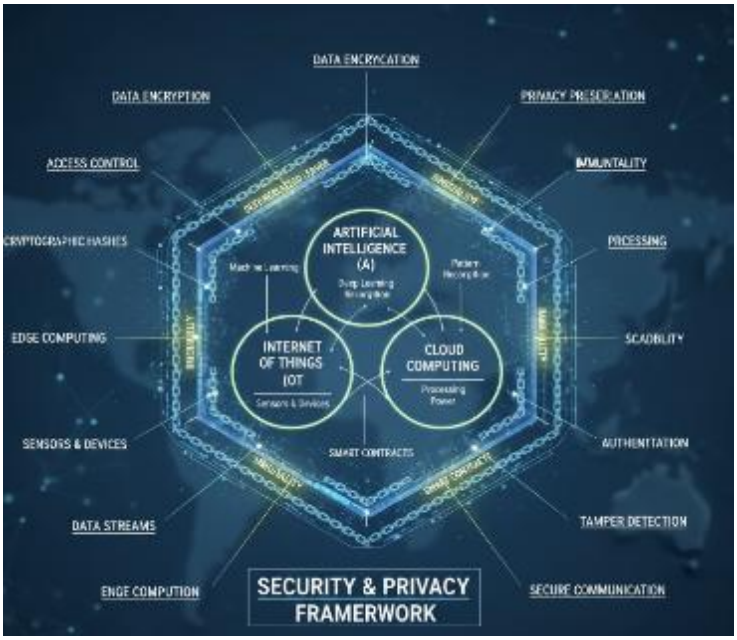

Fig 7 . 4 : Future Focus & Enablers for Converged Security

The analysis of the security primordia of the AI-IoT-Cloud paradigm is of paramount importance for achieving a full realisation of the Convergence Architecture, capable of withstanding modern cyber-attacks. When addressing ICN naming challenges in the Convergence Architecture, the choice of name is of vital importance in providing a varying degree of content verification, privacy-awareness, and routing efficiency towards both content and IoT devices. While the threat detection capabilities of DL are leveraged to enhance NDN's traffic monitoring solutions, the train-of-thought mechanism of the Transformer model improves the semantic awareness of the Convergence Architecture, enabling the detection of anomalies that would potentially elude an isolated IoT or Cloud perceptron. Following the emergence of 5G NTN, the Convergence Architecture security layer is well positioned to support novel services for high-mobility and remote-area coverage. M2M devices must reside within a secure perimeter before accessing network resources to prevent the exploitation of back-end services. Finally, deterministic M2M services require the fine-tuning of the Convergence Architecture components to conform to strict latency, bandwidth, and reliability constraints.

7.8.1. Summary and Key Takeaways

The following presents a concise overview of recent advances in the deployment of artificial intelligence (AI) in Internet of Things (IoT) applications, reflecting a broad survey undertaken during 2019 and 2020. These rapidly evolving areas have generated a huge number of scientific and commercial projects that involve AI techniques assembled in IoT solutions. The enabled applications span smart cities, smart health, social/medical assistants, smart robots and drones, and autonomous navigation. The challenges and advantages of AI in terms of the architectural hierarchy of cloud, fog, and edge processing are analysed and discussed. Finally, the security challenges open to the community in the transition from distributed IoT research to AI deployment for IoT sensors are outlined, completing a global analysis of the AI-IoT-Cloud framework.

The AI research community and the IoT application community both have clear indicators: from the AI perspective, sensor and actuator behaviour can be controlled and guided by AI networks that provide training and control data; from the IoT perspective, a huge number of sensors can be connected and completely managed, delivering data for AI system training and functioning. The IoT community is developing and providing potential input data for AI systems using a vast community of interconnected, low-cost sensors; the AI community can leverage the increasingly popular IoT systems to support the implementation of more sophisticated, yet scalable, new applications.

References

[1] Singh KD. (2023). Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics. EAI Endorsed Transactions on AI and Robotics, 2(1). https://doi.org/10.4108/airo.3616

[2] Munnangi, A. S. M., Reddy Koppolu, H. K., Nayeem, S. M., Polineni, I., & Reddy Munnangi, S. (2025). Experimental Measurements, Molecular Dynamics Simulations, and Machine Learning Predictions for the γ-Butyrolactone–N, N-Dimethylacetamide Binary System. ChemistrySelect, 10(28), e02391.

[3] AI-Based Financial Advisory Systems: Revolutionizing Personalized Investment Strategies. (2021). International Journal of Engineering and Computer Science, 10(12). https://doi.org/10.18535/ijecs.v10i12.4655

[4] Fang Z, Li Q. (2025). A Survey on Privacy and Security Issues in IoT-based Environments: Technologies, Protection Measures and Future Directions. Computers & Security, 148. https://doi.org/10.1016/j.cose.2025.104099

[5] Sneha Singireddy. (2024). The Integration of AI and Machine Learning in Transforming Underwriting and Risk Assessment Across Personal and Commercial Insurance Lines . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 3966–3991. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/2732

[6] Alwarafy A, Al-Thelaya KA, Abdallah M, Schneider J, Hamdi M. (2020). A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things. arXiv preprint. https://doi.org/10.48550/arXiv.2008.03252

[7] Researcher. (2023). Decision Support Systems for Government Auditing: The Role of AI in Ensuring Transparency and Compliance. Zenodo. https://doi.org/10.5281/ZENODO.15489803

[8] Radanliev P, De Roure D, Maple C, Nurse JRC, Nicolescu R, Ani U. (2024). AI Security and Cyber Risk in IoT Systems. Frontiers in Big Data, 7. https://doi.org/10.3389/fdata.2024.1402745

[9] Koppolu, H. K. R., & Sheelam, G. K. (2024). Machine Learning-Driven Optimization in 6G Telecommunications: The Role of Intelligent Wireless and Semiconductor Innovation. Global Research Development (GRD) ISSN: 2455-5703, 9(12).