International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Data Management: An Integrated Solution for Database Backup, Recovery, Conversion, and Encryption Capabilities.

Siddharth Sutar[1], Kevin Jose[2], Vidya Gaikwad[3], Vaishali Mishra[4], Disha Wankhede[5], Madhuri Karnik[6]

Submitted: 25/09/2023 **Revised**: 16/11/2023 **Accepted**: 28/11/2023

Abstract: In today's world, there is a growing need for a flexible solution that can handle the complexities of SQL and MongoDB databases while providing reliable backup, recovery, conversion, and data protection in the constantly changing world of data management. The creation of an integrated backup, recovery, and conversion tool with encryption and decryption capabilities is described in this work. This application offers platform support for SQL and MongoDB databases, scheduling, backups, point-in-time recovery, and secure storage to meet the urgent needs of businesses and data professionals. Additionally, it provides smooth data transformation and schema mapping during conversion. The solution integrates strong encryption algorithms for data protection at rest and in transit and permits secure decryption utilising encryption keys and strategies like symmetric and Caesar cyphers. This improves data security. Essentially, the goal of our suggested technology is to improve and streamline data management, making it an essential resource in the current data-driven environment.

Keywords: *DBMS, SQL, MongoDB, Data Transformation, Cloud, Encryption*

1. Introduction

Database BRC is a state-of-the-art technology that revolutionizes the storage and handling of massive data sets. It offers an advanced infrastructure for efficiently managing and converting large volumes of information. With its cutting-edge algorithms and robust architecture, Database BRC guarantees data integrity and security, making it the optimal solution for organizations dealing with sensitive and critical information.

One of the key features of Database BRC is its ability to handle large amounts of data effectively. It employs innovative techniques that optimize storage and retrieval processes, allowing for swift and seamless data operations. This capability is especially beneficial for organizations that generate vast quantities of data, such as research institutions, financial companies, and healthcare providers.

Additionally, Database BRC provides comprehensive tools and utilities for data management and analysis. These features empower organizations to efficiently organize, query, and extract insights from their data sets. By leveraging the advanced functionalities of Database BRC, businesses can gain valuable insights, make informed decisions, and drive innovation.

Vishwakarma Institute of Information Technology, Pune
ssiddharthsutar@gmail.com[1], kevinjose44774@gmail.com[2], vidya.gaikwad@viit.ac.in[3], vaishali.mishra@viit.ac.in[4], disha.wankhede@viit.ac.in[5], madhuri.chavan@viit.ac.in[6]

Database backup, recovery, and conversion all play critical roles in ensuring an organization's data integrity and availability.

A. Database Backup

Data Loss Prevention: Database backups provide as a safety net in the event of inadvertent data loss, hardware problems, software faults, or natural catastrophes. They allow you to restore the database to a prior state.

Compliance and Legal Requirements: Many industries have specific regulations regarding data protection and retention. Regular backups help organizations meet these requirements and avoid legal repercussions.

B. Database Recovery

Data Restoration: After a breakdown or disaster, database recovery enables organisations to return their databases to a stable and well-known condition. To restore the database to a workable state, techniques including point-in-time recovery, rollback, and roll forward are used.

Minimized Downtime: Rapid recovery reduces the negative effects of system malfunctions or faults on corporate operations, guaranteeing continuity and minimising losses.

Data Integrity: Recovery processes validate and restore the integrity of the database, ensuring that the recovered data is consistent, accurate, and reliable.

C. Database Conversion

System and Technology Upgrades: Database conversion enables organizations to migrate from older or

incompatible database systems to newer, more efficient platforms. It facilitates system upgrades, scalability, and improved performance.

Data Consistency and Standardization: Database conversion enhances the quality and integrity of data by enabling uniform data formats, structures, and rules across many systems.

2. Literature Survey

In [1] by utilising write-ahead logging (WAL) in database systems, the authors had suggested an effective backup and recovery technique. The important concept was to divide the recovery range into numerous threads and apply backup data to each area separately. It had a backup system that used the system log data already there to manage backup data without requiring additional I/O activities. However, using many threads to optimise the WAL crash recovery process does not achieve the desired result.

The authors in [2] explored and proposed that one in can eliminate the effects of bad activities by reversing operations with the help of NOSQL UNDO, a recovery strategy and tool that returns the system to a consistent state. Incorrect MongoDB actions can be deleted using the tool described in the paper by a database administrator. The utility provides focused recovery and comprehensive recovery as two options for restoring a database. The study does not, however, offer a way to balance performance and the quantity of undo operations.

The researchers in [3] reviewed various threats and challenges, as well as their impact on sensitive data, and presentation of various safety models. All database dangers, challenges, and viable solutions are covered in this document. It is acknowledged that a task is to carefully craft bugs and use cutting-edge technology to detect and thwart security threats while also preserving the privacy and security of sensitive data. The security measures suggested, though, are not especially good at spotting hazards and threats. They were unable to recognise several vulnerabilities as a result.

S. Gokulakrishnan in [4] attempted to provide a description of data integrity & recovery management in cloud systems. To do this, a brand-new methodology known as the tailing method, which is used for data recovery and management, is focused on and proposed to ensure high-level scalability and high order reliability in cloud-based systems to segment data and generate tokens for the data split-up by adding the cloud address or locations of cloud storage that offer fault recognition and fault tolerance. Despite providing an effective optimised method and successfully demonstrating an accuracy rate of 1.67 when compared to other usual systems and third-party service providers, the model is not used in unsupervised cloud systems.

Management choices to secure data security and disaster recovery alternatives have been foretold by the growing relevance of enormous amounts of data and data analysis for business agility. In [5], The databases should be housed on many servers, with each server supporting one or more related schemas, as opposed to a single central disaster recovery structure, according to authors' proposals. Cyclic backup strategy, which offers superior decentralisation and is more secure, is employed to achieve this. The update frequency and query forwarding both affect this schema. However, when distributed databases are used, designing the backup strategy to account for existing fragmentation will need more dynamic decision-making.

[6] Bigdata is becoming increasingly popular in cloud computing, and many current systems must expand their services to keep up with the exploding rate of data collection. NoSQL databases can manage massive amounts of data. A data adaptor that supports relational databases, NoSQL databases, and hybrid database systems is suggested in this work. The development of hybrid database systems is also supported by a seamless mechanism that enables simultaneous access to both databases. Three distinct approaches are given for its database queries. blocking transformation, blocking truncation, and direct access modes. For data synchronisation, three techniques have been developed: direct access, dump blocking, and transformation blocking. The query parser, database converter, and query strategies all still require improvement, despite the fact that each approach has a different set of principles for prohibiting queries.

[7] Authors suggest an interactive protocol and communication design known as Dex to increase the capacity of analytics for big data in SQL databases. Next, we can combine a big data system with SQL database system into one holistic analysis of data platform by utilizing Dex protocol. Operators of the integrated system can use a straightforward SQL statement to access sophisticated analytics capabilities offered by the analytics system of big data. We test our concept using PostgreSQL along with Spark to show possible efficiency improvements over plain SQL UDF solutions. Dex makes it possible to integrate heterogeneous systems while paying less for management and having more flexibility. Our system improves overall performance while requiring little additional development work, yet additional protocol structure, communication of data, and other implementation concerns need to be optimised for this database. We compare our system to existing methods for enhancing the database's analytics capabilities.

[8] A blended learning approach for Relational Database Systems that provides students with a variety of connected tools and learning resources was reviewed by the authors. This uses TestSQL, a query tool that provides automatic feedback to students on SQL query exercises but is not used to evaluate the students. The evaluation is done using a variety of questions that evaluate not just the ability to write SQL, but also other abilities related to the subject, such as optimisation, physical modelling, PL/SQL, and questions that indirectly test SQL knowledge, like processing order. This analysis demonstrates that students' usage of additional resources is highly connected with higher results, but that performance at the many subtopics assessed is not at all well correlated, demonstrating that students might be strong in some areas while yet being unprepared for others. More investigation is required to confirm this finding and pinpoint precisely what types of queries make for the best summative evaluation in SQL.

[9] When dealing with NoSQL Data Stores, security methods, and privacy solutions, Vonitsanos and others have highlighted security and privacy challenges. When users first connect to the system, one such approach where they can access different services by entering their credentials just once. It is possible to protect data at rest and in motion, safeguard integrity, and implement authentication, fine-grained authorization, and access control in a distributed context. Kerberos is used in NoSQL databases to authenticate clients and data nodes. Data are specifically organised into groups based on their security level to ensure fine-grained permission. In contrast, MongoDB administrators must put rules in place to make sure that users and applications only have access to the data they need to maintain a secure MongoDB deployment. Cassandra employs TDE approach to protect data at rest.

[10] Unstructured data present in the NOSQL MongoDB database has been subjected to a security study by the authors of this paper. They used symmetric cryptographic methods to ensure the privacy of unstructured data contained in MongoDB's NoSQL documents. Additionally, the document data is encrypted and decrypted using the DES, AES, and blowfish algorithms with random key generation before being stored in and retrieved from the NoSQL MongoDB database. Zlib compression technique is used to reduce the storage size used by the encrypted data and provide comparison results, even if the encrypted data in MongoDB databases takes up more storage space than the original data. Although the research offers a more effective method for encrypting data for document-oriented MongoDB, secrecy and integrity are not yet concurrently attained, though they might be in the near future.

[11] The authors of this study presented two different types of databases, examined their security, and then suggested a fix for securing and upholding the confidentiality, availability, and integrity of the data kept in these databases. They suggested fusing NoSQL and RDBMS, with permissions being recorded in both NoSQL and RDBMS data. Two lines of defence would be provided by such a combination, ensuring the security of the RDBMS's stored data. This was done with the intention of avoiding DDOS attacks, NoSQL injections, and the loss of any stored data. Only the users' identities and hashed passwords would be stored in NoSQL. If a network specialist were installed, this would function properly because when the system detects any abnormality, it must enter lockdown mode by disconnecting all networks using network management. Based on a recent DDOS attack against a hospital, this study was conducted.

[12] Users who possess the secret key can do keyword searches on encrypted material without having to first decrypt it thanks to searchable symmetric encryption. A searchable symmetric encryption system that can produce indexes suited for DBMSs has been put forth by Takato and others. This uses a symmetric encryption method that may produce an index appropriate for database management systems and is tag-based searchable. They also put out a plan that would include deterministic tags, which are short chunks of values produced by cryptographically deterministic functions, along with the probabilistic tags of the standard tag-based SSE system. This system offered the user a way to govern their own information disclosure, allowing them to gradually reveal some deterministic tag information. Although they had established the concept of their scheme's security and demonstrated the evidence of it, well-known attacks against searchable encryption had not yet been investigated, necessitating the need to investigate its efficacy.

[13] In order to improve efficiency when retrieving encrypted data from a multilevel database, the authors of this study updated the select operation model. The system first verifies the user's security, following which it sets the encryption key in accordance with user-level security, and then it determines if the user is authorized to access the encrypted data contained in the database. The elimination of numerous decryptions made this modification operate better and faster. They take a single call to both encryption and decryption. When managing and processing massive amounts of data, the model performs better than the original model, which is extremely obvious.

[14] One of the essential components of a scalable and adaptable system, asynchronous replication, has been outlined by the authors in this study. The primary objective is to compare the time performance for CRUD

operations across several NoSQL document-oriented system implementations in a distributed setting. The results are compared with test results obtained for three relational database management systems: Microsoft SQL Server, MySQL, and PostgreSQL. The execution time for CRUD operations for a single database instance and for a distributed environment with two nodes is taken into consideration. When used to design applications, it advises selecting the option that, after a comprehensive examination of all the characteristics it provides, best meets the requirements.

[15] The Double Chaining Algorithm (DCA), which the authors of this work proposed, is a new symmetric-key encryption algorithm. This approach has a low level of complexity since it chains operations using the XOR function. The chaining stage and the substitution stage are the two key steps of the encoding process. The key's SHA-256 digest is utilised to create the key that is used during the chaining stage. The suggested algorithm section describes how this algorithm's high Avalanche Effect is achieved without any complicated operations, making it efficient and safe to implement on both software and hardware platforms.

[16] The authors of this study described how to translate MySQL requests into a database structure based on MongoDB. It is divided into four stages: parsing, producing a query dictionary, converting the data to a structured tree, and establishing a database from the dictionary. This article's conclusion displays the findings from trying the suggested strategy with various queries. Since index optimisation has not yet been optimised, it has been left as a future area of study.

[17] With the help of a quantitative description, this study aims to determine the current state of document-oriented database MongoDB and emphasise the advancement of NoSQL databases. Two datasets—the MongoDB dataset and the MySQL dataset—are used in the experiment. These are a web application's sign-up and login pages. The study was completed after one million records had been entered into the tables because the authors wanted to assess the performance after so many records had been added to the databases. The functionality provided by the application's registration page allows for the database-based registration of any user with valid information to the website.

[18] With the use of a co-design methodology, the authors of this work describe an enhanced AES-ECC system in which ECC's scalar multiplication is implemented as a hardware accelerator and AES operates on NIOS II's softcore. The suggested solution depends on improvements to both ECC (Point Addition/Doubling layer) and AES (MixColumn/InvMiColumn operation). When compared to similar studies, the software optimisation of AES and the incorporation of a productive Montgomery Scalar Multiplication for ECC have produced an overall effective cryptosystem in terms of execution time, surface occupation, and power consumption. The integration of software and hardware defences against Side-Channel Attacks (SCA) has not been completed, leaving this as a potential future project.

[19] The database forensics and its security measures were briefly covered by the authors in this work. Investigating and analysing digital databases to find unapproved access, data breaches, or cyberattacks is known as database forensics. Organisations must employ strong security measures like encryption, access controls, and auditing to protect sensitive data within their systems in order to defend against cyber threats. These security measures help identify offenders and stop such breaches by not only discouraging possible attackers but also allowing forensic professionals to trace and recreate activities in the case of a breach. A proactive database security approach must include routinely updating security procedures and monitoring for new threats.

[20] Using Elliptic Curve Cryptography (ECC) to construct a Distributed Certificate Authority (CA) in a Big Data context is a cutting-edge method of managing and safeguarding cryptographic certificates. In order to provide a decentralised CA infrastructure and improve scalability and resilience in large-scale data settings, this system makes use of the efficiency and security advantages of ECC. It reduces single points of failure and potential bottlenecks by spreading out the certificate issuance and validation processes across several nodes, ensuring strong cryptographic security for the expanding demands of Big Data applications while upholding cryptographic integrity and ecosystem trust. The experiment demonstrates that the certificate management services' availability and response times are greatly improved.

[21] This work focuses on addressing security and efficiency concerns in IoT cloud integration by implementing a secure lightweight key establishment system that utilizes symmetric lightweight and AES algorithms. This approach helps secure IoT device communications and facilitates the sharing of sensor data in a cloud environment.

[22] This survey paper serves as a valuable resource for researchers new to the field and provides insights into the current security challenges and future research directions in cloud computing security. It emphasizes the need for robust security measures in cloud environments due to the storage of sensitive data and the shared nature of cloud computing services.

[23] Paper highlights the critical importance of securing communication between IoT devices and cloud servers

due to the sensitivity of the data involved. It acknowledges the challenges posed by insecure IoT devices and the complexity of selecting suitable security mechanisms. The primary focus of the paper is to propose a lightweight key establishment mechanism to address these security concerns and prevent common types of attacks, ultimately ensuring the security of IoT-Cloud communication.

[24] The paper seems to emphasize the significance of early brain tumor diagnosis through MRI scans and highlights the benefits of using deep learning techniques to improve the efficiency and accuracy of this diagnostic process. It also discusses recent trends and evaluates the performance of the proposed approach in comparison to existing methods. This kind of research is essential in advancing medical imaging and improving patient outcomes.

[25] Author's work outlines a comprehensive approach to brain tumor detection and diagnosis, with an emphasis on glioblastoma, using deep learning techniques applied to MRI images. The method involves data collection, pre-processing, radiomics feature extraction, tumor segmentation, dimensionality reduction, and a novel model architecture to achieve accurate and efficient diagnosis of brain tumors.

[26] Research focuses on the development of machine learning-based models and radiomics techniques to predict the risk of recurrence in GBM patients. It addresses data preprocessing challenges, handles unbalanced data using RNN-GAN, and achieves high accuracy in predicting patient outcomes. The proposed method shows improvements in accuracy, specificity, and sensitivity compared to existing models like SVM and LR, which is promising for enhancing the prediction of GBM recurrence.

[27] This invention integrates IoT, cloud computing, and simulation tools to create a comprehensive solution for building and managing IoT systems. This combination enhances the scalability, efficiency, and data analysis capabilities of these systems, making it valuable for various industries and applications.

[28] The proposed system depends on the strength of encryption methods employed, the security of authentication mechanisms, and the overall implementation of the system. Careful consideration of these factors is crucial to ensure the desired level of data security and privacy protection.

[29] This study explores the field of controlled abstractive summarization, summarizing the progress made in this area. Researchers have developed various techniques and methodologies to allow users to control the summarization process.\The study also reviews the assessment methodologies used to evaluate the quality of controlled abstractive summaries.

3. Proposed Methodology

In figure 1, we study the working of the Backup and Recovery Tab. We can upload data to AWS S3 where user credentials such as S3 bucket ID and Access Key are taken. These files are uploaded in S3 bucket due to Boto3 which is a Python library that provides an interface to interact with Amazon Web Services (AWS). For backup, we select a directory where we provide the database details. SQL and Mongo backup commands run via the subprocess module of python. Then for recovery, we enter its details and select a file for recovery and recovery has been completed. This tab also provides security measure which include encryption and decryption. This gives us the choice of symmetric encryption and Caesar Cipher. Symmetric encryption involves key generation post file encryption and Caesar Cipher involves key encryption post key input from user. For Symmetric decryption, select the generated key and encrypted file which through the algorithm gets decrypted while for Caesar Cipher, enter the key which was entered in the form and all characters will be shifted back to the original words.

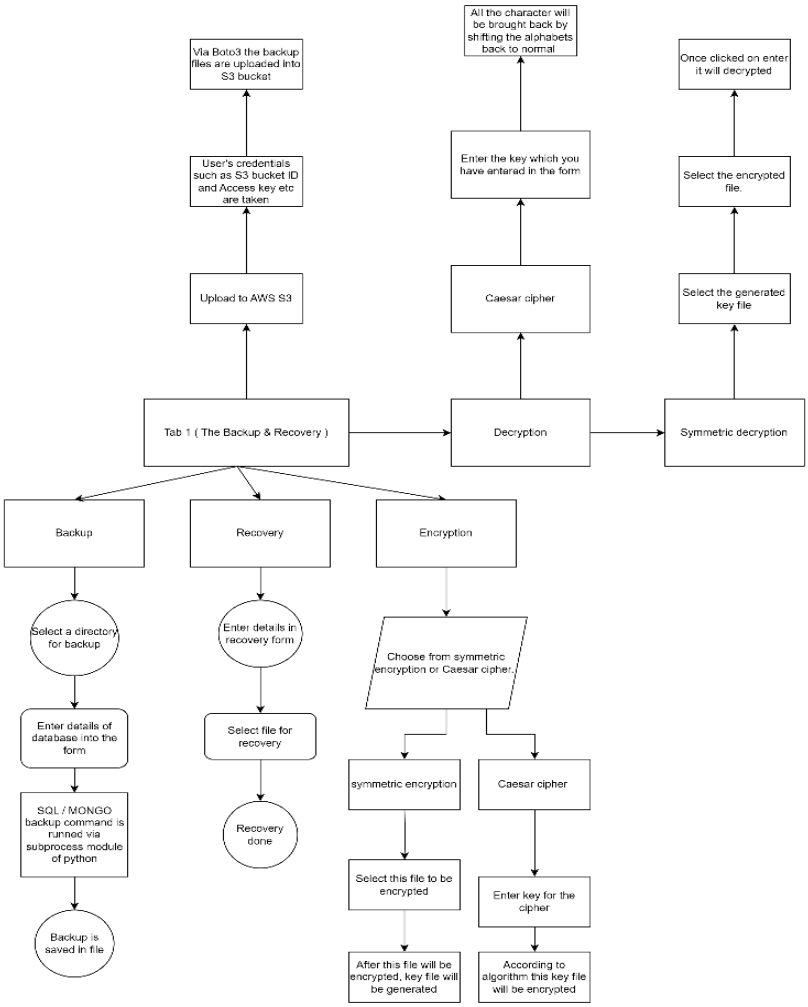

Fig 1: Block Diagram of Tab 1

In figure 2, we see the working of the Query Tab. This tab consists of two queries – SQL and Mongo. In SQL query, data for the database is taken from the user. This data is then passed to subprocess module of python and is made into SQL query. In Mongo query, selection can be done in two type – 1 and 2. Type 1 selects all queries where user enters the data and leaves the query section blank. After clicking on the button, query is handled by mongo connectors and result is displayed. Type 2 is a singular search query where user enter the fields as "fieldsToQuery Query" into input. The data again is handled and displayed in the same manner.

Fig 2: Block Diagram/Flowchart of Tab 2

In figure 3, we see the working of the conversion tab. This tab converts SQL to MongoDB and vice-versa. For SQL to MongoDB conversion, the schema is taken from the user. Select all query is made into the table after user enters the database details through which the data is parser into a json. This is done through mongo connectors and because of this data is put into the collection. For MongoDB to SQL conversion, schema is again taken from the user. Query is then created according to the schema. Data is then converted into strings and gets added to pandas' data frame. NaN values are removed from the data frame. Data is then added to SQL as an insert query is performed on the database table. This is how both conversions take place in the software.

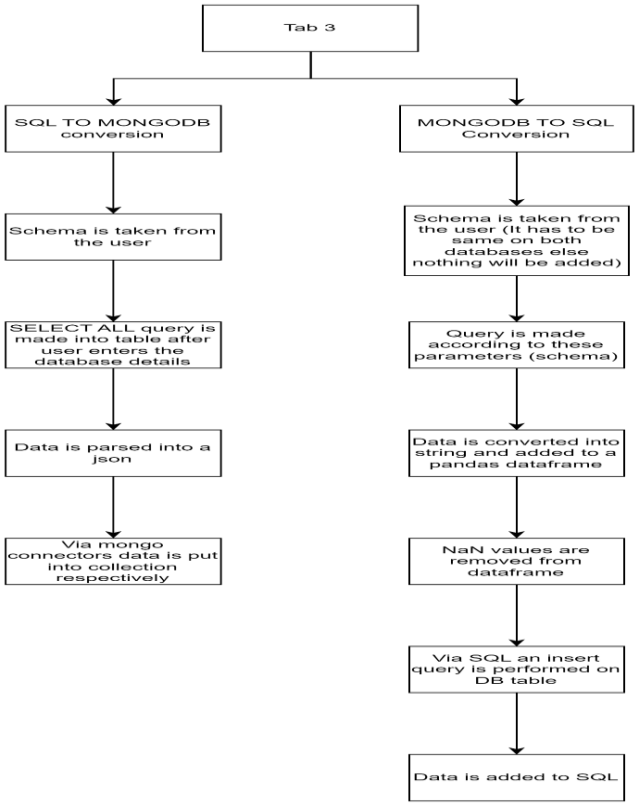

Fig 3: Block Diagram/Flowchart of Tab 3

In today's data-driven world, our project stands as a dependable and adaptable solution. It equips users to unlock the full potential of their data assets, whether through database management, query execution, or data schema conversion. Our software facilitates better-informed decisions and improved data management practices, ultimately contributing to enhanced productivity and efficiency.

4. Results & Discussions

The methodology for our software application involves a combination of technologies and functionalities encapsulated within three distinct tabs: Backup and Recovery, Query, and Conversion. Our software utilizes a tech stack comprising PyQt5 for the graphical user interface, Pandas for data manipulation, MySQL and MongoDB connectors for database operations, and boto3 for interactions with Amazon Web Services (AWS) S3.

1. Tab 1 - Backup and Recovery:

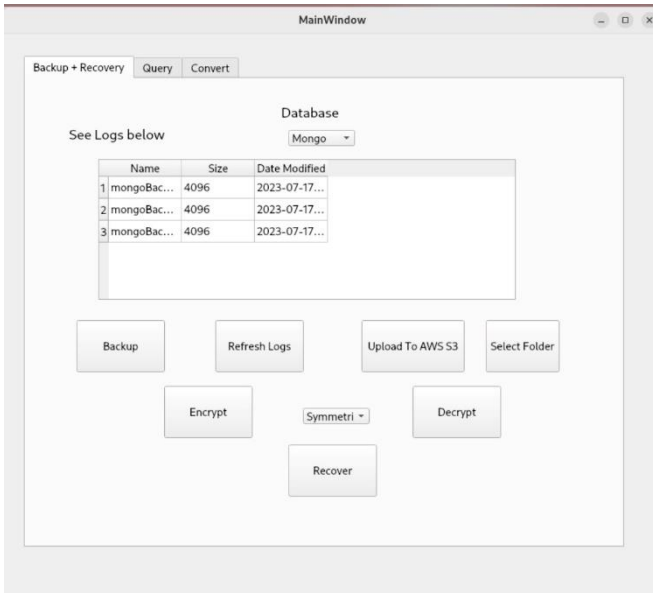

Fig 4: Tab 1 - Backup and Recovery

In figure 4, we look at the backup and recovery tab. Here, users can perform backup and recovery operations for their data. Backup and recovery are carried out through MongoDB and SQL commands, requiring the specification of a file path for MongoDB and SQL databases. Users also have the option to back up files to AWS S3 using boto3. Additionally, this tab includes encryption and decryption features, utilizing both symmetric and Caesar ciphers for secure data handling.

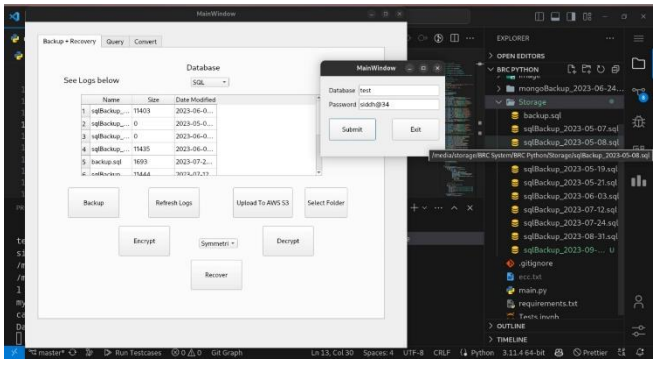

Fig 5: SQL Backup

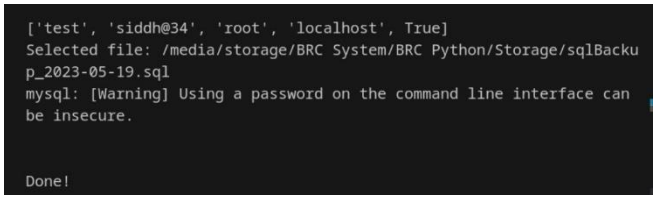

Fig 6: SQL Recovery

In figures 5 and 6, we can see SQL Backup and SQL Recovery respectively as discussed. The output is given in the command line.

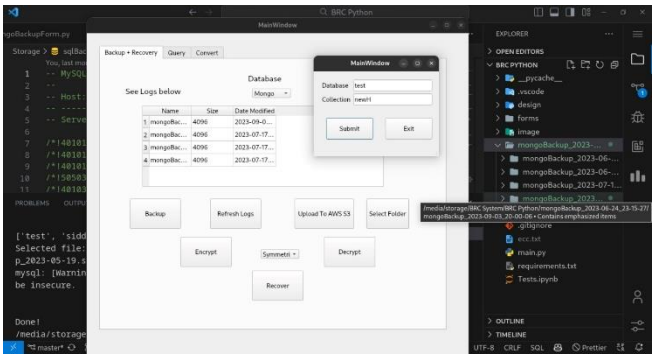

Fig 7: Mongo Recovery

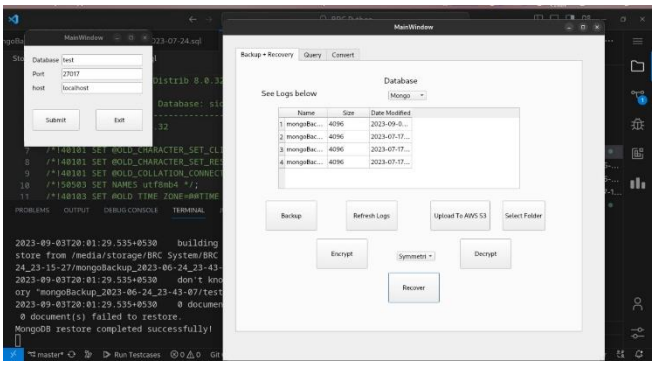

Fig 8: Mongo Recovery

In figures 7 and 8, we can see Mongo Backup and Mongo Recovery respectively as discussed.

a. Encryption and Decryption

i. Symmetric

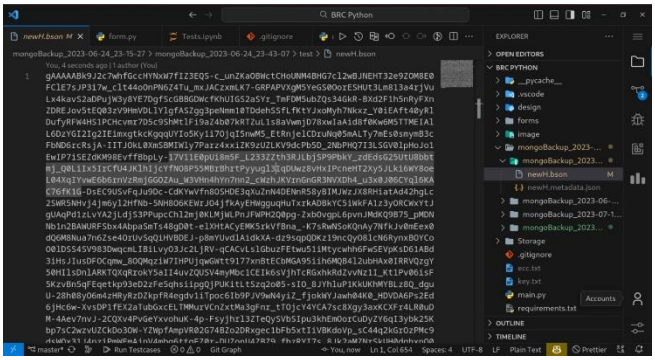

Fig 9: Symmetric Encryption

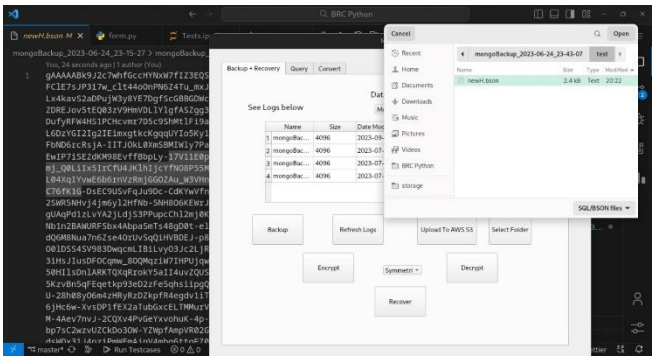

Fig 10: Key Generation

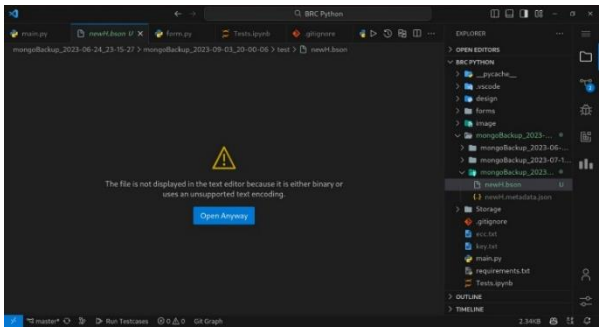

Fig 11: Symmetric Decryption

In figure 9, 10 and 11, shows images of symmetric encryption, key generation and decryption respectively as per the proposed methodology.

ii. Caesar Cipher

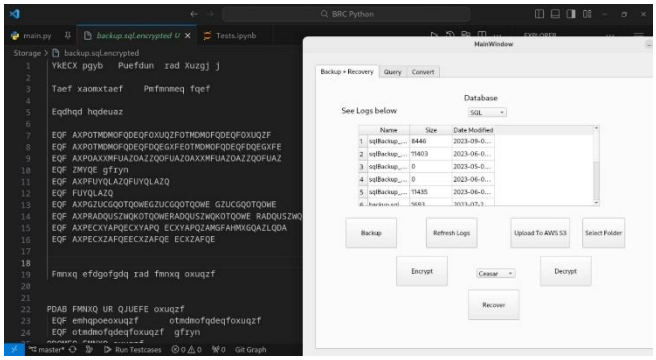

Fig 12: Caesar Cipher Encryption

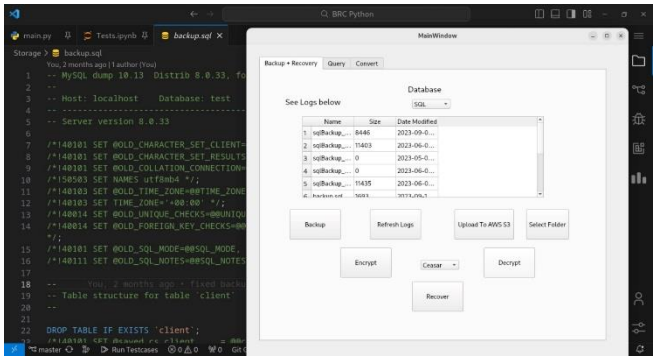

Fig 13: Caesar Cipher Decryption

In figure 12 and 13, shows images of Caesar Cipher encryption and decryption respectively as per the proposed methodology.

2. Tab 2 - Query:

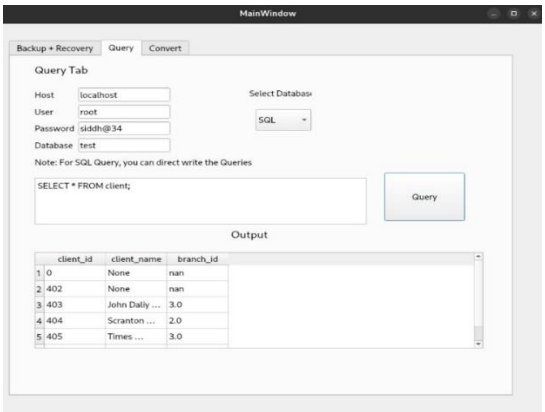

Fig 14: Tab 2 – Query

In figure 14, we look at the Query tab. This allows users to interact with their databases. SQL queries are executed through a command-line interface (CLI) and the results can perform two types of queries: retrieving all documents and querying using a single document entry. displayed within the graphical user interface (UI). For MongoDB, users can perform two types of queries: retrieving all documents and querying using a single document entry.

a. SQL

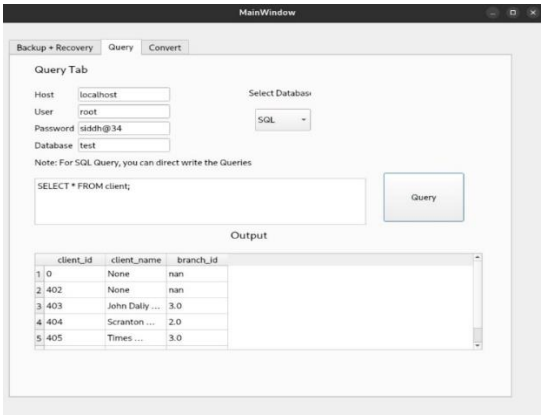

Fig 15: SQL Query

In figure 15, we can see the SQL query generation.

b. MongoDB

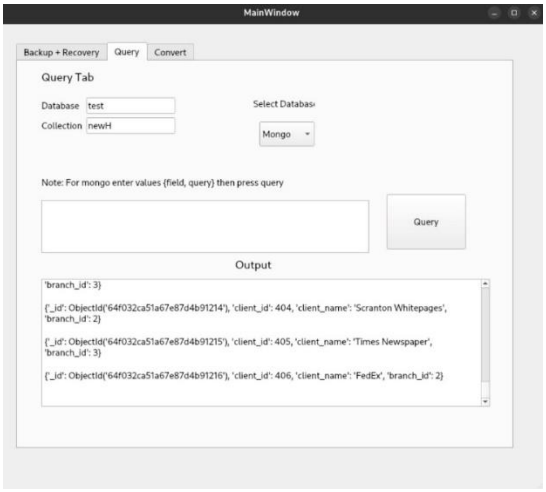

Fig 16: Mongo Query

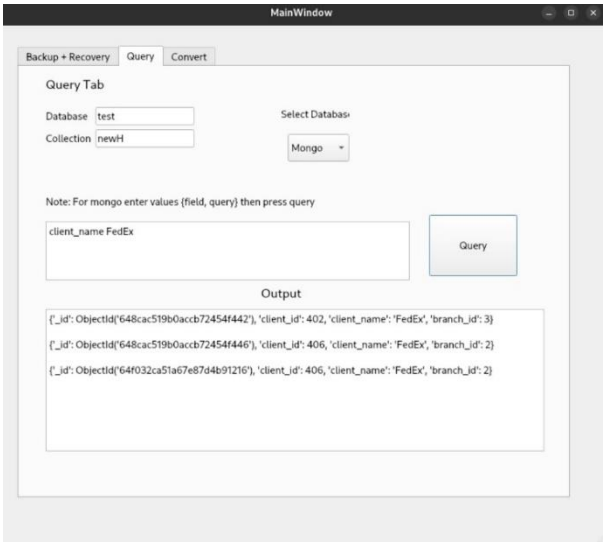

Fig 17: Single Mongo Query

In figures 16 and 17, we can see the Mongo query and single line Mongo query generation respectively.

3. Tab 3 - Conversion:

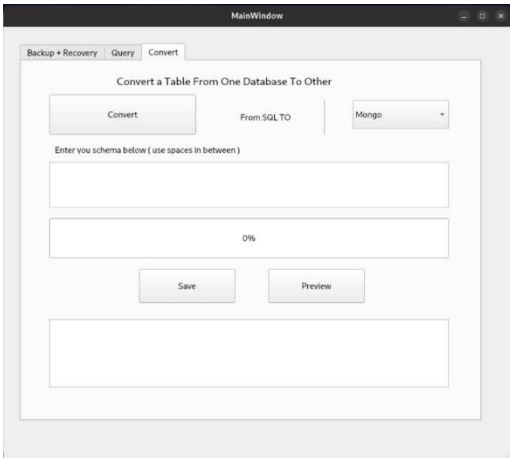

Fig 18: Tab 3 – Conversion

In figure 18, we look at the Conversion tab. Users can convert data between different database schemas. To convert from SQL to MongoDB, the software uses a simple JSON object that iteratively accumulates data and inserts it into the MongoDB database with an autogenerated ID field. When converting from MongoDB to SQL, Pandas is employed to extract the desired schema elements while representing other schema parts as empty strings during data insertion into the SQL database.

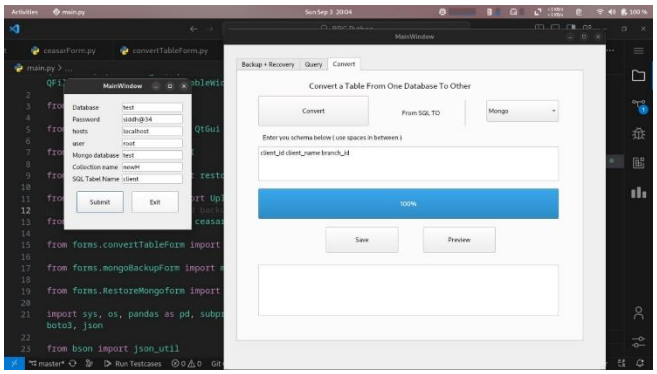

Fig 19: Conversion of SQL to Mongo

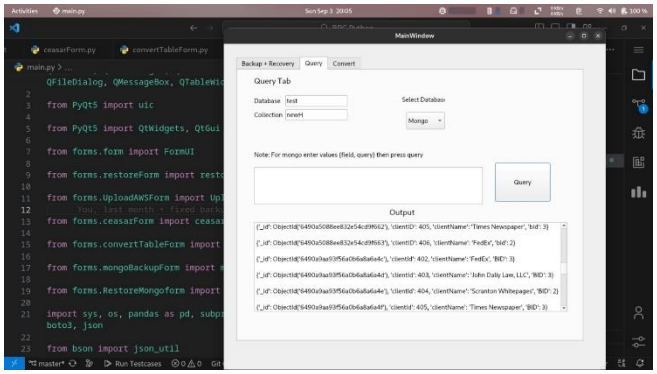

Fig 20: Output of Mongo after conversion

In figure 19 and 20, we see the conversion of SQL to Mongo and output of Mongo after conversion respectively as discussed above.

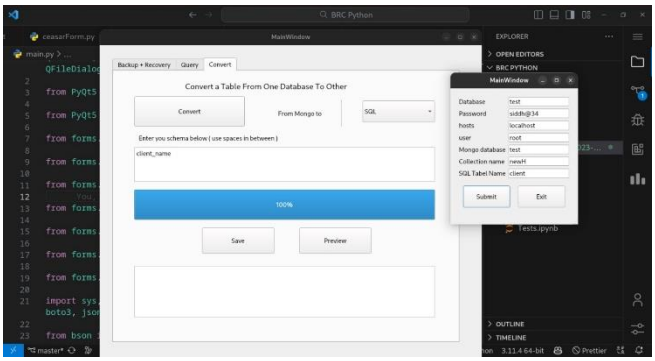

Fig 21: Conversion of Mongo to SQL

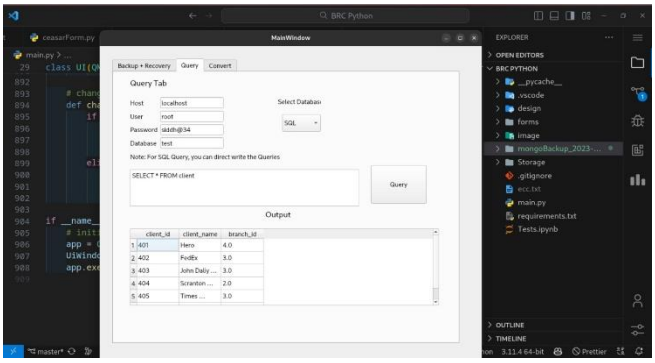

Fig 22: Output of SQL after conversion

In figure 21 and 22, we see the conversion of Mongo to SQL and output of SQL after conversion as discussed above.

Overall, our methodology combines a user-friendly interface with a powerful tech stack to provide a versatile set of features for data management, backup, recovery, querying, and schema conversion.

5. Conclusion

In this paper a comprehensive and versatile solution for database management, data manipulation, and data security is presented. By combining a sophisticated tech stack comprising PyQt5, Pandas, MySQL and MongoDB connectors, and boto3, we have created a powerful platform that caters to the diverse needs of our users.

Our software's three tabs—Backup and Recovery, Query, and Conversion—offer a wide range of functionalities. The Backup and Recovery tab provides secure data backup, recovery, and encryption features, ensuring data integrity and confidentiality. The Query tab simplifies database interactions through a user-friendly interface, accommodating both SQL and MongoDB queries. The Conversion tab facilitates seamless data schema conversion between SQL and MongoDB, enhancing data portability.

In the future scope, we will be working on adding more databases, implementing better encryption algorithms such as Elliptical Curve Encryption (ECC) and improving the UI of the software.

Reference

[1] H. KIM, H. Y. YEOM AND Y. SON, "AN EFFICIENT DATABASE BACKUP AND RECOVERY SCHEME USING WRITE-AHEAD LOGGING," 2020 IEEE 13TH INTERNATIONAL CONFERENCE ON CLOUD COMPUTING (CLOUD), BEIJING, CHINA, 2020, PP. 405-413, DOI: 10.1109/CLOUD49709.2020.00062.

[2] Matos and M. Correia, "NoSQL Undo: Recovering NoSQL databases by undoing operations," 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2016, pp. 191-198, doi: 10.1109/NCA.2016.7778616.

[3] Mousa, M. Karabatak and T. Mustafa, "Database Security Threats and Challenges," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116436.

[4] S. Gokulakrishnan and J. M. Gnanasekar, "Data Integrity and Recovery Management in Cloud Systems," 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2020, pp. 645-648, doi: 10.1109/ICISC47916.2020.9171066.

[5] S. Bhattacharya, A. Roy, S. Sen and N. C. Debnath, "Distributed data recovery architecture based on schema segregation," 2017 IEEE International Conference on Industrial Technology (ICIT), Toronto, ON, Canada, 2017, pp. 1238-1243, doi: 10.1109/ICIT.2017.7915540.

[6] G. B. Solanke and K. Rajeswari, "SQL to NoSQL transformation system using data adapter and analytics," 2017 IEEE International Conference on Technological Innovations in Communication, Control and Automation (TICCA), Chennai, India, 2017, pp. 59-63, doi: 10.1109/TICCA.2017.8344580.

[7] M. Cai, T. Bai, M. Cheng and C. Xu, "A Protocol for Extending Analytics Capability of SQL Database," 2016 7th International Conference on Cloud Computing and Big Data (CCBD), Macau, China, 2016, pp. 110-115, doi: 10.1109/CCBD.2016.031.

[8] C. Boisvert, K. Domdouzis and J. License, "A Comparative Analysis of Student SQL and Relational Database Knowledge Using Automated Grading Tools," 2018 International Symposium on Computers in Education (SIIE), Jerez, Spain, 2018, pp. 1-5, doi: 10.1109/SIIE.2018.8586684.

[9] G. Vonitsanos, E. Dritsas, A. Kanavos, P. Mylonas and S. Sioutas, "Security and Privacy Solutions associated with NoSQL Data Stores," 2020 15th International Workshop on Semantic and Social Media Adaptation and Personalization (SMA, Zakynthos, Greece, 2020, pp. 1-5, doi: 10.1109/SMAP49528.2020.9248442.

[10] J. Kumar and V. Garg, "Security analysis of unstructured data in NOSQL MongoDB database," 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, 2017, pp. 300-305, doi: 10.1109/IC3TSN.2017.8284495.

[11] O. Abahussain and A. Alqaddoumi, "DBMS, NoSQL and Securing Data: the relationship and the recommendation," 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 2020, pp. 1-6, doi: 10.1109/3ICT51146.2020.9311958.

[12] T. Hirano, Y. Kawai and Y. Koseki, "DBMS-Friendly Searchable Symmetric Encryption: Constructing Index Generation Suitable for Database Management Systems," 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 2021, pp. 1-8, doi: 10.1109/DSC49826.2021.9346255.

[13] Y. Mahmoud and M. M. Abu-Saqer, "Modification of Select Operation Model for Multilevel Security: Medical Database Systems as an Application," 2020 International Conference on Assistive and Rehabilitation Technologies (iCareTech), Gaza, Palestine, 2020, pp. 47-50, doi: 10.1109/iCareTech49914.2020.00016.

[14] -O. Truica, F. Radulescu, A. Boicea and I. Bucur, "Performance Evaluation for CRUD Operations in Asynchronously Replicated Document Oriented Database," 2015 20th International Conference on Control Systems and Computer Science, Bucharest, Romania, 2015, pp. 191-196, doi: 10.1109/CSCS.2015.32.

[15] H. Kurniawan and R. Munir, "Double Chaining Algorithm: A secure symmetric-key encryption algorithm," 2016 International Conference On Advanced Informatics: Concepts, Theory And Application (ICAICTA), Penang, Malaysia, 2016, pp. 1-6, doi: 10.1109/ICAICTA.2016.7803097.

[16] M. Ha and Y. Shichkina, "The Query Translation from MySQL to MongoDB Taking into Account the Structure of the Database," 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, 2021, pp. 383-386, doi: 10.1109/ElConRus51938.2021.9396591.

[17] M. M. Patil, A. Hanni, C. H. Tejeshwar and P. Patil, "A qualitative analysis of the performance of MongoDB vs MySQL database based on insertion and retriewal operations using a web/android application to explore load balancing — Sharding in MongoDB and its advantages," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 325-330, doi: 10.1109/I-SMAC.2017.8058365.

[18] Hafsa, N. Alimi, A. Sghaier, M. Zeghid and M. Machhout, "A hardware-software co-designed AES-ECC cryptosystem," 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), Hammamet, Tunisia, 2017, pp. 50-54, doi: 10.1109/ASET.2017.7983665.

[19] P. S. Murthy and V. Nagalakshmi, "Database Forensics and Security Measures to Defend from Cyber Threats," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1302-1307, doi: 10.1109/ICISS49785.2020.9316042.

[20] O. S. F. Shareef and A. M. Sagheer, "Implementing a Distributed Certificate Authority Using Elliptic Curve Cryptography for Big Data Environment," 2020 2nd Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 2020, pp. 132-140, doi: 10.1109/AiCIS51645.2020.00031.

[21] Shrimant, Gaikwad Vidya, Ravindranath, K. & Prasad, Gudapati Syam(2023) A mathematical model for secure Cloud-IoT communication: Introducing the revolutionary lightweight key mechanism, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1341–1354, DOI: 10.47974/JDMSC-1750

[22] Prasad, Gudapati & Gaikwad, Vidya. (2018). A Survey on User Awareness of Cloud Security.

International Journal of Engineering and Technology (UAE). 7. 131-135. 10.14419/ijet.v7i2.32.15386.

[23] Gudapati, S.P., Gaikwad, V. (2021). Light-Weight Key Establishment Mechanism for Secure Communication Between IoT Devices and Cloud. In: Satapathy, S., Bhateja, V., Janakiramaiah, B., Chen, YW. (eds) Intelligent System Design. Advances in Intelligent Systems and Computing, vol 1171. Springer, Singapore. https://doi.org/10.1007/978-981-15-5400-1_55

[24] Mrs. Disha Sushant Wankhede, Dr. Selvarani Rangasamy,"REVIEW ON DEEP LEARNING APPROACH FOR BRAIN TUMOR GLIOMA ANALYSIS" Journal of Information Technology in Industry, VOL. 9 NO. 1 (2021) pp. 395 - 408 , DOI: https://doi.org/10.17762/itii.v9i1.144

[25] Disha Sushant Wankhede, R. Selvarani, Dynamic architecture based deep learning approach for glioblastoma brain tumor survival prediction, Neuroscience Informatics, Volume 2, Issue 4, 2022, 100062, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2022.100062. (https://www.sciencedirect.com/science/article/pii/S2772528622000243)

[26] Mrs. Disha Sushant Wankhede, Dr. Selvarani Rangasamy, Dr. Chetan J. Shelke,"Risk Prediction of Brain Glioblastoma Multiforme Recurrence Using Deep Neural Networks " Journal of Algebric Statistics ,Volum13 issue 3 ,2022, https://www.publishoa.com/index.php/journal/article/view/1198, e-ISSN: 1309-3452

[27] Kurhade Anirudha, Moon Aditya,Pratham Shaantanu, Dudhane Akash, Lonari Gaurav, Gaikwad Vidya S, Sable Nilesh P., IOT SIMULATION AND CLOUD INTEGRATION SYSTEM, 2023/03129, 2023/6/28.

[28] Thakare, P., Telang, A., Sonawane, H., Mantri, Y., Gaikwad, V., & Vishwakarma Institute of Information Technology. (2020). Secure File Storage on Cloud using Homomorphic Encryption. International Research Journal of Engineering and Technology (IRJET), 7(5). https://www.irjet.net/archives/V7/i5/IRJET-V7I5861.pdf

[29] Karnik, M.P., Kodavade, D.V. (2023). A Survey on Controllable Abstractive Text Summarization. In: Abraham, A., Pllana, S., Casalino, G., Ma, K., Bajaj, A. (eds) Intelligent Systems Design and Applications. ISDA 2022. Lecture Notes in Networks and Systems, vol 715. Springer, Cham. https://doi.org/10.1007/978-3-031-35507-3_30