Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

Heterogeneous IoT based Cloud Data Retrieval System

Dr Nagaraja G S
Professor & Assoc.dean
Dept of CSE, RV College of Engineering
Bangalore

Sangeetha S
M.Tech in Computer Network Engineering
Dept of CSE, RV College of Engineering Bangalore

***Abstract* - A system that collects and retrieves data from different sources of IoT devices and stores them in the cloud to handle diverse types of data, including structured and unstructured data, from a variety of devices is called heterogeneous IoT based Cloud data retrieval system. The homogeneous IoT based system only suitable for retrieving data from similar kind of devices, but the proposed solution will provide flexible and efficient method of gathering, storing, and retrieving data from variety of devices. This solution includes creation of virtual devices in Node-red and storing device details in database. This paper able to retrieves the data i.e, device details from the database with the help of data retrieval microservice in the form of file. A dedicated data retrieval microservice acts as an intermediary between the application and the database. It provides a secure API for users to request data from specific devices. This microservice is equipped with safeguards against unauthorized access and potential security breaches.**

***Keywords* - REST API, Microservice, Cloud technology**

I. INTRODUCTION

A data retrieval system is one that is created to quickly and effectively extract information from a collection of data, such as a database. Users can search and obtain specific data from a huge data source using the system. An element of a data storage and management system that makes use of cloud computing technology is a cloud-based data retrieval system, as shown in figure 1.1. Accordingly, rather than being kept on local PCs or servers, the data is kept and controlled remotely on servers that are hosted by a third-party supplier. Users can access their stored data via a web browser or specialized software

Fig 1. Overview of Cloud based data retrieval system

retrieval system through the internet. As long as there is an internet connection, the system is built to give users quick, dependable, and secure access to data from anywhere in the globe. Systems for retrieving data from the cloud storage can be used by different sizes of people, companies, and organizations. They are employed for data backup, disaster recovery, and teamwork. Large amounts of data that would be prohibitively expensive or challenging to manage on local servers or hard drives can also be stored and managed using them.

Components of cloud-based data retrieval system

Cloud storage: The infrastructure must be kept up to date, and data security must be guaranteed, according to the cloud storage provider. In the cloud, the data is managed and kept here.

Data retrieval APIs: Application programming interfaces that allow users to retrieve their data from the cloud storage service. These APIs can be accessed through software applications or web-based interfaces.

Data retrieval software: The software that users use to retrieve their data from the cloud. The software can be a web-based application or a desktop application.

Security features: Security is a critical component of any cloud-based data retrieval system. The system must have measures in place to protect the data from unauthorized access, data breaches, and other security threats.

Data redundancy and backup: The system should have redundant data and backup procedures in place to guarantee data availability and avoid data loss. So as to protect against data loss due to system failures or disasters, numerous copies of the data are kept in various places, and backups are frequently made[33].

Network infrastructure: A strong network infrastructure is necessary for the cloud-based data retrieval system to offer quick and dependable access to the data. This includes the data centers, servers, and other networking elements, as well as the internet connectivity.

Data encryption: To prevent unauthorized access, data must be encrypted and converted into a coded language. Data encryption is an essential part of a cloud-based data retrieval system that helps to protect the confidentiality and privacy of the data. The system should encrypt the data both in transit and at rest using robust encryption methods.

Access controls: Access controls are mechanisms that limit access to the data to authorized users only. In a cloud-based data retrieval system, access controls are necessary to prevent unauthorized access, data breaches, and other security threats. The system should have granular access controls that allow users to set different levels of permissions for different users or groups.

II. LITERATURE SURVEY

A Cloud-Enabled Heterogeneous IoT Framework for Data Retrieval and Processing [1] that offers a literature review that provides a thorough study and knowledge of the work done in the field of heterogeneous IoT infrastructure for cloud data retrieval systems. A system that gathers and retrieves data from various IoT device sources and saves it in the cloud is known as a heterogeneous IoT-based cloud data retrieval system. This kind of system is made to handle many data kinds, including unstructured and structured data, from a number of devices, including sensors, cameras, and other Internet of Things (IoT) devices.

Design and Implementation of a Heterogeneous IoT-Based Cloud Data Retrieval System for Smart Agriculture [2] that presents a system for data retrieval in smart agriculture using IoT devices and cloud computing and provides a comprehensive overview of the proposed system and its implementation. The paper lacks a comprehensive evaluation of the proposed system with metrics such as response time, throughput, and CPU usage, they have not compared their system's performance with other similar systems in the literature. Heterogeneous IoT-Based Data Retrieval System for Smart Energy Management in Buildings[3]It provides an intelligent energy management system for buildings based on an IoT cloud data retrieval technology. The system comprises of a gateway, several devices, cloud servers, and a mobile application. A system called "smart energy management" integrates IoT to bring information about tracking, measuring, controlling, and optimizing energy consumption across buildings. These systems struggle with issues like restricted scope and scalability. Goals of this system include climate protection and a reduction in greenhouse gas emissions.An Efficient Named-Data-Networking-Based IoT Cloud Framework In order to increase data retrieval success rates and lower costs, we offer a practical NDN-based IoT cloud architecture. IoTC may be made possible by the named data networking (NDN), which offers a new data-centric paradigm. This finding has encouraged us to use NDN to achieve IoTC. However, it is difficult to install NDN in the IoT due to various designs and operating systems. For instance, NDN uses restricted floods and reverse pathways to acquire data, which may result in frequent data capture failures and high costs in mobile contexts like the Internet of Things.

[3] Enabling secure cross modal retrieval over encrypted heterogeneous iot databases with collective matrix factorization This modality contains information about a multimodal retrieval system that transports sensitive data. In order to create an effective and precise method for cross-modal retrieval without losing any sensitive data, this work combines homomorphic encryption (HE) and collective matrix factorization (CMF). The method obtains the mapping matrices for out-of-sample objects and determines the unified feature vectors for each object in the training set using several modalities.

[4] An Efficient Named-Data-Networking-Based IoT Cloud Framework In order to increase data retrieval success rates and lower costs, we offer a practical NDN-based IoT cloud architecture. IoTC may be made possible by the named data networking (NDN), which offers a new data-centric paradigm. This finding has encouraged us to use NDN to achieve IoTC. However, it is difficult to install NDN in the IoT due to various designs and operating systems. For instance, NDN uses restricted floods and reverse pathways to acquire data, which may result in frequent data capture failures and high costs in mobile contexts like the Internet of Things.

[5] Enabling secure cross modal retrieval over encrypted heterogeneous iot databases with collective matrix factorization This modality contains information about a multimodal retrieval system that transports sensitive data. In order to create an effective and precise method for cross-modal retrieval without losing any sensitive data, this work combines homomorphic encryption (HE) and collective matrix factorization (CMF). The method obtains the mapping matrices for out-of-sample objects and determines the unified feature vectors for each object in the training set using several modalities.

An energy efficient heterogeneous IoT data retrieval approach based on cloud computing and compressed sensing [6] The Internet of Things (IoT) networks have become the infrastructure to enable the detection and reaction of anomalies in various domains, where an efficient sensory data gathering mechanism is fundamental since IoT nodes are typically constrained in their energy and computational capacities. To decrease the energy consumption of IoT networks, this includes an energy-efficient sensory data gathering mechanism, where the category of sensory data is processed by adopting the compressed sensing algorithm.

[7] A survey of cloud storage retrieval systems provides a comprehensive survey of cloud storage retrieval systems, which are used to access data stored in the cloud. The categorization existing cloud data retrieval system into three major groups such as content-based data retrieval system, metadata-based retrieval system and hybrid retrieval system. The metadata-based retrieval systems rely on the metadata associated with the data objects to locate and retrieve them from the cloud storage. The content-based retrieval systems, on the other hand, use the content of the data objects to search and retrieve them from the cloud storage. The hybrid retrieval systems combine the metadata-based and content-based retrieval techniques to leverage the strengths of both approaches.

III. CLOUD DATA RETRIEVAL SYSTEM ARCHITECTURE

A heterogeneous IoT-based cloud data retrieval system is a system that collects and retrieves data from different sources of IoT devices and stores them in the cloud. This type of system is designed to handle diverse types of data, including structured and unstructured data, from a variety of devices, such as sensors, cameras, and other IoT devices as shown in figure2.

A network of Internet of Things (IoT) devices in the system gather and transmit data to a cloud-based data storage system. The solution enables seamless data transfer between IoT devices and the cloud by utilizing a number of communication protocols, including MQTT, CoAP, and HTTP. The acquired data must be stored and managed by the cloud-based data storage system. To handle multiple data kinds, it leverages a variety of data storage methods, including relational and NoSQL databases. The system also incorporates data processing and analysis tools to offer in-the-moment insights and allow for data-based decision-making.

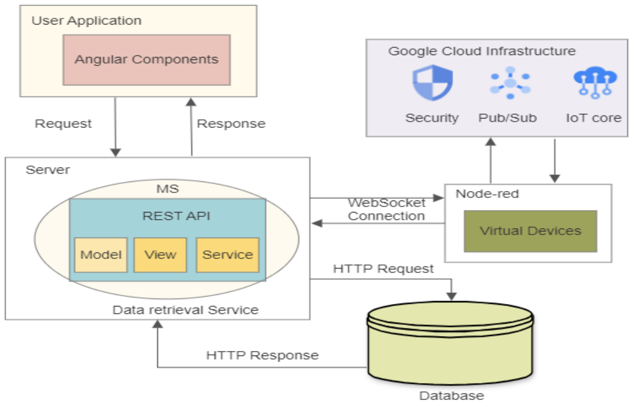


Fig 2. Heterogeneous IoT cloud data retrieval system architecture

To ensure data security and privacy, the system implement various security measures such as access control, data encryption, and data anonymization. IoT devices can generate large amounts of data, and this data can be valuable for a variety of purposes such as monitoring, analysis, and decision-making. However, collecting, storing, and retrieving this data can be challenging, especially when dealing with multiple types of devices that have different communication protocols and data formats.

The system includes user application, microservice, cloud technologies and database. Users or applications send data retrieval requests to the Cloud Server. The Cloud Server processes the requests and retrieves the requested data from the Cloud Storage. The retrieved data is sent back to the User Interface, where users or applications can access and view the data.

1. User Interface (UI): The user interface provides a platform for users to interact with the system. It could be a web-based application or a mobile app. Users can monitor and control IoT devices, visualize data, set up triggers or alerts, and manage their devices and data.
2. Data Retrieval Microservice: The data retrieval microservice is responsible for handling data requests from various sources, processing data, and forwarding it to the appropriate destinations. It interacts with the IoT devices, Node-RED, and other components to retrieve data.
3. Node-RED: Node-RED is a flow-based development tool for visual programming. In this architecture, it can be used to create virtual devices, simulate IoT device behavior, generate test data, and perform data transformations before sending it to the cloud. Node-RED provides a user-friendly way to create data flows and logic.
4. Cloud Technologies: The cloud technologies you've mentioned include Pub/Sub, IoT Core, and security. Here's how they fit into the architecture:
   - Pub/Sub: Google Cloud Pub/Sub is used as a messaging system for communication between different components of the system. It facilitates real-time data exchange and event notifications. The data retrieval microservice can subscribe to relevant topics to receive data updates from various sources.
   - IoT Core: Google Cloud IoT Core provides the infrastructure for managing IoT devices at scale. It allows you to securely connect and manage IoT devices, set up device communication, and manage device metadata. IoT Core can handle device registration, authentication, and communication encryption.
   - Security: Implement security measures such as user authentication and authorization for accessing the UI and interacting with the system.
5. MongoDB Database: MongoDB is a NoSQL database that can be used to store and manage the collected IoT data. It provides flexible schema-less data storage, which can accommodate varying data structures from different types of IoT devices. Data retrieved from devices can be stored in MongoDB for later analysis and retrieval.
6. Interconnections: The components in this architecture are interconnected in the following ways:
   - IoT devices communicate with the IoT Core for secure device management and data transmission.
   - Virtual devices created using Node-RED can simulate IoT devices and send simulated data to the data retrieval microservice.
   - The data retrieval microservice subscribes to Pub/Sub topics to receive data from various sources, including real IoT devices and virtual devices.
   - The microservice processes the data, performs any necessary transformations, and stores it in the MongoDB database.
   - The user interface interacts with the data retrieval microservice to request data, display visualizations, and allow users to control IoT devices.

IV. KEY THEORIES AND CONCEPTS

The following are some essential theories and principles regarding Heterogeneous IoT based Cloud Data Retrieval:

Internet of Things (IoT): The Internet of Things (IoT) is a network of physically connected, interconnected objects that can exchange data in a variety of ways as shown in figure 3. In this project, IoT devices play a significant role. Homogeneous and heterogeneous IoT devices are two different types of IoT devices that can be categorized. IoT devices come in a wide variety, including both IoT and Non-IoT devices.

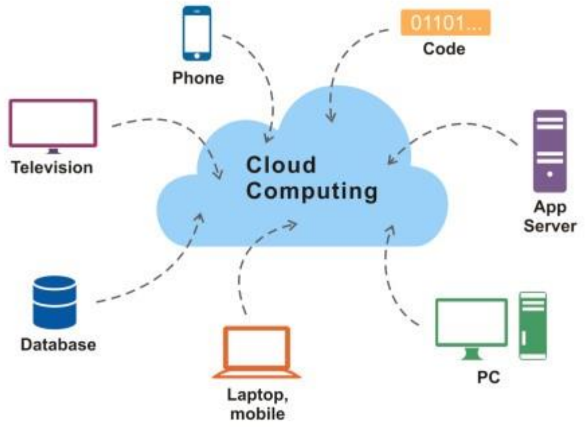


Fig 3. Interconnection of physical devices to internet

Cloud computing: Cloud computing is a type of technology that allows customers to access more servers, storage, databases, and applications online. Users can store, analyze, and retrieve data on remote servers rather than local devices thanks to the cloud computing environment. This technology plays a significant part in this project because it is challenging to create connection between IoT devices and Non-IoT devices without using a cloud platform. In order to provide a single platform for data retrieval, the storage of vast amounts of data from a range of devices, including as sensors, cameras, and other IoT devices, should be able to handle multiple types of devices with diverse processing power, storage capacity, and communicationprotocols.

Microservice: Microservices architecture is an approach to designing and building software applications where the application is broken down into a collection of smaller, independent services. Each of these services, known as microservices, focuses on a specific business capability and can be developed, deployed, and managed separately from the others. Instead of creating a single, monolithic application, where all the code is tightly integrated, microservices architecture promotes modularity and loose coupling. Each microservice operates as a separate entity with its own codebase, data storage, and functionality. They communicate with each other through well-defined APIs, often using lightweight protocols like HTTP or messaging systems.

Communication Protocols: IoT core communicates with the cloud using the MQTT/HTTP protocols. Messaging Queue Telemetry Transport, or MQTT, is a resource-constrained network protocol created for the Internet of Things. The small code footprint and low bandwidth requirements of MQTT make it simple and effective. According to the publish/subscribe messaging model used, as seen in figure 4, clients subscribe to topics, and publishers then deliver messages to those topics. This

enables scalable and effective communication between devices.

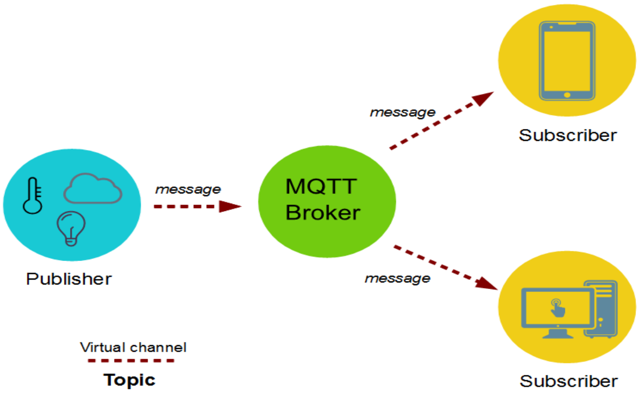


Fig 4. Working of MQTT protocol

MQTT uses a straightforward binary format to minimize the amount of data transmitted over the network and runs on top of the TCP/IP protocol. In order to guarantee dependable message delivery, it also provides Quality of Service (QoS) levels.

REST API: Application Programme Interface and REST are acronyms for representational state transfer and respectively. The architectural style of software known as REST specifies the set of guidelines to be followed while developing web services. Those web services that adhere to the REST architectural design are referred to as RESTful web services. Through the use of a uniform and predetermined set of rules, it enables requesting systems to access and modify web resources. The Hypertext Transfer Protocol (HTTP) over the Internet is used for communication in REST-based applications.

V. DESIGN

Secure and effective access to data storage is provided by heterogeneous IoT-based data retrieval systems. Based on the condition of the devices, the user can authenticate and authorize himself before requesting the data from the server. The server asks Node-RED to connect the virtual devices when the user sends a request. Node-red develops DTCO devices, which are virtualized versions of actual Internet of Things hardware, based on software. Google IoT core device registry is in charge of managing device information. Users can request data from specific devices once they are online. All device-related information is kept in a database. A data retrieval microservice is used to facilitate effective communication between an application and a database. Server stores the device details in database. If data is valid client get the device details and user can request to download the data based on the status of device. The design of the system is shown in the figure 5. Combining WebSocket and HTTP communication in a heterogeneous IoT-based cloud data retrieval system can provide a balanced and efficient approach to handle real-time data streams and traditional request-response interactions. WebSocket communication is ideal for real-time data streaming and bidirectional communication between the IoT devices (Node-RED) and the data retrieval service.

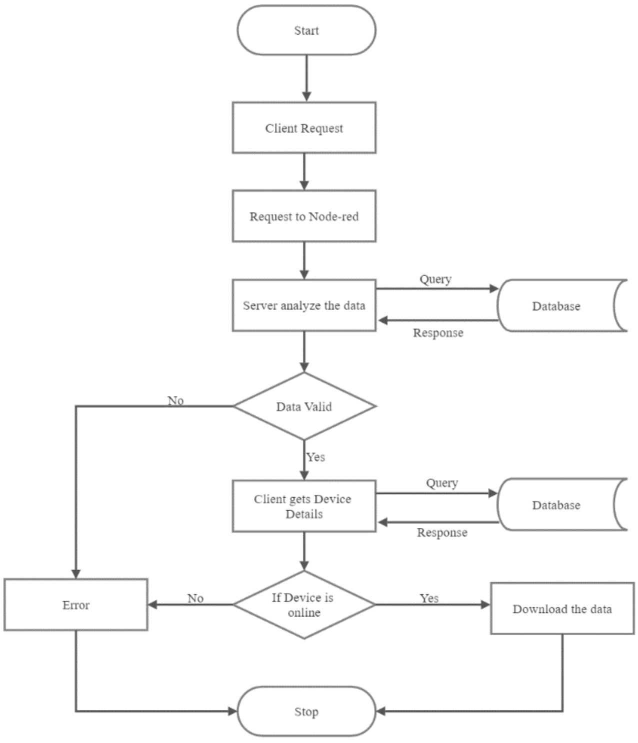


Fig 5. Design of Heterogeneous IoT based cloud data retrieval system.

HTTP communication is suitable for traditional request-response interactions, especially when fetching data from a database.

VI. METHODOLOGY

The methodology for implementing the secure and effective access to data storage in the heterogeneous IoT-based data retrieval system. It includes considerations for user authentication, device management, data retrieval, and communication using both WebSocket and HTTP protocols.

User Authentication and Authorization: Users are required to authenticate themselves using their credentials. This ensures that only authorized individuals can access the system.

Device Management: Device information is maintained using Google IoT Core's device registry. Virtualized versions of physical IoT devices, known as DTCO devices, are created within Node-RED. These software-based devices are orchestrated to respond to user requests for data.

Data Retrieval Microservice: A dedicated data retrieval microservice acts as an intermediary between the application and the database. It provides a secure API for users to request data from specific devices. This microservice is equipped with safeguards against unauthorized access and potential security breaches.

Data Storage and Database: A structured database stores comprehensive device-related information, including metadata, ownership, and status details. Historical data from devices can also be stored for future analysis and reference, if necessary.

WebSocket Communication: WebSocket connections are established between Node-RED and the data retrieval service. These connections enable seamless, bidirectional communication, supporting real-time data streaming and control signal transmission to the virtual devices.

HTTP Communication: HTTP endpoints are established within the data retrieval microservice to cater to users' data retrieval requests. Users can conveniently request data from specific devices using standard HTTP requests. The microservice retrieves the data from the database and provides a response.

Secure Communication: All forms of communication, including WebSocket and HTTP, are fortified with encryption protocols (such as SSL/TLS). This safeguards data against interception and maintains the privacy of sensitive information. Additionally, stringent authentication and authorization mechanisms are in place for both WebSocket and HTTP communication.

User Interaction: Upon device connectivity, users can initiate data requests for specific devices. These requests trigger the server to establish WebSocket connections with the relevant virtual devices. Subsequently, the virtual devices fetch the requested data and transmit it through the WebSocket connection. The data is then relayed to the user for reporting purposes. By adhering to these approaches, the heterogeneous IoT-based cloud data retrieval system ensures secure access to data storage, enabling effective reporting of IoT device information and real-time data streams.

VII. RESULTS

Results achieved by utilizing Node-RED for creating virtual devices through Google Cloud IoT Core, as well as implementing a data retrieval system with a device API to fetch device details from a database.

Node-RED and Virtual Devices:

Node-RED, a powerful visual programming tool, has been harnessed to create virtual devices, known as DTCO (Device-To-Cloud Orchestrator) devices. These software-based replicas mirror the behavior of actual IoT hardware. Through Node-RED's intuitive interface, these virtual devices are orchestrated to interact with cloud services seamlessly.The virtual devices created in Node-RED are seamlessly integrated with Google Cloud IoT Core. The core's device registry takes charge of managing critical device information. This integration empowers users to interact with these virtual devices efficiently and access real-time data streams.

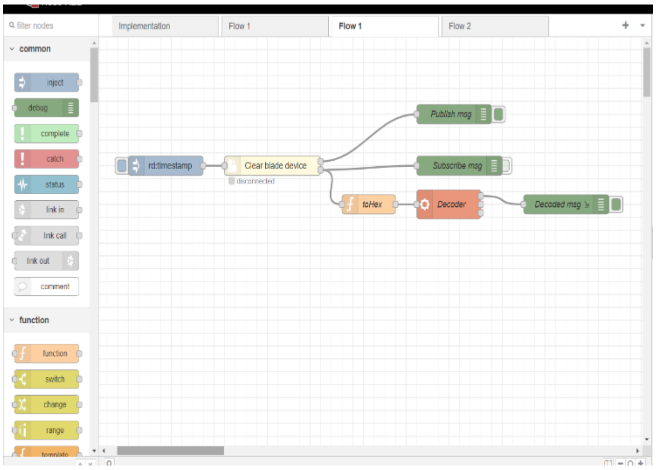
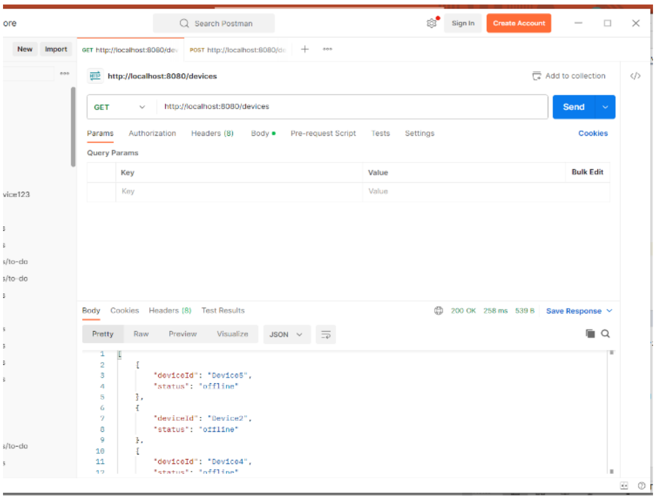


Fig 6. Virtual device creation using Node-red

Data Retrieval Service:

A dedicated data retrieval system has been meticulously designed to streamline data access and retrieval. This system acts as an intermediary, ensuring smooth communication between applications and databases. By encapsulating data-related complexities, it enables users to focus solely on accessing the information they need.
Device API for Database Interaction:

Within the data retrieval system, a robust Device API has been developed. This API serves as a gateway for users to request device details from the database. This design decision simplifies the user experience by enabling them to request data from specific devices without delving into complex database interactions.



http://localhost:8080/devices

GET http://localhost:8080/devices

200 OK 258 ms 539 B

```
[
    {
        "deviceId": "Device5",
        "status": "offline"
    },
    {
        "deviceId": "Device2",
        "status": "offline"
    },
    {
        "deviceId": "Device4",
        "status": "offline"
```

Fig 7. Device details of Device API

VIII. CONCLUSION

In conclusion, the heterogeneous IoT-based cloud data retrieval system represents a comprehensive and successful endeavor in harnessing the power of IoT technology to efficiently manage and utilize data from diverse sources. The project integrates various key components, including Node-RED for virtual device creation, Spring Boot for data retrieval microservices, Google Cloud IoT Core for device management, and MongoDB for data storage.

Throughout the project, each component demonstrated its effectiveness and contributed to the system's overall success. Node-RED's capability to create virtual devices and simulate real-time data flows provided a realistic testing environment. Spring Boot's microservices architecture ensured efficient data retrieval, processing, and storage, while MongoDB facilitated secure and accessible data storage. Integration with Google Cloud IoT Core elevated the system's security and device management capabilities, ensuring data integrity and compliance with industry standards. Future work incorporating non-IoT device integration such as sensors, industrial equipment, or even traditional machinery, into the system's architecture. This expansion broadens the scope of data sources, allowing the system to gather information from a wider array of devices, both IoT and non-IoT.

REFERENCES

[1] A Cloud-Enabled Heterogeneous IoT Framework for Data Retrieval and Processing" by Y. Zhang, Y. Liu, and Y. Yu. IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1903-1913, 2020

[2] Design and Implementation of a Heterogeneous IoT-Based Cloud Data Retrieval System for Smart Agriculture" by L. Xu, X. Liu, and Z. Wang. IEEE Access, vol. 8, pp. 143976- 143986, 2020.

[3] Heterogeneous IoT-Based Data Retrieval System for Smart Energy Management in Buildings" by S. A. Alsaba, S. M. El-Sayed, and S. A. El-Rabaie. IEEE Access, vol. 8, pp. 190355-190369, 2020.

[4] X. Wang and S. Cai, "An Efficient Named-Data-Networking-Based IoT Cloud Framework," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3453-3461, April 2020, doi:10.1109/JIOT.2020.2971009.

[5] Cui, X., Chen, M., Zhang, Y., & Zhang, Y. (2021). A secure and efficient heterogeneous data retrieval method based on cloud storage in IoT. Cluster Computing, 24(2), 1309-1319.

[6] H. Zhou et al., "An energy-efficient heterogeneous IoT data retrieval approach based on cloud computing and compressed sensing," IEEE Internet of Things Journal, vol. 8, no. 12, pp.9882-9892, Jun. 2021.

[7] Y. Zhang, Y. Sun, and W. Liu, "A survey of cloud storage retrieval systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 10, pp. 2774-2789, Oct. 2015,

[8] Yudong Li, Feng Li, and Xiaojun Li, "A High Performance Data Retrieval System Based on Cloud Computing for Internet of Things," Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 1, pp. 109-117, Jan. 2018. DOI: 10.1007/s12652-017-0544-7.

[9] Guoqing Li, Yawei Li, and Hao Yu, "Scalable Data Retrieval System Based on Cloud Computing and Inverted Index," Journal of Parallel and Distributed Computing, vol. 130, pp. 37-46, Nov. 2019. DOI: 10.1016/j.jpdc.2019.04.010.

[10] Y. Zhang, Y. Sun, and W. Liu, "A survey of cloud storage retrieval systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 10, pp. 2774-2789, Oct. 2015, doi: 0.1109/TPDS.2014.2383781.

[11] M. Elhoseny, R. M. Alarifi, M. Abdel-Aziz, A. Salama, and M. A. Abou-Elnour, "A Survey on Heterogeneous IoT Cloud Data Storage and Retrieval," IEEE Access, vol. 9, pp. 32031-32049, 2021. DOI: 10.1109/ACCESS.2021.3056616.

[12] Jianyi Huang, Guanchen He, Yiyuan Huang, and Guoquan Lu, "Design and Implementation of IoT Application Development System Based on Node-RED," Journal of Physics: Conference Series, vol. 1766, no. 1, p. 012013, Apr. 2021. DOI: 10.1088/1742-6596/1766/1/012013.

[13] Ayan Banerjee, Anupam Dutta, Arijit Ukil, and N. R. Das, "Internet of Things: A Review of Node-RED Architecture, Applications, and Security Concerns," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 1749-1772, May 2021. DOI: 10.1007/s12652-021-03228-6.

[14] Saniya Zahoor, Roohie Naaz Mir, Resource management in pervasive Internet of Things: A survey,Journal of King Saud University -

Computer and Information Sciences,Volume 33, Issue 8,2021,Pages 921-935,ISSN 1319-1578,https://doi.org/10.1016/j.jksuci.2018.08.014.

[15] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain and T. Hayajneh, "Secured Data Collection With Hardware-Based Ciphers for IoT-Based Healthcare," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 410-420, Feb. 2019, doi: 10.1109/JIOT.2018.2854714.

[16] A. Aragues et al., "Trends and challenges of the emerging technologies toward interoperability and standardization in e-health communications," in IEEE Communications Magazine, vol. 49, no. 11, pp. 182-188, November 2011, doi: 10.1109/MCOM.2011.6069727.

[17] G. Chu, N. Apthorpe and N. Feamster, "Security and Privacy Analyses of Internet of Things Children's Toys," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 978-985, Feb. 2019, doi: 10.1109/JIOT.2018.2866423.

[18] V. Sankaradass, P. Karthikeyan, T. N. Ravishankar and J. S. Murugan, "An Enhanced Content Based Image Retrieval in Cloud Computing with Privacy Towards EMD," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 371-375, doi: 10.1109/I-SMAC47947.2019.9032678.

[19] P. Kaushik, A. M. Rao, D. P. Singh, S. Vashisht and S. Gupta, "Cloud Computing and Comparison based on Service and Performance between Amazon AWS Microsoft Azure and Google Cloud", Proceedings of International Conference on Technological Advancements and Innovations ICTAI 2021, pp. 268- 273, 2021.

[20] M. Saraswat and R. C. Tripathi, "Cloud Computing: Comparison and Analysis of Cloud Service Providers- AWS Microsoft and Google", Proc. 2020 9th Int. Conf. Syst. Model. Adv. Res.Trends SMART 2020, no. 1, pp. 281-285, 2020

[21] L. Logeswaran, H.M.N.D. Bandara and H.S. Bhathiya, "Performance resource and cost-aware resource provisioning in the cloud", IEEE International Conference on Cloud Computing CLOUD, pp. 913- 916, Jan 2017

[22] F. Petrillo, P. Merle, N. Moha and Y.-G. Guéhéneuc, "Are REST APIs for Cloud Computing Well-Designed? An Exploratory Study", the International Conference on Service-Oriented Computing (ICSOC), pp. 157-170, 2016

[23] Alam, T. (2021). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1, 108-115.

[24] Aldowah, H., Al-Samarraie, H., & Fauzy, W. M. (2019). Educational data mining and learning analytics for 21st century higher education: A review and synthesis. Telematics and Informatics, 37, 13-49.

[25] Ali, A., & Alourani, A. (2021). An Investigation of Cloud Computing and ELearning for EducationalAdvancement. IJCSNS, 21(11), 216-222.

[26] Ali, A., Manzoor, D., Alouraini, A., The implementation of Government Cloud for the Services under E-Governance in the KSA. Science International Journal, 2021. 3(3): 249- 257.

[27] Ali, A., Cloud computing adoption at higher educational institutions in the KSA for Sustainable Development. International Journal of Advanced Computer Science and Applications, 2020. 11(3):413- 419.

[28] AlKhunzain, A., & Khan, R. (2021). The Use of M- Learning: A Perspective of Learners' Perceptions on M-Blackboard Learn.

[29] Azam, M. G. (2019). Application of cloud computing in library management: innovation, opportunities and challenges. Int. J. Multidiscip., 4(1), 2-11.

[30] Bhardwaj, A., & Goundar, S. (2019). A framework to define the relationship between cyber security and cloud performance. Computer Fraud & Security, 2019(2), 12-19.

[31] Blau, I., & Caspi, A. (2009). What type of collaboration helps? Psychological ownership, perceived learning and outcome quality of collaboration using Google Docs. Paper presented at the Proceedings of the Chaisconference on instructional technologies research.

[32] Bora, U. J., & Ahmed, M. (2013). E-learning using cloud computing. International Journal of Science and Modern Engineering, 1(2), 9-12.

[33] Clark, R. C., & Mayer, R. E. (2016). E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning: john Wiley & sons.

[34] Galić, S., Lušić, Z., & Stanivuk, T. (2020). Elearning in maritime affairs. Journal of Naval Architecture and Marine Engineering, 17(1), 38-50.

[35] Pan Jun Sun, "Security and privacy protection in cloud computing: Discussions and challenges", Journal of Network and Computer Applications, vol. 160, pp. 102642, 2020.