INTERNATIONAL JOURNAL OF ACTA INFORMATICA
VOLUME (2023)

# INTELLIGENT DATA FLOW TAGGING ACROSS LAYERED WEB APPLICATION ARCHITECTURES: A PRIVACY-BY-DESIGN APPROACH FOR NET ENTERPRISE SYSTEMS

**Divya Sai Jaladi**[1*]

[1]Application Developer, SCDMV, Charlotte, NC, UNITED STATES

## ABSTRACT

Blockchain technology is rapidly gaining prominence globally. Blockchain, characterized by its decentralized, transparent, and secure attributes, has emerged as a transformative technology for the forthcoming generation of various industrial applications. One such concept is the Cloud of Things, facilitated by the integration of cloud computing and the Internet of Things. In this context, blockchain offers unique ways to tackle difficulties in the Cloud of Things regarding decentralization, data privacy, and network security, while the Cloud of Things provides elasticity and scalability features to enhance the efficiency of blockchain operations. Consequently, a new paradigm of blockchain and Cloud of Things integration, termed BCoT, is increasingly recognized as a promising facilitator for various application scenarios. This paper offers a comprehensive study of BCoT integration, aimed at providing general readers with an overview of BCoT, encompassing basic information, motivation, and integrated architecture. Specifically, we offer a comprehensive analysis of BCoT applications across various use-case domains, including smart healthcare, smart cities, smart transportation, and smart industry. Subsequently, we examine the latest advancements in BCoT alongside the burgeoning blockchain and cloud platforms, applications, and research initiatives. Ultimately, significant research problems and prospective approaches are emphasized to stimulate additional inquiry in this intriguing field.

**KEYWORDS:** Data Flow Analysis; Privacy by Design; Software Architecture; Data Lineage; Sensitive Data Detection; Enterprise Web Applications.

## INTRODUCTION

In recent years, there has been a significant surge in interest in blockchain technology, including a diverse range of applications from cryptocurrencies to various businesses [1], [2]. The swift advancement in the use of blockchain as a transformative technology is facilitating the emergence of the next generation of financial and industrial service sectors. New research endeavors on blockchain and its uses occur daily, influencing several facets of our existence, including finance [3], energy [4], and governmental services [5].

From a technical standpoint, blockchain is a distributed ledger system initially employed as the public digital ledger for the cryptocurrency Bitcoin financial exchanges. The blockchain is fundamentally a decentralized, immutable, and public database. The blockchain concept relies on a peer-to-peer network structure where transaction data is not governed by any singular centralized authority. Transactions recorded in a series of blocks are transparently available to all members of the blockchain network in a reliable manner. Blockchain employs consensus processes and cryptography to authenticate the validity of data transactions, ensuring the resilience of interconnected blocks against modifications and alterations [7]. Specifically, blockchain technology possesses the advantageous traits of decentralization, accountability, and security, which enhance service efficiency and reduce operating costs. Such remarkable attributes have facilitated the adoption of blockchain-based apps in recent years. Consequently, this is an opportune moment to focus on this prominent research subject.

The revolution in information and communication has generated numerous opportunities for advanced technologies, particularly the Internet of Things (IoT) and cloud computing. The Internet of Things (IoT) has redefined and revolutionized our existence through many industrial, consumer, and commercial services and applications [8], [9]. IoT is generally a network of physical entities that may be seen, managed, or engaged with by pervasive electronic devices to facilitate widespread industrial services, such as smart cities and smart industries. Owing to the constrained resources of IoT devices, they consistently assign IoT application duties to Cloud computing, resulting in the emergence of the Cloud of Things (CoT) paradigm [10], [11]. The CoT offers a versatile and resilient cloud computing framework for the processing and management of IoT services, demonstrating significant potential to enhance system performance and service delivery efficiency [12]. Nevertheless, traditional CoT infrastructures can prove unsuccessful due to several problems. The traditional Chain of Trust solutions predominantly depend on centralized communication models, such as central cloud systems, for IoT service operations, complicating scalability as IoT networks proliferate. Furthermore, most contemporary CoT systems require reliance on a third party, such as a cloud provider, for IoT data processing, hence elevating data privacy concerns. The centralized network infrastructure ultimately leads to increased communication latency and power consumption for IoT devices due to prolonged data transmission, hence impeding the large-scale implementation of CoT in real-world applications [14].

firmly posited that blockchain will be a formidable contender for achieving complete decentralization of future CoT networks. The merging of blockchain and CoT results in a novel paradigm known as BCoT. The integration of these developing technologies yields significant advantages for both sectors, hence fostering enduring interest in

academia and industry. The blockchain and CoT exhibit several complementary relationships for practical applications. In the realm of cloud computing, blockchain is recognized as a service termed Blockchain as a Service (BaaS). Blockchain can facilitate entirely novel cloud storage capabilities through a decentralized storage architecture utilizing virtual storage nodes, which exhibit significant resistance to data alterations. Blockchain interconnects computer nodes, including virtual machines on the cloud and external computers, to establish a fully decentralized storage system, eliminating the need for a central authority, rather than depending on conventional cloud data centers. Blockchain furthermore serves as network management services, closely associated with apps built on smart contracts. In these scenarios, blockchain serves as a communication layer between cloud servers, IoT devices, and end users. The implementation of blockchain can offer numerous possible advantages for CoT systems as outlined below.

• Decentralization: The decentralized nature of blockchain presents a promising approach to successfully address bottlenecks and single-point failure issues by obviating the need for a trusted third party within the CoT network [15]. Moreover, the peer-to-peer design of blockchain enables all network participants to validate the accuracy of IoT data and guarantees immutability with equal validation rights.

The BCoT system ensures reliable access control through blockchain-enabled smart contracts, which automatically authorize all operations of cloud providers and IoT devices, mitigate potential threats to cloud resources, and enhance fine-grained control over IoT data. Furthermore, the blockchain allows users to monitor their transactions across the network to uphold device and data ownership, hence enhancing information privacy.

• Corporation: Blockchain facilitates a novel cooperative ecosystem among several companies, allowing for unrestricted data sharing without necessitating mutual confidence. The elimination of the third party facilitates the establishment of an open environment.

Forums where IoT users and cloud providers interested in the system can engage and work to attain shared objectives inside the BCoT ecosystem [18].

Conversely, CoT can enhance blockchain platforms by providing the following essential advantages:

• Scalable support for blockchain transactions: In extensive blockchain applications, the volume of transactions inside blockchain networks might be substantial. Consequently, it is imperative to deliver robust data processing capabilities to expedite transaction execution, thereby facilitating scalable blockchain services. In this context, the cloud provides on-demand computing resources for blockchain operations due to its flexibility and scalability capabilities [19]. Public clouds can provide an extensive

network of resources for blockchain service operators inside a federated cloud environment. Consequently, the amalgamation of cloud computing with blockchain can attain significant scalability within the integrated system.

• Fault tolerance: The cloud facilitates the replication of blockchain data across a network of interconnected computing servers through collaborative clouds [20]. This would mitigate single-failure risks arising from the disruption of any cloud node, hence ensuring continuous services. Moreover, the inter-cloud ecosystem can facilitate the uninterrupted operation of the blockchain system in the event that a specific cloud server is compromised.

An examination of the current advancements in the field reveals that BCoT garners significant interest from research communities, as illustrated in Fig. 2. Cloud computing and the Internet of Things have surged in popularity during the past five years, accompanied by a significant increase in academic publications. Blockchain has emerged as a prominent study domain in recent years, exhibiting a rapid growth trajectory and presenting a potential subject for both academia and industry moving forward. The sustained advancement of CoT and blockchain will catalyze transformative breakthroughs to enhance intelligent services and applications.

## ASSOCIATED WORKS AND CONTRIBUTIONS OF THIS SURVEY

Numerous studies on CoT, blockchain, and associated concerns have been conducted in recent years, encompassing a broad spectrum of technological aspects. Numerous endeavors have been undertaken to furnish review articles on this research domain across many scopes.

Survey articles provided an assessment of recent initiatives regarding the deployment of blockchain technology across diverse IoT scenarios and applications. The writers in [24] also examined the amalgamation of blockchain technology with the Internet of Things (IoT). This work primarily investigates the possibilities of blockchain for IoT applications, including smart manufacturing, the Internet of aircraft, unmanned aerial aircraft, and 5G networks. The survey in [25] focused on the analysis of the technical aspects of blockchain, including foundational principles, networking, and consensus mechanisms. Simultaneously, the writers in [26] examined the research difficulties, constraints, and potential associated with the integration of blockchain and cloud computing. The study [27] conducted a survey on the deployment of blockchain technology to deliver security services and its technical attributes to address related difficulties across many sectors, including IoT and cloud computing. The survey [28] recently examined the comprehensive model integrating blockchain and edge computing, an advanced idea of cloud computing. Table I encapsulates the principal themes and contributions of the literature reviews pertinent to BCoT and our manuscript.

Despite widespread examination of blockchain and CoT in the literature, to our knowledge, no comprehensive assessment exists that integrates these significant research domains. This paper presents a thorough survey on the integration of blockchain and the Internet of Things (IoT), encompassing a detailed discussion on various aspects, including conceptual background, integrated architectures, application domains, service platforms, and research challenges, in contrast to the aforementioned review works. The primary objective of this survey is to furnish readers with comprehensive insights into the integration of blockchain and CoT, derived from relevant websites, technical studies, academic articles, and newspapers. This survey's primary contributions are delineated as follows.

We present a cutting-edge assessment on the integration of blockchain and CoT, encompassing an extensive examination of several technical facets, including the background of BCoT, motivations for integration, and the conceptual framework of integrated BCoT.

## ARCHITECTURAL DESIGN

We offer the revised review on the implementation of BCoT models across many areas. We examine the advantages of BCoT adoption and subsequently outline the key lessons learned from each use case. Additionally, the nascent BCoT platforms and services are introduced and examined.

3) Through a comprehensive assessment of BCoT integrations, we uncover potential research challenges and unresolved concerns in the domain. Future research directions are examined to broaden the applicability of BCoT in subsequent services and applications.

Mitigating single point failure risks resulting from the disruption of central authority, reducing operational costs, and augmenting reliability. Moreover, blockchain maintains the immutability of transaction data across time. The hashing process of a new block consistently incorporates metadata of the previous block's hash value, rendering the chain highly immutable. Consequently, it is infeasible to alter, amend, or remove data from the block once it has been confirmed and incorporated into the blockchain. A crucial characteristic is transparency, arising from the visibility of all transaction information on the blockchain to all network participants. The identical replica of blockchain records disseminates via an extensive network for public verification. Consequently, all blockchain users possess equal rights to access, verify, and monitor transaction activities across the network.

Despite these security advantages, blockchain presents certain challenges that must be addressed to ensure its effective integration with the Internet of Things (IoT). Achieving energy efficiency in blockchain applications within BCoT is a significant concern.

Decentralized consensus methods in blockchains frequently necessitate substantial processing power and significant energy consumption to mine blocks and sustain the blockchain network. This renders blockchain impractical for resource-limited IoT devices in CoT applications. While energy-intensive blockchain mining can be executed in a centralized cloud, this would fundamentally undermine the benefits of a distributed CoT system. A further concern pertains to the throughput of blockchain systems. Indeed, blockchain exhibits much poorer throughput relative to non-blockchain applications. For instance, Bitcoin can perform a maximum of only four transactions per second, and the throughput should be considered in the architecture of blockchain platforms for sustained BCoT applications.

2) Cloud of Things: Currently, the Internet of Things (IoT) has become an integral component of the future Internet, garnering heightened interest from scholars and industries due to its significant potential to provide innovative services across many applications. The Internet of Things (IoT) effortlessly integrates diverse devices and things to establish a physical environment in which sensing, processing, and communication occur autonomously, devoid of human intervention. Nonetheless, the substantial data quantities produced by numerous devices in contemporary IoT systems hinder the assurance of the appropriate Quality of Service (QoS) due to the limited power and storage capabilities of IoT devices. Cloud computing offers boundless resources for storage and computational power, delivering on-demand, robust, and efficient services for IoT applications. The integration of cloud computing with IoT facilitates a novel paradigm known as CoT, which enhances both domains. The extensive resources accessible via the cloud significantly enhance IoT systems, while the cloud's integration with IoT platforms can increase its prevalence in practical applications. Furthermore, CoT has the potential to revolutionize existing IoT service delivery models with little management exertion, enhanced system performance, and improved service availability. The overarching principle of CoT is illustrated in the figure. 5 including a network architecture comprising IoT devices, cloud computing, analytical services, and an application layer. In this hierarchy, IoT devices are employed to detect and gather data from surrounding areas. Consequently, owing to their constrained computational capabilities, IoT devices will relay recorded data to the cloud for data gathering. Cloud computing offers a robust capacity for data processing.

INTERNET OF THINGS DEVICES CLOUD COMPUTING

Privacy management: While centralized cloud IoT offers easy services, this model presents significant data privacy issues due to the extensive collection, transit, storage, and utilization of IoT data within dynamic cloud networks. IoT customers frequently rely on cloud providers to manage apps, often lacking knowledge about data transmission and the present consumers of their information [44]. In distributed cloud

IoT models including several clouds, IoT data are not entirely decentralized but are concentrated in certain cloud data centers at high density [45]. In this scenario, IoT data could be compromised if a cloud server is breached.

and storage. Analytical services can be offered to enhance IoT systems, including historical data monitoring, information storage, and statistical analysis. The outcomes of cloud data processing are used to support end applications, with the objective of enhancing IoT service delivery and fulfilling end-user requirements.

The CoT platform provides instantaneous services to customers at any location and time, facilitated by the automated resource provisioning capabilities of cloud computing. It facilitates autonomous service provision without requiring human involvement. With the boundless virtual processing capabilities of cloud computing, CoT creates new options to augment IoT computation through data offloading and distant execution. This enhances the computational capabilities of local devices while efficiently addressing energy conservation and bandwidth preservation challenges in IoT systems. CoT can provide streamlined and automated IT maintenance and management solutions by utilizing cloud servers, virtual machines, and resource infrastructure. IoT users can seamlessly engage with cloud computing to execute capabilities without necessitating software installation or human intervention. Furthermore, the availability of cloud-based system management models facilitates seamless communication and interconnection among IoT devices, as well as between devices and users, thereby enhancing ubiquitous applications and fostering comprehensive collaborations among various IoT ecosystems in the future Internet.

## RATIONALE FOR THE INTEGRATION OF BLOCKCHAIN AND THE INTERNET OF THINGS

This subsection emphasizes the rationale for integration, stemming from the security issues of CoT, the technical constraints of blockchain, and the intriguing opportunities presented by the amalgamation of these two technologies.

1) Security Challenges in CoT: While CoT facilitates ubiquitous computing services with substantial data storage and elevated system performance, it continues to face some key challenges [42][43] as follows.

Data availability: In contemporary cloud network architectures, cloud services are centrally offered and managed by a governing authority. This setup is susceptible to single-point failures, posing risks to the availability of cloud services for on-demand IoT access. A centralized cloud IoT solution does not provide uninterrupted delivery of IoT services when several users concurrently request data or when cloud servers experience disruptions due to software malfunctions or cyber-attacks.

Data integrity: The storage and processing of IoT data in cloud environments may raise

concerns regarding integrity. Indeed, reliance on centralized cloud providers exposes outsourced data to the possibility of modification or deletion by third parties without user agreement. Furthermore, enemies may manipulate cloud data resources for financial or political motives, thereby compromising data integrity. Consequently, numerous solutions employing public verification systems reliant on a third-party auditor have been suggested; however, they may introduce various concerns, such as negligent verification leading to biased data integrity outcomes or compromised verification due to malevolent auditors. Consequently, it is imperative to devise innovative ways to effectively address data integrity concerns in CoT systems.

2) Technical Limitations of Blockchain: Despite its potential to revolutionize services such as CoT, blockchain has some significant hurdles in its development, particularly with complexity and security vulnerabilities.

In IoT networks, to validate transactions, IoT devices function as blockchain participants to execute the consensus process, necessitating the resolution of intricate mathematical riddles that demand robust computational hardware. Regrettably, fulfilling such needs is difficult due to the limitations of IoT resources. Even in the case of IoT devices with relatively high computing capacities, running complex blockchain process may require intensive resources involving electricity and human management. This would generate user worries around elevated running costs, which would impede the extensive deployment of blockchain-based solutions.

The ultimate constraint of contemporary blockchains may be an inescapable security vulnerability. If a majority of machines functioning as blockchain nodes possess computational power, attackers might alter consensus mechanisms and obstruct new transactions from receiving confirmations for nefarious purposes. This is referred to as a 51% attack, which is emphasized in the notion of Bitcoin. In the absence of comprehensive transaction management, blockchain is susceptible to data breaches and system damage.

The decentralization of the Cloud of Things (CoT) establishes a foundation for blockchain as a solution for data security and privacy, while blockchain can utilize CoT's cloud resources for intensive mining calculations and dependable data storage.

3) The Advantages of Integrating Blockchain and CoT: Given the complimentary functions of blockchain and CoT, together with their prospective benefits, the integration of both technologies is warranted.

Disruptive technologies present numerous BCoT prospects, as outlined below.

Decentralized administration: Inspired by the entirely decentralized nature of blockchain, a decentralized BCoT management architecture can be established under the distributed control of a peer-to-peer network comprising cloud nodes and IoT

devices. All blockchain participants uphold identical versions of the ledger data records by decentralized consensus, with trust spread uniformly among the network entities. This decentralized framework completely eradicates single point failure bottlenecks, effectively prevents disruption of BCoT services, and considerably boosts data availability. Enhanced data privacy: The ongoing process of outsourcing IoT data to cloud services and the data interchange between cloud providers and IoT users are susceptible to information breaches and assaults perpetrated by adversaries or third parties. Blockchain, with its characteristics of immutability, integrity, and transparency, is exceptionally well-suited for data protection in CoT networks. To execute a data modification attack in a BCoT system, an adversary would attempt to edit the records or modify data stored in the blockchain. Nonetheless, this is virtually unattainable in actual situations where blockchain is maintained and governed by safe and unchangeable consensus methods. The intrinsic qualities of blockchain can substantially improve Data privacy for BCoT applications.

Enhanced system security: Blockchain can deliver solutions to augment security for the Internet of Things (IoT) by providing essential security attributes such as confidentiality and availability that are intrinsic to blockchain technology. In BCoT networks, all blockchain records are cryptographically hashed, and transactions are signed by participants, ensuring that user interactions with clouds stay confidential using blockchain-enabled signatures. Moreover, the inherent decentralization of blockchain ensures data replication across all network participants, eliminating single points of failure, hence enhancing availability in BCoT. Specifically, the innovative cloud computing can offer off-chain storage options to enhance data availability of the on-chain storage systems when the primary BCoT network is compromised by external threats. The deployment of blockchain algorithms on cloud platforms may augment the security of the blockchain system itself. For instance, clouds can employ their existing network security technologies to safeguard blockchain applications, such as mining mechanisms, against potential threats. The benefits of cloud computing for blockchain are evidenced by recent successful integrations, like the Oracle blockchain project (2017) and the iExec blockchain project (2018) [47].

Decreased system complexity: The integration of blockchain with cloud computing allows BCoT to substantially simplify system implementations. This integration is referred to as blockchain-as-a-service, wherein established platforms facilitate the setup and operation of blockchain for BCoT projects without concern for the underlying hardware technology. Furthermore, blockchain algorithms can now be executed online utilizing cloud infrastructure, which holds the potential to decrease resource expenditures associated with blockchain operations. The integration of blockchain and the Internet of Things presents numerous chances to Expedite BCoT deployments on a broad scale through straightforward and cost-effective implementations.

4) Feasibility of BCoT Integration: Currently, an increasing number of significant corporations are executing BaaS studies to evaluate the viability of integrating blockchain into cloud computing. Prominent corporations including Amazon, Microsoft, IBM, and Oracle have initiated the development of BaaS systems for IoT within cloud computing environments. The Amazon cloud provider creates a BaaS framework for IoT business models. An IoT healthcare system was created in [50] utilizing Amazon BaaS architecture. This project utilizes the Ethereum blockchain platform hosted on Amazon Cloud to establish a secure and private health data exchange framework for mobile clouds. Furthermore, IBM Cloud [51] presents a sophisticated BaaS platform for IoT consumers. The platform has been demonstrated in a vehicular network [206]. This project integrates the IBM IoT platform with IBM BaaS services to manage vehicle sensor data, including vehicle-to-vehicle communications and vehicle monitoring information, while ensuring security in data sharing within the vehicular network. Simultaneously, Oracle Cloud's BaaS platform has demonstrated significant potential through various BCoT initiatives, including banking, healthcare data management, and the payment sector. The aforementioned examples demonstrate the considerable viability of blockchain adoption in cloud computing for addressing complicated security and network performance challenges in IoT applications. The subsequent sections will elucidate the evolution of BaaS models across diverse IoT sectors.

## THE ARCHITECTURAL FRAMEWORK OF INTEGRATION BLOCKCHAIN AND COT

This section provides a comprehensive analysis of the literature concerning combined BCoT models of blockchain and CoT. We offer a conceptual BCoT architecture that encompasses the essential principles and foundational ideas of integration, applicable across diverse contexts.

### Associated Works

The increasing interest in blockchain and CoT has led to the proposal of numerous integrated BCoT platforms and systems in scholarly literature to offer security solutions and applications [53], [54], [55], [56], [57]. The research [58] introduced a cloud-centric Internet of Things framework facilitated by smart contracts and blockchain technology for safe data provenance. Blockchain integrates with cloud computing to establish a robust security framework, wherein IoT metadata (e.g., cryptographic hash) is preserved on the blockchain, while the actual data resides in cloud storage, hence enhancing scalability for extensive IoT implementations. A separate study in [59] presented a blockchain-cloud network for access control with four primary components: IoT devices, a data owner, a blockchain network, and a cloud computing platform. A hierarchical access control framework for BCoT was examined in [60]. The blockchain network structure consists of distributed side blockchains implemented at

fog nodes and a multi-blockchain system functioning in the cloud, enhancing access verification speed and providing adaptable storage for scaling IoT networks. Furthermore, to safeguard A forensic investigation architecture utilizing decentralized blockchain is proposed for security-critical applications in BCoT [61]. Subsequent to the benefits of BCoT combination, [62],

[63] offered secure identity management solutions enabling cloud service providers to independently manage and validate user identities in BCoT. Blockchain is integrated with virtual clouds to facilitate identity verification without necessitating prior trust between cloud users and suppliers. Conversely, data management is essential in interconnected CoT, where the vast volume of IoT data necessitates meticulous oversight to achieve data privacy goals. Inspired by this, the work [64] introduced a blockchain-based data protection method capable of effectively preventing incorrect IoT data transfer resulting from criminal manipulation during Virtual Machine (VM) migration in cloud computing. A Mchain creation method is utilized for the integrity assessment of VM measurement data [65]. This architecture features a two-layer blockchain network comprising a data validation layer and a Proof of Work (PoW) task layer, linked with Infrastructure as a Service (IaaS) cloud to augment system integrity [66].

Additionally, the study in [67] examined an integrated blockchain-CoT architecture aimed at addressing the mining challenge by delegating mining tasks from IoT devices to cloud nodes. A dual problem of user access association and cloud resource allocation is proposed and subsequently addressed using deep reinforcement learning (DRL). Similarly, the authors in [68] and [69] addressed the offloading challenge in BCoT networks to optimize the economic costs associated with IoT devices. The research in [70] focused on the quality of cloud services within BCoT systems. In this instance, the blockchain is important in ensuring trust and reliability for premium cloud service offerings. The integration of cloud computing and blockchain was also examined in [71]. The computing resources of the remote cloud are distributed at the network edge to deliver low-latency and real-time computing services for IoT devices. Simultaneously, the resource management within BCoT systems was examined in [72], where blockchain technology effectively maintains data privacy during resource transactions between cloud providers and IoT consumers.

Generally, the aforementioned BCoT platforms are predicated on a singular cloud and may suffice for certain applications. Nonetheless, in intricate IoT systems that necessitate substantial network resources to accommodate numerous IoT users, inter-cloud BCoT integration would prove to be more efficient and comfortable [18]. Consequently, BCoT architectures have been adapted to multi-cloud frameworks for intricate collaboration situations [73], [74]. A BCoT framework was developed in a

collaborative cloud environment where various clouds are securely joined by a peer-to-peer ledger network [75]. Additionally, the singular cloud can provide immediate services for IoT consumers through blockchain technology, which significantly reduces the dangers of hostile assaults [76]. Furthermore, [45] developed a cloud federation approach that facilitates distributed resource provisioning through an individual cloud managed by a blockchain network. Additionally, a BCoT architecture incorporating micro-clouds was presented by [77] utilizing blockchain-enabled distributed ledgers.

## THE CONCEPTUAL BCOT FRAMEWORK

Inspired by a comprehensive literature review, we suggest a hypothetical BCoT architecture as seen in Fig. Six components, including three primary layers: the IoT layer, the cloud blockchain layer, and the application layer. The specifics of each layer and the overarching notion will be delineated as follows.

1) IoT Layer: IoT devices are tasked with collecting data from local environments and wirelessly relaying it to proximate gateways, like base stations, routers, or wireless access points. An IoT device possesses a blockchain account (similar to a Bitcoin wallet) enabling it to connect to the blockchain network for executing transactions (e.g., data offloading) and engaging with cloud services. Each resource-constrained IoT device, such as a wearable sensor, may function as a lightweight node that participates in the transaction validation process via its representative gateway. It is viable in blockchain-based sensor network contexts, such as [105], [209], [214], when diminutive sensors are linked to the blockchain through a gateway (e.g., a smartphone or a fog node). All sensor interactions with the blockchain, including transaction creation, data dumping, and mining duties, are executed by the gateway [58]. Conversely, IoT devices with substantial resources, such as laptops or high-performance smartphones, possess adequate capabilities to support other lightweight IoT sensors and sustain the entire blockchain. IoT devices can connect with one another via IoT gateways to facilitate corporate communication, such as device-to-device (D2D) communication in collaborative networks. This hybrid communication paradigm provides IoT users with extremely customizable services in a secure and effective manner.

2) Cloud Blockchain Layer: This functions as middleware between the IoT network and industrial applications inside the BCoT architecture. In a generic architecture, we focus on a blockchain platform that encompasses various clouds, while also thoroughly addressing the technical facets of a single-cloud BCoT architecture. This solution demonstrates two advantages: 1) guaranteeing more secure network administration with blockchain and

Providing reliable and on-demand computing services for extensive IoT applications. The integrated cloud blockchain layer comprises blockchain services and cloud

computing services.

- Blockchain services: The primary use of blockchain in the proposed architecture is to facilitate secure network management. The blockchain network is implemented and maintained on a cloud platform as Blockchain as a Service (BaaS). BaaS can provide various blockchain-enabled services to facilitate IoT applications.

• Shared ledger: It denotes the database that is collectively maintained and disseminated among BCoT members (e.g., IoT users, cloud nodes, and blockchain companies). The distributed ledger documents transactions, including information exchange or data sharing between IoT devices and the cloud. It facilitates industrial networks that allow cloud users to manage and authenticate their transactions while interfacing with blockchain cloud.

• Consensus: It offers verification services for user transactions through consensus processes such as Proof of Work (PoW).

Proof of Stake operated by a consortium of miners. This service is essential for BCoT in enhancing blockchain integrity and guaranteeing robust security for the system. Notably, IoT users can utilize their virtual cloud devices to participate in the consensus process and earn rewards, such as cryptocurrency in Bitcoin, for their contributions.

• Shared contract: BCoT further provides smart contract services to applications. Smart contracts, with their self-executing and autonomous characteristics, are advantageous for establishing business logic and trust within the BCoT system. Moreover, smart contracts offer security services for user access authentication and data sharing verification as IoT peer nodes execute transactions, hence enhancing security within the cloud blockchain.

• Cryptography: This ensures the use of public-key cryptography to safeguard information and data storage between IoT and cloud entities. Electronic signatures

Verify that all data recorded on the blockchain is accurate and unaltered, hence enhancing immutability and security for user transactions.

BaaS additionally provides cloud blockchain storage services. The blockchain-based decentralized cloud storage can be constructed on the cloud platform. Blockchain-based storage governs IoT data via hash values and conducts periodic verification to identify any potential data alterations. The InterPlanetary File System (IPFS) [78] is a blockchain-based storage system now accessible via the cloud, enabling secure storage across several nodes. This has been demonstrated to efficiently address data storage challenges associated with centralized cloud models including data leaking and storage management.

Cloud computing services: In the BCoT architecture, cloud computing employs its comprehensive services to facilitate applications, encompassing Software as a Service

(SaaS) and Infrastructure as a Service (IaaS).

Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Data collected by IoT gateways will be transmitted to cloud servers and stored in cloud blockchain storage. The cloud server provides intelligent services for offloaded IoT data utilizing available capabilities like data mining and machine learning. IoT data may be kept off-chain in a cloud database or on-chain in a blockchain. Conversely, many clouds can be utilized to facilitate functions such as data exchange or collaborative system management. In this scenario, the blockchain layer serves as a crucial intermediary, managing and regulating cloud interactions to enhance cloud service delivery to IoT customers and prevent disputes among clouds.

3) Application Layer: Numerous industrial applications can get advantages from the integration of BCoT across various domains involving IoT scenarios, such as smart healthcare, smart transportation, smart cities, smart energy, and smart industry. BCoT offers valuable services for industrial applications, including network management and QoS enhancement, while also ensuring security and privacy for the relevant domains. In smart healthcare, BCoT can facilitate data processing services due to the computational capabilities of the cloud, aiding healthcare practitioners in the intelligent analysis of patient information for improved medical care. Currently, the network security of healthcare is maintained using blockchain, which provides traceability and verification services throughout medical data exchange and processing. The subsequent part will thoroughly study the implementation of BCoT integration and its advantages in IoT application areas, including smart industry, smart energy, and smart transportation.

## REFERENCES

[1] van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2012, October). Designing privacy-by-design. In *Annual Privacy Forum* (pp. 55-72). Berlin, Heidelberg: Springer Berlin Heidelberg.

[2] Sethuraman, P. (2023). Implicit Channel Inference Techniques for Pilotless OFDM Reception in Next-Generation Wireless Systems. *International Journal of Emerging Research in Engineering and Technology*, *4*(1), 143-152.

[3] Chennareddy, R. K., & Sethuraman, P. (2023). Enterprise and RAN-Aware Data and Analytics Platforms for Mission-Critical and Low-Latency Digital Services. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(4), 184-192.

[4] Jandl, C., Nurgazina, J., Schöffer, L., Reichl, C., Wagner, M., & Moser, T. (2019, September). SensiTrack-a privacy by design concept for industrial IoT applications. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1782-1789). IEEE.

[5] Sethuraman, P., & Chennareddy, R. K. (2022a). Intelligent Vehicular Traffic Flow Prediction Using Learning-Based Spatio-Temporal Models for Data-Driven Wireless

Transportation and Urban Analytics Systems. *International Journal of Emerging Trends in Computer Science and Information Technology, 3*(2), 111-121.

[6] Arfaoui, S., Mezrioui, A., & Belmekki, A. (2020). A methodology for assuring privacy by design in information systems. *International Journal of Communication Networks and Information Security, 12*(3), 364-375.

[7] Sethuraman, P., & Chennareddy, R. K. (2022b). Machine Learning Assisted Design of Wireless Access Systems for Reliable and Low-Latency Financial and Smart Commerce Services. *International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3*(4), 133-142.

[8] Chennareddy, R. K. (2023). Enterprise-Scale AI and Analytics Strategy for End-to-End Business Transformation across Global Organizations. *International Journal of AI, BigData, Computational and Management Studies, 4*(3), 134-145.

[9] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726.*

[10] Sethuraman, P., & Chennareddy, R. K. (2023a). AI-Based Fraud Detection and Prevention at the Radio Access Network: Architectures and Mechanisms for Financial Wireless Service. *International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4*(4), 132-141.

[11] Chennareddy, R. K. (2021). Designing Data and Analytics Ecosystems for High Volume Transaction Processing Applications. *International Journal of AI, BigData, Computational and Management Studies, 2*(2), 95-106.

[12] Islam, M. B., Iannella, R., Watson, J., & Geva, S. (2015). Privacy architectures in social networks' state-of-the-art survey. *International Journal of Information Privacy, Security and Integrity, 2*(2), 102-137.

[13] Sethuraman, P., & Chennareddy, R. K. (2023b). System-Level Design and Orchestration of Large-Scale Cellular Access Networks for Regulatory-Compliant Financial Services. *International Journal of Emerging Research in Engineering and Technology, 4*(3), 140-150.

[14] Chennareddy, R. K. (2020). Engineering Intelligence Systems Using Big Data and Cloud Architectures for Modern Data Intensive Applications. *International Journal of AI, BigData, Computational and Management Studies, 1*(2), 41-50.

[15] Croitoru, I., Turcu, C. E., & Turcu, C. O. (2026). Privacy-by-Design in AI-Assisted Systems for Caregivers of Children with Autism: A Secure Multi-Agent Architecture. *Applied Sciences (2076-3417), 16*(4).

[16] Sethuraman, P. (2022). Latency-Aware Scheduling and Resource Control Algorithms for Emergency and Public Safety Wireless Networks. *International Journal of Emerging Research in Engineering and Technology, 3*(4), 133-140.