ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 3 Issue 4 December 2023 / Page No: 158-165
Paper Id: JETA-V3I8P118 / Doi: 10.56472/25832646/JETA-V3I8P118

Original Article

Securing the Cloud of Things: A Comprehensive Analytics of Architecture, Use Cases, and Privacy Risks

Vaidehi Shah
Independent Researcher

Received Date: 29 November 2023 Revised Date: 13 December 2023 Accepted Date: 27 December 2023

Abstract: *Combining cloud computing with the Internet of Things (IoT), the Cloud of Things (CoT) is a robust paradigm for intelligent, scalable, and adaptable services across domains. This integration brings up privacy and security challenges because of the scattered nature, limited resources, and heterogeneous design of CoT environments. This study delves into the architectural aspects of CoT, its real-world uses, and the significant privacy and security concerns it encounters. Cover important dangers like data leaks, social engineering, ransomware, and zero-day vulnerabilities. The research also details multi-tiered security measures, such as encryption, strong authentication, AI-based anomaly detection, and data protection rule compliance. Recent research advances and key shortcomings in current frameworks are highlighted in a comprehensive literature review. The study finishes by stressing the importance of security measures that are lightweight, scalable, and context-aware in order to guarantee the safe and dependable deployment of CoT systems in actual settings.*

Keywords: *Cloud of Things (CoT), Internet of Things (IoT), Cloud Computing, Security Architecture, Privacy Preservation, Data Protection, Edge Computing etc.*

I. INTRODUCTION

Data processing, communication, and service provisioning have all been transformed by the Cloud of Things (CoT), an umbrella word for the convergence of cloud computing and the Internet of Things (IoT). The real-time data analytics, intelligent automation, and ubiquitous connectivity offered by CoT have the potential to revolutionize a range of industries, such as transportation, smart cities, healthcare, and industrial automation. Cloud computing's scalability and the Internet of Things' ubiquitous sensing capabilities allow businesses to gain new insights and improve operations like never before. It is impossible to ignore the security and privacy risks that this integration brings. Security issues with the cloud, such as data breaches, unauthorized access, and loss of control, are made worse by the inherent complexity of the Internet of Things (IoT) architecture, which involves the continuous generation of large amounts of sensitive data by distributed IoT devices and their transmission to remote cloud environments [1]. Cyberattacks, data tampering, and denial-of-service incidents are becoming more commonplace in CoT systems because to the increased dependence on shared infrastructure and third-party service providers.

Additional vulnerabilities that hostile actors can use to breach data confidentiality and integrity include API reusability, user misconfigurations, and multi-tenancy hazards. Encryption, decryption, and secure key management are now essential components of any strong CoT security plan. Secure storage techniques, real-time anomaly detection, and granular access controls are necessary for their full effectiveness [2]. Compliance with industry standards and user trust is becoming more of a concern as more and more organizations outsource data management to cloud service providers. This is particularly true in sensitive areas like banking, defence, and healthcare. Networked storage systems (NAS) and storage area networks (SAN) with inadequate security measures exacerbate these issues by making sensitive data susceptible to distributed storage assaults, unauthorized access, and insider threats. An exhaustive examination of the Cloud of Things is the goal of this analysis, which will centre on its architectural underpinnings, many use cases, and the critical privacy and security concerns it encounters. The research emphasizes the critical need for integrated, context-aware, privacy-preserving security frameworks that can safeguard CoT systems on a large scale by examining existing problems and potential solutions.

A. Paper Structure

The structure of the paper is the following: Section II deals with its architecture and principles. Section III comments on the important use cases in different domains and describes the significant security issues, whereas Section IV is dedicated to the privacy risks and several types of threats. Section V presents security solutions and best practices. Section VI offers a literature survey and identifies existing research gaps. Section VII provides conclusion with findings.

II. FUNDAMENTALS OF THE CLOUD OF THINGS (COT)

The Cloud and IoT are complementary to each other and this is the reason why the researchers propose to integrate to gain more benefits. The integration of these two evolving technologies into a new paradigm called Cloud of Things (CoT) will facilitate the implementation of ample number of smart application scenarios [3]. Things and devices connected to avail IoT applications have limited processing capabilities, energy constraints and with less storage. To overcome this issue, cloud offers unlimited processing capabilities. It also facilitates real-time data analysis for complex applications. So, computation is also a key driver in integrating IoT and Cloud giving birth to a new paradigm called CoT. Figure 1 describes the general actors making up the CoT environment. The actors include IoT layer, the Gateway and Cloud layer

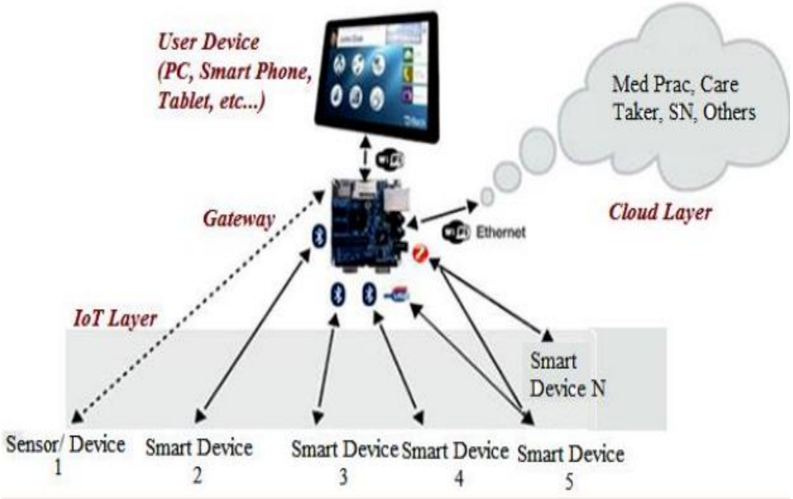

Figure 1 : CoT Environment

The computational and storage capacities of the CoT model may be infinite. An adaptable and reliable CC environment that permits real-time data integration from an extensive network of IoT devices may also be made available. In Figure 2 shows the operational picture of the CoT environment, which comprises internet-connected things (IoT) and those that gather data from their surroundings.

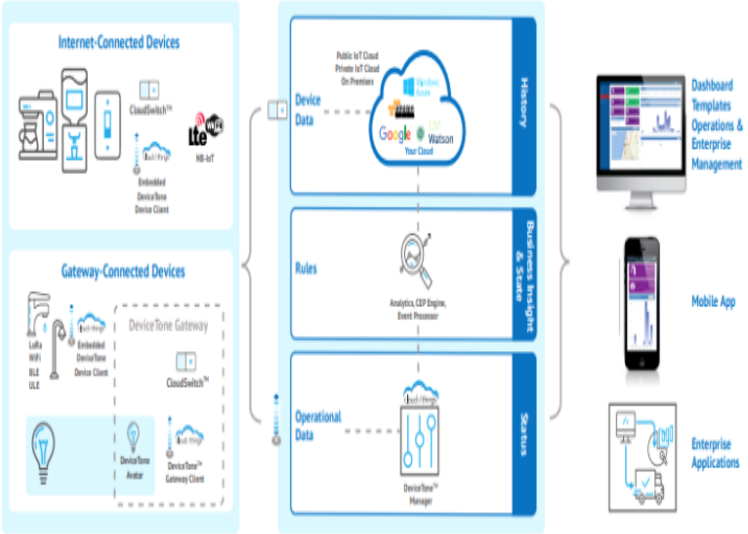

Figure 2 : CoT a Functional View [4]

Cloud layer is involved in control of devices over the internet or through a gateway, while not exempting from storing and analyzing the data. Application-specific monitoring (eg., status of patient, status of fuel in vehicle, status of room temperature and so on) is also employed which uses the data on the cloud. Therefore, the concept of the "CoT" is based on the IOT paradigm and envisions commonplace items, or "smart objects," being entirely networked and integrated with cloud(s) for the purposes of data storage, processing, analytics, and displays. Various applications, perhaps in an as-a-service approach, can take advantage of CoT.

A. Cloud of Things Architecture

Application, Network, and Perception Layers are the fundamental building blocks of an IoT architecture. The data is sent to the Network layer by the Perception Layer after it has been collected from the physical world [5]. The data is sent to the Applications layer by the Network Layer, and there are several intriguing uses for it [6]. See Figure 3 for the cloud-based IOT architecture.

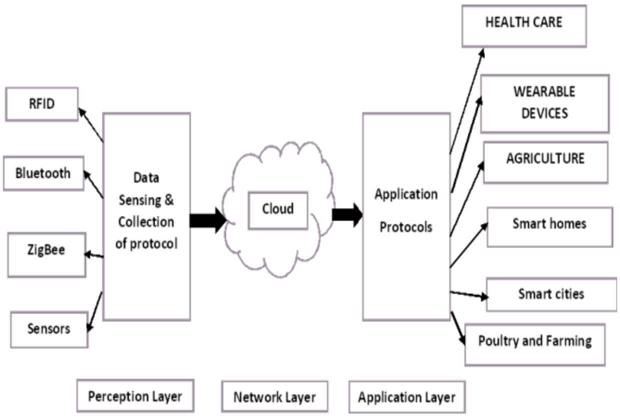

Figure 3 : Cloud of Things Architecture[1]

The IoT and the cloud go hand in hand. When it comes to industrial IoT applications, the data generated by sensors can be rather big, making it impossible for a gateway to handle and store. A safe database should be used to store this data, and it should be handled in an easy and scalable way. Into this context, the IOTS and the cloud enter. End users were constantly impacted by the cloud-based IoT approach's various apps and astute administrations.

III. USE CASES OF THE CLOUD OF THINGS

In the information technology sector, the CoT paradigm has triggered a sea change and several noteworthy transformations. An example of this shift is the proliferation of new smart applications with the potential to completely alter the way live their lives. M2M communications, in which machines talk to each other directly rather than via a human intermediary is one of the new technologies on the list. Figure 4 shows the most important uses of CoT in this context.

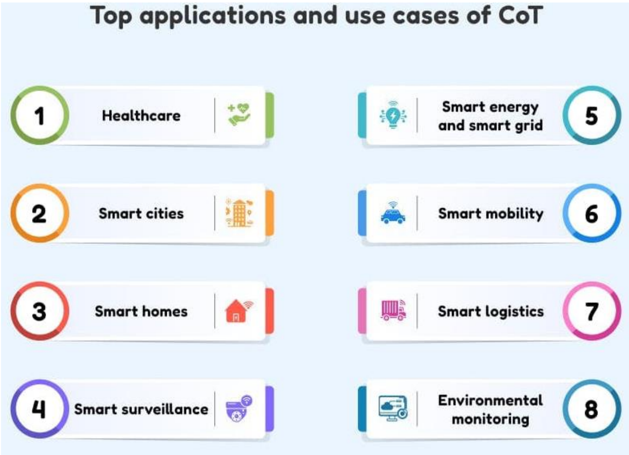
Top applications and use cases of CoT
1 Healthcare
2 Smart cities
3 Smart homes
4 Smart surveillance
Smart energy and smart grid 5
Smart mobility 6
Smart logistics 7
Environmental monitoring 8

Figure 4 : Top Applications and use Cases of CoT

A. Healthcare

The current trend of escalating health issues has resulted in a scarcity of hospital resources and a greater dependence on residential healthcare. For instance, with the use of linked devices and cutting-edge health tech, a person can bring their medical checking service to their home. Algorithms and models that can interpret data for decision-making purposes, such as medical diagnosis and treatment planning, can be developed more efficiently with this configuration.

B. Smart Cities

A shortage of natural resources is a direct result of the urban population boom in many parts of the world. More and more people are worried about the environment, and there's an ongoing need to ensure that everyone can use public services and infrastructure. To enhance the smart city experience and make it more engaging and effective, CoT promotes new generation services and applications. The issues of public safety, mobility, tourism, and urban consumption are some of the everyday difficulties that it helps tackle.

C. Smart Homes

Security and user-friendliness are the backbone of the smart home concept. Most of the capabilities for controlling and monitoring smart home devices rely on the user's home network [7]. IoT applications simplify the utilisation of heterogeneous embedded devices, paving the way for the automation of mundane operations. The use of internet-connected sensors, actuators, and local networks in smart homes enables the collection, processing, and exchange of data in real-time.

D. Smart Surveillance

Smart video surveillance systems have the capability to transmit live video feeds to several consumer devices that are linked to the internet. Video Surveillance as a Service (VSaaS) and other cloud-based technologies are essential to these systems because they efficiently store, handle, and process vital facility security data. In order to meet the needs of these kinds of applications, CoT processes complicated data in order to offer insights.

E. Smart Energy and Smart Grid

Using the monitoring and automation technologies provided by modern ICT (Information and Communications Technologies), smart energy systems and smart grids can boost their performance. These have a wide range of potential uses, one of which is in the industrial sector, where they can dramatically reduce energy use. The use of CoT facilitates optimal consumption-based energy distribution management in varied scenarios.

F. Smart Mobility

Shared mobility's meteoric ascent has shaken up the car sector. Thanks to the IoT and the cloud, consumers now have more transportation options than ever before [8]. The electrification of cars and autonomous fleets are two examples. People can save money and protect the environment with some of the choices. Mobility as a Service (MaaS) has grown in popularity due to the rise of smart cars, which aid in cost savings.

G. Smart Logistics

The demand for improved logistics services has increased in response to the enormous expansion in the e-commerce business. The implementation of COTS in that industry has resulted in a massive shift in how companies operate. As time goes on, traditional systems get smarter and can handle difficulties like traffic jams and weather changes autonomously.

H. Environmental Monitoring

The installation of sensors and actuators in areas prone to extreme weather, like farms, oil rigs, and industrial facilities, can help mitigate the increasing frequency and severity of natural disasters. Implementing the devices enhances performance by providing an ideal setting and enabling stakeholders to share data in real-time. The use of CoT can facilitate the rapid transfer of data via environmental monitoring devices.

IV. SECURITY CHALLENGES IN THE CLOUD OF THINGS

Concerns that cloud providers might not be able to trust or understand the exact location of data transmitted to the cloud through different IoT agreements have long been source of anxiety regarding cloud computing and the IoT. Storage infrastructure for cloud services with several tenants is a source of concern. There is a higher chance of data leakage and violation of confidentiality when different kinds of consumer data are stored in the same place [9]. This kind of vulnerability, which is driven by cloud service providers' distrust, has been one of the biggest surprises in the IT market thus far. Here are some of the most significant challenges with Cloud-IoT [10]:

- Security: Data collected from the IoT was automatically saved to the cloud for future use. Secure data access and storage in the cloud is an important part of this, as is the encryption of data while it is transferred to and from the cloud. Since few people understand cloud computing, data owners have no idea where their data is physically stored. Since data is now ubiquitous, protecting it under the Cloud-IoT paradigm is a popular topic of discussion [11].
- Storage and Computational performance: A high level of performance objective requirements is necessary for plans that incorporate cloud-based IoT devices. Because there are so many uses for cloud-based IoT devices, it can be challenging to match such standards in every environment.
- Maintenance: Very efficient strategies and methods for monitoring and managing cloud security and efficiency are required to satisfy the demands of up to 50 billion IoT devices.
- Edge Computing: Immediate cloud response is required by latency-bound, mobility-bound, or geo-distributed IoT implementations [12]. Edge computing, then, is a compromise between cloud computing and conventional computing; it makes more sense for some uses, but it's difficult to implement because of the need for position awareness.

- Interaction with Devices: The processing and implementation of cloud-IoT systems frequently necessitates input from a diverse array of devices. Space for storage and computing power on the cloud are two requirements that can become difficult to meet in this context.
- User-aided IoT Devices: Users are anticipated to provide information and advantages in these IoT implementations in order to be rewarded for their involvement in the exchange. This is a very difficult problem to solve since it involves social issues, where the customer's background plays a role [13].
- Reliability: The IoT devices rely on cloud computing to collaborate with service providers for mission-critical applications, and the impact would mirror the results of the program. For instance, in vehicles, medical tools, or the security industry.
- Big Data Storage: The predicted 50 billion IoT devices that will be operational by the end of the year will be a big challenge for cloud service providers when it comes to quickly and securely accessing data [14].

A. Privacy Risks and Threat Landscape

Cyberattacks, attack tactics, and vectors that target individuals, governments, and organizations are always changing, and this dynamic environment is referred to as the threat landscape. The proliferation of cloud computing, IoT devices, and linked supply chains has added complexity to a landscape already shaped by threat actors such as hackers, nation-states, and criminal organizations. Numerous cyber dangers make up the threat landscape. Organizations should keep an eye on these major assault types:

B. Zero-Day Exploits

Software, hardware, or firmware vulnerabilities that have not been discovered yet are known as zero-day exploits. Attacks can easily exploit their unpatched state. Until a patch is developed, threat actors employ these vulnerabilities to compromise systems, which can lead to devastating damages or data loss.

C. Ransomware and Malware

Ransomware attacks are among the most dangerous cyber threats. It demands ransom in exchange for sensitive data. Operating system vulnerabilities, cloud services, and IoT devices are still targets for malware development. Some ransomware organizations can employ double extortion by threatening to reveal previously stolen information if the demands are not met.

D. Social Engineering Attacks

Social engineering assaults aim to acquire access by manipulating human behaviour. Phishing, pretexting, and baiting are common attack methods that use human error to compromise security. These kinds of attacks are extremely dangerous for any business since they bypass defences and exploit trust among employees.

E. Advanced Persistent Threats (APTs)

APTs are presently focused, long-term assaults that are often orchestrated by well-funded groups or even nation-states. In order to breach networks and steal sensitive information, it aims for low-profile vectors. APTs can accomplish their goals by conducting reconnaissance, compromising systems initially, and maintaining access for an extended length of time.

F. Data Breaches and Data Leaks

Concerns regarding unauthorized access to sensitive data have been raised. Threat actors exploit unprotected credentials and databases to gain unauthorized access to sensitive information. Leaks of sensitive information occur because they take advantage of careless password practices. Companies typically have to spend a lot of money on damage control and compliance when a breach occurs.

G. Denial of Service (DoS)

The goal of these types of assaults is to flood systems with traffic. The majority of the time, they are led to vital online resources. At the very least, DDoS attacks are being weaponized to cause reputational harm, which can lead to financial losses. An ever-increasing number of attackers are taking advantage of botnets, making it harder to contain them.

V. SECURITY SOLUTIONS AND BEST PRACTICES

The Cloud of Things (CoT) poses distinct challenges to on account of its hybrid nature, sheer size, and non-stop streaming of data that is created by heterogeneous devices. In order to respond to the security and privacy issues in CoT environments, the given layered and integrated solutions are suggested:

A. Secure Architectural Design

- Decentralized Security Models: Implement edge and fog computing layers as a form of processing offloading and shortening data transmission distances to reduce attack surfaces and latency.
- Microservices-Based Security: Ensure that the blast radius of possible breaches is restricted by utilizing modular, and isolated microservices in the cloud.

- Zero Trust Architecture (ZTA): Adopt never trust, always verify concepts to devices, networks and users.

B. Data Protection Mechanisms

- End-to-End Encryption: Encrypt the data at all points in their lives: at rest, in transit, and in use by employing resource-efficient cryptographic protocols with IoT devices with limited resources.
- Homomorphic Encryption and Secure Multiparty Computation: Provide a way of data processing which do not involve decryption to uphold privacy within shared cloud ecosystems.

C. Robust Authentication and Access Control

- Multi-Factor Authentication (MFA): Conduct combined passwords, biometrics, and device authentication to CoT access services freely.
- Attribute-Based Access Control (ABAC): Improve the classic Role-Based Access Control (RBAC) with fine-grained user, device, and context-based policy enforcement.

D. Intrusion Detection and Anomaly Monitoring

- Threat Detection using AI: Monitor based on behavior and identify malicious activity, detect zero-day attacks and respond in real-time using machine learning algorithms.
- Blockchain-Based Logging: Use blockchain chain to record transactions and track activity of devices irreversibly to enhance responsibility and auditability.

E. Privacy-Preserving Frameworks

- Data Minimization and Federated Learning: Retain only the minimum amount of data and apply decentralized training procedures in order to improve privacy.
- Context-Aware Privacy Policies: Adjust privacy settings according to a specific location, application sensitivity, and context.

F. Regulatory Compliance and Governance

- Automated Compliance Checking: Integrate compliance tools to automatically verify adherence to regulations like GDPR, HIPAA, and ISO/IEC 27001.
- Security SLAs with Cloud Providers: Establish clear service-level agreements defining shared responsibilities for data protection and incident response.

VI. LITERATURE SURVEY

A wide range of technological aspects have been investigated in recent studies pertaining to the IoT and cloud-based technologies. Review articles on this topic of study from a variety of disciplines have been the subject of much effort.

Gattobigio et al. (2022) offer a design that may be used to realize a network service mesh, allowing for the connection, interaction, and data exchange of numerous IoT edge devices hosted in separate contexts. The elements required, as well as possible uses, are defined in a logical architecture that is put forth. Just to prove that the system can work, an implementation is carried out. It is feasible to bring the advantages of a service mesh to IoT edge devices and the apps running on them with just a little increase in processing power and time, according to the measurements [15].

Kashyap et al. (2021) reveal crucial safety measures and a number of serious issues that require fixing. The research group has recently been concentrating on the security issues and problems surrounding the IoT that is hosted in the cloud. Recently, there has been a surge in the number of surveys covering topics including intrusion detection systems, new technology, threat modelling, and future threats. In this study, the impact of the IoT on data security is described in order to illustrate the gap. IoT security is the focus of this article, which takes a multi-layered approach to the idea of cloud-based IoT architecture and suggests several threats and solutions [16].

Nguyen et al. (2020) offer a comprehensive overview of the BCoT covering its history, purpose, and architecture in order to give laypeople a feel for what it's all about. Their comprehensive review of BCoT applications in several use-case areas, including smart cities, smart transit, smart healthcare, and smart industry, is a particular strength of their findings. Their next stop is a survey of current BCoT initiatives that incorporate new blockchain and cloud applications, platforms, and studies. As a conclusion, stress a few key areas for further study and research directions to encourage more investigation into this exciting field [17].

Suresh and Kumar (2020) environmental monitoring applications can be seamlessly incorporated into a plug-and-play architecture based on the IoT and VIoT. Subsequently, two applications built using the aforementioned architecture are demonstrated. To respond to the data inputs and outputs generated by a wide range of devices integrated into real-time applications, the automation and actuators in this context are carried out according to predefined constraints [18].

Eugster et al. (2019) Cloud of Things (CoT) is an emerging concept that combines cloud computing with the IoT. However, its foundational ideas are not yet established. Public clouds already have security issues due to multitenancy; adding resource-constrained IoT devices to the mix further complicates cyber trust. One such solution is to perform computations on encrypted data stored in an untrusted cloud using partially homomorphic encryption intelligently. summarize the takeaways from the transition from the idea of confidentiality-preserving CoT to its practical implementation as it pertains to handling ongoing enquiries on streams of sensitive data generated by IoT devices [19].

Lin, Hsieh and Li (2018) secure cloud-based map-reduce operations through the use of elliptic curve cryptography on the IoT and group signatures with threshold secret sharing techniques. A security gateway, a server that acts as the controller and the cloud service itself comprise the proposed architecture. Data transfer security, mutual authentication of IoT items, and cloud computing platform intrusion prevention are all goals of this study's architecture [20].

A number of important knowledge gaps persist in Cloud of Things (CoT) security, despite substantial progress in this area. When it comes to scaling across heterogeneous IoT-cloud systems, the majority of current solutions are too domain-specific. Table I summarizes the current state of research into different technologies, but it shows that no comprehensive, interoperable security framework has been developed yet that can respond to real-time threats with minimal latency and wasted resources. The computational overheads imposed by current encryption algorithms are sometimes too great for resource-constrained IoT devices, even when they are effective. Additionally, the practical deployment of privacy-preserving technologies such as federated learning and homomorphic encryption is still in its early phases. There is a lack of research on issues like safe device authentication, decentralized trust management, and the smooth integration of fog and edge computing. To fill these gaps and guarantee end-to-end protection throughout the entire CoT architecture, need security solutions that are lightweight, scalable, and context-aware.

Table 1 : Summary of Previous Research Studies on Securing the Cloud of Things (COT)

Author	Focus	Technologies Used	Key Contributions	Challenges / Recommendations
Gattobigio et al. (2022)	Facilitating communication and data transfer between Internet of Things edge devices in various settings	Service Mesh, Network Virtualization	Proposed a logical architecture and implemented a service mesh for IoT edge with minimal overhead	Scalability in heterogeneous environments: real-world deployment in diverse IoT use cases
Kashyap et al. (2021)	Identifying security issues in cloud-based IoT layers	Cloud-IoT Architecture, IDS, Threat Modeling	Highlighted major IoT-cloud vulnerabilities and proposed multi-layered security considerations	Need for stronger intrusion detection systems and secure integration frameworks
Nguyen et al. (2020)	Comprehensive review of Blockchain-Cloud-IoT integration (BCoT)	Blockchain, Cloud Services, Smart Applications	Surveyed BCoT use cases across domains; summarized trends and emerging platforms	Calls for standardized frameworks and solutions for BCoT interoperability and scalability
Suresh & Kumar (2020)	VIoT-based plug-and-play framework for real-time environmental monitoring	Virtual IoT (VIoT), Automation, Real-Time Actuation	Designed a plug-and-play model for real-time application response and automation	Need for enhanced support for dynamic constraints and real-time performance validation
Eugster et al. (2019)	Confidentiality-preserving cloud of things using secure processing	Partially Homomorphic Encryption, Stream Processing	Demonstrated secure data processing using encryption in untrusted cloud environments	High computational cost; suggested need for lightweight privacy-preserving solutions
Lin, Hsieh & Li (2018)	Securing cloud-IoT communication using cryptographic methods	ECC, Group Signature, Threshold Secret Sharing	Developed architecture to ensure authentication and secure MapReduce operations	Complexity in key management; recommended optimizing cryptographic operations for IoT limits

VII. CONCLUSION

The IoT gives people a new way to connect with the Internet through networks that are everywhere. Objects can connect to cloud computing lets easily connect to a shared pool of flexible computer resources over the internet whenever it needs to. The main topic of this paper is the Cloud Things architecture, which is a popular way to connect the IoT and Cloud Computing. The main problems with CoT systems have been found in this study. These problems include data breaches, insider risks, and denial-of-service attacks. The analysis also highlights the need for robust, layered security frameworks incorporating encryption, real-time threat detection, access control, and privacy-preserving mechanisms. Additionally, regulatory compliance and trust management must be integrated into the security design. Although existing research has proposed various solutions from edge computing to blockchain and homomorphic encryption, many approaches lack scalability, interoperability, or practicality in real-world settings. Thus, future research must focus on developing lightweight, adaptive, and context-aware security models tailored to the dynamic nature of CoT environments. Securing CoT systems is essential not only for protecting sensitive data but also for ensuring the trust, reliability, and long-term viability of next-generation smart applications.

VIII. REFERENCES

[1] M. Ansari, S. A. Ali, and M. Alam, "Internet of things (IoT) fusion with cloud computing: current research and future direction," International Journal of Advanced Technology and Engineering Exploration. 2022. doi: 10.19101/IJATEE.2021.876002.

[2] J. Lee, A. Abid, F. Le Gall, and J. S. Song, "Recent Trends on Artificial Intelligence-Enabled Internet of Things Platform and Standard Technologies," in 2022 IEEE 8th World Forum on Internet of Things, WF-IoT 2022, 2022. doi: 10.1109/WF-IoT54382.2022.10152226.

[3] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," Futur. Gener. Comput. Syst., 2016, doi: 10.1016/j.future.2015.09.021.

[4] V. K. Sanjeevi, "An integrated secured architecture for Cloud of things," 2019.

[5] S. Haq, A. Bashir, and S. Sholla, "Cloud of things: Architecture, research challenges, security threats, mechanisms and open challenges," Jordanian Journal of Computers and Information Technology. 2020. doi: 10.5455/jjcit.71-1592021856.

[6] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering. 2017. doi: 10.1155/2017/9324035.

[7] S. Garg, "Next-Gen Smart City Operations with AIOps & IoT : A Comprehensive look at Optimizing Urban Infrastructure," J. Adv. Dev. Res., vol. 12, no. 1, 2021.

[8] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.

[9] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. Saifullah Sami, and R. R. Zebari, "IoT and Cloud Computing Issues, Challenges and Opportunities: A Review," Qubahan Acad. J., vol. 1, no. 2, pp. 1–7, Mar. 2021, doi: 10.48161/qaj.v1n2a36.

[10] S. S. Gill et al., "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges," Internet of Things (Netherlands). 2019. doi: 10.1016/j.iot.2019.100118.

[11] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," Appl. Sci., 2020, doi: 10.3390/APP10124102.

[12] V. Singh, "Lessons Learned from Large-Scale Oracle Fusion Cloud Data Migrations," Int. J. Sci. Res., vol. 10, no. 10, pp. 1662–1666, 2021.

[13] K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed, and N. Guizani, "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs," IEEE Access, vol. 7, pp. 79980–79988, 2019, doi: 10.1109/ACCESS.2019.2922971.

[14] S. S. S. Neeli, "Ensuring Data Quality: A Critical Aspect of Business Intelligence Success," Int. J. Lead. Res. Publ., vol. 2, no. 9, 2021.

[15] L. Gattobigio, S. Thielemans, P. Benedetti, G. Reali, A. Braeken, and K. Steenhaut, "A multi-cloud service mesh approach applied to Internet of Things," in IECON Proceedings (Industrial Electronics Conference), 2022. doi: 10.1109/IECON49645.2022.9968384.

[16] N. Kashyap, A. Rana, V. Kansal, and H. Walia, "Improve Cloud Based IoT Architecture Layer Security - A Literature Review," in Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021, 2021. doi: 10.1109/ICCCIS51004.2021.9397146.

[17] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," IEEE Commun. Surv. Tutorials, 2020, doi: 10.1109/COMST.2020.3020092.

[18] K. Suresh and G. V. Kumar, "Integrated Cloud Internet of Things for Realtime Applications," in 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Oct. 2020, pp. 631–635. doi: 10.1109/I-SMAC49090.2020.9243454.

[19] P. Eugster, S. Kumar, S. Savvides, and J. J. Stephen, "Ensuring Confidentiality in the Cloud of Things," IEEE Pervasive Comput., vol. 18, no. 1, pp. 10–18, Jan. 2019, doi: 10.1109/MPRV.2018.2877286.

[20] H. Y. Lin, M.-Y. Hsieh, and K.-C. Li, "Researches on secure data transmission mechanisms in cloud Internet of Things architectures," in 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, Aug. 2017, pp. 1–4. doi: 10.1109/UIC-ATC.2017.8397645.