iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51633

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Watermarking and Encryption Technique to Avoid Data Leakage Based on Block Chain

Mr. S. Prabhu[1], Veeramani. P[2], Santhosh Kumar. C[3], Vijay. M[4]
Paavai college of Engineering

Abstract: ***For end users to access various systems, services, and applications, multimedia data sharing is increasingly becoming an essential part of their daily lives. Cloud storage services in the real world frequently disclose data. In secure data transfer media, authenticity and copyright protection of multimedia content have always been a concern. As more people use the Internet and digital technologies, the issue has become more serious. Creating copyright protection, on the other hand, is more difficult and complicated. In proposed approach both Watermarking and Intermediary Re-encryption (PRE) approach used for productive mixed media content sharing. Watermarking is accustomed to concealing the data, for example, conceal privileged intel in computerized media like pictures. Data security is provided by encryption methods. In proposed work, secret key can be encoded utilizing encryption calculation with the assistance of key. The user's private key is then combined with the encrypted key information and can be embedded using LSB (Least Significant Bit) in the image or audio. The ECC Encryption algorithm can be used to encrypt an image or audio after secret information has been embedded. Finally, the embedded data verification process enables authorized users to extract the decryption key. When user information does not correspond with embedded information, illegal or unauthorized access can be identified. Furthermore, Block chain technology is used to safeguard these transaction details.***

I. INTRODUCTION

Cloud computing is a type of Internet-based computing that provides watermarking and encryption are two commonly used techniques in information security that can be used to prevent data leakage.

In this context, blockchain can be used as a decentralized and immutable storage system that ensures the authenticity, integrity, and confidentiality of the data. Watermarking is the process of embedding a hidden message or information within a digital file, such as an image, video, or audio recording. The watermark can be visible or invisible, and it serves as a digital signature that can identify the owner of the file or track the distribution of the file. In the context of blockchain, watermarking can be used to identify the origin of the data, trace its movement on the blockchain, and prevent unauthorize modifications.

Encryption, on the other hand, is the process of converting plaintext into ciphertext using a secret key or algorithm. The ciphertext can only be decrypted with the correct key, ensuring that the data remains confidential and secure. In the context of blockchain, encryption can be used to protect sensitive data from unauthorized access or interception, and to prevent data leakage.

To avoid data leakage based on blockchain, watermarking and encryption techniques can be combined to provide a more robust and secure solution. For example, data can be encrypted before being stored on the blockchain, and a watermark can be embedded in the encrypted data to identify its origin and track its movement.

The blockchain can then be used to store the encrypted data, ensuring that it is tamper-proof and accessible only to authorized parties with the correct decryption key.

Watermarking can be used in blockchain to ensure the authenticity and ownership of the data stored on the blockchain. By embedding a unique digital signal or code into the data, it becomes possible to verify the ownership of the data and detect any attempts to tamper with it.

Watermarking can also be used to trace the origin of the data and ensure that it has not been altered or manipulated. Encryption can also be used in blockchain to prevent unauthorized access to the data stored on the blockchain.

By encrypting the data using a strong encryption algorithm, it becomes impossible for anyone without the correct decryption key to access the data. Encryption can also be used to ensure the confidentiality of the data, so that only authorized parties can read the data. Overall watermarking and encryption are important tools in the fight against data leakage, and their combination with blockchain technology can provide a powerful and effective solution for protecting sensitive information.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

II. RELATED WORK

In this section, we review some of the applications of the technologies used in this article in relation to data sharing and access control in the block.

Watermarking and encryption techniques are widely used to protect digital data from unauthorized access and distribution. The use of blockchain technology has also gained popularity in recent years for securing and managing data in various applications. Encryption is an interaction that transforms data into a code to forestall unapproved access. It is used to safeguard confidential business information, financial data, and personal information. Encryption Calculations are numerical recipes that scramble and unscramble information. Unauthorized parties must guess the sender's cipher and the variables' keys when they intercept an encrypted message. Because guessing this information takes time and is hard, encryption is a useful security tool. Governments and militaries have historically utilized encryption to safeguard sensitive data. Encryption is currently used to safeguard data transmitted over networks and stored on computers and other storage devices.

III. WATERMARKING TECHNIQUE

Watermarking is a technique used to embed a digital signal or piece of information into a multimedia object such as an image, video or audio file. The aim of watermarking is to make the embedded information difficult to remove or alter without affecting the quality of the original content.

There are two types of watermarking techniques: visible and invisible. Visible watermarks are often used to protect the ownership of an image or video, and they are typically overlaid onto the original content in a way that makes it difficult to remove without damaging the quality of the image or video. Invisible watermarks, on the other hand, are embedded into the content itself and are not visible to the human eye. Spatial Domain Watermarking is technique, the watermark is embedded directly into the image or video file. This can be done by modifying the pixel values of the image or video in a specific pattern. Frequency Watermarking is technique, the watermark is embedded into the frequency domain of the image or video. Overall, the choice of watermarking technique depends on the specific requirements of the application, such as the level of security needed and the desired level of robustness to attacks.

IV. SYSTEM IMPLEMENTATION

In this part, we give substantial subtleties of the work process of the framework and how the blockchain fills in too.

Blockchain innovation is a decentralized and secure approach to putting away and sending information. It is an excellent choice for establishing a system workflow that is both transparent and resistant to tampering because it makes use of cryptographic methods to guarantee the confidentiality and integrity of data.

When the information is input, it should be confirmed by the organization. This should be possible utilizing savvy contracts, which are self-executing contracts with the conditions of the arrangement among purchaser and dealer being straightforwardly composed into lines of code.

The savvy contracts guarantee that the information is exact and satisfies the expected guidelines. A block is formed when the verified data are combined with other verified data. Each block is cryptographically connected to the past block, shaping a chain of blocks or a blockchain.

Data access is the final step in the system workflow. The data that is kept in the ledger can be viewed by anyone who has access to the blockchain. This straightforwardness makes it simple to track and review the information and guarantees that the framework is secure and dependable. When the savvy contract is conveyed, the hubs can begin executing the work process. Transactions can be submitted by any node to the blockchain network, where they are checked. In general, blockchain technology may enable the development of a system workflow in a secure and transparent manner. It makes sure that data is accurate, can't be changed, and anyone with access to the network can easily check it.

V. ARCHITECTURE DIAGRAM

The high-level structure of a software system's abstraction is known as software architecture. It is accomplished through decomposition and composition using architectural style and quality attributes. Non-functional requirements like dependability, scalability, portability, and availability must also be met by a software architecture design in order to meet the system's major functionality and performance requirements.

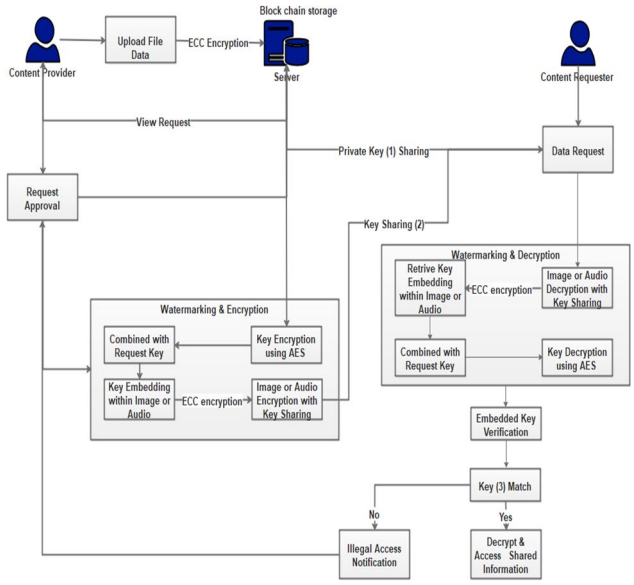


Figure 1 System architecture of the encryption

VI. FILES AND DATABASE DESIGN

Database Design is a set of procedures that make enterprise data management system design, development, deployment, and upkeep easier. A well-designed database is cost-effective in terms of disk storage space, easy to maintain, and improves data consistency. The database designer decides what data needs to be stored and how the data elements relate to one another. The primary goals of data set planning are to create intelligent and actual plans models of the proposed information base framework. Data accuracy, data redundancy, and data access and retrieval all benefit from a well-designed database.

Table 1
Admin table

Field name	Data type	Constraints
Id	Bigint	Unchecked
Admin name	nvarchar(50)	Checked
Gender	nvarchar(50)	Chceked

The database should be designed to ensure data privacy, security, and availability. The database should be designed to handle large volumes of data and should have backup and recovery mechanisms in place. The process of designing, developing, implementing, and maintaining enterprise data management systems is made easier with the help of database design. A well-designed database is cost-effective in terms of disk storage space, easy to maintain, and improves data consistency. The database designer decides what data needs to be stored and how the data elements relate to one another. The creation of logical and physical models of the proposed database system are the primary goals of database design.

VII. SYSTEM TESTING

A method for evaluating a software program's functionality is software testing. Software testing can take many different forms, but dynamic and static testing are the two most common types. An evaluation that takes place while the program is being carried out is known as dynamic testing. On the other hand, static testing is a look at the program's code and documentation. It is common practice to combine static and dynamic approaches. Testing is a predetermined activity that can be planned and carried out in a methodical way. Testing starts at the module level and work towards the mix of whole PCs based framework. Testing is essential to the system's success, so nothing is complete without it. In the event that testing is led effectively as per the goals as expressed above, it would uncover mistakes in the product. Additionally testing exhibits that product capabilities appear to the working as indicated by the particular, that presentation prerequisites seem to have been met.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

VIII. SYSTEM STUDY AND FEASIBILITY

It will be introduced to investment analysis, project appraisal, and feasibility studies in this chapter. Systems analysis can be seen in things like feasibility studies. A system is a description of the connections that exist between an organization's internal and external inputs of labor, machinery, materials, and management procedures. It is essential to have a clear understanding of the audit's objectives both during the planning and execution phases. Organizations ought to endeavor to adjust their business goals to the targets of the review. This will lower the likelihood of a qualified opinion and ensure that spent time and resources will contribute to the establishment of a robust internal control environment. A method for evaluating a software program's functionality is software testing. There are various kinds of programming testing yet the two fundamental classifications are dynamic trying and static testing. An evaluation that takes place while the program is being carried out is known as dynamic testing. static testing, then again, is an assessment of the program's code and related documentation. It is common practice to combine static and dynamic approaches. Testing is a predetermined activity that can be planned and carried out in a methodical way. Testing begins at the module level and progresses toward the computer-based system's integration. Testing is essential to the system's success, so nothing is complete without it.

Objectives of Feasibility Study

- To describe the automation's current state.
- To determine whether the end user will benefit from the finished product.
- To recommend the conceivable elective arrangements.

Overall, system study in blockchain technology is an important area of research and development that can lead to new and innovative applications of this technology.

A. Economic Feasibility

The most common method for determining a project's efficiency is economic feasibility analysis. It is otherwise called cost examination. It is helpful in determining a project's expected profit and investment. The most important aspects of this field of study are cost and time. Any system can be considered economically viable if the anticipated benefits are equal to or greater than the anticipated costs. Cost benefit analysis, in which anticipated costs and benefits are evaluated, is performed in economic feasibility. The proposed system's efficacy is evaluated using economic analysis.

B. Operational Feasibility

The system will be used in the event that it is developed and put into use is part of operational feasibility, which is dependent on the human resources that are available for the project. A system's operational feasibility is measured by how well it meets the requirements of the requirements analysis phase of system development, how well it takes advantage of opportunities identified during scope definition, and how well it solves problems. The organization's willingness to support the proposed system is looked at in terms of operational feasibility. This is presumably the most troublesome of the attain abilities to measure. To decide this attainability, understanding the administration obligation to the proposed project is significant. It is likely that management will support the request and the system will be accepted and utilized if it was initiated by management. However, it is also critical that the workforce embraces the change.

C. Schedule Feasibility

In this type of feasibility, the skills needed to properly apply the new technology can be learned in a short amount of time and evaluated in order to implement or extend the new project in a short amount of time. A project's schedule feasibility ensures that it can be completed before technology or the project itself become out of date or unnecessary. The research period can be used to determine the schedule's feasibility.

IX. RESULT AND DISCUSSION

Watermarking and encryption-based data sharing methods are important techniques for protecting the privacy and security of digital data. The problem that watermarking and encryption-based data sharing methods aim to solve is the protection of digital data from unauthorized access, copying, and modification during transmission and storage. With the growth of digital communication and the ease of data sharing, it has become increasingly important to protect sensitive information from cyber threats, piracy, and intellectual property theft. Encryption, on the other hand, involves encoding data in such a way that only authorized parties can access it.

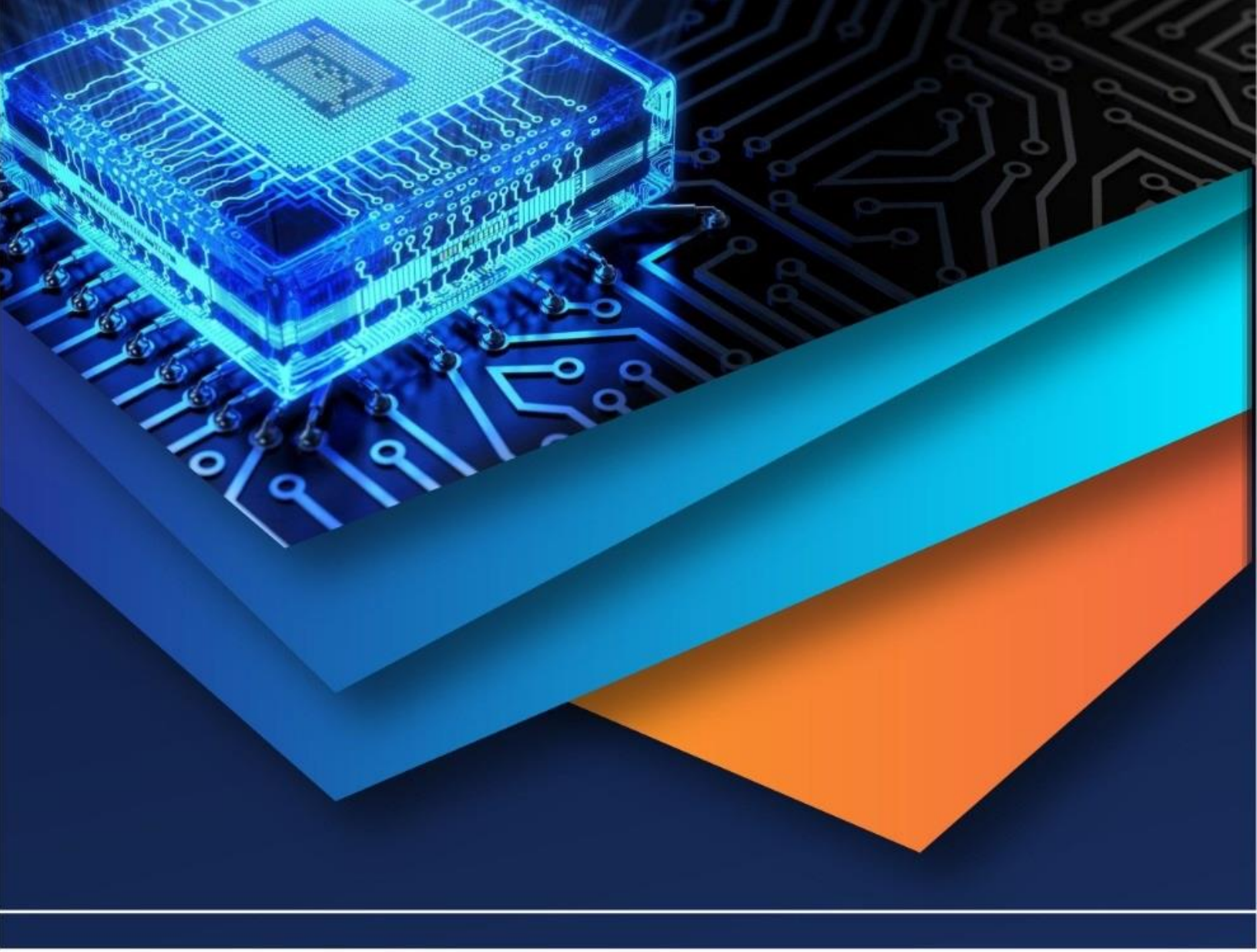
The challenge with encryption is to ensure that the encryption key is kept secure and that the decryption process is fast and efficient. Moreover, encryption does not protect against attacks on the data before or after it is decrypted, and there is always a risk that the encryption key may be compromised. Watermarking is a process of embedding hidden information (a watermark) into digital content, such as images or videos, in order to identify the owner or to protect against unauthorized copying. Encryption, on the other hand, involves encoding data in such a way that only authorized parties can access it. The use of watermarking and encryption-based methods for data sharing has become increasingly important due to the growth of digital communication and the need for secure transmission and protection of intellectual property.

X. CONCLUSION

Make a suggestion for a method that combines watermarking and cryptography for safe data transfer via clouds. While encryption is carried out using ECC and AES cryptography, watermarking is done using the LSB approach. The suggested method is designed to offer multimedia data integrity and verification services in addition to copyright protection. Because of this, its objective is to spot any illicit actions on the watermark rather than to be immune to change attempts. This method can be used to determine whether the authenticity and integrity of conveyed data have been affected at the receiving end. The suggested method detected this change at the receiving end and informed the content provider of the unauthorized distribution. The watermarking technology offers network authentication, stability, and shared information secrecy.

REFERENCES

[1] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Common. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.
[2] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.
[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53.
[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506–522.
[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Citeseer, Feb. 2004, pp. 5–6.
[6] D. Balfanz et al., “Secret handshakes from pairing-based key agreements,” in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.
[7] R. Canetti, S. Halevi, and J. Katz, “Chosen-ciphertext security from identity-based encryption,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207–222.
[8] T. Koponen et al., “A data-oriented (and beyond) network architecture,” in Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., Aug. 2007, pp. 181–192.
[9] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, “Developing information networking further: From PSIRP to pursuit,” in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1–13.
[10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, “Secure naming for a network of information,” in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops,2010, pp. 1–6.
[11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, “A routing scheme for content-based networking,” in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.
[12] Psaras, W. K. Chai, and G. Pavlou, “Probabilistic in-network caching for information-centric networks,” in Proc. 2nd ed. ICN Workshop Inform.Centric Netw., Aug. 2012, pp. 55–60.
[13] Y. Sun et al., “Trace-driven analysis of ICN caching algorithms on videoon-demand workloads,” in Proc. 10th ACM Int. Conf. Emerging Netw. Exp. Technol., Dec. 2014, pp. 363–376.
[14] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. Available: https://bitcoin. org/bitcoin. Pdf.
[15] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.
[16] N. Park, “Secure data access control scheme using type-based reencryption in cloud environment,” in Semantic Methods Knowledge Management and Communications. Berlin, Germany: Springer, 2011, pp. 319– 327.
[17] G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,” Comput. Secur., vol. 30, no. 5, pp. 320–331, Jul. 2011.
[18] J. Hur, “Improving security and efficiency in attribute-based data sharing,” IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Apr. 2011.
[19] P. K. Tysowski and M. A. Hasan, “Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186, Nov. 2013.
[20] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inform. Sci., vol. 258, pp. 355–370, Feb. 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY