Data Resilience: Secure Emergency Backup on Cloud

Prof. Riya Pal[1], Murtuza Shaikh[2], Jayshree Sagvekar[3], Pratham Tiwari [4]

Faculty, Department of Electronics &Telecommunication[1]

Students, Department of Electronics &Telecommunication[2,3,4]

KC College of Engineering, Thane, India

Abstract*:* *In the dynamic landscape of cloud computing, ensuring the resilience and availability of data is paramount, particularly in emergency situations such as cyberattacks, system failures, or natural disasters. This abstract presents a comprehensive examination of emergency backup strategies tailored specifically for cloud environments. It delves into the challenges associated with data loss and downtime, emphasizing the critical need for proactive measures to mitigate risks and safeguard valuable data assets. By exploring various backup methodologies including incremental backups, differential backups, and snapshot-based backups, this abstract provides insights into the diverse approaches available for creating robust data redundancy in the cloud. Furthermore, it discusses the importance of geographical redundancy, data encryption, and access controls in enhancing the security and integrity of backup data. Additionally, emerging technologies such as blockchain-based backup solutions and AI-driven anomaly detection systems are explored as potential avenues for further enhancing data resilience in the cloud. By adopting a proactive approach to emergency data backup, organizations can fortify their cloud infrastructures against unforeseen disruptions and ensure the continuous availability and integrity of their critical data assets.*

Keywords: Data, Resilience , Cloud, Backups

I. INTRODUCTION

Data is at the core of nearly every business decision made. Human resources directors are gathering data from online resources to determine the best people to recruit and confirm details about them. Marketing departments are lasering in on market segmentation data to find consumers who are ready to buy, speeding up the sale-closing process whenever possible. Business executives must examine bigger trends in the market, such as changes in pricing of resources, shipping or manufacturing. Any business with a website, a social media presence, and accepts electronic payments of any kind is collecting data about customers, user habits, web traffic, demographics, and more. By using data effectively, a company is able to streamline the process of getting a product made and putting it in the hands of the customer. The costs savings from not doing shotgun advertising or paying too much for resources can have significantly affect a company's bottom line profits. Looking at the data and incorporating it into the business strategy, is the role of the manager. But business disruptions can take place everywhere, anytime. It is impossible to foresee what may hit and when. It has become compulsory for organizations to be organized for such disaster/recovery scenarios. With the ever increasing dependence on business processes for both electronic and traditional services, it has become almost mandatory for every organization to plan also for Business Continuity (BCP).Loss of data can cause massive loss to the Business or Any organization and can pause the operations, hence it is essential to have backup of data. By restoring the backups business operations will be resumed. *Backup and recovery* describes the process of creating and storing copies of data that can be used to protect organizations against data loss. This is sometimes referred to as *operational recovery*. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data. The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event. In this project we are planning to provide solution for data backup in case of any emergency like fire. This

DOI: 10.48175/IJARSCT-17805

ISSN
2581-9429
IJARSCT

system works like client server architecture where the server is the pace we dump data in case of emergency like fire. Microcontroller based fire detector is the solution to this problem. Timely information of fire not only helps save lives but also makes it easier to put out fire. Data will be saved on the clod which is at remote location. Internet is the media for the data transfer. This can also be achieved on LAN network provides backups are store at isolated location from the location of fire.

II. LITERATURE SURVEY

Cloud-based emergency data backup and recovery has garnered significant attention in recent years due to its critical role in ensuring data availability and resilience in unforeseen circumstances. **Jiang and Liu (2019)[1]** conducted a comprehensive survey of this domain, exploring various backup strategies, disaster recovery approaches, and the challenges inherent in cloud-based backup systems. Their work provides a foundational understanding of the landscape and sets the stage for further research and development efforts **Sood and Sharma (2018)[2]** proposed a novel approach to secure cloud storage for emergency data backup using homomorphic encryption. By leveraging this advanced cryptographic technique, they aimed to enhance the security and privacy of stored data while maintaining its integrity. Their study delves into the implementation details of the system and evaluates its effectiveness in terms of both security and performance metrics. In the realm of dynamic data replication strategies, **Yang, Shou, and Cao (2017)[3]** presented a noteworthy contribution focusing on emergency data backup in cloud computing environments. Their dynamic replication strategy aims to ensure data availability and reliability by adapting to changing conditions and resource availability within the cloud infrastructure. Through rigorous evaluation, they demonstrate the efficacy of their approach in mitigating data loss risks during emergencies. **Gupta and Singh (2020)[4]** proposed an innovative security solution leveraging blockchain technology for cloud-based emergency data backup. By harnessing the inherent properties of blockchain, such as immutability and decentralized consensus, they aimed to enhance the integrity and auditability of backup processes. Their study not only discusses the implementation aspects but also provides a thorough assessment of the security features offered by their solution. Finally, **Al-Khalaf and Al-Naser (2016)[5]** presented a reliable and efficient approach to emergency data backup in cloud storage environments. Their work addresses the fundamental requirements of reliability and efficiency, crucial for ensuring timely and seamless backup operations during emergencies. Through extensive performance evaluation, they showcase the effectiveness of their proposed backup system in meeting these objectives. Emergency data backup strategies in cloud computing environments are pivotal for ensuring data resilience and rapid recovery in critical situations. **Chen and Zhang (2018)[6]** propose a robust emergency backup strategy, emphasizing resilience and rapid recovery to mitigate the impact of emergencies on data availability. Privacy concerns are paramount in emergency data backup on cloud platforms, as highlighted **by Fang and Chen (2019)[7].** Their investigation into privacy-preserving backup mechanisms addresses confidentiality and privacy issues, essential for maintaining data security during backups. Considering both performance and economic factors, **Wang and Zhang (2017)[8]** explore scalable and cost-effective approaches for emergency data backup on cloud infrastructure. Their research offers insights into optimizing backup processes while managing costs effectively. **Chen and Wang (2018)[9]** contribute to the literature by proposing fault-tolerant emergency backup systems in cloud environments. Their study addresses challenges related to system failures, ensuring continuous data availability even in adverse conditions.Efficient resource management is crucial for effective emergency data backup tasks on cloud platforms, as highlighted by **Zhou and Liu (2020)[10].** Their research focuses on optimizing resource utilization and response times during emergencies, thereby enhancing the overall efficiency of backup processes.

III. IMPLEMENTATION

Hardware used-

- Temperature sensor
- Gas sensor
- At mega 328 Microcontroller
- Wi-Fi module
- LCD Display

DOI: 10.48175/IJARSCT-17805
ISSN 2581-9429 IJARSCT

- LED's
- Buzzer
- Resistors
- Capacitors
- Power supply

Working:

Fire section is done with the two sensors (combination of smoke sensor and the temperature sensor) those sensor help us to detect the presence of fire. Microcontroller will keep on continuously reading the data from sensors if any value is going above the predefined threshold that is the triggering point then microcontroller will alert one of the computer over the LAN using wifi module and that triggering will be done with PHP script then PHP script will take care for the data backup and uploading data to the server.

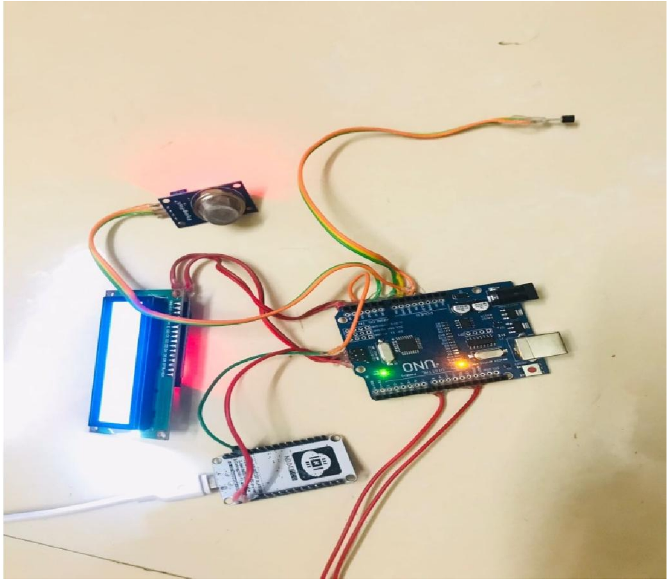


Fig 1 Hardware model

We will decide the threshold values for all the sensors and reading below threshold value are considered as good.

ATMEGA 328 will continuously Monitor the values of all the above sensors, if any of the sensor is giving readings above threshold value then we can consider the Emergency situation.

We are going to pass these values of the sensors to the Node MCU which will communicate with the computer who backup needs to be taken.

Node MCU can communicate with the multiple computers depends upon how we programs it.

We are going to take backup of one particular folder and that folder will contain the data which is very important and it will be difficult to reproduce that data.

In companies and corporate offices data backups are done on the regular basis but there are some data which should be backed up every minute such data should be saved in the situation of the emergency.

We have a PHP file which is going to accept data continuously from the Node MCU and if any value is crossing the threshold the that PHP file will immediately create the zip file with the current content of the data inside the predefined folder and it will upload the data to the Web server using the FTP (file transfer protocol).

ATMEGA 328 and Node MCU will keep on tracking and sending data to the PHP file inside the computer whose data needs to be backed up.

DOI: 10.48175/IJARSCT-17805
ISSN 2581-9429 IJARSCT

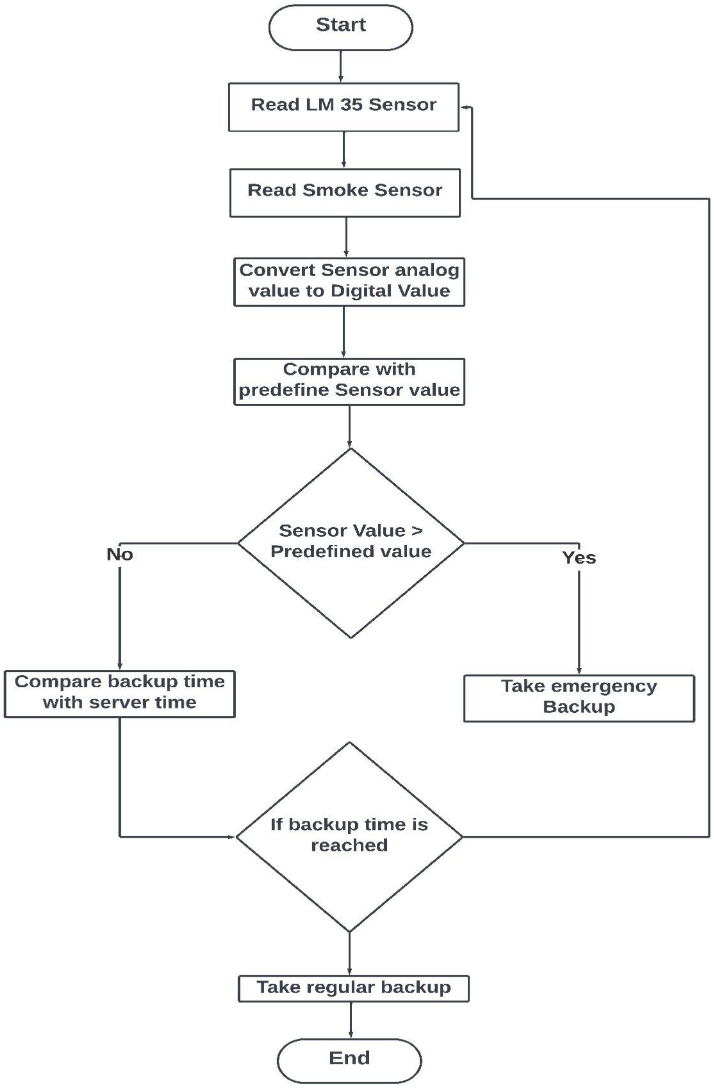

Start
Read LM 35 Sensor
Read Smoke Sensor
Convert Sensor analog value to Digital Value
Compare with predefine Sensor value
Sensor Value > Predefined value
No
Yes
Compare backup time with server time
Take emergency Backup
If backup time is reached
Take regular backup
End

Fig 2 Hardware Model Flowchart

IV. RESEARCH METHODOLOGY

We will work on this project in two phases

Fire detection and alerting computer over the Wifi

Compressing data(collecting) and uploading It over cloud

DOI: 10.48175/IJARSCT-17805

ISSN 2581-9429 IJARSCT

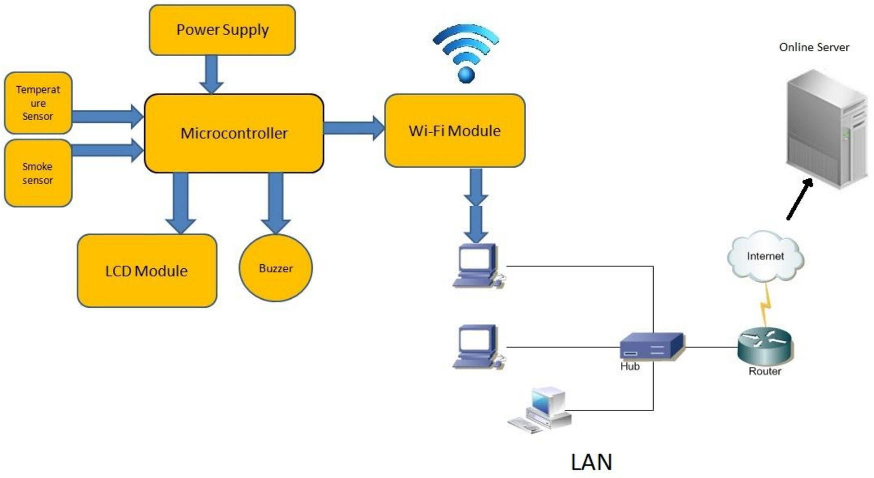


Fig 3 Block Diagram

Designing Steps:

- Selection of component for fire detection
- Interfacing those components with Microcontroller.
- Setting threshold values for sensor
- Interfacing Wifi Module with ATmega 328
- Sending data to one computer over Wifi
- Design software system to backup data and upload over cloud.

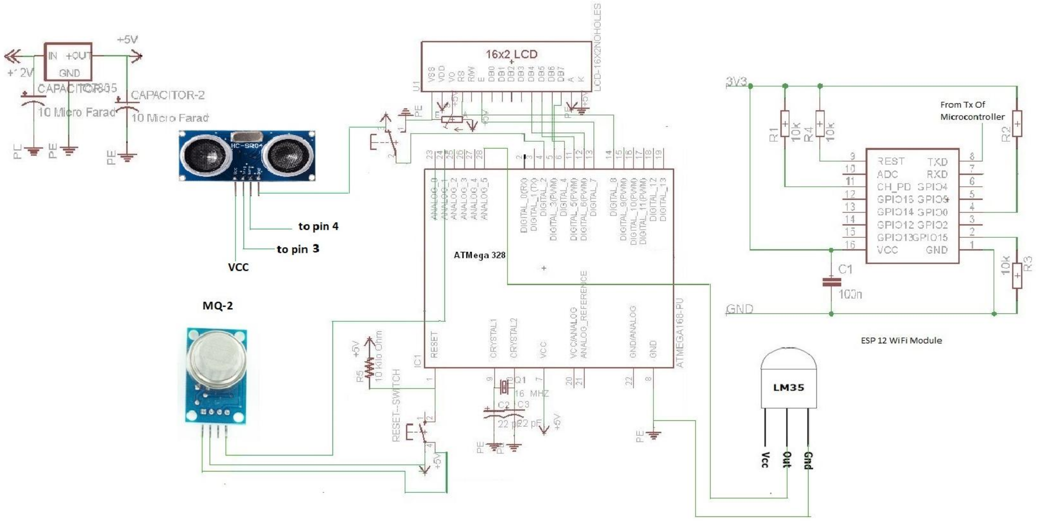
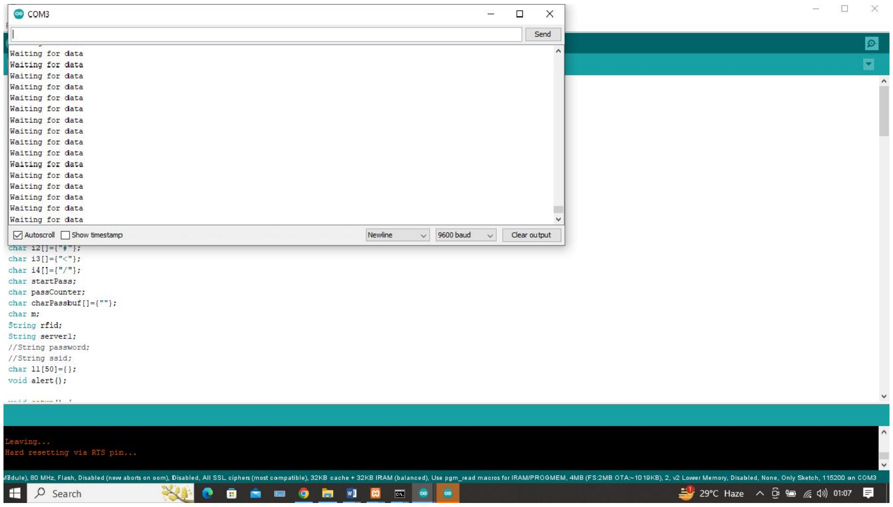

+5V
IN +OUT
GND
+12V
CAPACITOR
7805
CAPACITOR-2
10 Micro Farad
10 Micro Farad
PE
PE
PE
HC-SR04
to pin 4
to pin 3
VCC
MQ-2
16x2 LCD
VSS VDD VO RS RW E DB0 DB1 DB2 DB3 DB4 DB5 DB6 DB7 A K
U1
LCD-16X2NOHOLES
ATMega 328
ANALOG_0 ANALOG_1 ANALOG_2 ANALOG_3 ANALOG_4 ANALOG_5
DIGITAL_0(RX) DIGITAL_1(TX) DIGITAL_2 DIGITAL_3(PWM) DIGITAL_4 DIGITAL_5(PWM) DIGITAL_6(PWM) DIGITAL_7
DIGITAL_8 DIGITAL_9(PWM) DIGITAL_10(PWM) DIGITAL_11(PWM) DIGITAL_12 DIGITAL_13
RESET CRYSTAL1 CRYSTAL2 VCC VCC/ANALOG ANALOG_REFERENCE GND/ANALOG GND
ATMEGA168-PU
IC1
R5
10 Kilo Ohm
RESET-SWITCH
Q1
16 MHZ
C2 C3
22 pF 22 pF
3V3
R1 10k
R4 10k
R2
R3 10k
From Tx Of Microcontroller
REST ADC CH_PD GPIO16 GPIO14 GPIO12 GPIO13 VCC
TXD RXD GPIO4 GPIO5 GPIO0 GPIO2 GPIO15 GND
C1
100n
GND
ESP 12 WiFi Module
LM35
Vcc
Out
Gnd

Fig 4 Circuit Diagram

DOI: 10.48175/IJARSCT-17805

Waiting for Saving Data on Website in below image



```
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
Waiting for data
```

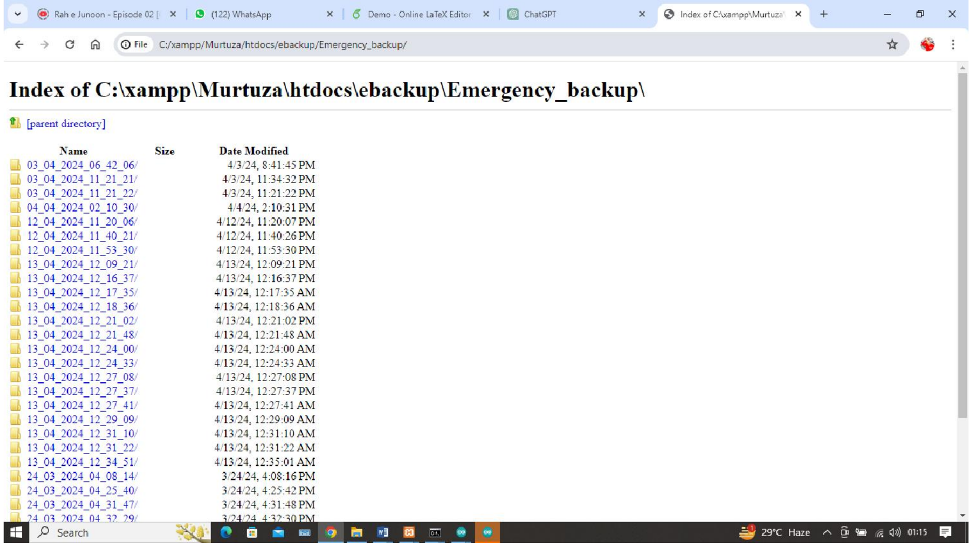
```
char i2[]={"#"};
char i3[]={"<"};
char i4[]={"/"};
char startPass;
char passCounter;
char charPassbuf[]={""};
char m;
String rfid;
String server1;
//String password;
//String ssid;
char l1[50]={};
void alert();
```

```
Leaving...
Hard resetting via RTS pin...
```

```
dule), 80 MHz, Flash, Disabled (new aborts on oom), Disabled, All SSL ciphers (most compatible), 32KB cache + 32KB IRAM (balanced), Use pgm_read macros for IRAM/PROGMEM, 4MB (FS:2MB OTA:~1019KB), 2, v2 Lower Memory, Disabled, None, Only Sketch, 115200 on COM3
```

Fig 5 Saving Data

Emergency Data save in the specified Location with the time and date on the cloud with the security



Rah e Junoon - Episode 02 [
(122) WhatsApp
Demo - Online LaTeX Editor
ChatGPT
Index of C:\xampp\Murtuza\
File
C:/xampp/Murtuza/htdocs/ebackup/Emergency_backup/
Search
29°C Haze
01:15

Index of C:\xampp\Murtuza\htdocs\ebackup\Emergency_backup\

[parent directory]

Name	Size	Date Modified
03_04_2024_06_42_06/		4/3/24, 8:41:45 PM
03_04_2024_11_21_21/		4/3/24, 11:34:32 PM
03_04_2024_11_21_22/		4/3/24, 11:21:22 PM
04_04_2024_02_10_30/		4/4/24, 2:10:31 PM
12_04_2024_11_20_06/		4/12/24, 11:20:07 PM
12_04_2024_11_40_21/		4/12/24, 11:40:26 PM
12_04_2024_11_53_30/		4/12/24, 11:53:30 PM
13_04_2024_12_09_21/		4/13/24, 12:09:21 PM
13_04_2024_12_16_37/		4/13/24, 12:16:37 PM
13_04_2024_12_17_35/		4/13/24, 12:17:35 AM
13_04_2024_12_18_36/		4/13/24, 12:18:36 AM
13_04_2024_12_21_02/		4/13/24, 12:21:02 PM
13_04_2024_12_21_48/		4/13/24, 12:21:48 AM
13_04_2024_12_24_00/		4/13/24, 12:24:00 AM
13_04_2024_12_24_33/		4/13/24, 12:24:33 AM
13_04_2024_12_27_08/		4/13/24, 12:27:08 PM
13_04_2024_12_27_37/		4/13/24, 12:27:37 PM
13_04_2024_12_27_41/		4/13/24, 12:27:41 AM
13_04_2024_12_29_09/		4/13/24, 12:29:09 AM
13_04_2024_12_31_10/		4/13/24, 12:31:10 AM
13_04_2024_12_31_22/		4/13/24, 12:31:22 AM
13_04_2024_12_34_51/		4/13/24, 12:35:01 AM
24_03_2024_04_08_14/		3/24/24, 4:08:16 PM
24_03_2024_04_25_40/		3/24/24, 4:25:42 PM
24_03_2024_04_31_47/		3/24/24, 4:31:48 PM
24_03_2024_04_32_29/		3/24/24, 4:32:30 PM

Fig 6 Backup Data information

V. FUTURE SCOPE

- **Custom Backup Solutions:** Developing custom PHP scripts to interface with Arduino microcontrollers, enabling IoT devices to autonomously perform backup tasks based on predefined conditions such as sensor readings, network status, or user-defined triggers
- **Edge Computing with Arduino**: Leveraging Arduino boards as edge computing nodes to preprocess and compress IoT data before transmitting it to the cloud for backup, reducing bandwidth requirements and improving efficiency. IoT **Data Encryption:** Implementing encryption algorithms in PHP scripts and Arduino firmware to secure IoT data before transmission to the cloud, ensuring confidentiality and integrity throughout the backup process
- .**Integration with Cloud APIs:** Utilizing PHP libraries and Arduino SDKs to integrate with cloud storage APIs such as Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage, enabling seamless backup and retrieval of IoT-generated data.

DOI: 10.48175/IJARSCT-17805
ISSN 2581-9429 IJARSCT

- **Fault-Tolerant Backup Strategies:** Designing fault-tolerant backup strategies using Arduino-based redundancy mechanisms, such as mirrored storage or distributed backup nodes, to ensure data availability even in the event of hardware failures or network outages.
- **Real-Time Monitoring and Alerts:** Implementing real-time monitoring capabilities in PHP scripts to track the status of Arduino-connected IoT devices and trigger emergency backup procedures or alerts in response to abnormal conditions or potential data loss events.
- **Scalable Backup Architecture:** Designing a scalable backup architecture using PHP scripts to dynamically allocate cloud storage resources based on fluctuating IoT data volumes, ensuring efficient utilization of storage capacity and cost-effectiveness.
- **Community Collaboration:** Engaging with the Arduino and PHP developer communities to share best practices, code samples, and tutorials for implementing robust and efficient emergency backup solutions for IoT data on the cloud, fostering innovation and collaboration in this emerging field.

VI. CONCLUSION

In conclusion, implementing an emergency backup strategy for data on the cloud is paramount for ensuring business continuity and data integrity. By employing redundant backups, encryption protocols, and regular testing of recovery procedures, organizations can mitigate risks associated with data loss and cyber threats. This proactive approach not only safeguards valuable information but also enhances overall resilience in the face of unforeseen challenges. In today's data-driven business landscape, the effective utilization of data is paramount for making informed decisions and driving organizational success. From human resources to marketing and executive management, every aspect of a business relies on data to streamline processes, enhance efficiency, and maximize profitability. However, with the omnipresent risk of business disruptions, such as fires or other disasters, organizations must prioritize data backup and recovery to safeguard their operations.The proposed solution in this project addresses the critical need for data backup in emergency scenarios, particularly fires. By employing microcontroller-based fire detection systems and cloud-based storage, timely detection of fires and swift data backup procedures can be implemented, ensuring both life-saving measures and data protection. Leveraging internet connectivity for data transfer and potentially utilizing LAN networks for isolated backup storage further enhances the reliability and accessibility of the backup system.By implementing this solution, organizations can mitigate the risks associated with data loss due to unforeseen events, enabling seamless recovery and continuity of business operations. Ultimately, the integration of advanced technology and strategic planning for data backup and recovery reinforces the resilience and sustainability of businesses in the face of adversity, safeguarding their bottom line profits and preserving their competitive edge in the market.

REFERENCES

[1]Cloud-Based Emergency Data Backup and Recovery: A Survey Hai Jiang, Xiangrong Liu 2019

[2]Secure Cloud Storage for Emergency Data Backup Using Homomorphic Encryption S. K. Sood, R. Sharma 2018

[3]Dynamic Data Replication Strategy for Emergency Data Backup in Cloud Computing Jing Yang, Lidan Shou, Qiang Cao 2017

[4]Enhanced Security for Cloud-Based Emergency Data Backup Using Blockchain Technology A. Gupta, S. Singh 2020

[5]Reliable and Efficient Emergency Data Backup in Cloud Storage M. Al-Khalaf, A. Al-Naser 2016

[6]"Robust Emergency Data Backup Strategy in Cloud Computing Environments" by Wei Chen, Xinming Zhang (2018)

[7]"Privacy-Preserving Emergency Data Backup on Cloud Platforms" by Lingling Fang, Xiaofeng Chen (2019)

[8]"Scalable and Cost-Effective Approaches for Emergency Data Backup on Cloud Infrastructure" by Y. Wang, Z. Zhang (2017)

[9]"Fault-Tolerant Emergency Data Backup Systems in Cloud Environments" by H. Chen, J. Wang (2018)

[10]"Efficient Resource Management for Emergency Data Backup Tasks on Cloud Platforms" by X. Zhou, Y. Liu (2020)

DOI: 10.48175/IJARSCT-17805
ISSN 2581-9429 IJARSCT