IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

QR Code Secure Cloud Auditing System using Areal Time

Dr.P.Jayasree, Mr.A.Syed Riyaz Ahamed

Associate Professor, Department of Computer Applications (UG), Hindusthan College of Arts & Science, Coimbatore, India

III BCA Student, Department of Computer Applications (UG), Hindusthan College of Arts & Science, Coimbatore, India

ABSTRACT: In order to improve security in cloud-based systems, this abstract presents a revolutionary Real-Time Auditing System that makes use of QR Code technology. Assuring real-time data security and integrity might be difficult for traditional auditing techniques. As a result, this system incorporates QR Code technology to offer a reliable solution. To ensure secure transmission and cloud storage, the system dynamically creates QR Codes with encrypted audit information. Stakeholders can instantly obtain the most recent audit data by utilising real-time scanning capabilities. While protecting data confidentiality, this method improves audit trail accuracy and efficiency.Furthermore, scalable and accessible auditing procedures across various organisational contexts are made possible by the cloud-based design of the System. The suggested approach solves important issues with data security and audit trail dependability in modern digital ecosystems through cloud integration and QR Code encryption.

I. INTRODUCTION

In today's digitally interconnected world, the integrity and security of data have become paramount concerns for organizations across all sectors. With the exponential growth of cloud- based infrastructures, traditional auditing systems face significant challenges in ensuring real- time monitoring and verification while maintaining data confidentiality. To address these complexities, this project introduces a ground breaking solution a Real-Time Auditing System that leverages QR code technology to enhance security and efficiency with in cloud environments.

This introduction sets the stage for an in-depth exploration of the project's objectives, methodologies and outcomes. It elucidates the pressing need for innovative auditing mechanisms in the face of evolving cyber security threats and underscores the potential of QR code technology to revolutionize auditing processes. Through this project, we aim to develop a robust and scalable system that not only meets the stringent security requirements of cloud-based operations but also provides stakeholders with real-time access to accurate and verifiable audit data.

Background

The Background subsection serves as a foundation for understanding the necessity and relevance of the proposed Real-Time Auditing System Using QR Code for Secure Cloud. It delves into several key aspects

Challenges in Current Auditing Systems

It begins by outlining the limitations and shortcomings of traditional auditing methodologies, especially when applied within the dynamic and interconnected landscape of cloud-based environments. Issues such as delayed data processing, lack of real-time monitoring capabilities, and vulnerability to cyber threats are highlighted. These challenges underscore the critical need for more agile and robust auditing systems capable of addressing the evolving demands of cloud computing.

Trends and Gaps in Cloud-Based Auditing

The subsection explores emerging trends in cloud-based auditing, such as the increasing reliance on digital platforms for data storage and processing. It discusses the unique challenges posed by the distributed and virtualized nature of cloud infrastructures, including the complexities of data management and the heightened risk of security breaches. Furthermore, it identifies gaps in existing auditing systems that fail to adequately address these challenges, emphasizing

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

the need for innovative solutions.

Risks and Vulnerabilities Associated with Digital Systems
Given the growing dependence on digital systems for auditing purposes, this section also examines the inherent risks and vulnerabilities associated with such platforms. Factors such as data breaches, insider threats, and malware attacks are discussed, highlighting the importance of implementing robust security measures to safeguard sensitive information.

Evolution of QR Code Technology
In addressing the need for enhanced security and efficiency in auditing processes, the subsection explores the evolution of QR code technology and its potential applications in various domains. It traces the origins of QR codes and their transformation from simple barcodes to sophisticated data encoding mechanisms capable of storing vast amounts of information securely. Furthermore, it discusses how QR code technology can be leveraged to streamline auditing procedures, improve data integrity, and facilitate real-time access to audit information.

By providing this comprehensive contextual backdrop, the Background subsection lays the groundwork for understanding the rationale behind the development of the Real-Time Auditing System Using QR Code for Secure Cloud. It underscores the urgency of addressing the shortcomings of current auditing systems and highlights the potential of QR code technology to revolutionize auditing practices in cloud-based environments.

OBJECTIVES
In the Objectives subsection, the specific aims and goals of the real-time auditing system using QR code technology for secure cloud environments are articulated with precision and clarity. This section serves as a roadmap for the development and implementation of the system, delineating both the overarching objectives and the specific outcomes anticipated from its deployment. The objectives encompass a range of crucial aspects aimed at enhancing the effectiveness, efficiency, and security of auditing processes within cloud-based infrastructures. Here's an expansion of the objectives

Enhancing Data Integrity
The primary objective of the real-time auditing system is to bolster data integrity within cloud environments. By leveraging QR code technology, the system aims to implement robust mechanisms for verifying the accuracy and authenticity of audit data. This involves ensuring that all data stored and transmitted through the system remains tamper-proof and verifiable, thereby instilling trust and reliability in auditing outcomes.

Ensuring Real-Time Access to Audit Information
Another key objective is to provide stakeholders with seamless and real-time access to auditinformation.Thesystemseekstoeliminatedelaysindataprocessingandretrieval,enabling users to access up-to-date audit records instantaneously. This real-time accessibility enhances decision-making capabilities and facilitates prompt responses to emerging audit-related issues or anomalies.

Strengthening Security Measures
A critical aim of the system is to bolster security measures within cloud-based auditing processes. This involves implementing robust encryption techniques to safeguard audit data against unauthorized access, manipulation, or interception. Additionally, the system incorporates stringent authentication protocols to ensure that only authorized personnel can access sensitive audit information, thereby mitigating the risk of security breaches.

Improving Auditing Efficiency
The system aims to streamline auditing processes and enhance overall efficiency. By automating routine audit tasks and reducing manual intervention, the system minimizes the time and resources required for conducting audits. Furthermore, it employs advanced analytics capabilities to identify patterns, trends, and anomalies in audit data, thereby facilitating more effective risk assessment and compliance monitoring.

This section of the document clarifies the purpose and desired outcomes of the proposed real-time auditing system, providing a clear direction for the ensuing research or development effort. By articulating these objectives, stake holder scan align their efforts towards the successful implementation of the system, ultimately contributing to enhanced

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

security, efficiency, and reliability in cloud-based auditing practices.

Scope

In the Scope subsection, the boundaries and parameters of the study or project are clearly Out lined, providing a roadmap for the development and implementation of the real-time auditing systemusingQRcodetechnologyforsecurecloudenvironments.Thissectionservesasacritical framework for managing expectations, guiding decision-making processes, and ensuring alignment with project objectives. The Scope delineates various aspects, including functionality, technological requirements, organizational context, audit types, user groups, and constraints. Here's an expanded breakdown

Functionality

The Scope defines the functionalities and capabilities of the real-time auditing system. This includes specifying the core features such as data encryption, QR code generation, real-time monitoring, audit trail management, and reporting functionalities. Additionally, it may outline any advanced features such as anomaly detection, predictive analytics, or integration with existing auditing software.

Technological Requirements

This section identifies the technological infrastructure and requirements necessary for the successful implementation of the system. It may specify hardware components, software platforms, programming languages, databases, and communication protocols required to develop and deploy the system effectively.

Organizational Context

The Scope considers the organizational context within which the real-time auditing system will operate. This includes identifying the organizational stakeholders, such as audit teams, IT departments, management personnel, and regulatory bodies. Moreover, it may address organizational structures, policies, and procedures that may impact the implementation and utilization of the system.

Audit Types and Data Handling

This section outlines the types of audits and data that the system will handle. It may specify the scope of audits, such as financial audits, compliance audits, security audits, or operational audits. Furthermore, it defines the types of data that will be collected, processed, and stored by the system, including transaction records, log files, configuration data, and metadata.

User Groups

The Scope identifies the targeted user groups who will interact with there al-time auditing system. This may include auditors, compliance officers, IT administrators, executives, and other stakeholders involved in audit-related activities. Additionally, it may address user roles, permissions, and access levels within the system to ensure proper governance and security.

Constraints

Lastly, the Scope acknowledges any constraints or limitations that may impact the development and implementation of the system. This may include budget aryconstraints, resource limitations, time constraints, regulatory requirements, or technological constraints. By identifying these constraints upfront, the project team can proactively address challenges and mitigate risks throughout the project lifecycle

II. SYSTEM ANALYSIS

2.1 LITERATURE SURVEY

1. Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE]

Advantages

- A privacy-preserving public auditing system for data storage security in Cloud Computing.
- We utilize the homomorphism linear authenticator and random masking to guarantee that the TPA would not learn

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

- It is provably secure and highly efficient.

Disadvantage

- The individual auditing of these growing tasks can be tedious and cumbersome.
- The technique of public key based homomorphism linear authenticator, which enables TPA to perform the auditing without demanding the local copy of data and thus drastically reduces the communication and computation overhead as compared to the straightforward data auditing approaches.

2. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data
(1**Y.Prasanna,**2**Ramesh) Advantages:**

- Theefficientandsecurerankedmulti-keywordsearchonremotelystoredencrypted database model where the database users are protected against privacy violation.
- We appropriately increase the efficiency of the scheme by using symmetric-key encryption method rather than public- key encryption for document encryption.

Disadvantages

- The computation and communication costs of this method are quite large since every search term in a query requires several homomorphism encryption operations both on the server and the user side.
- They retrieving all files containing the queried keyword further incurs unnecessary network traffic.

3. Oruta:Privacy-PreservingPublicAuditingforSharedDataintheCloud(BoyangWang †,††, Baochun Li †† and Hui Li † † State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China †† Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada Email:{bywang,bli}@eecg.toronto.edu, lihui@mail.xidian.edu.cn)

Advantages

- Oruta,theTPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users.
- We exploitring signatures to compute the verification information needed to audit the integrity of shared data.
- The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.
- They share the data effectively and competent.

Disadvantages:

- To preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a more valuable target than others.
- The information is confidential to the group and should not be revealed to any third party.

4. Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud
(Boyang Wang, Baochun Li, Member, IEEE, and HuiLi, Member, IEEE)

Advantages:

- Anewpublicauditingmechanismforshareddatawithefficientuserrevocationinthe cloud.
- When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures.
- Thegroupcansaveasignificantamountofcomputationandcommunicationresources during user revocation.

Disadvantages:

- This revoked user should no longer be able to access and modify shared data.
- The integrity of the entire data can still be verified with the public keys of existing users only.

5. Remote Data Checking for Network Coding-based Distributed Storage Systems(Bo Chen, Reza Curtmola Department of Computer Science New Jersey Institute of Technology

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

{bc47,crix}@njit.edu, Giuseppe Ateniese, Randal Burns Department of Computer Science Johns Hopkins University {ateniese, randal}@cs.jhu.edu)

Advantages:

- A secure and efficient RDC scheme for network coding-based distributed storage systems that rely on untrusted server..
    - RDC-NC scheme can be used to ensure data remains when faced with data corruption, replay, and pollution attacks.
- The RDC-NC is in expensive for both clients and servers.

Disadvantages:

- Thecodeis not systematic; itdoes not embed theinputas part ofthe encoded output.
- Smallportionsofthefilecannot bereadwithout reconstructingtheentirefile.
- Onlinestoragesystemsdonotusenetworkcoding,becausetheyprefertooptimize performance for read (the common operation).
- They usesystematiccodes to support sub-fileaccess to data. Network-coding for storagereally only makes sense for systems in which data repair occurs much more often than read.

6. Short Group Signatures(Dan Boneh1,?, Xavier Boyen2, and Hovav Shacham3 1 Stanford University, dabo@cs.stanford.edu 2 Voltage Security, xb@boyen.org 3 Stanford University, hovav@cs.stanford.edu)

Advantages:

- Signatures in our scheme are approximately the size of a standard RSA signature with the same security.
- The group signature is based on the Strong Diffie-Hellman assumption and anew assumption in bilinear groups called the Decision Linear.

Disadvantages:

- Signature generation requires no pairing computations ,and verification requires a single pairing.

7. Storing Shared Data on the Cloud via Security-Mediator (Boyang Wang†§, Sherman S. M. Chow‡, Ming Li§, and Hui Li† †State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China Department of Information Engineering, Chinese University of Hong Kong, Hong Kong §Department of Computer Science, Utah State University, Logan, Utah, USA)

Advantages:

- Webelieveistherightapproachtoachieveanonymityinstoringdatatothecloudwith publicly-verifiable data-integrity in mind.
- Thedecouplestheanonymousprotectionmechanismfromtheprovabledatapossession mechanism via the use of security mediator.
- Theyminimizethecomputationandbandwidthrequirementofthismediator,butalso minimize the trust placed on it in terms of data privacy and identity privacy.

Disadvantages:

- To preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a more valuable target than others.
- The information is confidential to the group and should not be revealed to any third party.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing auditing system typically relies on manual or semi-automated processes for conducting audits within cloud-based environments. This system may involve the use of traditional auditing tools and software, often characterized by batch processing of audit data and periodic reporting. However, such systems face several limitations

1. Lack of Real-Time Monitoring The existing system lacks real-time monitoring capabilities, resulting in delays in

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

detecting and responding to audit-related issues or anomalies.

2. Limited Data Integrity Data integrity may be compromised due to the absence of robust encryption mechanisms and tamper-proof audit trails, leading to concerns regarding the accuracy and reliability of audit findings.
3. Security Vulnerabilities The system may be susceptible to security vulnerabilities, including unauthorized access, data breaches, and inside threats, posing risks to sensitive audit information.
4. Manual Processes Manual processes involved in data collection, analysis, and reporting can be time-consuming, error-prone, and inefficient, hindering the overall effectiveness of the auditing process.

3.1.1 Disadvantages

- LackofReal-TimeMonitoringTheexistingsystemoftenlacksreal-timemonitoring capabilities, resulting in delayed detection of audit-related issues.
- Limited Data Integrity Data integrity may be compromised due to the absence of robust encryption and tamper-proof audit trails.
- Security Vulnerabilities The system may be susceptible to security vulnerabilities, including unauthorized access and data breaches.
- Manual Processes Manual processes involved in data collection and analysis can be time- consuming and error-prone, hindering efficiency.

3.2 PROPOSED SYSTEM

The proposed real-time auditing system aims to address the limitations of the existing system by leveraging QR code technology and cloud-based infrastructure. Key features and enhancements of the proposed system include

- Real-Time Monitoring The system facilitates real-time monitoring of audit data, enabling stakeholders to access up-to-date audit information instantaneously.
- Enhanced Data Integrity QR code technology is utilized to ensure data integrity by encrypting audit information and generating tamper-proof audit trails. This enhances the accuracy and reliability of audit findings.
- Improved Security Measures Robust encryption techniques and authentication protocols are implemented to safeguard audit data against unauthorized access, manipulation, and interception, thereby mitigating security risks.
- Automation and Efficiency The system automates routine audit tasks and processes, reducing manual intervention and streamlining auditing procedures. Advanced analytics capabilities enable the identification of patterns, trends, and anomalies in audit data, enhancing risk assessment and compliance monitoring.
- Cloud Integration The system is designed to seamlessly integrate with cloud-based infrastructures, leveraging the scalability, flexibility, and accessibility offered by cloud computing. This ensures compatibility with existing IT systems and facilitates efficient data storage, processing, and retrieval.

Overall, the proposed real-time auditing system represents a significant advancement over the existing system, offering enhanced security, efficiency, and reliability in auditing processes within cloud environments. By leveraging QR code technology and cloud-based infrastructure, the system provides stakeholders with real-time access to accurate and verifiable audit information, thereby facilitating informed decision-making and ensuring compliance with regulatory requirements.

3.2.1 Advantages

Real-TimeMonitoringTheproposedsystemfacilitatesreal-timemonitoringofaudit data, enabling prompt detection and response to audit-related issues.

- Enhanced Data Integrity QR code technology ensures data integrity by encrypting audit information and generating tamper-proof audit trails.
- ImprovedSecurityMeasuresRobustencryptionandauthenticationprotocolsenhance security, safeguarding audit data against unauthorized access and manipulation.
- Automation and Efficiency The system automates routine audit tasks, reducing manual intervention and streamlining auditing procedures.
- Cloud Integration Integration with cloud-based infrastructure offers scalability, flexibility, and accessibility, facilitating efficient data storage and processing.

A QRcode is a type of matrix bar code or two-dimensional code that can store data informationanddesignedtobereadbysmartphones.QRstandsfor“QuickResponse”indicating that the code contents should

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

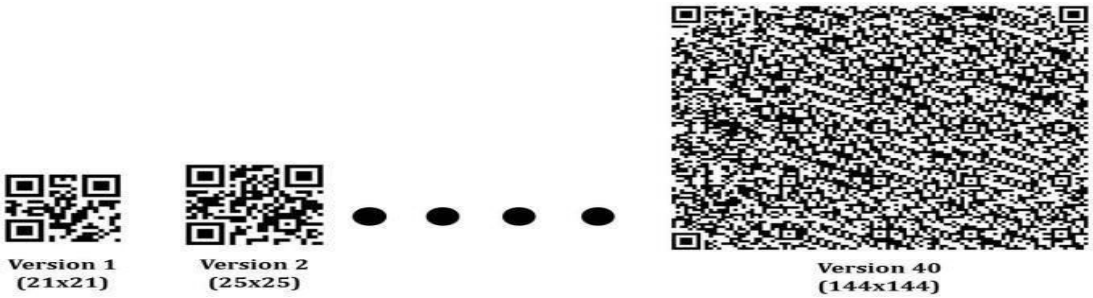
be decoded very quickly at high speed. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL or other data [1] [2]. The QR code was designed to allow its contents to be decoded at high speed. The popularity of QR codes is growing rapidly all around the world. Nowadays, mobile phones with built-in camera are widely used to recognize the QR Codes.

QR Codes are created by the Toyota subsidiary Denso Wave in 1994, and was initially used for tracking inventory in vehicle parts manufacturing. The idea behind the development of the QR code is the limitation of the barcode information capacity (can only hold20 alphanumeric characters).

While they are developed for tracking parts in vehicle manufacturing, QR codes now are used in many other fields, from commercial tracking to entertainment, in-store product labeling, and in those applications that are aimed at smartphone users. Users may open URL; receive text after scanning QR codes. By using QR code generating sites or apps, user scan generate and print their own QR codes for others to scan and use.
The QR code system consists of a QR code encoder and decoder. The encoder is responsible for encoding data and generation of the QR Code, while the decoderd codes the data from the QR code.

Overview of the QR code working. The plain text, URL, or other data are given to the QR code encoder, and it generates the required QR code and when we want to access the data of the QR code, QR code is decoded via QR Code decoder(scanner)which retrieves the data of QR code [1] [3].

INFORMATION CAPACITY AND VERSIONS OF THE QRCODE
The symbol versions of the QR Code range from Version 1 to Version 40 [4]. Each version has a different module configuration or number of modules. (The module refers to the black and white dots that make up QR Code.) "Module configuration" refers to the number of modules contained in a symbol, commencing with Version1(21×21modules) upto Version.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

DATA CAPACITY OF QRCODE VERSION40

Version	Modules	ECC Level	Data Bits (mixed)	Numeric	Alpha-numeric	Binary	Kanji
40	177x177	L	23,648	7,089	4,296	2,953	1,817
		M	18,672	5,596	3,391	2,331	1,435
		Q	13,328	3,993	2,420	1,663	1,024
		H	10,208	3,057	1,852	1,273	784

Each QR Code symbol version has the maximum data capacity, according to the amount of data, character type and error correction level. In other words, as the amount of data increases, more modules are required to comprise QR Code, resulting in larger QR Code symbols. Table 1 show the data capacity of version 40 for different type of data.

QRCODE ERROR CORRECTION

QR Code employs error correction to generate a series of error correction code words which are added to the data code word sequence which enable symbol to be read even if it is dirty or damaged. The QR code achieves powerful error-correction capability by using Reed-Solomon codes, a widely used mathematical error-correction method. Four levels of error correction are available, higher level has high capability of recovery. Table 2 shows error-correction levels and their approximate ability of error correction.

When selecting the level of error correction, environmental conditions as well as the desired size of the QR Code symbol need to be taken under consideration.

ERRORCORRECTIONLEVELSAND%OFCORRECTION

S No.	Error-Correction Level	Approximate Amount of Correction
1.	L	7%
2.	M	15%
3.	Q	25%
4.	H	30%

For example, Level Q (25% error correction) or H (30%) may be required for factories or other applications where the QR Code is likely to become dirty or damaged. For clean environments and codes containing a large amount of data, Level L (7%) may be selected. In general, Level M (15%) is most frequently used [3] [4].

STRUCTURE OFA QRCODE

EachQRCodesymbolshallbebuiltofsquaremodulesarrangedinaregularsquarearray and shall consist of function patterns and encoding region. And the whole symbol shall be surrounded on all four sides by a quiet zone border [4] [5].

Function patterns are the shapes that must be placed in specific areas of the QR code to ensure that QR code scanners can correctly identify and orient the code for decoding. There are 4 types of function patterns; they are finder pattern, separator, timing patterns, and alignment patterns.

Encoding region contains data, which represents version information, format information, data and error correction code words.

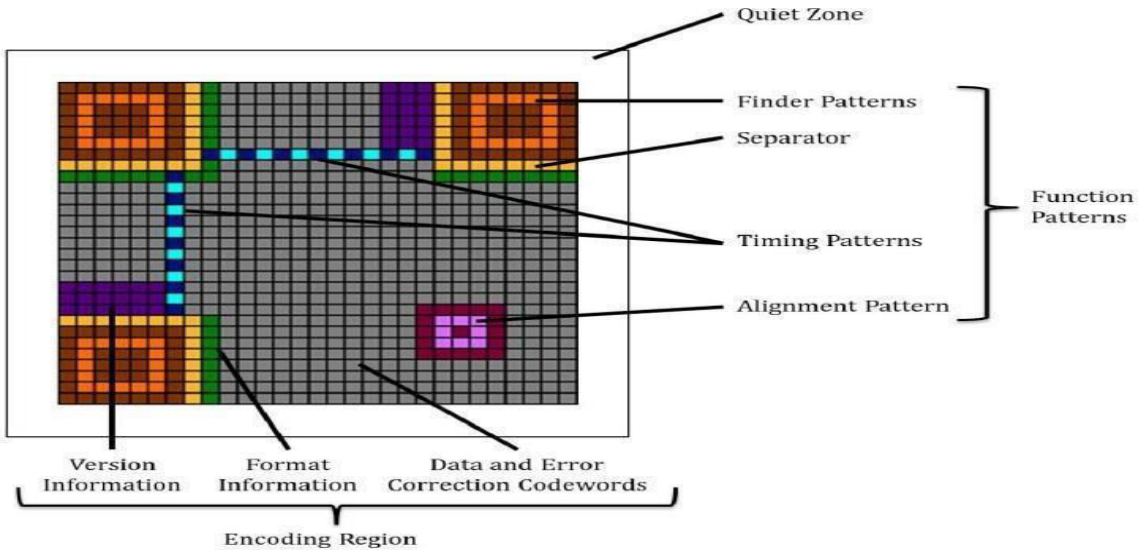
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

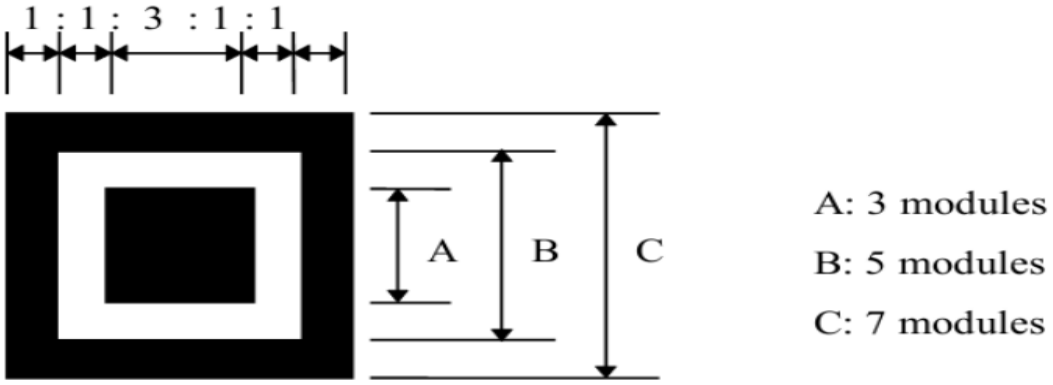
Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|



Illustrates the structure of a QR Code symbol Finder Pattern

Finder patterns are the special position detection patterns located in three corners (upper left, upper right, and lower left) of each symbol. It consists of an outer dark square that is 7 × 7 modules, an inner light square that is 5 × 5 modules, and a solid dark square in the center that is3×3modules. The ratio of module widths in each positiondetectionpatternis11311.Thefinder pattern is designed to be a pattern that is unlikely to appear within the other sections of the QR code so that QR code scanners can search for this ratio of light to dark modules to detect the finder patterns and correctly orient the QR code for decoding.



FinderPattern Separators

Separators are the one-module wide areas of whitespace between each finder pattern and encoding region.

Timing Patterns

There are 2 timing patterns, i.e. horizontal timing pattern and vertical timing pattern. They are consisting of alternating dark and light modules .The horizontal timing pattern is placed in the 6th row of the QR code between the separators. The vertical timing pattern is located in the 6th column of the QR code between the separators. These patterns are helpful in determining the symbol density, module coordinates and version information area.

Alignment Patterns

An alignment pattern is constructed of 5 × 5 dark modules, 3 × 3 light modules and a single dark module in the center. QR codes that are version 2 and larger must have alignment patterns and the number of alignment patterns depends on the symbol version.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

Encoding Region

Encoding region contains format information, version information, data and error correction codes. For format information, one-module array must be reserved near the top-left, top-right, bottom-left finder pattern and version information, an area of a 6 × 3 block above the bottom-left finder pattern and a 3 × 6 block to the left of the top-right finder pattern is reserved.

Quiet Zone

It is a 4-module wide area containing no data, and it used to ensure that the surrounding text or markings should not misguide the QR code data.

ENCODING AND DECODING OF AQRCODE

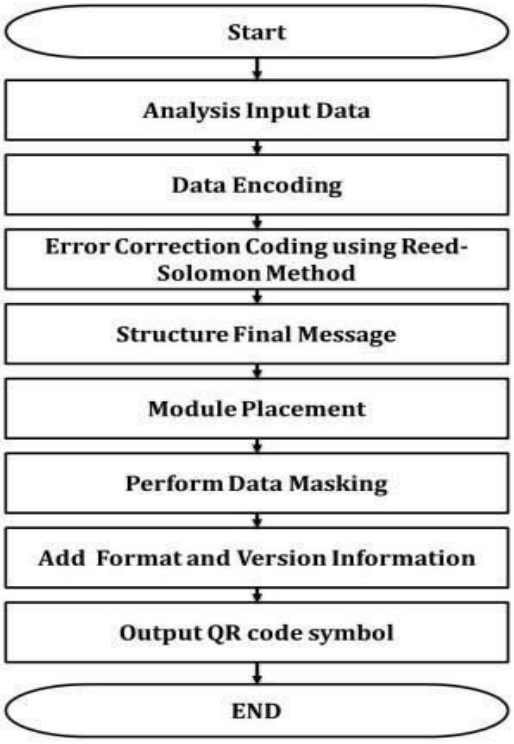
Data Analysis

A QR code encodes a string of text. The QR standard has four modes for encoding text numeric, alphanumeric, byte, and Kanji. Each mode encodes the text as a string of bits (1s and 0s), but each mode uses a different method for converting the text into bits, and each encoding method is optimized to encode the data with the shortest possible string of bits.

Therefore, first step should be to perform data analysis to determine whether text can be encoded in numeric, alphanumeric, byte, or Kanji mode, and then select the most optimal mode for your text.

Data Encoding

Next step is to encode text. The result of this step is a string of bits that is split up into data code words that are each 8 bits long. The mode used for encoding is identified by the Mode Indicator, which is astringof4bits.Encoded data must start with the appropriate mode indicator which is used for encoding. The number of characters that are being encoded is represented by the string of bits known as Character Count Indicator. Character Count Indicator is placed after the mode indicator and its length is version dependent.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

QR code encoding

Error Correction Coding

QR codes use error correction. This means that the string of data bits that represent our text, we must then use those bits to generate error correction code words using a process called Reed-Solomon error correction. QR scanners read both the data code words and the error correction code words. By comparing the two, the scanner can determine that it reads the data correctly or not, and if it did not read the data correctly it can correct errors.

Structure Final Message

The data and error correction code words generated in the previous steps must now be arranged in the proper order. For large QR codes, the data and error correction code words are generated in blocks, and these blocks must be interleaved according to the QR code specification.

Module Placement in Matrix

After generating the data code words and error correction code words and arranging them in the correct order, you must place the bits in the QR code matrix. The code words are arranged in the matrix in a specific way.

Data Masking

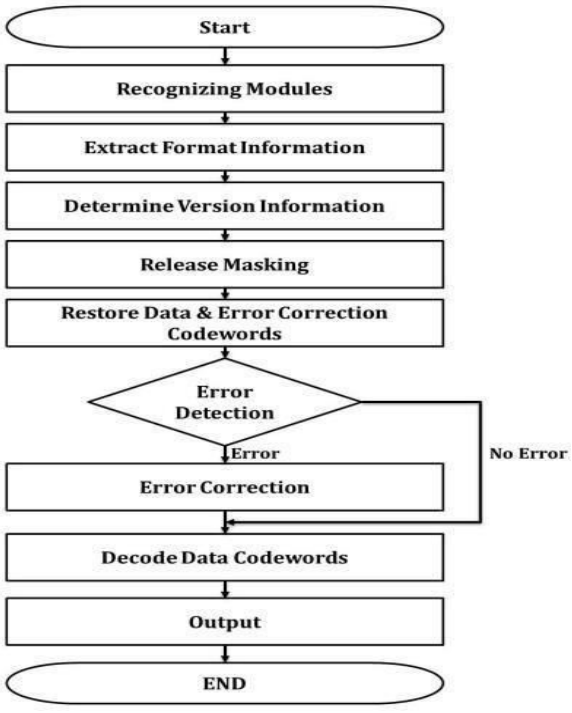
Certain patterns in the QR code matrix can make it difficult for QR code scanners to correctly read the code. To counteract this, the QR code specification defines eight mask patterns, each of which alters the QR code according to a particular pattern.

Format and Version Information

The last step is to add format and (if necessary) version information to the QR code by adding pixels in particular areas of the code that were left blank in previous steps. The format pixels identify the error correction level and mask pattern being used in this QR code. The version pixels encode the size of the QR matrix and are only used in larger QR codes [4].

Procedure for decoding a QR Code

Decoding data from the QR code is the reverse of the encoding procedure. Figure 6shows an overview of the decoding process [5] [6].



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

QR code decoding Recognizing Modules
Recognize dark and light modules as an array of "0" and "1" bits by locating and getting an image of the symbol.

Extract Format Information
Decode the format information and release the masking pattern and apply error correction on the format information modules as necessary. Also obtain a mask pattern reference.

Determine Version Information
If version information is applicable then decode it from the version information area and then determine the version of the QR code symbol.

Release Masking
In order to release the masking, XOR the encoding region bit pattern with the Mask Pattern whose reference has been extracted from the format information.

Restore Data and Error Correction Code words
Restore the data and error correction code words of the message by reading the symbol characters (according to the placement rules for the model).

Error Detection and Correction
By utilizing the error correction code words, identify errors and if any error is detected, correct it.

Decode Data Code words
Divide the data code words into segments according to the Mode Indicators and Character Count Indicators. And finally, decode the data characters according to the mode(s) in use and out put the decoded text as result.

IV. CONCLUSION

In conclusion, a real-time auditing system using QR codes for secure cloud offers several benefits for ensuring the integrity and authenticity of data. By encrypting data and including metadata in QR codes, the system can provide a secure and efficient way to conduct audits. The use of QR codes simplifies the auditing process, allowing for quick and easy scanning, while ensuring that only authorized users can access and validate the data. However, to ensure the effectiveness of such a system, proper security measures must be in place, including robust encryption, key management practices, and access control mechanisms. Compliance with relevant regulations and standards is also crucial to protect sensitive information. Overall, a real- time auditing system using QR codes for secure cloud can enhance data security, streamline audit processes, and improve overall transparency and trustworthiness in data management.

FUTUREENHANCEMENT

- **Integration with Block chain**

Implement block chain technology to provide an immutable and transparent audit trail, ensuring the integrity and authenticity of audit records.

- **Enhanced QRCode Security**

ImplementadvancedencryptiontechniquestosecuretheQRcodes,preventing unauthorized access and tampering.

- **Real-Time Monitoring and Alerts**

Integrate real-time monitoring capabilities to detect and alert on any suspicious or unauthorized access attempts.

- **Integration with Compliance Standards**

Ensure that the auditing system complies with relevant industry standards and regulations, such as GDPR or HIPAA, to ensure data privacy and security.

- **Machine Learning for Anomaly Detection**

Utilize machine learning algorithms to analyze audit data and detect anomalies or unusual patterns, enhancing the system's ability to detect and prevent security breaches.

User-Friendly Interfaces

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307077|

REFERENCES

1. WilliamGrosso,"JAVA",O'ReillyMedia,Inc.;1edition,2001
2. JohnZukowski,"DefinitiveGuidetoSwingforJava2",1999
3. RogerS.Pressman,"SOFTWARE ENGINEERING–APRACTIONERS APPROACH", TataMcGrawHill Publishing Company,1997.
4. JAVA2Platform,standardEdition,V1.3.1APISpecification
5. Java RMI Remote method Invocation(Paperback)Troy Bryan Downing
6. PatrickNaughton"TheJavaHandBook"TataMcGrawHill,2006
7. Mark Grand and Jonathan Knudsen,"Java Fundamental Classes Reference", Tata McGraw-Hill Publishing Company Limited, 1st Edition, May 1997.
8. Dietel & Deitel,Java HowToProgram,BPBPublishers,NewDelhi,2000.
9. O'reilly, Java Swings ,TataMc Graw Hill,Fifth Edition,2002.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details