[1,2.]Mircea ȚĂLU

SECURITY IN INTERNET OF THINGS AND CLOUD COMPUTING CONVERGENCE: CURRENT TRENDS, CHALLENGES, AND PERSPECTIVES

[1.] The Technical University of Cluj–Napoca, Faculty of Automation and Computer Science, Cluj–Napoca, ROMANIA.
[2.] SC ACCESA IT SYSTEMS SRL, Constanța St., Cluj–Napoca, ROMANIA

Abstract: The increasing overlap between Internet of Things (IoT) networks and cloud computing (CC) platforms is revolutionizing the operating model for data–driven applications, especially for sectors such as smart cities, industrial automation, and intelligent transportation. The merger offers more scalable resource management, quicker decision–making, and more automation across areas. It also introduces new security threats. They are primarily because of the restricted capabilities of edge devices and distributed and heterogeneous nature of cloud infrastructures. This paper discusses a large number of security threats in those environments. These range from established threats of illicit data access and application programming interface (API) vulnerabilities to more recent ones like adversarial machine learning, quantum computing attacks against existing cryptography practices, and sophisticated insider threats. We consider traditional defenses—encryption, layers of access controls, and policy–enforced contracts—and more recent options like blockchain–based trust models, artificial intelligence–driven anomaly detection, and lightweight cryptography for embedded systems. Through its review of contemporary practice and research, this study identifies existing knowledge gaps and indicates the direction of future research. Some of the most urgent are the establishment of cross–layer security models working across multiple system levels, the application of post–quantum cryptography appropriate for low–power devices, and enhanced tenant isolation controls for cloud–native.

Keywords: Cloud computing, Internet of Things, IoT–cloud convergence, cybersecurity, quantum–resilient security, AI–based intrusion detection, lightweight cryptography

1. INTRODUCTION

The convergence of the Internet of Things (IoT) and cloud computing (CC) is a milestone change in the architecture of distributed, data–centric computing systems. IoT establishes the pervasive application of networked physical objects – from embedded actuators and sensors to autonomous cyber–physical objects – that can generate, send, and receive data on the basis of ubiquitous networking protocols. These edge devices, through their pervasive embedding in industrial, city, and household infrastructures, provide end–to–end observation, control, and optimization of the physical world by creating high–resolution, real–time streams of data [1–3].

Cloud computing is now a permanent support in the current digital framework, providing efficient access to compute power and centralized data control. By using service–based infrastructures that provide compute power, storage, and network supply on request, cloud platforms offer scalable and efficient solutions. This reduces the processing load on user–end devices, allowing applications with high content data to be executed on equipment with limited capacities [4–6].

When married with the Internet of Things (IoT), cloud infrastructure creates a robust platform for real–time processing of large, heterogeneous data sets gathered from dispersed devices. The integration of the two—alternatively referred to as IoT–cloud integration—provides a way in which data from sensors can be transmitted to distant cloud servers, to be processed and aggregated, and utilized in a bid to influence intelligent decision–making. Implementations of the model appear in a variety of sectors, ranging from smart energy and manufacturing to networked transport systems [7–9].

Although it has its benefits, this integrated approach is plagued with high security and privacy issues [10–12]. The majority of IoT devices have limited computing power and power sources, which makes it challenging to implement conventional security measures such as strong encryption, multi–factor authentication, or real–time intrusion detection [13–16]. In parallel, cloud

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

infrastructures—owing to their virtualized environments, shared environments, and broadened exposure to potential vulnerabilities—are subjected to attacks of data leakage, privilege abuse, side–channel attacks, and intra–system abuse [17, 18].

The most difficult issue is the lack of unified security models that transcend both IoT devices and cloud platforms. Most modern solutions address individual components in isolation without considering how one layer's weaknesses can be attacked across the entire ecosystem. This fragmented approach leaves systems open to advanced cross–domain attacks. Furthermore, the security environment is in a state of continuous flux, with new threats like adversarial AI, quantum decryption methods, and polymorphic malware introducing new levels of risk [19–22].

This review responds to these urgent questions by examining the varied security challenges that accompany IoT–cloud fusion. It reviews the efficacy of existing solutions and pinpoints the essential areas that require further exploration. Particular attention is accorded to potential technologies such as blockchain for trust management, ultra–lightweight cryptographic processes for low–energy consumption, and AI–based solutions for detection and reaction to developing threats. Together, these technologies have the power to shape more resilient, adaptable, and secure architectures for the future.

2. RESEARCH METHODOLOGY

This research utilizes a systematic literature review in investigating how security issues are changing in systems that integrate the IoT with CC. The review utilizes a step–by–step method based on established academic standards. The process began with defining clear research objectives, followed by an extensive search for academic literature that relates to the research. Second, the materials chosen were looked at for both quality and relevance, then overarching themes and conclusions categorized. Last, the outcomes were looked at to determine what current trends, current gaps, and where further study could be conducted. In order to allow for a review that includes preliminary work as well as current findings to be presented, literature that spans the time period of 2014–2025 was reviewed. Research articles were downloaded from authentic databases like IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, MDPI, and Google Scholar. The search methodology was based on precision–engineered Boolean searches involving key phrases such as "IoT–cloud security architecture," "AI–based intrusion detection systems," and "privacy–preserving mechanisms in cloud computing." The filtering process tackled peer–reviewed journal articles, valid conference proceedings, and technical surveys with novel contributions or insightful examination of security measures specific to the IoT–cloud context. Insights received from these sources were utilized to build a conclusive taxonomy of security measures and allocate current constraints that hinder the creation of secure, scalable, and responsive IoT–cloud systems. This approach establishes a foundation for making well–informed inferences and bringing eventualities to drive the security of combined IoT and cloud ecosystems forward.

3. INTERNET OF THINGS ARCHITECTURE

A typical IoT five–layer structure includes the physical perception layer, the network and protocol layer, the edge (or fog) layer, the middleware layer, and the application layer, as shown in Figure 1. All of them are made up of a diverse collection of hardware devices, communication protocols, and service platforms, each having various, layer–dependent security problems to be addressed using integrated solutions:

— Perception layer (alternatively referred to as device layer), where the physical world intersects with digital. It includes a range of sensors, actuators, RFID tags, etc., other edge

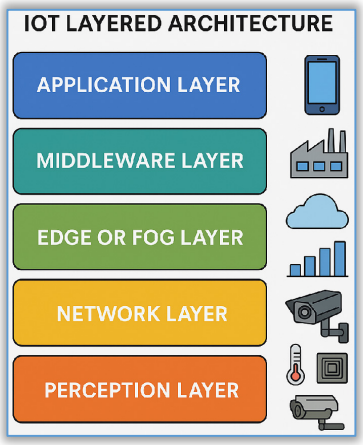

Figure 1. A conceptual IoT five–layer architecture

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN–L 1584 – 2665

devices which capture raw data like location, temperature, humidity, motion, level of illumination, etc. Perception layer plays a pivotal role in environmental sensing and control, providing the groundwork whereupon IoT infrastructure functions. Nevertheless, the Perception layer possesses immense security issues. Devices within this layer usually have minimal processing power, memory, and power resources to implement safe mechanisms, thus making them vulnerable to be easily attacked, intruded with unauthorized access, and data leaked. The preservation of data integrity and device verification is vital to avoid the loss of trustworthiness of information received in this layer.

— The network layer transfers the data that the perception layer has gathered to the rest of the IoT system. The network layer uses many communication technologies like LANs, WANs, cellular networks, and IoT–specific protocols like 6LoWPAN, Zigbee, and LoRa. The network layer provides transparent communication between devices and provides routing, addressing, and mobility management for the data. Security is a major concern in the network layer. The layer is susceptible to attacks like man–in–the–middle, denial of service (DoS), and routing attacks like wormhole attacks. The combination of heterogeneous communications technology and high device density increases the attack surface, and strong encryption, authentication practices, and intrusion detection need to be enforced to secure data exchange.

— The edge or fog layer embodies a decentralized model of computing that places data processing near data sources. By doing computations at or near data sources, the layer saves latency, saves bandwidth, and enhances potential for real–time decision–making. It is especially useful for applications that need quick response, including autonomous vehicles, industrial control, and health monitoring systems. This layer is usually composed of two tiers: the lower tier processes incoming streams of data from devices, and the upper tier performs higher–order operations such as data analysis and distributed storage. The edge layer facilitates existing technologies such as 5G networks and embedded artificial intelligence, which allow for the deployment of sophisticated machine learning algorithms near the data source. Security operations at this layer should handle issues of data privacy, safe storage of data, and blocking unauthorized access.

— In this case, the middleware layer is an intermediary between the hardware devices and the application layer and offers a suite of services for communication, data processing, and device interoperability. It hides the complexity of the hardware and communication protocols and offers a consistent platform for application development. Middleware services comprise data storage, device management, and protocol translation, which are necessary for fault handling in heterogeneous IoT device integration. With increasing IoT devices and technologies such as 5G, the middleware layer should deal with more data, provide low–latency communications, and be highly reliable. Security measures at this level include protection of data integrity, imposition of access controls, and providing secure channels for device–to–device and device–to–application communications.

— The application layer is the highest layer in the IoT architecture and provides user–centric services and interfaces. It converts processed data into operational knowledge and specialized domain services, e.g., intelligent homes, medicine, transportation, and factory automation. It provides a level for facilitating other communication protocols for interoperability of products of other organizations. Application Layer Security is essential because it consists of processing personal data of users and offering services with deep implications in the real world. Having strong authentication controls, encryption of data, and user access rights is imperative to realize avoidance of threats and privacy and integrity of services offered.

In brief, five–layered IoT system architecture provides a practical framework through which to analyze their intricate elements and interactivities. Each layer has a specific function and is susceptible to various forms of security threats. Mitigation of such challenges at each stage is

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

essential in the creation of IoT solutions that are not just scalable and efficient but also secure and resistant to evolving threats.

4. CLOUD COMPUTING ARCHITECTURE

Cloud computing today is a pillar of the new digital foundation, supporting a diverse range of emerging technologies like artificial intelligence, big data analytics, IoT, and mobile computing. Cloud Service Providers (CSPs) provide different models of services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), through which users can utilize computer resources on–demand and tailor them according to certain requirements in certain application domains [4–6]. Cloud storage is one such important building block of this infrastructure, which provides efficient, scalable, and distributed data management. It plays a crucial part in making data stored, synchronized, and moved between nodes seamlessly so that cloud–native applications can perform effectively.

Cloud deployment models are categorized into five various types, each of which is intended to cater to certain organizational and operation needs (Figure 2). The models are available on diverse levels of control, scalability, and resource allocation. Table 1 presents a comparison of the deployment paradigms based on the parameters.

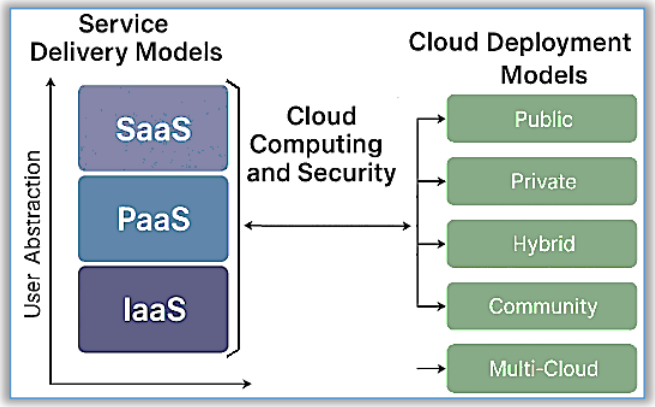

Figure 2. Mapping of service models to various cloud deployment frameworks

— Public Cloud: Third–party providers provide services and infrastructure that are shared by many users over the internet. It is cost–effective, scalable, and convenient but uses a multi–tenant, shared environment that is a possible source of data privacy and control issues.
— Private Cloud: Constructed entirely for a single organization, private clouds allow for more control over infrastructure, data management, and security processes. They tend to be the option of organizations that have high compliance or regulatory demands.
— Hybrid Cloud: The hybrid cloud combines public and private cloud features to enable organizations to achieve flexibility and control in proportions that are evenly balanced. It promotes workload portability and enables smooth integration of on–premises infrastructures and cloud services.
— Community Cloud: For a community of organizations with like goals or regulatory requirements, community clouds are a typical configuration where infrastructure is shared to meet some degree of compliance, security, or performance requirements.
— Multi–Cloud: Diversifies workloads across several cloud providers to minimize dependence on a single vendor, optimize service deployment, and capitalize on the capabilities of several vendors. This improves system fault tolerance and allows companies to use the best features of various platforms.

Table 1. Comparative analysis of the cloud deployment models

Parameter	Public cloud	Private cloud	Hybrid cloud	Community cloud	Multi–cloud
Cost Efficiency	High	Low	Medium	Medium	Medium
Security	Moderate	High	High	High	Variable (depends on providers)
Control	Low	High	Medium to high	Medium	Medium
Scalability	High	Limited	High	Medium	High
Customization	Low	High	High	Medium	Medium
Vendor lock–in	High	Low	Medium	Medium	Low
Use case Suitability	Startups, SMEs	Government, finance sectors	Enterprises with hybrid needs	Research institutions, Consortiums	Enterprises needing flexibility & resilience

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

5. THREAT LANDSCAPE AND SECURITY CHALLENGES IN IoT–CLOUD INTEGRATION

The meeting of IoT technologies with cloud computing created the opportunities for revolutionary transformation in different spheres. Intelligent infrastructure, smart services—this technology is all about a new era of networked applications. At the same time, however, it also introduces a wide and dynamic set of security challenges. Defending against these challenges calls for more than conventional defenses—it calls for agile, scalable, and context–sensitive methods to secure systems [23]. This chapter examines the most important security challenges caused by IoT–cloud infrastructures and calls for stringent requirements of end–to–end systems that can evolve according to evolving threat environments.

Device–level security problems.

IoT devices, in general, have restricted computing powers and therefore it is quite challenging to incorporate conventional security measures [24]. Comparative evaluation of the shortcomings of conventional cryptography on IoT devices is shown in Table 2.

Table 2. Limitations of traditional cryptography on IoT devices

Crypto–graphic algorithm	Key strength	Resource demand	Processing overhead	Energy consumption	Scalability in IoT networks	Suitable for IoT?
AES (Advanced Encryption Standard)	High (128/192/256–bit)	High	Moderate to high	Medium	Moderate	Partially
RSA (Rivest–Shamir–Adleman)	Very high (2048+ bits)	Very high	Very high	High	Poor	No
SHA–256 (Secure Hash Algorithm 256)	High (256–bit digest)	Moderate	Medium	Medium	Good	Partially
ECC (Elliptic Curve Cryptography)	Very high (160–256–bit with RSA–equivalent strength)	Moderate	Low to moderate	Low	Good	Yes
Blowfish	High (32–448–bit)	Moderate	Medium	Medium	Moderate	Partially
DES / 3DES (Data Encryption Standard)	Low to medium (56/168–bit)	Low	Low	Low	Moderate	No
MD5 (Message Digest 5)	Low (128–bit digest)	Low	Low	Low	Good	No
ChaCha20	High	Moderate	Low	Low	Good	Yes

AES provides adequate encryption but is very resource–intensive, so it is less suitable for low–resource IoT devices. RSA provides adequate security but huge key sizes and high computational costs, so it is unsuitable in most IoT uses. SHA–256 provides adequate data integrity with moderate resources, but generates high CPU loads on low–power IoT nodes. ECC, however, provides equivalent security to RSA but with much shorter keys and is therefore more suitable for resource–limited IoT devices. Blowfish can beat AES under some circumstances but does not have widespread support and standardization that guarantees secure IoT usage. DES/3DES are antiquated as they have poor encryption keys and well–known vulnerabilities and therefore cannot be used in IoT. MD5 is also no longer advisable either, since it is vulnerable to cryptographic attacks like collisions, though it is very resource–low. ChaCha20 is another that is secure and lightweight over AES and has good hardware performance on constrained hardware devices. Countermeasures are still the subject of active research for protection against the vulnerabilities but are usually found to fail in offering adequate protection on constrained devices.

Network–level security issues

The heterogeneous and dynamic characteristics of IoT networks create tremendous threats in the network layer. The networks are typically built upon wireless communication protocols (e.g., Zigbee, LoRaWAN, NB–IoT, 6LoWPAN, and Wi–Fi), which inherently are more vulnerable to interference, spoofing, and interception than wireline infrastructures [25–28]. Furthermore, the vast disparity in capability between ultra–low–power sensors and high–capability edge nodes creates disparity in security configurations and enforcement. The most well–known network–layer attack is probably the replay attack, wherein attackers capture and replay genuine data packets to masquerade or

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

gain unauthorized access to IoT–cloud services. Replay attacks tend to exploit the lack of robust mutual authentication, nonces, or timestamp checks. Likewise, man–in–the–middle (MitM) and routing attacks (e.g., sinkhole, wormhole) are also common because of weak encryption schemes and decentralized routing in most IoT protocols. The scalability of IoT deployments aggravates these concerns even more. With the volume of device counts ranging from thousands to millions, the imposition of homogeneous and strong security policies is impossible using traditional approaches. The absence of standardized, interop–compatible security protocols makes it even more difficult for real–time threat detection and coordinated response. To mitigate such issues, researchers are considering lightweight encryption techniques, intrusion detection systems (IDS) for IoT network traffic, and SDN–based architectures for the delivery of central management over different segments of IoT. Network–level security mechanisms in IoT–Cloud systems are compared in table 3. A conceptual diagram on network–level threats and mitigation strategies is shown in Figure 3.

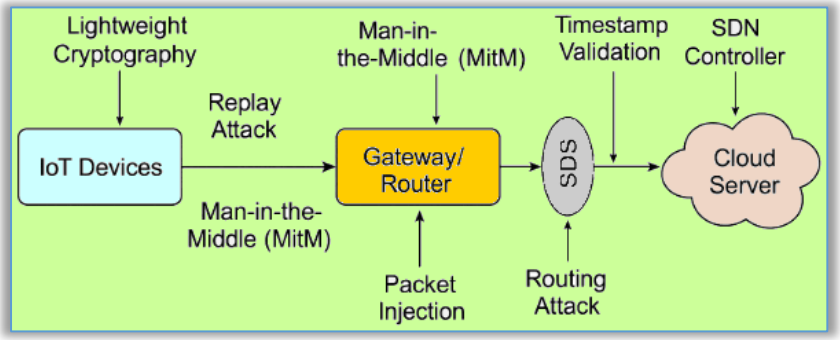

Figure 3. A conceptual diagram on network–level threats and mitigation strategies.

Table 3. Comparative analysis of network–level security mechanisms

Security mechanism	Description	Advantages	Disadvantages	Suitable protocols
Lightweight Encryption (e.g., ECC, AES–CCM)	Optimized encryption for constrained devices	Low overhead, fast, scalable	Vulnerable if key exchange is weak	Zigbee, LoRaWAN, CoAP
Replay Attack Mitigation (Nonce/Timestamps)	Prevents replay via time–based or random tokens	Effective for time–sensitive systems	Sync and delay issues in low–power devices	MQTT, CoAP
SDN–based Security Architecture	Centralizes control over dynamic IoT networks	Real–time updates, adaptive policy enforcement	Complex to implement, central point of failure	IP–based, hybrid networks
Intrusion Detection Systems (IDS)	Detects abnormal traffic patterns or known signatures	High detection accuracy with AI integration	High false positives, resource–intensive	All protocols (via gateway)
Blockchain for Network Access Logs	Immutable audit trails for network access events	Trustless, tamper–proof history	Latency, scalability issues in high–throughput cases	Hybrid networks

Cloud–level security issues

The intersection of IoT and cloud computing introduces an intricate set of security issues that transcend traditional perimeter protection. While as much as cloud platforms introduce beneficial benefits like scalability flexibility, on–demand provisioning of resources, and centralized storage of data, they also increase the vulnerability of IoT systems to more threats. The most significant issues include data privacy, identity management, risks from multi–tenancy, and compliance. The most serious among such risks is the risk of data breaches where sensitive information gathered by IoT devices can be leaked while in transit, while being stored in clouds, or while being processed when in the cloud. Such breaches typically occur due to breached encryption procedures, poorly configured storage, or not sufficiently stringent access controls. In multi–tenant clouds, lack of isolation between virtual machines or containers is risky in the form of side–channel attacks or data leakage between users. Shared responsibility as a cloud model can sometimes be ambiguous regarding whose responsibility is what layer in the system. This such ignorance between IoT developers, cloud service providers, and users can render vulnerabilities exposed to attack. This is particularly problematic in very regulated industries like health and finance, where very strict data protection regulations like GDPR and HIPAA have to be complied with. New security paradigms including zero–trust architectures, confidential computing, and more sophisticated access controls through attribute–based encryption (ABE) and federated identity management are being explored

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

as possible solutions. Securing data across its complete lifecycle—from when it is first collected on the edge to when it is being processed in the cloud—is the focus of IoT–cloud ecosystem protection today [29–31]. A summary of typical cloud–level threats and their respective countermeasures is shown in Table 4. A conceptual diagram on cloud–level threats and security countermeasures is shown in Figure 4.

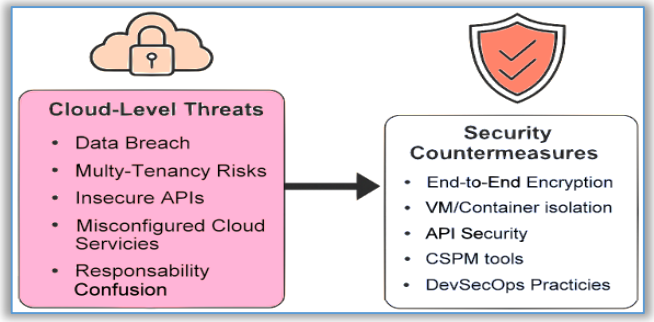

Figure 4. A conceptual diagram on cloud–level threats and security countermeasures.

Table 4. Common cloud–level threats and countermeasures

Threat	Description	Mitigation strategy	Advantages	Disadvantages
Data breach	Unauthorized access to sensitive data during transmission or storage	End–to–end encryption (e.g., TLS 1.3, AES), access tokens	Protects confidentiality	Performance overhead in constrained devices
Multi–tenancy exploits	Side–channel or hypervisor attacks due to shared cloud infrastructure	VM/container isolation, confidential computing (e.g., Intel SGX)	Improves tenant isolation	Complexity and hardware dependency
Insecure APIs	Poorly secured cloud APIs enabling unauthorized actions	API gateways, input validation, OAuth2.0, rate limiting	Easy integration and scalability	Still vulnerable to zero–day exploits
Misconfigured cloud services	Default credentials, open ports, or misassigned permissions	Automated configuration audits, CSPM tools	Reduces human error	Needs constant updates
Responsibility confusion	Lack of clarity in shared responsibility model among stakeholders	Clear security SLAs, DevSecOps policies, user education	Clarifies roles and compliance	Depends on cooperation from all parties

API and interface security issues

Application Programming Interfaces (APIs) are essential in facilitating communication among IoT devices and cloud environments. APIs enable devices to exchange data, receive commands, and communicate with numerous services as the foundation for IoT ecosystems. But if APIs lack proper security, they become the first target for hacking, resulting in great security loopholes. Common vulnerabilities include poor authentication, excessive exposure of sensitive data, and poor input validation, which can lead to security breaches like data breaches, injection attacks, or service disruption. Poor authentication practices—e.g., using easily guessable, weak passwords or not using multi–factor authentication—can expose APIs to unauthorized use. Similarly, inappropriately exposed APIs can lead to inadvertent exposure of confidential information, which is a threat to confidentiality and privacy. APIs lacking robust input validation are also vulnerable to injection attacks under which malicious input causes changes to the behavior of the API, potentially affecting the overall connected system. Counteracting these security dangers involves adopting stringent API design and security practices. With robust authentication methods such as OAuth or token–based authentication, unauthorized access can be minimized. Least privilege access controls in place ensure that sensitive resources can only be accessed by permitted systems or users and the effect of a breach is minimized. Added on top of this are strong input validation and

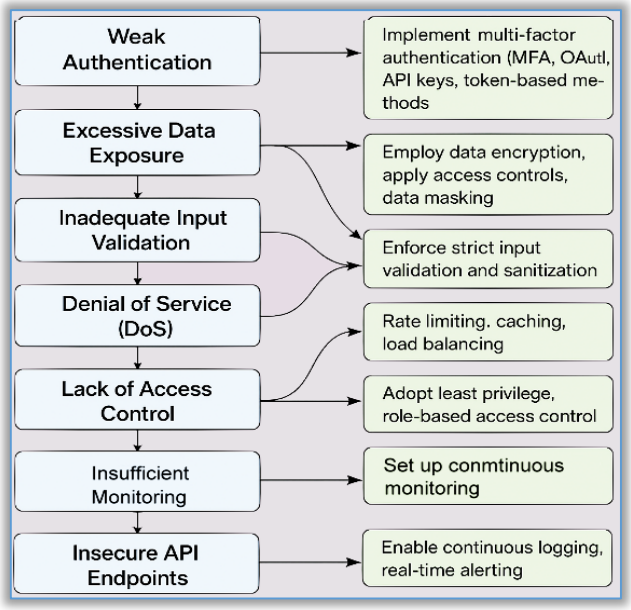

Figure 5. A conceptual diagram on the key API security challenges and their mitigations

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

sanitization controls necessary to stop attacks such as SQL injection or cross–site scripting (XSS). In IoT systems, API security complexity is additionally enhanced by perpetual addition of new devices, continuous updates, and continuous network architecture changes. Subsequently, the APIs must be built under support of these varying conditions, and they must have perpetual monitoring, dynamic access control, and elastic security since the IoT environment keeps varying [32–34]. Some of the primary API security issues and solutions are given in Table 5. A conceptual diagram on the key API security challenges and their mitigations is shown in Figure 5.

Table 5. The key API security challenges and their mitigations

API security challenge	Description	Mitigation Strategy
Weak authentication	Weak authentication methods, such as easily guessable passwords, can allow unauthorized access.	Implement multi–factor authentication (MFA), use OAuth, API keys, and token–based authentication methods.
Excessive data exposure	Sensitive data may be exposed through unsecured API endpoints.	Encrypt sensitive data, enforce strict access controls, and apply data masking to prevent unauthorized exposure.
Inadequate input validation	Failure to validate incoming data properly, opening the door to injection attacks like SQL injection or cross–site scripting (XSS).	Use rigorous input validation and data sanitization to block malicious inputs from affecting the system.
Denial of Service (DoS)	APIs may be overwhelmed by excessive or malicious traffic, disrupting service.	Implement rate–limiting, caching, and load balancing to mitigate the impact of DoS attacks.
Lack of access control	Unauthorized users may gain access to sensitive resources due to insufficient access control measures.	Adopt least privilege access control principles and implement role–based access control (RBAC) to restrict access.
Insufficient monitoring	Without real–time monitoring, security incidents may go undetected for too long.	Set up continuous monitoring, automated alerting systems, and comprehensive logging to detect anomalies promptly.
Insecure API endpoints	Unsecured API endpoints can expose vulnerabilities, leading to potential data leaks or attacks.	Secure all endpoints with TLS/SSL, enforce endpoint security policies, and carefully validate every incoming request.

Security issues related to AI

Intersection of Artificial Intelligence (AI) and Machine Learning (ML) with IoT and cloud infrastructure has significantly promoted real–time threat detection and adaptive security reactions. The technologies support high–volume processing of large volumes of diverse data from spread–out IoT devices and cloud infrastructures and support the identification of unusual patterns that signal potential security problems. However, application of AI to such systems introduces novel threats in the form of adversarial attacks against the AI model learning process. Adversarial attacks undermine the confidentiality, integrity, and dependability of AI–powered security by compromising input data or finding flaws in the model itself. A few of the most prominent adversarial attacks are evasion, poisoning, and model inversion, which each offer several different threats to AI–powered security mechanisms (see Fig. 6). To counteract such threats, there must be an end–to–end plan incorporating additional model training, extensive data validation, and use of privacy–preserving methods [35–38].

Some of the most critical adversarial attacks include evasion attacks, poisoning, and model inversion attacks, which harm confidentiality, integrity, and availability the most in AI–integrated cloud infrastructure.

— Evasion attacks occur when an attacker manipulate data in a way that misleads an AI model into making wrong decisions. These attacks exploit the model's vulnerability to small, usually imperceptible, changes in the input data. For instance, in cloud applications such as intrusion detection systems (IDS), an attacker can make small changes to packet content or network timing, render malicious activity imperceptible, and render it as benign. What makes evasion attacks hard to block is that they do not need access to the training data or internal mechanisms of the model, and therefore can even be performed if the attacker has only observed the model's outputs. When such attacks happen in mission–critical environments—like smart grids or autonomous cloud applications—the consequences can be catastrophic, causing unauthorized access, data breaches of sensitive information, or even system crashes that impact entire systems.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

— Poisoning attacks, however, target the disruption of the AI model while it is being trained. In such attacks, the attackers insert carefully designed, malicious information in the training data to sabotage the process of the model's learning. The attacker could have a range of goals: an attacker could try to decrease the general performance of the model (an availability attack), stealthily modify the model in such a way that it misclassifies particular data (a backdoor attack), or manipulate the model to make unsafe predictions. This type of attack is very dangerous in cloud–based IoT systems that depend on ongoing updates from real–time data, for example, in industrial IoT (IIoT) or smart healthcare implementations. For example, if edge device data is tampered with—i.e., injecting spurious temperature values or mislabeling traffic flow—the AI model can learn from these spurious patterns and propagate erroneous decisions throughout the whole system. To safeguard against these attacks, the correct tracing of data origin must be ensured, data quality must be verified, and the process of learning must be protected.

— Model inversion attacks are also a critical threat under which the attackers use the output of an AI model to derive sensitive information from its training data. By repeatedly asking the model questions and observing its answers, a perpetrator could potentially piece together personal information, including health status, identifiers, or even confidential information such as biometric or facial images. This is especially relevant for cloud–hosted applications, like face recognition APIs, where the perpetrator has access to the model's output but not the workings of the model. These attacks compromise data integrity, can breach regulatory compliance such as GDPR or HIPAA, and breach anonymization methods, particularly in environments such as federated or collaborative learning. To protect against model inversion attacks, methods such as differential privacy, sanitizing outputs, and secure multi–party computations are necessary.

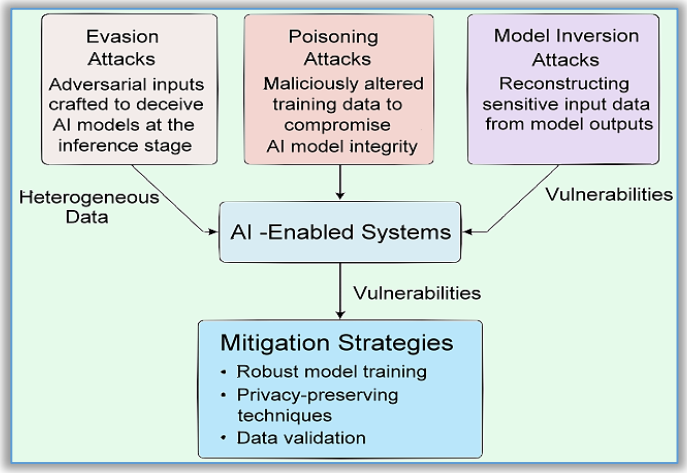

Figure 6. A conceptual diagram on AI–driven security challenges

6. ADVANCED SECURITY SOLUTIONS AND MITIGATION STRATEGIES

Interfacing IoT devices with cloud infrastructure introduces a new set of sophisticated security challenges. For the novel and ever–evolving cyber threats, professionals are increasingly turning towards implementing a multi–layered security strategy. This involves the use of lightweight cryptography, quantum–resistant encryption, decentralized replacements such as blockchain, adversarial AI defense systems, and robust API protection. Additionally, advancements in zero trust architectures, privacy–computing, and hardware–based security features are clearing the way for safer IoT–cloud systems in the future. A conceptual overview of the advanced security solutions and mitigation strategies is presented in Figure 7.

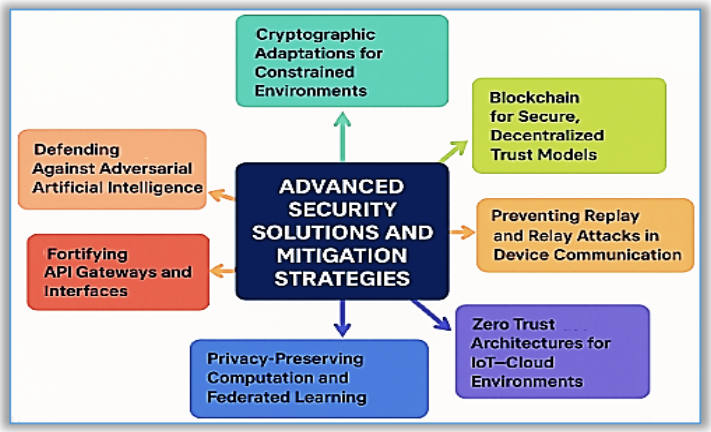

Figure 7. A conceptual diagram on the advanced security solutions and mitigation strategies

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN–L 1584 – 2665

Cryptographic extensions for resource–restricted environments

IoT devices are burdened with excessive computation and power resource constraints, rendering common encryption schemes infeasible. Thus, new cryptographic methods have been formulated to protect these devices without compromising their performance. Lightweight cryptography plays a crucial role, employing algorithms tailored for low–resource contexts. One such great example is Elliptic Curve Cryptography (ECC), which offers secure key strength with lesser keys, hence bandwidth as well as computational requirements saved. All other ciphers such as PRESENT, SIMON, and SPECK utilize virtually zero computational expense, and economical hash functions which ensure integrity of data make them cost–effective too. Meanwhile, quantum computing poses a very real threat to current encryption technologies, particularly public key infrastructure. Anticipating this, post–quantum cryptography (PQC) aims to develop algorithms that are resistant to quantum attacks. Lattice–based methods (e.g., NTRU), code–based cryptography, and multivariate polynomial systems are a few of the promising solutions. Of these, Dilithium and CRYSTALS–Kyber, two cryptographic primitives proposed by NIST, are researched for the purpose of utilizing them in IoT applications for safe key exchange as well as digital signatures. Though challenges like higher key sizes as well as complexity in integrations exist, they point towards developing more efficient forms of PQC that can be utilized on IoT devices.

Blockchain for decentralized, secure trust models

Blockchain offers a novel solution to safeguarding IoT–cloud infrastructure through the elimination of single points of failure and establishment of decentralized trust. Blockchain's inbuilt properties of immutability, cryptographic hash, and consensus algorithms provide integrity and allow for an auditable chain of security, especially relevant in settings where data tampering or manipulation could be a problem. By combining blockchain with edge computing and software–defined networking (SDN), it is achievable to utilize scalable security solutions that are still network latency sensitive. Solutions such as Blockchain–Enabled Distributed Trust (BEDT) and Adaptive Multi–Layer Security (AMLS) apply smart contracts so that there can be automated access control in that security policy can be imposed with accuracy. Also, blockchain–powered identity management does away with central authentication and enables devices to authenticate each other directly through digital certificates and distributed ledgers. This integration is further boosted when it is combined with decentralized storage solutions like IPFS, further amplifying data confidentiality and integrity in IoT applications involving masses of data. In spite of such benefits, more interest is seen in light–weight consensus algorithms like Delegated Proof–of–Stake (DPoS), Proof–of–Authority (PoA), and hybrid architecture. These are being proposed to handle latency issues as well as power usage, and thus are becoming increasingly resource–constrained network friendly.

Hostile Artificial Intelligence countermeasures

As artificial intelligence (AI) is the center of gravity in intrusion detection and threat analysis of IoT–cloud systems, it becomes all the more vulnerable to attacks by malicious actors. Malicious users can inject subtle manipulations into sensor data or data streams so that they become capable of evading anomaly detection mechanisms and subverting AI–powered decision–making processes. To offset such threats, countermeasures like adversarial training are being implemented. This approach exposes AI models to adversarial perturbed inputs during training, which allows them to learn detecting and resisting manipulation by an adversary. Additionally, explainable AI (XAI) is gaining prominence because it enhances the transparency of AI models so that analysts can better detect how the decision is being made and detect potential anomalies. Other defensive methods that are gaining traction are robust ensemble models, defensive distillation, and intense input sanitization. Model watermarking and model extraction detection techniques are also being applied to defend against inversion attacks as well as theft. Coming research is working on techniques such as federated adversarial learning and self–healing AI models that are capable of adapting

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

dynamically to newly emerging adversarial methods so that they are able to continue offering protection against continuously evolving threats.

- Replay and relay attacks prevention of device communication

Replay and relay attacks are fundamental security threats to the integrity of IoT–cloud communication. By retransmitting or intercepting valid packets or commands, an attacker may get unauthorized access to devices or disrupt data transportation. Mitigate these threats using measures like nonce–based authentication, timestamp verification, and session tokens. These techniques timestamp messages and bar attackers from replaying credentials or data. In addition, relying on channel binding—binding authentication tokens to distinctive device–session properties—is yet another step to mitigate vulnerabilities. Some of the new solutions are light–weight mutual authentication methods such as EAP–NOOB and DTLS–light, and edge–based intrusion detection systems that are able to identify abnormal communication behavior, which may prove to be a sign of a replay attack. Machine learning for behavior profiling can also assist in the identification of unusual sequences of commands, adding to overall detection of possible threats.

- Securing API gateways and interfaces

APIs are the main communication interface between IoT devices and cloud platforms but are usually exposed to security attacks like injection attacks, poor authentication, and open endpoints. To safeguard against these attacks, businesses can utilize OAuth 2.0 for token–based authentication in place of static API keys to more secure and revocable credentials. API gateways can also be leveraged by introducing a traffic filtering and rate limiting layer, which filters out malicious traffic and applies security policy compliance. Imposing strict input validation, the use of HTTPS, the use of certificate pinning, and the adoption of role–based access control (RBAC) are also mandated best practices. Ongoing monitoring of API activity by the implementation of AI–driven anomaly detection also assists in detecting malicious actions, notifying administrators of potential abuse or security risks in real time.

- Zero trust architectures for IoT–cloud environments

One of the emerging methods of securing distributed systems is the use of Zero Trust Architecture (ZTA), based on the presumption that no device or service can be inherently trusted. ZTA, in IoT–cloud deployments, requires ongoing verification of identity, integrity, and context prior to access allowance. Micro–segmentation, least privilege access enforcement, and identity–based controls are some of the main practices required to embrace Zero Trust. By adding these methods to context data analysis—e.g., device reputation or location information—and behavior–based authentication, the adaptive security is enhanced. Zero Trust structures for an IoT focus may also include hardware–based root–of–trust technology, e.g., Trusted Platform Modules (TPMs) or Physically Unclamable Functions (PUFs), for attestation and secure boot. In addition, using cloud–native security orchestration allows automated threat detection and response, enhancing security throughout the system.

- Privacy–preserving computation and federated learning

When people's data is processed over a variety of websites, the users' privacy becomes a priority. Federated learning offers an avenue for training models on device data that arrives in a direct form without the prior collection and storage of raw data at a centralized point. Additional privacy strengthening is explored by using techniques like homomorphic encryption, secure multiparty computation (SMPC), and differential privacy. These techniques enable private and secure analysis of data in cloud environments to allow collaboration in threat detection and behavior analysis without exposing the individual users' data while performing so.

7. FUTURE RESEARCH DIRECTIONS

Recent studies have identified several pivotal areas for future research directions (Figure 8):

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

— Scalable AI–driven Security Architectures

The developments in artificial intelligence (AI) and machine learning (ML) promise adaptive, real–time security responses. Nevertheless, existing models remain plagued by generalization, explainability, and adversarial attack vulnerability. Future research must tackle the design of scalable AI models with the integration of explainable AI (XAI), federated learning, and robustness against adversarial attacks. These advances would enable dynamic threat detection and autonomous defense in distributed and large–scale IoT–cloud infrastructures.

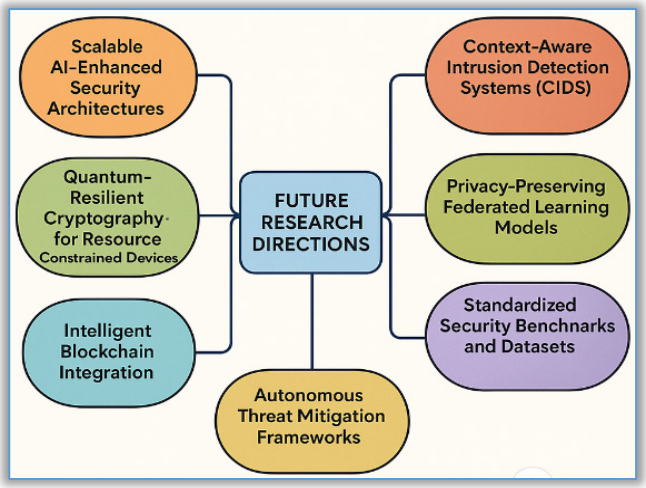

Figure 8. A conceptual diagram on future research directions

— Post–Quantum–Resistant Cryptography for Constrained Devices

With growing quantum computing capability, RSA and ECC cryptography will become insecure. Lightweight post–quantum cryptographic solutions for IoT devices, which have limited resources in terms of processing power, memory, and energy, are unavoidable. Combining PQC with existing lightweight ciphers in hybrid systems may make secure, quantum–resistant communication solutions for resource–constrained environments feasible.

— Blockchain Integration for Intelligence

Although blockchain has demonstrated promise in ensuring data integrity, access control, and decentralized trust, its application in IoT–cloud environments remains limited by scalability and latency. Future work should concentrate on working on lightweight and energy–efficient consensus protocols, such as PoA or DAGs that are optimized for low–power IoT networks. Another area ripe for exploration is the application of blockchain and AI for secure autonomous decision–making in distributed systems.

— Context–Aware Intrusion Detection Systems (CIDS)

Current anomaly detection systems may not be able to understand advanced behavior of rich IoT environments. Future work should be focused on creating context–aware intrusion detection systems (CIDS) that learn to keep up with changing network behavior, device trends, and user trends. Deep learning and semantic modeling–based sensor data processing may assist in improving detection rates without increasing false positives.

— Privacy–Preserving Federated Learning Models

Federated learning enables decentralized training of AI models without exposing raw data, but ensuring privacy and security for distributed learning poses a challenge. An exploration of current privacy–preserving technologies such as differential privacy, secure multi–party computation, and homomorphic encryption over federated learning will further strengthen security together with user information confidentiality in IoT cloud–connected devices.

— Standardized Security Benchmarks and Datasets

One of the significant issues with comparing and analyzing security solutions is the lack of common benchmarks and publicly available high–quality datasets for IoT–cloud settings. Future research should aim to generate varied testbeds, attack simulation environments, and labeled data for realistic attacks and deployment configurations. This would allow for more aggressive testing and reproducible outcomes for novel methods.

— Autonomous Threat Mitigation Frameworks

To develop self–defending systems, future effort would involve designing autonomous, smart threat mitigation systems. These would involve real–time monitoring, detection of threats, decision–

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN–L 1584 – 2665

making, and enforcement with minimal human participation. They must also learn from new and developing attack signatures by using learning and feedback mechanisms.

7. CONCLUSION

The convergence of CC with IoT technologies has introduced a powerful ecosystem with the ability to collect information in real–time, enable effortless connectivity, and process bulk data across sectors. However, the technology also introduces a vast range of security issues. Diversity of devices connected, decentralized data–sharing, and multi–layered cloud environments make the entire system more prone to cyber–attacks. This article has expounded on where security stands within IoT–cloud environments at the moment, covering some of the main threats such as data exposure, poor API defenses, risks of shared tenancy, and sophisticated threats involving adversarial manipulation of AI systems and the as–yet unsolved threat from quantum computing. All these are further compounded by the low levels of processing and memory capabilities present in most IoT devices, making the use of traditional security appliances particularly problematic. Adding to the problem is the lack of strong, comprehensive security standards that are specifically aimed at the particular needs of these hybrid environments. On the positive side, new technologies are starting to fill some of these gaps. AI–driven threat detection and defense solutions provide real–time dynamic adjustment, and blockchain technologies are proving their worth in decentralizing trust and enabling secure access controls. In the meantime, light encryption techniques and quantum–resistant cryptographics are poised to become a low–resource IoT standard to protect communication. The survey also found a sequence of promising future research directions—ranging from the development of AI–aided, scalable security architectures to federated learning's privacy–preserving models and judicious blockchain deployment. Standardized test facilities and evaluation standards were also mentioned as needed. A case study of the healthcare industry highlighted the practical ramifications of these weaknesses, particularly where patient information and life–sustaining equipment are concerned. Together, the findings emphasize the need for more intelligent, adaptive, and context–aware security solutions that can address the exceedingly quickly changing IoT–cloud environment.

References

[1] V. Tsiatsis, S. Karnouskos, J. Holler, D. Boyle, C. Mulligan, Internet of Things: technologies and applications for a new age of intelligence, 2nd ed., 2019, Academic Press, London, UK
[2] S.N. Mohanty, J.M. Chatterjee, S. Satpathy, Internet of Things and its applications, 1st ed., 2022, Springer Nature Switzerland AG.
[3] R. Dallaev, T. Pisarenko, Ş. Ţălu, D. Sobola, J. Majzner, N. Papež, Current applications and challenges of the Internet of Things, New Trends In Computer Sciences, 1(1): 51–61, 2023
[4] A. Wegener, Cloud computing: systems and technologies, Clanrye International, New York, USA, 2019.
[5] D. Comer, The cloud computing book, CRC Press, Taylor & Francis Group, Boca Raton, FL, USA, 2021.
[6] N. Antonopoulos, L. Gillam, Cloud computing: principles, systems and applications, Springer Cham, 2017
[7] R. Buyya, L. Garg, G. Fortino, S. Misra, New Frontiers in Cloud Computing and Internet of Things, 2022, Springer Cham.
[8] P.N. Mahalle, N.Ambritta P., G.R. Shinde, A.V. Deshpande, The Convergence of Internet of Things and Cloud for Smart Computing, 1st ed., CRC Press, , Boca Raton, FL, USA, 2022.
[9] P.D. Singh, M. Angurala, Integration of Cloud Computing and IoT: Trends, Case Studies and Applications, CRC Press, Boca Raton, FL, USA, 2024.
[10] M. Almutairi, F.T. Sheldon, IoT–cloud integration security: a survey of challenges, solutions, and directions. Electronics, 14(7): 1394, 1–28, 2025.
[11] W. Ahmad, A. Rasool, A.R. Javed, T. Baker, Z. Jalil, Cyber security in IoT–based cloud computing: a comprehensive survey. Electronics, 11(1): 16, 2022.
[12] A. Mughaid, I. Obeidat, I. Abualigah, S. Alzubi, M.Sh. Daoud, H. Migdady, Intelligent cybersecurity approach for data protection in cloud computing based Internet of Things. Int. J. Inf. Secur. 23, 2123–2137, 2024
[13] A. Nazarov, D. Nazarov, Ş. Ţălu, Information security of the Internet of Things, In: Proceedings of the International Scientific and Practical Conference on Computer and Information Security – INFSEC, SCITEPRESS – Science and Technology Publications, Lda, vol. 1, pp. 136–139, 2021. Eds.: D. Nazarov and A. Nazarov. International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021) Yekaterinburg, Russia, April 5th–6th, 2021.
[14] M. Ţălu, Security and privacy in the IIoT: threats, possible security countermeasures, and future challenges, Computing&AI Connect, vol. 2, article ID: 2025.0011, 2025
[15] M. Ţălu, Exploring IoT applications for transforming university education: smart classrooms, student engagement, and innovations in teacher and student–focused technologies. Buletin Ilmiah Sarjana Teknik Elektro, 7(1): 09–29, 2025

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

[16] M. Ţălu, DNA–based cryptography for Internet of Things security: concepts, methods, applications, and emerging trends, Buletin Ilmiah Sarjana Teknik Elektro, 7(2): 68–94, 2025
[17] D.G. Harkut, Cloud computing security: concepts and practice, IntechOpen, UK, 2020.
[18] A. Achari, Cybersecurity in cloud computing, Educohack Press, Delhi, India, 2025.
[19] M. Rath, J. Satpathy, G.S. Oreku, Chapter 6 – Artificial Intelligence and Machine Learning Applications in Cloud Computing and Internet of Things, Eds.: G. Kaur, P. Tomar, M. Tanque, Artificial Intelligence to solve pervasive Internet of Things issues, Academic Press, 2021, pp. 103–123,
[20] M.L. Hernandez–Jaimes, A. Martinez–Cruz, K.A. Ramírez–Gutiérrez, C. Feregrino–Uribe, Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures, Internet of Things, 23, 100887, 2023
[21] S. Kumar, M. Dwivedi, M. Kumar, S.S. Gill, A comprehensive review of vulnerabilities and AI–enabled defense against DDoS attacks for securing cloud services, Computer Science Review, 53, 100661, 2024
[22] T.G. Zewdie, A. Girma, IoT security and the role of AI/ML to combat emerging cyber threats in cloud computing environment, Issues in Information Systems, 21(4): 253–263, 2020.
[23] S. Kumar, D. Kumar, R. Dangi, G. Choudhary, N. Dragoni, I. You, A review of lightweight security and privacy for resource–constrained IoT devices, Computers, Materials and Continua, 78(1): 31–63, 2024
[24] B. Hussain, W. Elmedany, S. Sharif, The internet of things security issues and countermeasures in network layer: a systematic literature review. In Proceedings of the 2022 International Conference on Data Analytics for Business and Industry (ICDABI), Virtual, 25–26 October 2022; pp. 787–793.
[25] S.R. Mishra, B. Shanmugam, K.C. Yeo, S. Thennadil, SDN–enabled IoT security frameworks – a review of existing challenges. Technologies, 13(3): 121, 2025.
[26] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab, A.M. Caruso, An SDN perspective IoT–fog security: a survey. Comput. Netw. 229, 109732, 2023.
[27] F. De Keersmaeker, Y. Cao, G.K. Ndonda, R. Sadre, A survey of public IoT datasets for network security research. IEEE Commun. Surv. Tutor., 25, 1808–1840, 2023
[28] K.K. Karmakar, V. Varadharajan, S. Nepal, U. Tupakula, SDN–Enabled Secure IoT Architecture. IEEE Internet Things J., 8, 6549–6564, 2021.
[29] M. Pawlicki, A. Pawlicka, R. Kozik, M. Choraś, The survey and meta–analysis of the attacks, transgressions, countermeasures and security aspects common to the Cloud, Edge and IoT, Neurocomputing, 551, 126533, 2023
[30] I. Kanwal, H. Shafi, S. Memon, M.H. Shah, Cloud computing security challenges: a review. In: Jahankhani, H., Jamal, A., Lawson, S. (Eds.) Cybersecurity, privacy and freedom protection in the connected world. Advanced sciences and technologies for security applications. Springer, Cham, 2021.
[31] N. Singh, R. Buyya R, H. Kim, Securing cloud–based internet of things: challenges and mitigations. Sensors, 25(1): 79, 2025.
[32] N. Almurisi, S. Tadisetty, Cloud–based virtualization environment for IoT–based WSN: solutions, approaches and challenges. J Ambient Intell Human Comput 13, 4681–4703, 2022
[33] A.H. Annas, A.A. Zainuddin, A.A. Hussin, N.N.M.S.N.M. Kamal, N.M. Noor, R.M. Razali, Cloud–Based IoT System for Real–Time Harmful Algal Bloom Monitoring: Seamless Things Board Integration via MQTT and REST API," 2024 IEEE 22nd Student Conference on Research and Development (SCOReD), Selangor, Malaysia, 2024, pp. 317–322
[34] J. Hao, J. Liu, W. Wu, F. Tang, M. Xian, Secure and fine–grained self–controlled outsourced data deletion in cloud–based IoT, in IEEE Internet of Things Journal, 7(2): 1140–1153, 2020
[35] B. Pavithra, C. Vinola, N. Mishra, G. Naveen, Cloud security analysis using machine learning algorithms, 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 704–708.
[36] A.B. Nassif, M.A. Talib, Q. Nasir, H. Albadani, F.M. Dakalbab, machine learning for cloud security: a systematic review, in IEEE Access, 9: 20717–20735, 2021
[37] J. Sotiropoulos, Adversarial AI attacks, mitigations, and defense strategies: a cybersecurity professional's guide to AI attacks, threat modeling, and securing AI with MLSecOps, Packt Publishing, 2024.
[38] I.M. Khalil, A. Khreishah, M. Azeem. Cloud computing security: a survey. Computers, 3(1): 1–35, 2014

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665