research parks publishing

International Journal of Human Computing Studies (IJHCS)

e-ISSN: 2615 – 8159
p-ISSN: 2615 - 1898

Volume: 6 Issue: 1 | Jan 2024
https://journals.researchparks.org/index.php/IJHCS

A QR Code-Based Real-Time Auditing System for Safe Online Data Storage

S. Suman Rajest
Professor, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India

R. Regin
Assistant Professor, Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Ramapuram, India

Shynu T
Master of Engineering, Department of Biomedical Engineering,
Agni College of Technology, Chennai, Tamil Nadu, India

Steffi. R
Assistant Professor, Department of Electronics and Communication Engineering,
Vins Christian College of Engineering, Tamil Nadu, India

Abstract

Up until now, auditing systems have only had a web module; these modules are complicated and not user-friendly. Protecting sensitive data stored in the cloud requires the time-consuming and laborious procedure of encrypting all of the files. To verify a user's identification in the current system, the client must input biometric data. Next, in order to safeguard the user's identity and privacy, a signature key will be validated. One major problem with biometric data is that there are a lot of circumstances that might cause it to vary, so it can't always be matched precisely. An auditing and data storage app built for the cloud is the focus of this paper. The reference ID that the client creates is used to remotely store the financial audit data in the cloud. Using a QR code scanner, this reference ID that was generated for the client is immediately transformed into a QR code. You can access the required documents by downloading them and then opening them in a dedicated app. In the event that the client's internal storage becomes corrupted or lost, this file can be restored from the cloud.

Keywords: Auditing System, Safe Online, Data Storage, Cloud storage, Data Security, Android Studio, QR code.

Introduction

Users can access sophisticated data storage facilities through cloud storage, which can be requested. Users can forego the need for specialised hardware by storing their data on the cloud through the use of this service [10]. Therefore, it is difficult to ensure the data saved in the cloud will remain intact owing to the prevalence of software and hardware problems as well as human mistake [11-15]. Data owners or Third-Party Auditors (TPAs) have the option to use one of several auditing methodologies to determine if cloud-based data is affected. These plans address several facets of data integrity audits, including data dynamic operation, user identity and data privacy protection, key exposure resilience, certificate management simplicity, privacy-preserving authenticators, and

more [16-20]. All of the aforementioned methods of checking data integrity require the user to utilise his private key to create authenticators for data blocks. What this implies is that the user is responsible for keeping the private key in a safe place. The user often memorises the credentials needed to activate the private key and stores it on a portable secure hardware device (e.g., a USB drive, smart card, CD, or floppy disc). Not very user-friendly is the possibility that the user may have to memorise numerous passwords for various security applications. Not to mention the possibility of misplacing the physical device housing the private key [21-25]. There will be no way for the user to create an authenticator for any future data blocks after they or their hardware device loses access to their password generator. There will be a delay in processing the data integrity auditing. Finding a way to audit data integrity that doesn't include the private key is, thus, highly desirable [26].

This paper's overarching goal is to develop a cloud-based mobile app for data auditing and storage. Cloud computing allows for the distant storage of data [27-29]. The cloud file could include private information in certain cloud storage systems. No one else will be able to access the encrypted shared file. To verify their identification in the current system, users are required to input biometric data. Next, in order to safeguard the user's identity and privacy, a signature key will be validated [30]. The biggest problem with biometric data is that it can't be matched with any degree of accuracy because of all the things that can change biometric data. A reference ID is immediately transformed into a QR code, which, when scanned with a scanner, allows the user to download the specific document. In the event that the client's internal storage becomes corrupted or lost, this file can be restored from the cloud [31-37].

Literature Survey

Users should prioritise public auditing of cloud storage. Therefore, in order to ensure that the outsourced data is good, the users employ the services of a third-party auditor (TPA). Protecting user privacy while storing data in the cloud is made easier with public audits. The outcome is further refined to permit the employment of an independent auditor (TPA). The ability to efficiently conduct audits for multiple users simultaneously is greatly enhanced by this [38-43]. One way to make sure that data stored by third parties is secure is to implement an auditing process. Hash tables, fragment structures, and random sampling are some of the techniques that form the basis of the audit service. These techniques allow for the implementation of proven updates to outsourced data and deviance. To enhance the efficiency of the auditing services, a methodology based on probabilistic query and periodic verification is integrated. The end findings demonstrate the audit system's integrity verification and support the efficacy of approaches with little computational overhead and metadata storage requirements [44-47].

The IBDO technique is utilised for identity-based data outsourcing. In comparison to other solutions for protecting outsourced data, this one has some great characteristics that make it stand out. A user can upload files to the cloud server via proxies under this scheme. In distributed computing systems, these are identified by their unique identities in order to eliminate complex certifications. Information based on data origin, data type, and file consistency is used to conduct audits in this scheme, in addition to standard integrity audits. In terms of efficiency and safety, the IBDO plan comes out on top in the security examination [48-52].

Using bilinear pairings, the IDPUIC protocol's security model and system design are provided. The suggested IDPUIC protocol is secure according to the computational Diffie-Hellman problem's difficulty. Not only that, this protocol is efficient and very adaptable [53]. This protocol is well-versed in checking the distant data integrity, public remote probity, and delegated remote data probity, with an emphasis on cloud storage facilities. These cloud storage options are offered by three well-known cloud service providers. As an example, this plan sorts various facilities according to the space they need to store big data sets and compares their features [54]. In order to plan the storage services for anticipated needs, these data sets serve as an impetus. Cloud computing service levels (IaaS, SaaS, PaaS), network and storage layers, and deployment methods (private, public, and

hybrid) are all factors to consider when thinking about cloud security [55-61]. Traditional security and authorised security, which employs the technique of reviewing the parameters, are two alternatives described in this scheme. This study presents a unified approach to resolving problems with cloud layers [62].

Applications requiring access to a single record in a database containing several records abound; for instance, software for managing client records in telecom, persistent records in clinics, email handling software for retrieving a single email from a letter drop, and countless more. Access to informational indexes, which are both massive and fundamental, is a crucial component of these applications. New processing requirements, such as massive data sets that cannot be efficiently managed using a traditional registration framework, are met by distributed computing. Dewan and Hansdah [1] offered the capacity administrations provided by three successful cloud specialist co-ops and analysed their features to define the capacity requirements of huge data sets. We anticipate it will serve as a catalyst for future plans to implement capacity administrations to meet the demands of massive informational indexes. Also provided is a brief synopsis of several distributed computing capabilities that have emerged in the past. For the purpose of verifying the integrity of a stolen or untrusted capability, Zhu et al., [2] suggested a robust review administration. Supporting proven modifications to appropriated data and easy anomaly detection, the review administration is built on procedures, piece structure, random inspection, and file hash table. In addition, it is a method for enhancing the presentation of review administrations that relies on probabilistic inquiry and intermittent confirmation. Our review framework verifies respectability with reduced computational overhead and less extra capacity requirements for review metadata, as demonstrated by the testing results, which also demonstrate the efficiency of our methods.

According to Wang et al., [3], distributed storage makes it easier for consumers in different locations to store and share records. A personality-based information reappropriating (IBDO) plot with attractive highlights that are beneficial over existing recommendations in assurance about redistributed information is suggested to handle reliability, controllable redistribution, and beginning examination concerns on reappropriated documents. To begin, the IBDO diagram enables a client to assign certain intermediaries the task of transferring data to the distributed storage server on her behalf; for instance, a company could delegate document transfer control to a small group of employees. By virtue of their distinguishing features, the intermediaries are acknowledged and accepted, doing away with the need for the complicated declaration of the board in typically secure conveyed figure frameworks. In addition to the usual respectability evaluation that is possible with current plans for verifying reappropriated material, the IBDO plot also permits reviews of data regarding the information's origin, nature, and consistency of redistributed documents, which is a major benefit. Trial evaluation and security research show that our IBDO plot offers strong security-attracting performance.

As distributed computing continues to evolve at a rapid pace, more and more consumers may want to store their data on public cloud servers, or PCS. More clients should be allowed to process their information in broad daylight cloud if new security issues are revealed. The client will designate PCS's intermediary to handle the processing and transfer of his information when he is unable to obtain it directly. Open distributed storage also has a major problem with remote information uprightness testing. Customers can verify the integrity of their redistributed data without downloading any of it at all. To address these security concerns, Wang et al. [4] introduced IDPUIC, a new architecture for personality-based open key cryptography that uses intermediaries to facilitate the flow of information and verify its respectability remotely (character-based intermediary arranged information transferring and remote information uprightness checking in broad daylight cloud). Both the framework model and the security model are formally defined. Based on the bilinear pairings, a robust ID-PUIC convention can then be planned. Depending on how difficult the computational Diffie-Hellman problem is, the suggested ID-PUIC convention can be shown to be secure. We also have an ID-PUIC convention that is flexible and efficient. The proposed ID-PUIC convention can comprehend privately checked, designated, and openly checked remote information

uprightness in light of the specific customer's approval.

In many security applications, key-presentation opposition has long been a major concern for top-down digital defenders. Recent proposals and considerations have focused on managing the major presentation issue in distributed storage examination scenarios. In order to solve the problem, the current setup always asks the user to update his mystery entries every time. This can lead to new neighbourhood weights for the consumer, especially if they have limited computing resources like a cell phone. Yu et al., [5] explored the undeniable redistribution of key refreshes and offered an alternative perspective they dubbed distributed storage in an effort to make key updates as easy as possible for the client. Here, the customer won't have to worry about key updates at all because they may be safely transferred to an authorised group. Specifically, we direct the third-party auditor (TPA) in numerous preexisting open examination frameworks to act as the authorised group in our case, overseeing not only the capacity evaluation but also the protected key updates to prevent key presentation obstruction. As part of the scheme, TPA is only required to carry out certain particular tasks on behalf of the customer while holding an encoded version of the customer's secret key. While uploading new files to the cloud, all the client has to do is download the encrypted secret key from the TPA.

The client is also able to verify the authenticity of the encoded secret keys provided by TPA using our system. Careful consideration went into crafting all of these eye-catching features with the goal of streamlining the customer's evaluation process with significant introductory opposition. There is now a formalised definition and security model for this worldview. Proof of the efficacy and safety of the granular structure launches is provided by the display reenactment and the security confirmation.

The goal of an information storage emphasis in a proof-of-retrievability architecture is to convince a verifier that they are actually storing all of a customer's information. Building efficient and provably safe frameworks is the main challenge. This means that client data should be segregable from any prover that passes the confirmation check. In the most realistic model, Juels and Kaliski's, Shacham and Waters's [6] initial proposal for retrievability plans included complete pieces of evidence of protection from subjective foes. The initial strategy was stable in the irregular prophet model and derived from BLS markers. When compared to other retrievability evidence with 10 open obviousness, its inquiry and reaction time is the shortest. The following scheme has the quickest response of any verification of retrievability associated with private undeniable nature; it is secure in the standard model and is based exclusively on pseudorandom capacities (PRFs) (yet a more drawn-out inquiry). In order to reduce a proof to a single authenticator value, the two schemes rely on homomorphic features. Using the Juels-Kaliski model, the main proof of retrievability plans with complete confirmations of protection from aggressive enemies is provided. The first strategy is safe in the arbitrary prophet model and has the shortest question and response time of any retrievability evidence with an open, indisputable character. In the standard model, the following scheme is safe and has the shortest reaction time of any confirmation-of-retrievability plot with private unquestionable status (albeit a longer question).

Another kind of fuzzy identity-based encryption was introduced by Sahai and Waters [7] as an identity-based encryption (IBE) conspiracy. A Fuzzy IBE plot considers a personality's private key, ŭ, to decipher a character-encoded cypher text, ŭ, provided that the characters ŭ and ŭ are close together, as determined by the "set cover" separation metric. One way to implement biometric character encryption is with a Fuzzy IBE plot. This plot's error resistance feature accounts for the use of biometric characters, which will inevitably cause some noise whenever they are checked. The term "quality-based encryption" describes another application of Fuzzy-IBE. We suggest two enhancements to Fuzzy IBE plans. These new features might be thought of as a (fluffy) personality's identity-based encryption of a communication. The IBE plans are safe from conspiracy attacks and have an 11-blunder tolerance. In addition, non-standard prophets are not a part of the fundamental evolution. Using the Selective-ID security paradigm, we can prove that the plans are secure.

Distributed computing has been steadily gaining traction among corporations and associations, and it is quickly becoming one of the most innovative technologies. The security concerns of cloud computing are broken down into different layers by Kanickam et al., [8]. These layers include the service layer (IaaS, SaaS, PaaS), the organisation layer, the storage layer, and the arrangement models (public, private, and hybrid cloud). Here we indicate the approach employed to evaluate the metrics, and in this examination we look at the traditional and affirmed security arrangements. A new proposal is going to be discussed that would sort through all the cloud layers difficulties in one bundle. Research like this proves that no valid plan accounts for every possible cloud layer. Rather than concentrating on supplier-end security, most previous designers prioritised client-end cloud administration security. Everything related to the cloud layer is addressed in this proposal as a whole. The majority of cloud computing is based on online and remote personal computers or servers to store data for various applications. Problems with the system and with confirmation were addressed by the protection-saving concept. Use Bayes' hypothesis to conduct a detailed investigation of the suppliers and customers. Through the use of concepts like encryption and signature validation, the data area, security, and associated challenges are understood. The experts have a firm grasp of the methodological concepts, and SAML Security Assertion Markup Language has been prepared for this proposal. Additionally, the outsider examiner is used for trust necessary premise, but the process is time-consuming. However, the proposal states that an impartial third party is not necessary for the outsider examination. Though our proposal primarily aims at ensuring open cloud clients and suppliers and promotes long-term premise, it does acknowledge that an open cloud is less safe when considering private mists.

Cloud computing has long been an idealised picture of processing as a service, with users able to remotely store data in the cloud and access high-quality applications and administrations on demand from a shared pool of programmable registering assets. Clients can alleviate the burden of community information storage and support through information reappropriation. Information respectability security in distributed computing is a challenging and potentially massive undertaking, especially for clients with forced computing resources and capabilities, due to the fact that clients no longer physically own the potentially large quantities of redistributed data. Customers should be able to rely on an external review group to verify the authenticity of transferred data whenever necessary, which is why enabling open auditability for cloud information capacity security is fundamental. Two essential conditions must be satisfied before a strong outside examiner (TPA) can be presented safely: 1) TPA should be able to efficiently assess the cloud's data capacity without requiring a local copy of the data, and should not add any additional online burden on the cloud client; 2) The third party evaluation process should not introduce any new security holes that could compromise client data.

The security-saving open cloud information examining framework developed by Wang et al. [9] satisfies all of the aforementioned requirements; it employs and brilliantly combines the open key-based homomorphic authenticator with irregular concealing. In order to facilitate efficient handling of many examination tasks, we conduct additional research into the bilinear total mark technique to generalise the basic result to a multi-client environment, allowing TPA to execute multiple examination assignments concurrently. The suggested ideas are demonstrably safe and very productive, according to a thorough analysis of their security and execution. Information storage security in the cloud can be improved with the use of an open review architecture that provides protection. In order to prevent TPA from learning anything about the data stored on the cloud server, we use the homomorphic authenticator and irregular covering. This not only relieves the cloud client of the tedious and potentially expensive task of inspecting, but it also allays the clients' fears of data redistribution. In a multi-client environment, where TPA can execute the various evaluating assignments in a cluster, i.e., simultaneously, the protection is further expanded for saving open inspection convention. This is because TPA may handle multiple review meetings from different clients for their redistributed information documents at the same time.

Proposed Model

Only when data is securely handled can users grant authority to an external party to control their details. For the majority of web-based programmes, user data security is of the utmost importance. In order to circumvent the less secure area of a client's financial audit data, the suggested methodology is put forward.

Problem Statement

Regardless of size or legal form, an audit is an impartial review of any entity's financial records, whether for profit or not. They can keep track of all the transactions that have taken place so far with the help of an auditing system. A concept was developed to ensure the security of users' identities and data. It relies on biometric data and signature key verification [63]. User authentication is accomplished by scanning their fingerprint upon sign-in and then exchanging a private key that is known only by the user [64]. This key is generated automatically when the user profile is created. In order to access their account and download files, the user must input the key. Nevertheless, the primary concern here is user authentication, not file security [65-67]. Our goal is to create a system that can securely communicate data utilising QR codes and one-time passwords (OTPs). The main perk of this approach is that content may be created once and then revised as needed. Data is not lost and can only be scanned using the app's scanner because a fresh QR code is created every time the data is changed. In order to access or download the client details, the OTP must be typed [68-71].

After the auditor has made a profile for himself, he makes a profile for the customer by logging into the gis account. Keep in mind that an auditor manages numerous client profiles rather than just one organisation or client profile. When a user creates a client profile, the system immediately generates a client ID that they may use to access the mobile app [72-75]. The auditor has now submitted all of the financial audit files using the client's ID. When an auditor uploads files using a certain client ID, the files are immediately saved to the cloud. The client ID is used to produce a QR code. When you upload a new file, it automatically generates one. The client's registered email ID is used to send the QR code and client ID, granting access to the client's account. The pre-processing section is now finished [76-81].

Only the client's use of the mobile app is covered in the file access section. In order to access their account, clients must input the client ID that the auditor has generated, and they must also create a new password at the time of login. In order to move on to the next step, the client must input the password they just set a second time. The next screen instructs the user to open a scanner [82-89]. The auditor will have sent a QR code to the user's registered email address; the user must then scan this code. Upon client input of the one-time password (OTP), which is delivered to the client's registered cellphone number, a screen is shown allowing the client to download all files uploaded by the auditor up until that point in time [90]. Additionally, the QR code can only be deciphered by the scanner that comes with the mobile app; any other QR code scanner will merely show the client ID. The files will remain accessible in the cloud indefinitely, allowing the client to download them as many times as needed until their account is available, even if they remove them from their local storage [91-94].

Result

By thinking about every potential demand of the product's users, requirement analysis finds out what the product needs in order to be developed. In order to analyse the task's execution, two things are needed: probable input data and output data [95]. The following section elaborates on these prerequisites. The mobile application sends the client a QR code and their client ID as input data. In addition, the auditor can use the web module to upload client data to the cloud. The files that the client downloads from the mobile app after logging in successfully are called output data. Only files saved to the cloud will be accessible to them, both in terms of viewing and downloading. In order to complete the paper, you must meet these criteria [96-101]. We would not have been able to

complete the work without these programmes and technologies. In order to complete the paper, you will need the appropriate software and hardware. Since the hardware requirements could form the backbone of the system's execution, they ought to be an exhaustive and uniform description of the entire system. The software requirements specification is built upon the software requirements [102-105].

In order for a system to meet certain requirements, its design must first define its architecture, components, modules, interfaces, and data. Specifics regarding the system's structure, operations, and modules are provided by the design. The parts that follow provide a comprehensive breakdown of our suggested model's design [106-111]. System architecture provides a high-level description of a model's process and aids in comprehending the model's operations. Figure 1 specifies the system architecture for the suggested model and includes the details of the process that must be executed correctly [112-119]. When working on the online module, the auditor is alone in the pre-processing portion. All audit files are uploaded to the cloud, and client profiles are generated. The client ID is used to save these files in the cloud. Upon successful file upload, a QR code containing the client ID will be created [120-127]. The QR code is dynamic and updates with each submitted file. You can share a snapshot of the QR code with each client [128].

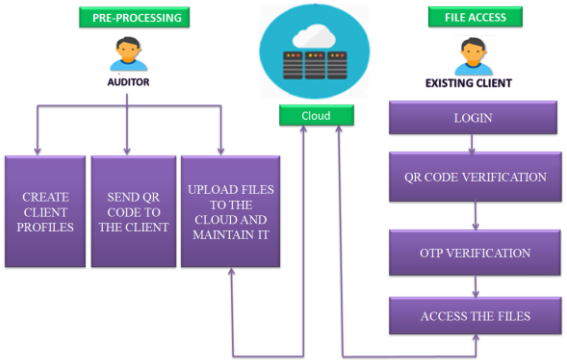

Figure 1: Interaction between the auditor and client

The Android module's file access section is where the client can access their files. The customer inputs their client ID and then sets a new password. Every time the client needs to access their files after creating a password, they will simply need to enter the password [129-134]. The next step is to open a scanner and scan the auditor's QR code. The customer's phone is now provided a one-time password (OTP). The files can be accessed and downloaded after entering the one-time password. The use case diagram illustrates the connection between the auditor and the user. You can see every single thing they do by looking at the arrows and states. An individual profile is developed by the auditor. After that, he makes the customer's profile [135-141]. Under the client's ID, all the files are uploaded. The auditor creates a QR code and emails it to the customer. From time to time, the auditor can add or remove files.

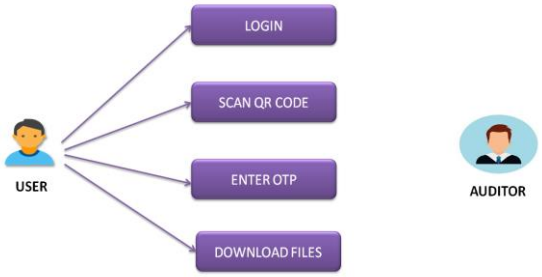

Figure 2: Mobile App

The client is the only one who uses the mobile app feature. The user is prompted to generate a password after entering their client ID. The auditor will provide a QR code, and the customer must

scan it after inputting the password [142-147]. After scanning it, the client's registered cellphone number receives a one-time password (OTP), which must be input. Here you can see all of the auditor's posted files; from here you can also download and view them (Figure 2). You can see how the five primary classes login/registration, produced QR code, scanned QR code, file upload, and file download are connected in the class diagram. Contains all members of the data set and their associated functions. This graphic shows how the system operates [148-151]. From one starting point to another, an activity diagram shows the control flow, including all of the possible decision options along the way [152]. The flow of all the activities that occur throughout the entire procedure is displayed (Figure 3).

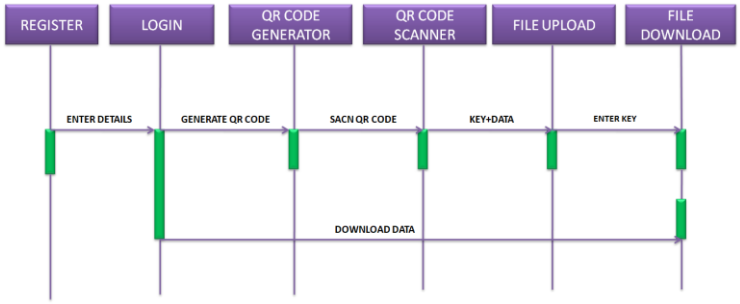

Figure 3: Sequence Diagram

A sequence diagram only shows the order in which objects interact with one another, or the sequentiality of these interactions. The relationship between the main classes is illustrated [153-157].

It is common practise to describe the static implementation view of a system using component diagrams, which are effectively class diagrams that concentrate on a system's components [158-159]. The essential components are displayed, and the steps are labelled to indicate the sequence of occurrences. Collaboration diagrams, often called communication diagrams, show how different items in the model communicate with one another and with the programme. The preceding graphic represents the connection between the categories.

Result and Discussion

In the web module, the auditor establishes his own profile. We add the audited files to the cloud and create the client's profile. The customer can access their files by logging into their account and using the reference ID that is automatically provided. The auditor has the ability to modify or delete the client's information from the database. We use XAMPP to import the details. By utilising the client's registered email address, the reference ID (client ID) is communicated to the client. We generate a QR code for the client's ID. Under this reference ID, the auditor saved the client's documents. Through the client's registered email ID, the QR code is transmitted to the client. Every time the client needs to access their account, they must input the client ID that was issued by the auditor along with a password. After the client enters the password, the scanner launches automatically, and the auditor sends a QR code that the user must scan. It is now requested that the customer input an OTP. The verification process is finished when the client's registered cellphone number receives the one-time password (OTP). Clients can download files, but they won't be able to access them using the regular Android device storage unless they use the ES File Explorer app.

Independent of the element's size or authoritative document, an audit is a self-evaluation of its financial data. This applies whether the benefit is planned or not. All the transactions that took place on that date—along with other auditing data—can be more easily managed with the use of an inspection framework. If a client's information is handled securely, any client who entrusts an external substance with their details will grant that substance authority. The primary requirement for most web-based applications is to provide a secure environment where the client's information is shielded. An strategy to overcoming the less secure space of the client's audit information is provided by the proposed model. The auditor makes a profile for himself by entering his details.

The files he uploads can be modified or deleted, and he can also add or remove customers. The auditor creates a profile for each of his clients by entering their essential facts. When an auditor creates a client profile, an automatic client ID is produced and sent to the client's registered email address. Through the use of the client's ID, the auditor uploads all of the audited files straight to the cloud storage. The auditor has the ability to make changes to the uploaded files, including adding or removing them. We use XAMPP to import the details.

By entering the client ID and creating a password on the mobile app, the client can access the files. After the auditor sends a QR code, the scanner is activated after the password is submitted. As soon as the QR code is scanned, a one-time password (OTP) is delivered to the client's registered mobile number. You can now download the files that were uploaded. You can't access the files through the internal storage or file explorer; you need to use the ES file explorer app. Only when data is securely handled can users grant authority to an external party to control their details. For the majority of web-based programmes, user data security is of the utmost importance. In order to circumvent the less secure area of a client's financial audit data, the suggested methodology is put forward. In order to protect the data from unauthorised access and to confirm the user's identity, the package includes a QR code generator and an OTP generator, which are essentially two-factor authentication. With just the password to keep in mind, the verification process becomes much simpler. Upon receiving data, the remaining steps of the process are initiated. Because the cloud is a permanent storage, clients can access and erase data at any time from their devices, and they can download data from the cloud as many times as they want. In order to access the files, one must install a dedicated file management application; otherwise, they will not be seen on the client's regular internal storage device.

Conclusion

The final product is a real-time, mobile app for an auditing system. Clients and auditors alike benefit from the system's simplification and speed. Particularly if their data is handled securely, any client who entrusts an external substance with their details will grant them power. For many web-based applications, the most important thing is to provide a secure environment where the client's information is kept safe. As a simple two-factor authentication measure to verify the client's identity and prevent data breaches, the QR code generator and an OTP generator are included. Once the secret phrase has been memorised and the different parts of the operation encounter the request for information, the confirmation step becomes easier. The data is stored in a basic and secure way; it can be viewed and deleted on the customer's device as needed, and it may be retrieved multiple times from the cloud because it is immutable. Customers' regular internal storage devices do not have access to the record. Still, the moment the documents become visible is the perfect time to offer a new document chief application. There will be further capabilities for automated result prediction in the future, such as the ability to simulate business intelligence for use in predictive analysis. One potential future method for cloud data classification is the CART algorithm. Classification or regression trees can be produced by this decision tree learning method.

References

1. H. Dewan and R. C. Hansdah, “A survey of cloud storage facilities,” in 2011 IEEE World Congress on Services, 2011.
2. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, G. Ho, and C.-J. An, “Dynamic audit services for integrity verification of outsourced storages in clouds”,” IEEE Transactions on Services Computing, vol.6, no. 2, pp. 1550–1557, 2013.
3. Y. Wang, Q. Wu, B. Qin, W. Shi, R. H. Deng, and J. Hu, “Identity-based data outsourcing with comprehensive auditing in clouds”,” IEEE Transactions on Information Forensics and Security, vol.12, no. 4, pp. 940–952, 2017.
4. H. Wang, D. He, and S. Tang, “Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1165–

1176, 2016.

5. J. Yu, K. Ren, and C. Wang, “Enabling cloud storage auditing with verifiable outsourcing of key updates,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1362–1375, 2016.
6. H. Shacham and B. Waters, “Compact Proofs of Retrievability,” in Advances in Cryptology - ASIACRYPT 2008, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 90–107.
7. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 457–473.
8. S. H. L. Kanickam, L. Jayasimman, and A. N. Jebaseeli, “A survey on layer wise issues and challenges in cloud security,” in 2017 World Congress on Computing and Communication Technologies (WCCCT), 2017.
9. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in 2010 Proceedings IEEE INFOCOM, 2010.
10. Venkatasubramanian, S., and R. Mohankumar. "DDoS Attack Detection in WSN Using Modified BGRU With MFO Model." Advanced Applications of Generative AI and Natural Language Processing Models, edited by Ahmed J. Obaid, et al., IGI Global, 2024, pp. 286-305.
11. S.Venkatasubramanian, "A Machine Learning Based Health Analytics in the Cloud Environment", Journal For Basic Sciences, Vol. 23, Issue. 12, , pp. 497-508, DEC 2023
12. T. Chen, J. Blasco, J. Alzubi, and O. Alzubi “Intrusion Detection”. IET Publishing, vol. 1, no. 1, pp. 1-9, 2014.
13. J. A. Alzubi, R. Jain, O. Alzubi, A. Thareja, and Y. Upadhyay, “Distracted driver detection using compressed energy efficient convolutional neural network,” J. Intell. Fuzzy Syst., vol. 42, no. 2, pp. 1253–1265, 2022.
14. J. A. Alzubi, O. A. Alzubi, M. Beseiso, A. K. Budati, and K. Shankar, “Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis,” Expert Syst., vol. 39, no. 4, 2022.
15. S. Abukharis, J. A. Alzubi, O. A. Alzubi, S. Alamri, and T. O. Tim O\’Farrell, “Packet error rate performance of IEEE802.11g under Bluetooth interface,” Res. J. Appl. Sci. Eng. Technol., vol. 8, no. 12, pp. 1419–1423, 2014.
16. O. A. Alzubi, I. Qiqieh, and J. A. Alzubi, “Fusion of deep learning based cyberattack detection and classification model for intelligent systems,” Cluster Comput., vol. 26, no. 2, pp. 1363–1374, 2023.
17. A. Jafar, O. A. Alzubi, G. Alzubi, and D. Suseendran, “+ A Novel Chaotic Map Encryption Methodology for Image Cryptography and Secret Communication with Steganography,” International Journal of Recent Technology and Engineering, vol. 8, no. IC2, 2019.
18. S. Samadi, M. R. Khosravi, J. A. Alzubi, O. A. Alzubi, and V. G. Menon, “Optimum range of angle tracking radars: a theoretical computing,” Int. J. Electr. Comput. Eng. (IJECE), vol. 9, no. 3, p. 1765, 2019.
19. N. Al-Najdawi, S. Tedmori, O. A. Alzubi, O. Dorgham, and J. A. Alzubi, “A Frequency Based Hierarchical Fast Search Block Matching Algorithm for Fast Video Video Communications,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 4, 2016.
20. Sholiyi A., O’Farrell T., Alzubi O., and Alzubi J., “Performance Evaluation of Turbo Codes in High Speed Downlink Packet Access Using EXIT Charts”, International Journal of Future Generation Communication and Networking, Vol. 10, No. 8, August 2017.
21. J. A. Alzubi, O. A. Alzubi, A. Singh, and T. Mahmod Alzubi, “A blockchain-enabled security management framework for mobile edge computing,” Int. J. Netw. Manage., vol. 33, no. 5, 2023.

22. S.venkatasubramanian, “Green IoT Edge Computing Towards Sustainable and Distributed Data Processing”, International Journal of Research Publication and Reviews, Vol 4, no 9, pp 431-436 September 2023.
23. Venkatasubramanian, S., and R. Mohankumar. "DDoS Attack Detection in WSN Using Modified BGRU With MFO Model." Advanced Applications of Generative AI and Natural Language Processing Models, edited by Ahmed J. Obaid, et al., IGI Global, 2024, pp. 286-305.
24. Venkatasubramanian Srinivasan, et al. “Detection of Data Imbalance in MANET Network Based on ADSY-AEAMBi-LSTM with DBO Feature Selection.” Journal of Autonomous Intelligence, vol. 7, no. 4, 2024.
25. Syed Omar Ballari, Dr. Ranjith A, Kalaimathi. D, Mr. Tanveer Ahmad, C. Venkata Siva Rama Prasad (2023). Experimental Investigations on Electric Arc Furnace Slag Concrete. Corrosion and Protection, 51(2).
26. Srikanth, S., Ballari, S. O., & Eswar, S. (2022). Framework for freight movement in Bangalore city, India. In IOP Conference Series: Earth and Environmental Science (Vol. 1084, No. 1, p. 012033). IOP Publishing.
27. H. P. Josyula, L. Thamma Reddi, S. Parate, and A. Rajagopal, “A Review on Security and Privacy Considerations in Programmable Payments,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 9S, pp. 256–263, 2023.
28. V. S. Settibathini, S. K. Kothuru, A. K. Vadlamudi, L. Thammreddi, and S. Rangineni, “Strategic Analysis Review of Data Analytics with the Help of Artificial Intelligence,” International Journal of Advances in Engineering Research, vol. 26, pp. 1–10, 2023.
29. K. Patel, “Revolutionizing Consumer Data Analysis: The Development and Impact of a Unique Customer Identifier,” International Journal of Computer Trends and Technology, vol. 71, no. 12, pp. 61–74, 2023.
30. V. S. Kumar, A. K. Vadlamudi, S. Rangineni, and L. Thammareddi, “Analysis of Data Engineering: Solving Data preparation tasks with Chatgpt to finish data preparation,” Journal of Engineering Technologies and Innovative Research, no. 9, 2023.
31. K. Patel, “Bridging Data Gaps in Finance: The Role of Non-Participant Models in Enhancing Market Understanding,” International Journal of Computer Trends and Technology, vol. 71, no. 12, pp. 75–88, 2023.
32. K. Patel, “Ethical Reflections on Data-Centric AI: Balancing Benefits and Risks,” International Journal of Artificial Intelligence Research and Development, vol. 2, no. 1, pp. 1–17, 2024.
33. K. Patel, “Big Data in Finance: An Architectural Overview,” International Journal of Computer Trends and Technology, vol. 71, no. 10, pp. 61–68, 2023.
34. Khan, S., & Alfaifi, A. (2020). Modeling of Coronavirus Behavior to Predict It’s Spread. International Journal of Advanced Computer Science Applications, 11(5), 394-399.
35. Alfaifi, A. A., & Khan, S. G. (2022). Utilizing Data from Twitter to Explore the UX of “Madrasati” as a Saudi e-Learning Platform Compelled by the Pandemic. Arab Gulf Journal of Scientific Research, 39(3), 200-208.
36. AlAjmi, M. F., Khan, S., & Sharma, A. (2013). Studying Data Mining and Data Warehousing with Different E-Learning System. International Journal of Advanced Computer Science and Applications, 4(1), 144-147.
37. Khan, S., & Altayar, M. (2021). Industrial internet of things: Investigation of the applications, issues, and challenges. International Journal of Advanced Applied Sciences, 8(1), 104-113.
38. Khan, S. (2020). Artificial Intelligence Virtual Assistants (Chatbots) are Innovative Investigators. International Journal of Computer Science Network Security, 20(2), 93-98.

39. AlAjmi, M., & Khan, S. (2015). Part of Ajax And Openajax In Cutting Edge Rich Application Advancement For E-Learning. Paper presented at the INTED2015 Proceedings.

40. Khan, S., Moorthy, G. K., Vijayaraj, T., Alzubaidi, L. H., Barno, A., & Vijayan, V. (2023). Computational Intelligence for Solving Complex Optimization Problems. Paper presented at the E3S Web of Conferences.

41. Khan, S., Alqahtani, S., & Applications. (2023). Hybrid machine learning models to detect signs of depression. J Multimedia Tools, 1-19.

42. Rao, M. S., Modi, S., Singh, R., Prasanna, K. L., Khan, S., & Ushapriya, C. (2023). Integration of Cloud Computing, IoT, and Big Data for the Development of a Novel Smart Agriculture Model. Paper presented at the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE).

43. Khan, S., Fazil, M., Imoize, A. L., Alabduallah, B. I., Albahlal, B. M., Alajlan, S. A., . . . Siddiqui, T. (2023). Transformer Architecture-Based Transfer Learning for Politeness Prediction in Conversation. Sustainability, 15(14), 10828.

44. Margiana, R., Alsaikhan, F., Al-Awsi, G. R. L., Patra, I., Sivaraman, R., Fadhil, A. A., ... & Hosseini-Fard, S. (2022). Functions and therapeutic interventions of non-coding RNAs associated with TLR signaling pathway in atherosclerosis. Cellular Signalling, 100, 110471.

45. Arif, A., Alameri, A. A., Tariq, U. B., Ansari, S. A., Sakr, H. I., Qasim, M. T., ... & Karampoor, S. (2023). The functions and molecular mechanisms of Tribbles homolog 3 (TRIB3) implicated in the pathophysiology of cancer. International Immunopharmacology, 114, 109581.

46. Lei, Z., Alwan, M., Alamir, H. T. A., Alkaaby, H. H. C., Farhan, S. S., Awadh, S. A., ... & Nekuei, A. (2022). Detection of abemaciclib, an anti-breast cancer agent, using a new electrochemical DNA biosensor. Frontiers in Chemistry, 10, 980162.

47. Bashar, B. S., Kareem, H. A., Hasan, Y. M., Ahmad, N., Alshehri, A. M., Al-Majdi, K., ... & Qasim, M. T. (2022). Application of novel Fe3O4/Zn-metal organic framework magnetic nanostructures as an antimicrobial agent and magnetic nanocatalyst in the synthesis of heterocyclic compounds. Frontiers in Chemistry, 10, 1014731.

48. M Abbas, M., W Abooud, K., Qasim Mohammed, A., Hasan Al-Zubaidi, S., Hussain, A., M Hameed, N., ... & Ahmad Batayneh, K. (2022). Effects of various irrigation levels and biochar-based fertilizers on peanut production. Journal of Nuts, 13(4), 289-300.

49. Hussein, H. A., Khudair, S. A., Alwan, M., Aljawahiry, T., T Qasim, M., & V Pavlova, I. (2022). Impact of pollution caused by salmon breeding centers on river water quality. Caspian Journal of Environmental Sciences, 20(5), 1039-1045.

50. Lafta, H. A., AbdulHussein, A. H., Al-Shalah, S. A., Alnassar, Y. S., Mohammed, N. M., Akram, S. M., ... & Najafi, M. (2023). Tumor-Associated Macrophages (TAMs) in Cancer Resistance; Modula-tion by Natural Products. Current topics in medicinal chemistry.

51. Al-Jassani, M. J., Sayah, M. A., Qasim, M. T., Kadhim, A. J., & Muhammad, E. H. (2022). Isolation and Evaluation of Antibacterial Agents Produced by Soil Bacillus SP. and Study Some of their Immunological Parameters. Revista Electronica de Veterinaria, 23(4), 105-111.

52. Sane, S., Mahoori, A., Abdulabbas, H. S., Alshahrani, S. H., Qasim, M. T., Abosaooda, M., ... & Darvishzadehdaledari, S. (2023). Investigating the effect of pregabalin on postoperative pain in non-emergency craniotomy. Clinical Neurology and Neurosurgery, 226, 107599.

53. Al Anazi, A. A., Barboza-Arenas, L. A., Romero-Parra, R. M., Sivaraman, R., Qasim, M. T., Al-Khafaji, S. H., ... & Gono, R. (2023). Investigation and Evaluation of the Hybrid System of Energy Storage for Renewable Energies. Energies, 16(5), NA-NA.

54. Hjazi, A., Nasir, F., Noor, R., Alsalamy, A., Zabibah, R. S., Romero-Parra, R. M., ... & Akram, S. V. (2023). The pathological role of CXC chemokine receptor type 4 (CXCR4) in colorectal

cancer (CRC) progression; special focus on molecular mechanisms and possible therapeutics. Pathology-Research and Practice, 154616.

55. Althomali, R. H., Al-Hawary, S. I. S., Gehlot, A., Qasim, M. T., Abdullaeva, B., Sapaev, I. B., ... & Alsalamy, A. (2023). A novel Pt-free counter electrode based on MoSe2 for cost effective dye-sensitized solar cells (DSSCs): Effect of Ni doping. Journal of Physics and Chemistry of Solids, 182, 111597.
56. Hjazi, A., Ahsan, M., Alghamdi, M. I., Kareem, A. K., Al-Saidi, D. N., Qasim, M. T., ... & Mirzaei, R. (2023). Unraveling the Impact of 27-Hydroxycholesterol in Autoimmune Diseases: Exploring Promising Therapeutic Approaches. Pathology-Research and Practice, 154737.
57. Gupta, J., Suliman, M., Ali, R., Margiana, R., Hjazi, A., Alsaab, H. O., ... & Ahmed, M. (2023). Double-edged sword role of miRNA-633 and miRNA-181 in human cancers. Pathology-Research and Practice, 154701.
58. Al-Hawary, S. I. S., Kadhum, W. R., Saleh, E. A. M., Yacin, Y., Abdullah, E. A., Qasim, M. T., ... & Alsalamy, A. (2023). Tunneling induced swapping of orbital angular momentum in a quantum dot molecule. Laser Physics, 33(9), 096001.
59. Gaffar Sarwar Zaman, Ibrahem Waleed, Ruaa Ali Obeid, Shaymaa Abdulhameed Khudair, Saafa Abaas Abd Al-Kahdum, Kadhum Al-Majdi, Ahmed S. Abed, Ali Alsalamy, Maytham T. Qasim, Ahmed Hussien Radie Alawadi. (2023). Electrochemical determination of zearalenone in agricultural food samples using a flower like nanocomposite-modified electrode, Materials Chemistry and Physics,Volume 305,127986. ISSN 0254-0584.
60. Al-dolaimy, F., Kzar, M.H., Hussein, S.A. et al. (2023). Incorporating of Cobalt into UiO-67 Metal–Organic Framework for Catalysis CO2 Transformations: An Efficient Bi-functional Approach for CO2 Insertion and Photocatalytic Reduction. J Inorg Organomet Polym.
61. Muzammil Khursheed, Kzar Mazin Hadi, Mohammed Faraj, et al. (2023). Methanol extract of Iraqi Kurdistan Region Daphne mucronata as a potent source of antioxidant, antimicrobial, and anticancer agents for the synthesis of novel and bioactive polyvinylpyrrolidone nanofibers. Frontiers in Chemistry. Vol.1, 2296-2646.
62. Batool, Kiran; Zhao, Zhen-Yu; Irfan, Muhammad; Żywiołek, Justyna (2023): Assessing the role of sustainable strategies in alleviating energy poverty: an environmental sustainability paradigm. w: Environmental science and pollution research international 30 (25), s. 67109–67130.
63. Nayyar, Anand; Żywiołek, Justyna; Rosak Szyrocka, Joanna; Naved, Mohd (2023): Advances in distance learning in times of pandemic. First edition. Boca Raton, FL: Chapman & Hall/CRC Press.
64. Zywiolek, Justyna; Matulewski, Marek; Santos, Gilberto (2023): The Kano Model As A Tool For Assessing The Quality Of Hunting Tourism - A Case From Poland. w: IJQR 17 (3), s. 1097–1112.
65. Żywiołek, Justyna (2018): Monitoring of information security system elements in the metallurgical enterprises. w: MATEC Web Conf. 183, s. 1007.
66. Żywiołek, Justyna (2019): Personal data protection as an element of management security of information. w: Multidisciplinary Aspects of Production Engineering 2 (1), s. 515–522.
67. Żywiołek, Justyna; Schiavone, Francesco: The Value of data sets in Information and Knowledge Management as a Threat to Information Security, Garcia-Perez, Alexeis; Simkin, Lyndon (red.), w: European Conference on Knowledge Management, s. 882–891, dostępne na stronie internetowej: https://tinyurl.com/ECKM21.
68. Żywiołek, Justyna; Schiavone, Francesco (2021): Perception of the Quality of Smart City Solutions as a Sense of Residents' Safety. w: Energies 14 (17), s. 5511.

69. Tak, A. (2023). Succeeding Against the Odds: Project Management in Complex IT Scenarios. Journal of Technology and Systems, 5(2), 41–49.
70. Tak, A. (2023). Artificial Intelligence and Machine Learning in Diagnostics and Treatment Planning. Journal of Artificial Intelligence & Cloud Computing, 2(1), 1-6.
71. Tak, A. (2022). The Role of Artificial Intelligence in US Healthcare Information. International Journal of Science and Research, 11(12), 1302-1308.
72. Tak, A. (2022). Advanced AI Applications in Gaming with Cloud-Powered Media and Entertainment Experiences. Journal of Artificial Intelligence & Cloud Computing, 1(1), 1-4.
73. Tak, A. (2021). Comprehensive Study of AI-Driven Market Forecasting Models and Their Applicability. International Journal of Science and Research, 10(2), 1705-1709.
74. Ananda Shankar Hati, and T. K. Chatterjee, "Symmetrical component filter based online condition monitoring instrumentation system for mine winder motor" Measurement (Elsevier), vol. 82, pp. 284-300, 2016.
75. Prashant Kumar and Ananda Shankar Hati "Review on Machine Learning Algorithm Based Fault Detection in Induction Motors," Archives of Computational Methods in Engineering, vol: 28, pp: 1929-1940, 2021.
76. Kumar Prashant and Hati, Ananda Shankar "Convolutional Neural Network with batch normalization for fault detection in SCIM," IET Electric Power Application, vol: 15, issue: 1, pp. 39-50, 2021.
77. Kumar Prashant and Hati, Ananda Shankar "Deep Convolutional Neural Network based on adaptive gradient optimizer for fault detection in SCIM," ISA Transactions, vol: 111, pp: 350-359, 2021.
78. Prince, Hati Ananda Shankar, Chakrabarti Prasun, Abawajy Jemal Hussein and Ng Wee Keong "Development of Energy Efficient Drive for Ventilation System using Recurrent Neural Network," Neural Computing and Applications, Vol. 33, no. 14, pp. 8659-8668, 2021.
79. Sinha Ashish Kumar, Hati Ananda Shankar, Benbouzid Mohamed and Chakrabarti Prasun "ANN-based Pattern Recognition for Induction Motor Broken Rotor Bar Monitoring under Supply Frequency Regulation" Machines (2021), vol: 9(5).
80. Prince and Hati Ananda Shankar "A Comprehensive Review of Energy-Efficiency of Ventilation System using Artificial Intelligence" Renewable and Sustainable Energy Reviews (2021), vol: 146, 2021.
81. Kumar Prashant and Hati, Ananda Shankar "Transfer Learning Based Deep CNN Model for Multiple Faults Detection in SCIM" Neural Computing and Applications (2021).
82. Prince and Hati Ananda Shankar "Temperature and Humidity Dependent MRAS Based Speed Estimation Technique for Induction Motor used in Mine Ventilation Drive" Journal of Mining Science, 2021, Vol. 57, No. 5, pp. 842–851.
83. Kumar Prashant and Hati, Ananda Shankar "Dilated Convolutional Neural Network Based Model For Bearing Faults and Broken Rotor Bar Detection in Squirrel Cage Induction Motors" Expert Systems With Applications (2022).
84. Prince and Hati Ananda Shankar "Convolutional Neural Network-Long Short Term Memory Optimization for Accurate Prediction of Airflow in a Ventilation System" Expert Systems with Applications (2022).
85. Vatsa Aniket and Hati Ananda Shankar "Depolarization Current Prediction of Transformers OPI System Affected From Detrapped Charge Using LSTM," in IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-11, 2022, Art no. 2511711.
86. Gorai Rahul, Hati Ananda Shankar, and Maity Tanmoy, "A new cascaded multilevel converter

topology with a reduced number of components" 3rd IEEE 2017 Conference on International conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017), 21-22 September 2017 | IEEE, Chennai, India., pp. 539-543.

87. Kumar Prashant, Hati, Ananda Shankar, Sanjeevikumar Padmanaban, Leonowicz Zbigniew and Prasun Chakrabarti "Amalgamation of Transfer Learning and Deep Convolutional Neural Network for Multiple Fault Detection in SCIM" 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 9th-12th June 2020, Madrid, Spain.
88. Sinha Ashish Kumar, Kumar Prashant, Prince and Hati, Ananda Shankar, "ANN Based Fault Detection Scheme for Bearing Condition Monitoring in SRIMs using FFT, DWT and Band-pass Filters" 2020 International Conference on Power, Instrumentation, Control, and Computing (PICC) 2020 IEEE.
89. Prince Kumar and Hati, Ananda Shankar, "Sensor-less Speed Control of Ventilation System Using Extended Kalman Filter For High Performance," 2021 IEEE 8th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2021, pp. 1-6.
90. Kumar Prashant and Hati, Ananda Shankar "Support Vector Classifiers based broken rotor bar detection in Squirrel cage induction motor" Machines, Mechanisms and Robotics, Springer, Singapore, 429-438.
91. Hati, Ananda Shankar, and Chatterjee, T. K., "Some studies on condition monitoring techniques for online condition monitoring and fault diagnosis of mine winder motor", International Journal of Engineering Science and Technology (IJEST), vol. 4, no. 08, pp. 3785-3793, August 2012.
92. Hati, Ananda Shankar, and Chatterjee, T. K., "Axial leakage flux-based online condition monitoring instrumentation system for mine winder motor" Journal of Mines, Metals & Fuels, vol. 63, no. 5&6, pp. 132-140, May-June 2015.
93. Hati, Ananda Shankar, and Chatterjee, T. K., "Current monitoring Instrumentation system for detecting airgap eccentricity in mine winder motor", International Journal of Applied Engineering Research, vol. 10, no. 22, pp. 43000-43007, 2015.
94. Hati, Ananda Shankar, "Vibration monitoring instrumentation system for detecting airgap eccentricity in mine winder motor" Journal of Mine Metals and Fuels, vol. 64, no. 5&6, pp. 240-248, May-June 2016.
95. H. Lakhani, D. Undaviya, H. Dave, S. Degadwala, and D. Vyas, “PET-MRI Sequence Fusion using Convolution Neural Network,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023, pp. 317–321.
96. F. Ahamad, D. K. Lobiyal, S. Degadwala, and D. Vyas, “Inspecting and Finding Faults in Railway Tracks Using Wireless Sensor Networks,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023, pp. 1241–1245.
97. D. Rathod, K. Patel, A. J. Goswami, S. Degadwala, and D. Vyas, “Exploring Drug Sentiment Analysis with Machine Learning Techniques,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023, pp. 9–12.
98. C. H. Patel, D. Undaviya, H. Dave, S. Degadwala, and D. Vyas, “EfficientNetB0 for Brain Stroke Classification on Computed Tomography Scan,” in 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2023, pp. 713–718.
99. V. Desai, S. Degadwala, and D. Vyas, “Multi-Categories Vehicle Detection For Urban Traffic Management,” in 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), 2023, pp. 1486–1490.

100. D. Vyas and V. V Kapadia, "Evaluation of Adversarial Attacks and Detection on Transfer Learning Model," in 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), 2023, pp. 1116–1124.

101. D. D. Pandya, S. K. Patel, A. H. Qureshi, A. J. Goswami, S. Degadwala, and D. Vyas, "Multi-Class Classification of Vector Borne Diseases using Convolution Neural Network," in 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2023, pp. 1–8.

102. D. D. Pandya, A. K. Patel, J. M. Purohit, M. N. Bhuptani, S. Degadwala, and D. Vyas, "Forecasting Number of Indian Startups using Supervised Learning Regression Models," in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023, pp. 948–952.

103. S. Degadwala, D. Vyas, D. D. Pandya, and H. Dave, "Multi-Class Pneumonia Classification Using Transfer Deep Learning Methods," in 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2023, pp. 559–563.

104. D. D. Pandya, A. Jadeja, S. Degadwala, and D. Vyas, "Diagnostic Criteria for Depression based on Both Static and Dynamic Visual Features," in 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 2023, pp. 635–639.

105. H. Gupta, D. Patel, A. Makade, K. Gupta, O. P. Vyas, and A. Puliafito, "Risk Prediction in the Life Insurance Industry Using Federated Learning Approach," in 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON), 2022, pp. 948–953.

106. S. Dave, S. Degadwala, and D. Vyas, "DDoS Detection at Fog Layer in Internet of Things," in 2022 International Conference on Edge Computing and Applications (ICECAA), 2022, pp. 610–617.

107. D. D. Pandya, A. Jadeja, S. Degadwala, and D. Vyas, "Ensemble Learning based Enzyme Family Classification using n-gram Feature," in 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 1386–1392.

108. V. B. Gadhavi, S. Degadwala, and D. Vyas, "Transfer Learning Approach For Recognizing Natural Disasters Video," in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 793–798.

109. J. Mahale, S. Degadwala, and D. Vyas, "Crop Prediction System based on Soil and Weather Characteristics," in 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2022, pp. 340–345.

110. M. Shah, S. Degadwala, and D. Vyas, "Diet Recommendation System based on Different Machine Learners: A Review," in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 290–295.

111. B. Trivedi, S. Degadwala, and D. Vyas, "Parallel data stream anonymization methods: A review," in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 887–891.

112. D. D. Pandya, N. S. Gupta, A. Jadeja, R. D. Patel, S. Degadwala, and D. Vyas, "Bias Protected Attributes Data Balancing using Map Reduce," in 2022 6th International Conference on Electronics, Communication and Aerospace Technology, 2022, pp. 1540–1544.

113. R. Baria, S. Degadwala, R. Upadhyay, and D. Vyas, "Theoretical Evaluation of Machine And Deep Learning For Detecting Fake News," in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 325–329.

114. P. Bam, S. Degadwala, R. Upadhyay, and D. Vyas, "Spoken Language Recognization Based on Features and Classification Methods: A Review," in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 868–873.

115. K. Butchi Raju, P. Kumar Lakineni, K. S. Indrani, G. Mary Swarna Latha and K. Saikumar, "Optimized building of machine learning technique for thyroid monitoring and analysis," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 1-6.

116. P. K. Lakineni, D. J. Reddy, M. Chitra, R. Umapriya, L. V. Kannan and S. R. Barkunan, "Optimal Feature Selection and Classification Using Convolutional Neural Network-Based Plant Disease Prediction," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6.

117. P. K. Lakineni, S. Kumar, S. Modi, K. Joshi, V. Mareeskannan and J. Lande, "Deepflow: A Software-Defined Measurement System for Deep Learning," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 1217-1221.

118. P. K. Lakineni, R. Singh, B. Mandaloju, S. Singhal, M. D. Bajpai and M. Tiwari, "A Cloud-Based Healthcare Diagnosis Support Network for Smart IoT for Predicting Chronic Kidney Failure," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 1858-1863.

119. P. K. Lakineni, K. M. Nayak, H. Pallathadka, K. Gulati, K. Pandey and P. J. Patel, "Fraud Detection in Credit Card Data using Unsupervised & Supervised Machine Learning-Based Algorithms," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2022, pp. 1-4.

120. V. Dankan Gowda, K. Prasad, R. Shekhar, R. Srinivas, K. N. V. Srinivas and P. K. Lakineni, "Development of a Real-time Location Monitoring App with Emergency Alert Features for Android Devices," 2023 4th IEEE Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2023, pp. 1-8.

121. S. Mandvikar, "Factors to Consider When Selecting a Large Language Model: A Comparative Analysis," International Journal of Intelligent Automation and Computing, vol. 6, no. 3, pp. 37–40, 2023.

122. S. Mandvikar, "Augmenting intelligent document processing (IDP) workflows with contemporary large language models (LLMs)," International Journal of Computer Trends and Technology, vol. 71, no. 10, pp. 80–91, 2023.

123. R. Boina, A. Achanta, and S. Mandvikar, "Integrating data engineering with intelligent process automation for business efficiency," International Journal of Science and Research, vol. 12, no. 11, pp. 1736–1740, 2023.

124. S. Mandvikar and A. Achanta, "Process automation 2.0 with generative AI framework," Int. J. Sci. Res. (Raipur), vol. 12, no. 10, pp. 1614–1619, 2023.

125. Mandvikar, S. (2023). Indexing robotic process automation products. International Journal of Computer Trends and Technology, 71(8), 52–56.

126. Tak, A. (2021). Multi-Modal Fusion for Enhanced Image and Speech Recognition in AI Systems. International Journal of Science and Research, 10(6), 1780-1788.

127. Tak, A. (2021). The Data Mining Techniques for Analyzing Employee Performance and Productivity. International Journal of Science and Research, 10(10), 1575-1578.

128. Tak, A. (2022). The Impact of Electronic Health Records on Patient Care in the US Healthcare System. Journal of Health Statistics Reports, 1(2), 1–7.

129. Tak, A. (2022). Big Data Analytics in Healthcare: Transforming Information into Actionable Insights. Journal of Health Statistics Reports, 1(3), 1-6.

130. Tak, A. (2023). The Role of Cloud Computing in Modernizing Healthcare IT Infrastructure. Journal of Artificial Intelligence & Cloud Computing, 2(2), 1–7.

131. Alarood, A. A., Faheem, M., Al-Khasawneh, M. A., Alzahrani, A. I., & Alshdadi, A. A. (2023). Secure medical image transmission using deep neural network in e-health applications. Healthcare Technology Letters, 10(4), 87-98.

132. Al-Khasawneh, M. A., Abu-Ulbeh, W., & Khasawneh, A. M. (2020, December). Satellite images encryption Review. In 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI) (pp. 121-125). IEEE.

133. Al-Khasawneh, M. A., Alzahrani, A., & Alarood, A. (2023). Alzheimer's Disease Diagnosis Using MRI Images. In Data Analysis for Neurodegenerative Disorders (pp. 195-212). Singapore: Springer Nature Singapore.

134. Al-Khasawneh, M. A., Alzahrani, A., & Alarood, A. (2023). An Artificial Intelligence Based Effective Diagnosis of Parkinson Disease Using EEG Signal. In Data Analysis for Neurodegenerative Disorders (pp. 239-251). Singapore: Springer Nature Singapore.

135. Al-Khasawneh, M. A., Faheem, M., Aldhahri, E. A., Alzahrani, A., & Alarood, A. A. (2023). A MapReduce Based Approach for Secure Batch Satellite Image Encryption. IEEE Access.

136. D. K. Srivastava and B. Roychoudhury, "Understanding the factors that influence adoption of privacy protection features in online social networks," J. Glob. Inf. Technol. Manag., vol. 24, no. 3, pp. 164–182, 2021.

137. D. K. Srivastava and B. Roychoudhury, "Words are important: A textual content based identity resolution scheme across multiple online social networks," Knowl. Based Syst., vol. 195, no. 105624, p. 105624, 2020.

138. Mahmoud, M., & Al-Khasawneh, M. A. (2020). Greedy intersection-mode routing strategy protocol for vehicular networks. Complexity, 2020, 1-10.

139. Markkandeyan, S., Gupta, S., Narayanan, G. V., Reddy, M. J., Al-Khasawneh, M. A., Ishrat, M., & Kiran, A. (2023). Deep learning based semantic segmentation approach for automatic detection of brain tumor. International Journal of Computers Communications & Control, 18(4).

140. R. Regin, S. S. Rajest, Shynu T, & Steffi. R. (2023). Relationship Between Employee Loyalty and Job Satisfaction in an Organization. European Journal of Life Safety and Stability (2660-9630), 36(12), 54-73.

141. R. Regin, S. Suman Rajest, Shynu T, & Steffi. R. (2023). Planning the Most Effective Itinerary for Tourists through the use of Data Analysis. International Journal of Human Computing Studies, 5(12), 77-92.

142. Rajest, S. S., Regin, R., T, Shynu., & R, Steffi. (2023). Treatment Method for Sewage Water Used in Horticulture. European Journal of Life Safety and Stability, 36(12), 11-27.

143. Regin, R., S. Suman Rajest, Shynu T, and Steffi. R. "Application of Machine Learning to the Detection of Retinal Diseases". European Journal of Life Safety and Stability, 37(1): 1-23.

144. S. Suman Rajest, R. Regin, Shynu T, & Steffi. R. (2023). An Approach Based on Machine Learning for Conducting Sentiment Analysis on Twitter Data. International Journal of Human Computing Studies, 5(12), 57-76.

145. S. Suman Rajest, R. Regin, Shynu T, & Steffi. R. (2023). Using Voice Guidance, an Intelligent Walking Assistance Mechanism for the Blind. Central Asian Journal of Theoretical and Applied Science, 4(11), 41-63. Retrieved from https://cajotas.centralasianstudies.org/index.php/CAJOTAS/article/view/1335

146. S. Suman Rajest, R. Regin, Shynu T, & Steffi. R. (2024). Analysis of Sentimental Bias the Implementation of Supervised Machine Learning Algorithms. International Journal of Innovative Analyses and Emerging Technology, 4(1), 8–33.

147. Shah, S. A. A., Al-Khasawneh, M. A., & Uddin, M. I. (2021, June). Street-crimes Modelled Arms Recognition Technique (SMART): Using VGG. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 38-44). IEEE.

148. Shah, S. A. A., Al-Khasawneh, M. A., & Uddin, M. I. (2021, June). Review of weapon detection techniques within the scope of street-crimes. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 26-37). IEEE.

149. Shynu T, S. Suman Rajest, R. Regin, & Steffi. R. (2023). Android Application for Remote Control of Personal Computers. International Journal on Orange Technologies, 5(12), 44-58.

150. Shynu T, S. Suman Rajest, R. Regin, & Steffi. R. (2023). Corporate Governance and Family Involvement as Performance Factors. Spanish Journal of Innovation and Integrity, 25(12), 76-94.

151. Shynu T, S. Suman Rajest, R. Regin, & Steffi. R. (2023). Region Segmentation and Support Vector Machine for Brain Tumour Stage Analysis, Detection, and Automatic Classification. Central Asian Journal of Medical and Natural Science, 25-43.

152. Shynu T, S. Suman Rajest, R. Regin, & Steffi. R. (2024). Using a Deep Convolutional Neural Network to Identify Vehicle Driver Activity. International Journal on Orange Technologies, 6(1), 1-19.

153. Steffi. R, Shynu T, S. Suman Rajest, & R. Regin. (2023). A Convolutional Neural Network with a U-Net for Brain Tumor Segmentation and Classification. Central Asian Journal of Medical and Natural Science, 4(6), 1326-1343.

154. Steffi. R, Shynu T, S. Suman Rajest, & R. Regin. (2023). Performance of Employees in Relation to The Effects of Change Management Practices. Central Asian Journal of Innovations on Tourism Management and Finance, 4(12), 1-23.

155. Steffi. R, Shynu T, S. Suman Rajest, & R. Regin. (2024). A Review of the System for Filtering Particulate Matter Affected by Cement Factor. Central Asian Journal of Theoretical and Applied Science, 5(1), 78-93.

156. Sukhni, H. A., Al-Khasawneh, M. A., & Yusoff, F. H. (2021, June). A Systematic Analysis for Botnet Detection using Genetic Algorithm. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 63-66). IEEE.

157. Sundararajan, V., Steffi, R., & Shynu, T. (2023). Data Fusion Strategies for Collaborative Multi-Sensor Systems: Achieving Enhanced Observational Accuracy and Resilience. FMDB Transactions on Sustainable Computing Systems, 1(3), 112–123.

158. Tak, A., & Sundararajan, V. (2023, December 2). Pervasive Technologies and Social Inclusion in Modern Healthcare: Bridging the Digital Divide. FMDB Transactions on Sustainable Health Science Letters, 1(3), 118-129.

159. V. K. Nomula, R. Steffi, and T. Shynu, "Examining the Far-Reaching Consequences of Advancing Trends in Electrical, Electronics, and Communications Technologies in Diverse Sectors," FMDB Transactions on Sustainable Energy Sequence, vol. 1, no. 1, pp. 27–37, 2023.