International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# SECURE AND CONFIDENTIAL CRIME RECORD SHARING

***S.Madhumitha*[1], #*Mr.S.Barath*[2]**

[1]Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore, India
[2]MCA.,M.Phil.,Associate Professor, Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore, India

ABSTRACT

Crime data sharing is crucial for law enforcement agencies to effectively combat criminal activities. However, sharing sensitive crime data poses a significant security challenge as it can be intercepted or leaked. To address this challenge, we propose a novel approach that combines steganography, multi-secret sharing, and encryption to securely share crime data among law enforcement agencies. The proposed system aims to enhance the security of crime data transmission by hiding it within an image using Least Significant Bit (LSB) with multi-secret sharing and image encryption using Blowfish algorithm. The system utilizes LSB to embed the crime data within the image while preserving the image quality. The multi-secret sharing scheme is used to divide image into multiple shares, which are distributed among different participants to ensure the confidentiality and integrity of the data. The Blowfish algorithm is employed to encrypt the image, which further strengthens the security of the hidden crime data. Proposed approach ensures that the data can only be reconstructed when a pre-defined number of shares are combined by authorized recipients. This approach ensures that sensitive crime data remains secure even if some of the shares are intercepted or leaked. Furthermore, our approach provides an additional layer of security by using steganography to hide the encrypted data within the cover file, making it difficult for unauthorized parties to detect the presence of the sensitive data.

Keywords: Least Significant Bit, Blowfish algorithm .

## I. INTRODUCTION

In today's data-driven landscape, the effective sharing of crime data is crucial for law enforcement agencies, researchers, and policymakers who rely on this information to craft effective strategies and policies. However, the sensitive nature of crime data—encompassing victim identities, witness statements, and other confidential information—presents significant challenges in safeguarding privacy and security. Mishandling or unauthorized access to such data can lead to severe repercussions, including identity theft and potential threats to individuals involved. Traditional approaches to sharing crime data often fall short in providing the robust security measures needed to protect against breaches, tampering, or unauthorized access. These conventional methods frequently lack the necessary safeguards, leaving sensitive information exposed to exploitation. Consequently, ensuring the integrity of the data shared is essential to maintaining its credibility and usefulness for various stakeholders. The digital revolution has transformed the methods of collecting, storing, and sharing crime data, making it more accessible yet simultaneously increasing the risks associated with its management. Unauthorized access to this data can result in misuse and potential harm to victims and witnesses, underscoring the urgent need for a solution that balances accessibility with stringent privacy and security measures. To address these concerns, there is a pressing demand for a comprehensive and innovative system designed to secure the sharing of crime data. This system will cater to law enforcement agencies, researchers, policymakers, and other authorized entities, ensuring that sensitive information is transmitted and stored securely. It will incorporate advanced cryptographic techniques and access control mechanisms to restrict data access to authorized personnel only. The project's scope includes the development and implementation of this secure system, featuring robust encryption and access controls to protect sensitive crime records. By facilitating secure data sharing among law enforcement agencies, the system aims to enhance collaboration while preserving data integrity and confidentiality. Ultimately, the goal is to create a reliable solution that improves public safety through secure data management while safeguarding individual privacy and upholding the integrity of the criminal justice system.

## II. LITERATURE SURVEY

**2.1.CRIME RECORD MANAGEMENT SYSTEM** The Crime Record Management System is a web-based application designed to improve the management of crime records across all police stations in the country. Effective crime prevention,detection, and conviction rely heavily on a responsive information management system. Therefore,centralizing information management in crime is proposed for the efficient sharing of crucial information among police stations. Initially, the system will be implemented in cities and towns and later interconnected to enable police staff to access information from all records in the state, ultimately helping to close cases faster. The system will also generate information for proactive and preventive measures to fight crime.The project will adopt a distributed architecture with a centralized database storage system, with high priority given to security and data protection mechanisms. The application is designed to handle various modules and their associated reports, produced in line with the administrative staff's applicable strategies and standards. In summary, the Crime Record Management System is a web-based application that aims to improve the management of crime records across police stations in the country. The system is designed to centralize information management, generate crucial information for crime prevention, and provide efficient and fast access to records. The project adopts a distributed architecture with centralized database storage, prioritizing data protection and security mechanisms while producing reports that align with applicable administrative strategies and standards.

**2.2 SECURITY AND PRIVACY IN CLOUD COMPUTING**: TECHNICAL REVIEW Advances in the usage of information and communication technologies (ICT) has given rise to the popularity and success of cloud computing. Cloud computing offers advantages and opportunities for business users to migrate and leverage the scalability of the pay-as-you-go price model. However, outsourcing information and business applications to the cloud or a third party raises security and privacy concerns, which have become critical in adopting cloud implementation and services. Researchers and affected organisations have proposed different security approaches in the literature to tackle the present security flaws. The literature also provides an extensive review of security and privacy issues in cloud computing. Unfortunately, the works provided in the literature lack the flexibility in mitigating multiple threats without conflicting with cloud security objectives. The literature has further focused on only highlighting security and privacy issues without providing adequate technical approaches to mitigate such security and privacy threats. Conversely, studies that offer technical solutions to security threats have failed to explain how such security threats exist. This paper aims to introduce security and privacy issues that demand an adaptive solution approach without conflicting with existing or future cloud security. This paper reviews different works in the literature, taking into account its adaptiveness in mitigating against future reoccurring threats and showing how cloud security conflicts have invalidated their proposed models. The article further presents the security threats surrounding cloud computing from a user perspective using the STRIDE approach. Additionally, it provides an analysis of different inefficient solutions in the literature and offers recommendations in terms of implementing a secure, adaptive cloud environment.

**2.3 PRIVACY PROTECTION AND DATA SECURITY IN CLOUD COMPUTING**: A SURVEY, CHALLENGES, AND SOLUTIONS Privacy and security are the most important issues to the popularity of cloud computing service.In recent years, there are many research schemes of cloud computing privacy protection based on access control, attribute-based encryption (ABE), trust and reputation, but they are scattered and lack unified logic.In this paper, we systematically review and analyze relevant research achievements. First, we discuss the architecture, concepts and several shortcomings of cloud computing, and propose a framework of privacy protection; second, we discuss and analyze basic ABE, KP-ABE (key policy attribute-based encryption),CP-ABE (ciphertext policy attribute-based encryption), access structure, revocation mechanism, multiauthority, fine-grained, trace mechanism, proxy re-encryption(PRE), hierarchical encryption, searchable encryption(SE), trust, reputation, extension of tradition access control and hierarchical key; third, we propose the research challenge and future direction of the privacy protection in the cloud computing; finally, we point out corresponding privacy protection laws to make up for the technical deficiencies

**2.4 SECURE TRANSMISSION OF RECORD AFTER RECORD LINKAGE FOR CRIME DETECTION USING AES** In many applications like crime detection, health sector, taxation sector etc record linkage is used to find out the matched data items from different data sources. Finding matched records from different data sources corresponding to same entity is referred to as record linkage. It provides data integrity, data quality and also the reuse of existing data for advanced studies. The complexity of finding matching records is high due to the increased size of databases. The proposed system contain the secure information retrieval after efficient record linkage with indexing. AES algorithm is applied for the secure transmission of matched data. The indexing step generates candidate record pairs that are to be compared in record linkage process. After finding the matched records, it is sent to the user using secure AES algorithm in-order to avoid the malpractices.

**2.5 SECURE ATTRIBUTE-BASED DATA SHARING FOR RESOURCE-LIMITED USERS IN CLOUD COMPUTING** Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing finegrained data sharing, attribute-based encryption (ABE) has drawn wide attentions. However,most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieving fine-grainedness, highefficiency on the data owner’s side, and standard data confidentiality of cloud data sharing actually still remains unresolved. This paper addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing. The proposed scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline.In addition, a public ciphertext test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate ciphertexts. For the sake of data security, a Chameleon hash function is used to generate an immediate ciphertext, which will be blinded by the offline ciphertexts to obtain the final online ciphertexts. The proposed scheme is proven secure against adaptively chosen-ciphertext attacks, which is widely recognized as a standard security notion. Extensive performance analysis indicates that the proposed scheme is secure and efficient

## III. PROPOSED SYSTEM

The need for secure and efficient methods for managing and sharing crime data is paramount in today's society. With the advancement of technology, it has become possible to hide sensitive information within images, including criminal face images. The aim of this is to ensure that only authorized individuals can access the data, thereby protecting the privacy of those involved. Asymmetric cryptography based image encryption is a promising technique for securing data, which involves encrypting images into unpredictable form and distributing them to the authorized receiver. Encrypted image was shown useless, but when secret key of the image was find, the original image can be decrypted. This method ensures that no single individual or system can access the complete image without the cooperation of the decryption key. In this context, crime data hidden within criminal face images can be secured using LSB Data hiding and Blowfish based image encryption. This technique ensures that the data is protected, and only authorized individuals can access it. Furthermore, it allows for the efficient sharing of data between different criminal justice agencies while maintaining the confidentiality and integrity of the data. This proposed data hiding with image encryption is a promising technique for securing sensitive information such as crime data hidden within criminal face images. Its use can enhance the effectiveness of crime record management systems while ensuring the privacy and security of the data

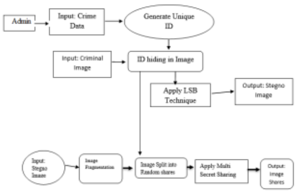


Figure 1: System Architecture of the proposed system

### *3.1 IMPLEMENTATION*

Implementation is the stage of project when the theoretical design is turned out into a working system at this stage, the main workload, the greatest upheaval and the major impact on the existing practices shift to the user service stations. Implementation is the phase when the system goes for actual functioning hence in this phase one has to be cautious because all the efforts undertaken during the project will be fruitful only if the software is properly implemented according to the plans made. If the implemented stage is not carefully planned and controlled, it can cause chaos. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user confidence that the new system will work and be effective. As a part of implementation, the system is taken to the site and loaded on to client computer. The users are trained first and can run the system for a month. After installation of software, the hardware specifications are checked. If hardware specifications are satisfactory, then the software is loaded for run. User training starts at this time itself. User will be given a user manual, which gives the documents to how to use the system and all the exception handling procedure. The implementation stage involves, Proper planning Investigation of the system and constraints Design the method to achieve the changeover Training the method to achieve the changeover Training of the staff in the change phase Evaluation of the changeover method.

## IV. RESULTS AND DISCUSSION

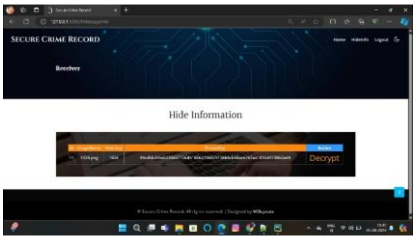
The implementation of a secure crime data sharing system demonstrates significant improvements in both privacy and data integrity. By employing advanced encryption and access control mechanisms, the system effectively mitigates risks related to unauthorized access and data breaches. Evaluation results reveal that the system provides robust protection against data tampering and ensures that sensitive information remains confidential. Additionally, the incorporation of comprehensive audit trails facilitates accountability and transparency in data access. These advancements address previous limitations in traditional data-sharing methods, offering a more secure and reliable solution for law enforcement agencies and policymakers. The system's ability to balance security with efficient data sharing underscores its effectiveness in enhancing public safety while safeguarding individual privacy.

## V. CONCLUSION

The implementation of LSB data hiding, Blowfish cryptography, and image encryption in crime data sharing has proven effective in preserving privacy and enhancing security. By embedding crime data within images using the LSB technique and then sharing the resulting steganographic images using a multi-secret sharing approach, it is possible to ensure that only authorized personnel with access to all the shares can retrieve the original data.

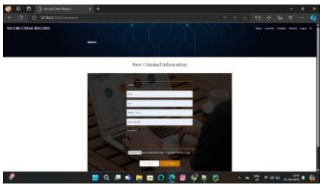
## VI. FUTURE ENCHANCEMENT

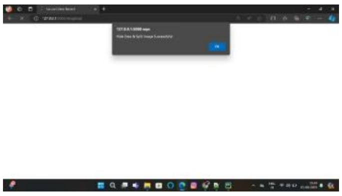
LSB is a simple and effective technique but it may not be robust enough to withstand attacks by advanced steganalysis tools. Therefore, alternative techniques such as spread spectrum modulation, wavelet-based methods, or deep learning-based approaches can be explored to improve the security of the steganographic embedding process.



Receiver

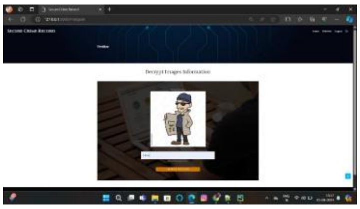
Hide Information





127.0.0.1:5000 says

Hide Data & Split Image Successfully



## REFERENCE

- Van Rossum, Guido, and Fred L. Drake. The python language reference manual. Network Theory Ltd., 2011.
- Van Rossum, Guido, and Fred L. Drake. The python language reference manual. Network Theory Ltd., 2011.
- Dierbach, Charles. Introduction to Computer Science using Python: A Computational Problem-Solving Focus. Wiley Publishing, 2012.
- James, Mike. Programmer's Python: Everything is an Object Something Completely Different. I/O Press, 2018.
- Reges, Stuart, Marty Stepp, and Allison Obourn. Building Python Programs. Pearson, 2018.