IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134195

Secure Police Complaint Registration System Using Twofish Algorithm

Nalina Sree K[1], Oviya S[2], Roselin Mary S[3], Dinakar Jose S[4]

Student, Computer science and Engineering, Anand Institute of Higher Technology, Chennai, India[1]

Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[2]

Head of The Department, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[3]

Assistant Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[4]

Abstract: Technology is becoming a vital component of modern law enforcement operations, helping to maintain the integrity of police work and strengthen security protocols. Even with the advancements in digitization, security issues still exist in the systems. Sensitive data integrity and security must still be prioritized. In order to protect user data, and their complaint, and stop unwanted access, this paper presents a robust system that enables safe police complaint registration. It does this by combining strong encryption techniques with biometric verification. The proposed solution encrypts complaints submitted through online, using the Twofish encryption technique, which is well-known for its strong security features. In addition, the system includes a selfie verification with facial recognition algorithm to increase complainants' credibility and reduce the possibility of false accusations.

Keywords*:* Twofish Algorithm, Data Security, Encryption Algorithm, Facial Recognition

I. INTRODUCTION

The advent of online complaint registration systems, which promise efficiency and accessibility, represents a significant turning point in the modernization of law enforcement practices. However, there are a number of risks associated with the growing reliance on digital platforms, especially with regard to data security. The confidentiality and dependability of complaint registration procedures may be jeopardized by cybercriminals skilled at taking advantage of flaws in digital infrastructure. The difficulty is exacerbated by problems citizens have when accessing these platforms. Though internet platforms offer convenience, people's worries about data security and privacy frequently prevent them from using them to their full potential. There is a widespread fear of identity theft, illegal access to personal data, and data breaches, which erodes public confidence in the effectiveness of online complaint registration systems. The emergence of advanced hacking methods and cyberattacks poses a serious threat since they can get past conventional security measures and access private information. In addition, police departments' resource constraints—such as limited funding and outdated technology—make it more challenging to protect digital infrastructure from ever-changing threats. In light of this, this paper offers a comprehensive solution meant to strengthen police complaint registration systems' security. It attempts to address the urgent issues related to user authentication and data security by utilizing cutting-edge technologies like the Twofish Algorithm and Selfie Verification. This study aims to provide guidance for law enforcement in India towards a more secure and robust digital infrastructure by thoroughly examining these technologies and their possible uses.

II. LITERATURE SURVEY

The article [1] proposes an implementation of the RSA algorithm. RSA ensures the privacy of criminal information stored in the database through its two-key-based security. Data security is enhanced by the use of the RSA algorithm in the criminal records system. System performance may be impacted by the computational cost of RSA encryption and decryption, particularly when handling big datasets or frequent data updates. The intricacy of key management, which involves creating, exchanging, and storing public and private keys, also presents challenges. These elements increase the likelihood of unauthorized access or key compromise. Furthermore, RSA's vulnerability to quantum computing compromises its long-term security, necessitating the adoption of quantum-resistant encryption methods as technology advances.

The article [2] suggests encrypting police complaints using Elliptic Curve Cryptography (ECC) and utilizing blockchain technology. By ensuring that every file has a unique encryption key, ECC lowers the possibility of attacks.

DOI: 10.17148/IJARCCE.2024.134195

However, the intricate key generation of ECC presents implementation and management difficulties, necessitating a strong infrastructure and specialized knowledge. In addition, it may be susceptible to side-channel attacks, implementation errors, and assaults using quantum computing. Furthermore, the absence of standardization in ECC creates issues with system interoperability, requiring more work in the areas of compatibility testing and integration.

The study[3] provides a novel authentication method that combines grid-based authentication with the MD5 algorithm to improve the security of the Online Crime Reporting System. Grid Based Authentication improves system security by preventing side-channel attacks like timing or cache attacks from taking use of AES encryption weaknesses that could compromise user credential privacy. Furthermore, vulnerabilities such as padding oracle attacks or chosen ciphertext attacks may target AES-encrypted data, highlighting the importance of using robust encryption techniques and secure authentication mechanisms. Strong password rules and secure cryptography procedures are essential, as evidenced by the possibility of attacks such as brute-force assaults targeting the MD5 hashing algorithm used to store passwords.

The study[4] investigates how adding AES encryption, which is well-known for its resilience against a variety of cryptographic assaults, can improve the security of online police complaint systems. However, one should take into account potential security issues such side-channel assaults and the requirement for frequent upgrades to combat developing threats. Concerns like data privacy, regulatory compliance, governance, and scalability constraints arising from the expanding blockchain ledger should be taken into consideration while integrating blockchain technology. To guarantee system integrity and dependability, consensus methods and governance structures must be carefully considered.

III. PROPOSED SOLUTION

The proposed solution is put out to address the issues raised and guarantee the security and integrity of online police complaint registration systems. This system boosts security while protecting user privacy by combining robust encryption techniques with creative authentication mechanisms.

The Twofish algorithm is mainly used for two purposes:

a) To protect the transmission and storage of complaint data, the robust and effective symmetric encryption technique Twofish is used. Strong encryption features provided by Twofish guarantee the privacy and accuracy of sensitive data during the complaint registration procedure.
b) Integration of face detection technology with selfie capture to improve user authentication procedures: Sophisticated facial recognition algorithms examine the taken picture to confirm the user’s identity, guaranteeing that only those with permission can access the complaint registration portal. By adding another layer of authentication, security measures are strengthened and the possibility of fraudulent or illegal activity is reduced. Before putting the snapped photo in the system database, the system encrypts it with the Twofish algorithm to prevent unauthorized access and disclosure of sensitive information. This protects user privacy while adhering to data protection laws by guaranteeing that user identities and personal information stay private and secure.

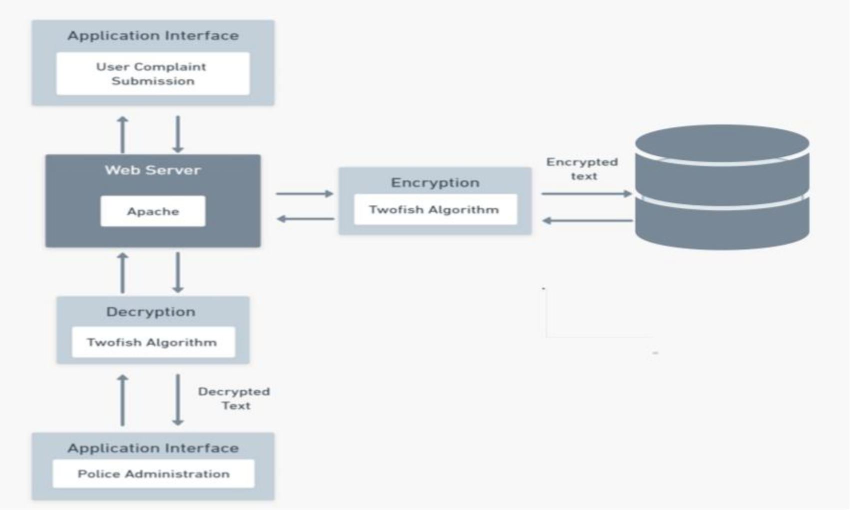


Fig. 1 System Architecture

DOI: 10.17148/IJARCCE.2024.134195

IV. METHODOLOGY

The symmetric key block cipher known as Twofish encryption has gained significant popularity due to its versatility and resilience in a range of applications, such as disk encryption, virtual private networks (VPNs), and secure email exchanges. Twofish encryption uses a single key for both encryption and decryption, functioning as a symmetric key block cipher. A key schedule algorithm, which produces round keys used in encryption and decryption, is essential to its functioning. Twofish encryption strengthens its security posture by utilizing a Feistel network structure and several rounds of substitution and permutation.

Moreover, Twofish encryption's key size varies from 128 to 256 bits to accommodate different security needs. Interestingly, Twofish encryption is compatible with a variety of modes of operation, including common ones like counter (CTR) mode, cipher block chaining (CBC), and electronic codebook (ECB).

In this project, after logging in with their credentials, users use the camera on the device to take a selfie, which enables facial recognition for user authentication. Before being safely stored in the system's database, captured selfies are encrypted using the powerful Twofish algorithm, guaranteeing the confidentiality and integrity of the image data.

Users submit detailed information about the incident, such as its location, description, and other pertinent details, when filing complaints. To prevent unwanted access, this data is encrypted using Twofish encryption before being entered into the database. Users must enter the unique complaint ID they were given upon registration in order to view the status of their registered complaints.

Administrators can decode complaint data for review purposes via an administrative dashboard. By examining taken selfies, they can also confirm user identities. Administrators have the ability to modify the status of complaints by designating them as closed, resolved, or still pending, based on the findings of their investigations. Transparency and accountability in the handling of complaints are guaranteed by the system's safe storage and reflection of all administrative actions.

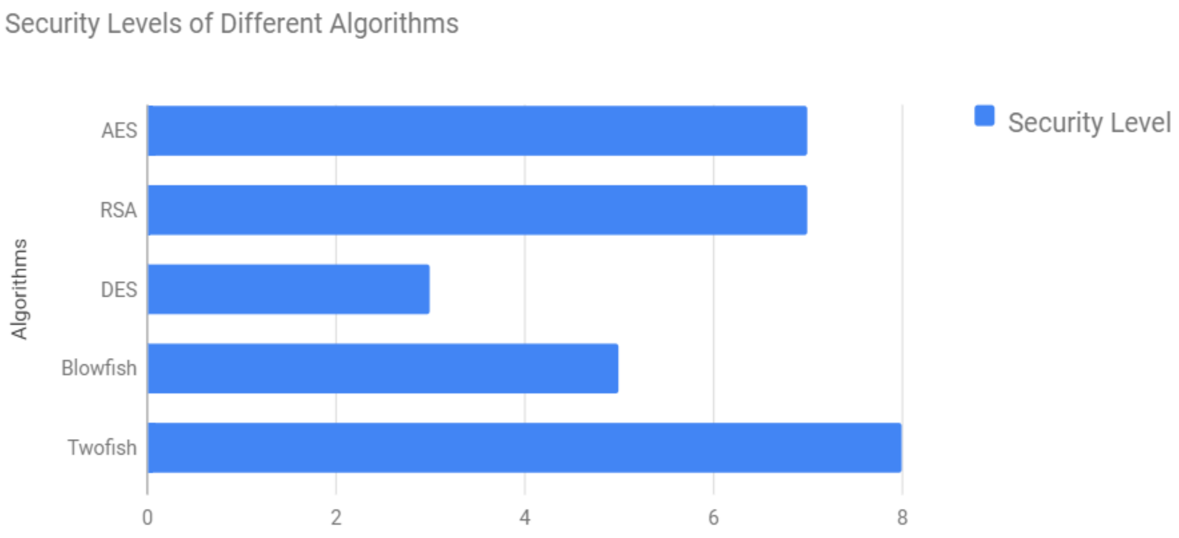


Fig.2 Comparison on different algorithms based on security level

V. IMPLEMENTATION

The implementation of secure complaint management system involves several key technologies and algorithm, for the system's functionality, security, and usability.

A. Development of Web Interfaces

The main platform for user engagement for filing complaints, changing user information, and monitoring the status of complaints is the web interface.

DOI: 10.17148/IJARCCE.2024.134195

For the front end, HTML, CSS, and JavaScript are used in its development, while the back end is handled by the Spring Boot framework. Users can navigate and interact with the interface with ease thanks to its responsive and intuitive design.

B. Encryption using Twofish Algorithm

The Twofish encryption technology is used to guarantee the security and privacy of customer complaints. Using cryptographic libraries and bouncy castle cryptography API, this approach is developed in Java and encrypts complaint data before saving it in a database. Strong encryption features are provided by Twofish, guarding against illegal access and data breaches.

C. Facial Recognition for Confirming Selfies

Face recognition technology is used by this complaint management system for selfie verification in order to strengthen security and guarantee the legitimacy of user submissions. The system utilizes the Haar Cascade classifier for frontal face detection and OpenCV in Java to evaluate selfies that users upload during the complaint reporting process.

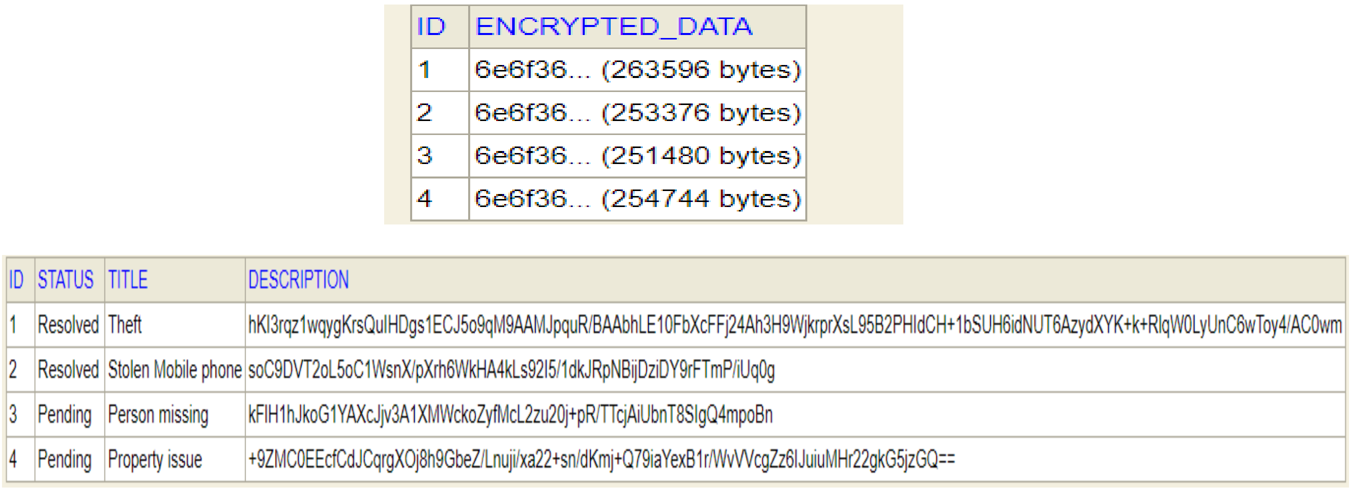
D. Validation and Testing of Systems

Thorough testing and validation methods are carried out during the implementation phase to guarantee the complaint management system's dependability and efficacy. To find and fix any possible problems or bugs, the system is tested end-to-end, individually component by unit, and as a whole by integration of system modules. In order to validate a system, its performance must be evaluated in a variety of scenarios, such as those involving user authentication, encryption settings, and complaint categories.

VI. RESULT AND DISCUSSION

Due to its vast key space and resistance to known threats, Twofish encryption provides strong protection for private data, improving system performance and real-time data protection. By using distinguishing features on the face to confirm the identity of the user, facial recognition technology that is integrated into the authentication process enhances security.

Encrypting selfies before saving them, however, allays worries about user permission and privacy by prohibiting unauthorized access to biometric data. Even if Twofish is still a good security solution, companies should keep up with developments in cryptography to be able to respond to changing threats.

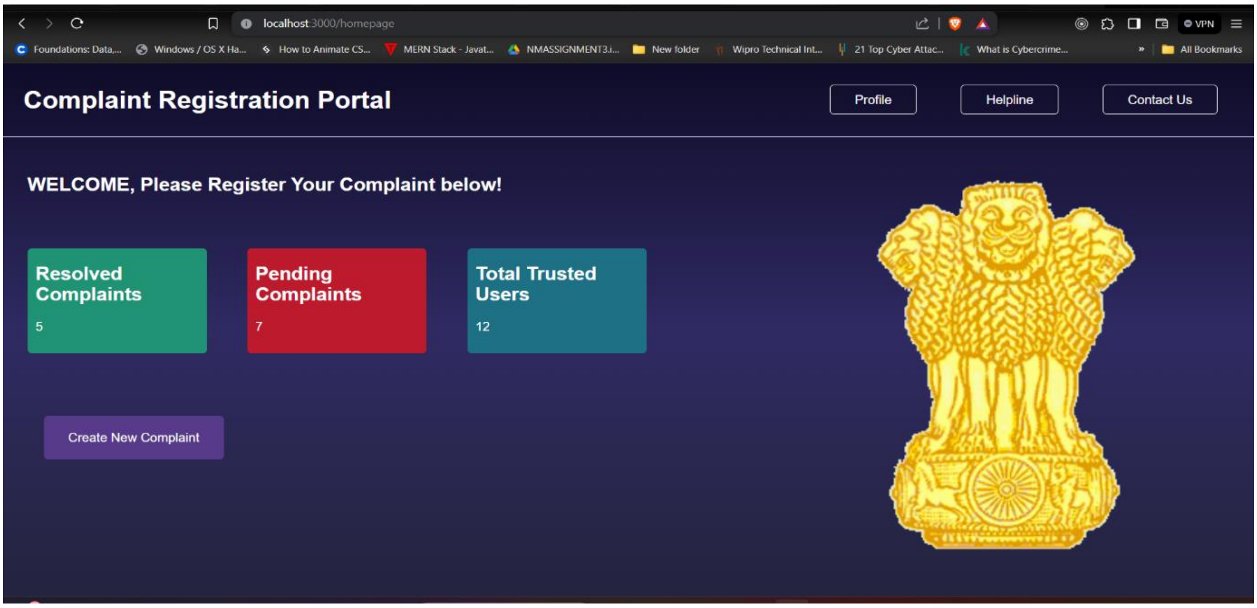


ID	ENCRYPTED_DATA
1	6e6f36... (263596 bytes)
2	6e6f36... (253376 bytes)
3	6e6f36... (251480 bytes)
4	6e6f36... (254744 bytes)

ID	STATUS	TITLE	DESCRIPTION
1	Resolved	Theft	hKI3rqz1wqygKrsQuIHDgs1ECJ5o9qM9AAMJpquR/BAAbhLE10FbXcFFj24Ah3H9WjkrprXsL95B2PHIdCH+1bSUH6idNUT6AzydXYK+k+RlqW0LyUnC6wToy4/AC0wm
2	Resolved	Stolen Mobile phone	soC9DVT2oL5oC1WsnX/pXrh6WkHA4kLs92I5/1dkJRpNBijDziDY9rFTmP/iUq0g
3	Pending	Person missing	kFIH1hJkoG1YAXcJjv3A1XMWckoZyfMcL2zu20j+pR/TTcjAiUbnT8SIgQ4mpoBn
4	Pending	Property issue	+9ZMC0EEcfCdJCqrgXOj8h9GbeZ/Lnuji/xa22+sn/dKmj+Q79iaYexB1r/WvVVcgZz6lJuiuMHr22gkG5jzGQ==

Fig.3 Database Design

DOI: 10.17148/IJARCCE.2024.134195



Complaint Registration Portal

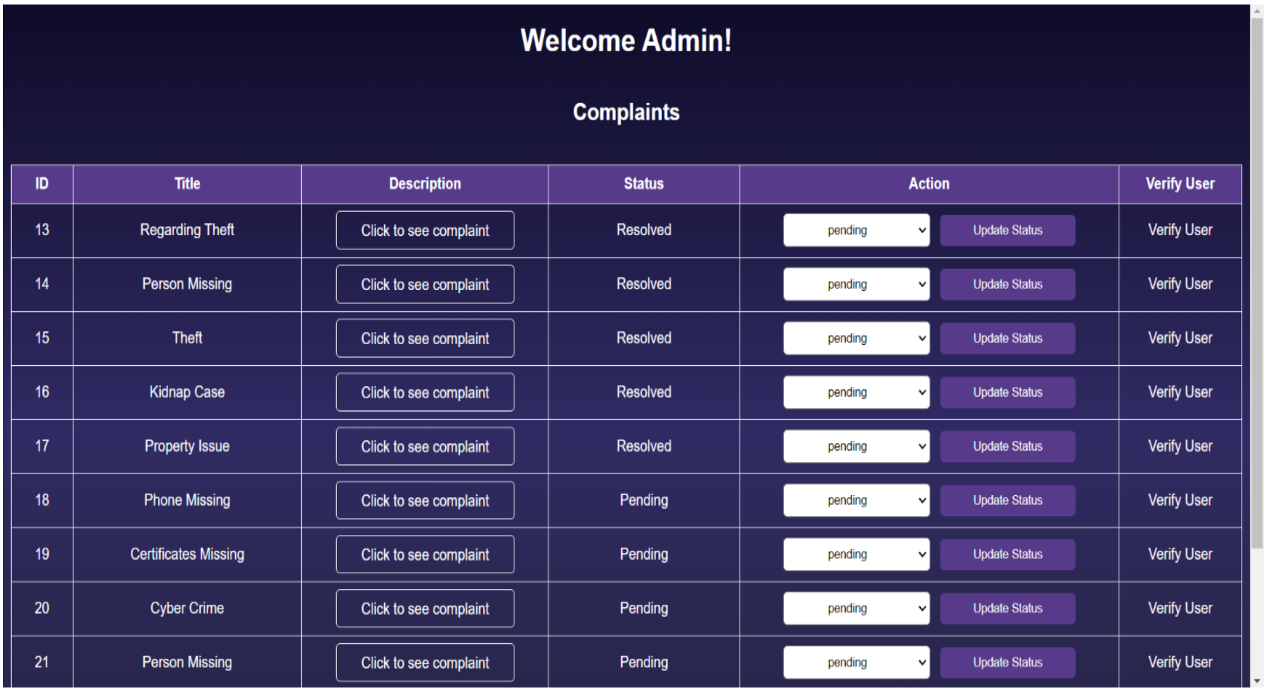
WELCOME, Please Register Your Complaint below!

Resolved Complaints
5

Pending Complaints
7

Total Trusted Users
12

Fig. 4 Home page

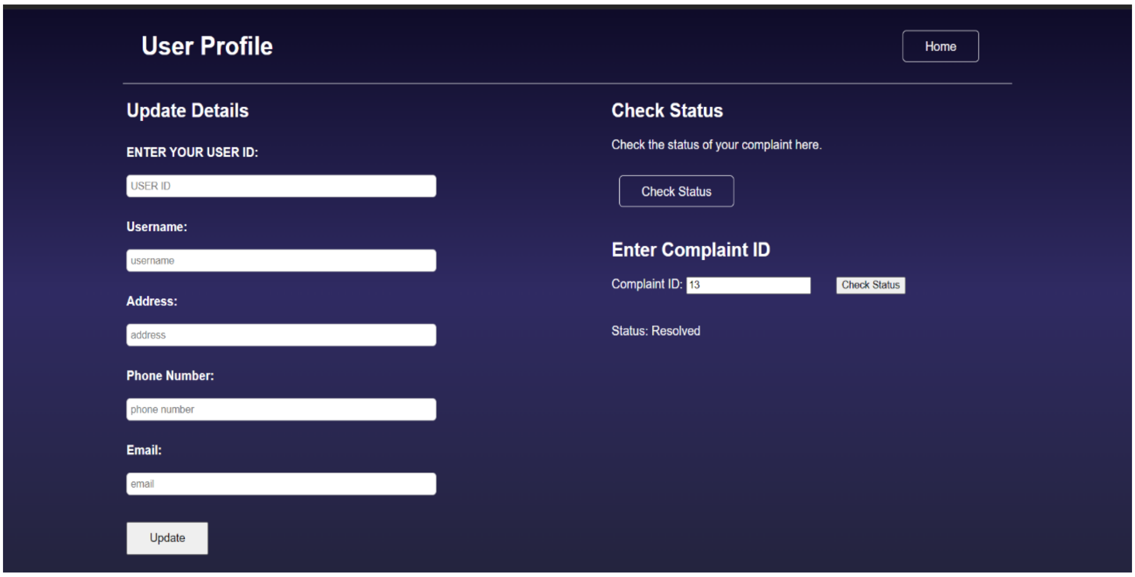


Welcome Admin!

Complaints

ID	Title	Description	Status	Action		Verify User
13	Regarding Theft	Click to see complaint	Resolved	pending	Update Status	Verify User
14	Person Missing	Click to see complaint	Resolved	pending	Update Status	Verify User
15	Theft	Click to see complaint	Resolved	pending	Update Status	Verify User
16	Kidnap Case	Click to see complaint	Resolved	pending	Update Status	Verify User
17	Property Issue	Click to see complaint	Resolved	pending	Update Status	Verify User
18	Phone Missing	Click to see complaint	Pending	pending	Update Status	Verify User
19	Certificates Missing	Click to see complaint	Pending	pending	Update Status	Verify User
20	Cyber Crime	Click to see complaint	Pending	pending	Update Status	Verify User
21	Person Missing	Click to see complaint	Pending	pending	Update Status	Verify User

Fig.5 Admin Page

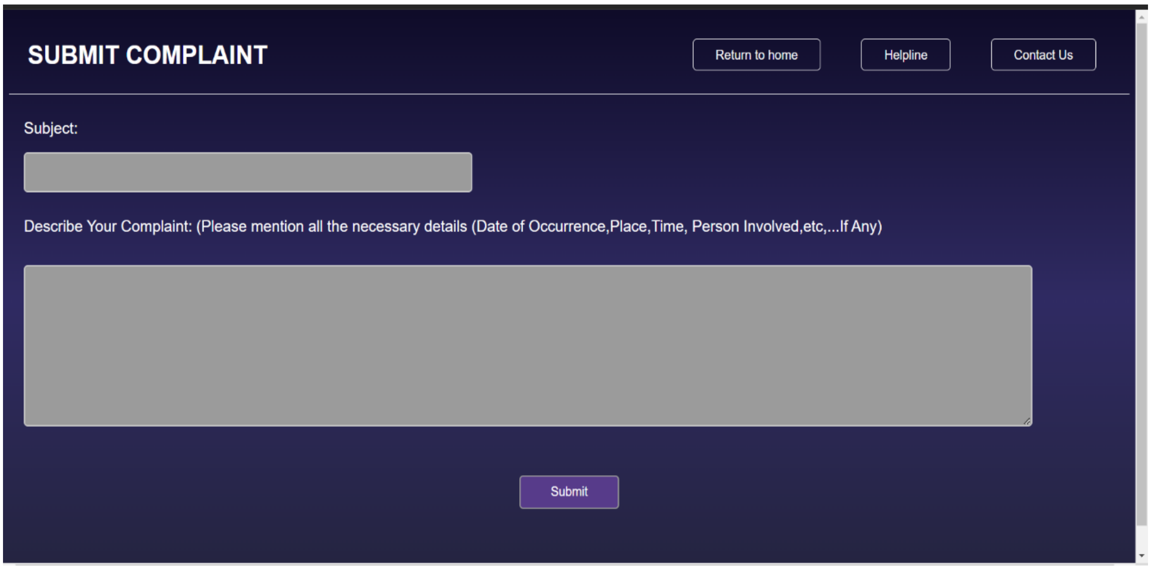


Check the status of your complaint here.

Complaint ID: 13

Status: Resolved

Fig.6 Update/Check Status page



Describe Your Complaint: (Please mention all the necessary details (Date of Occurrence,Place,Time, Person Involved,etc,...If Any)

Fig.7 Submission Page

VII. CONCLUSION

In conclusion, our complaint management system is a complete solution made to make managing user more efficient. Twofish encryption, as described in the earlier sections, shows remarkable efficacy in protecting private information from manipulation and illegal access. Its strong security features, which include a big key space and resistance to known threats, offer a solid framework for protecting private data. Modern technologies including facial recognition algorithms, web development frameworks, and encryption techniques are integrated into the system to provide users with a user-friendly interface coupled with strong security measures.

REFERENCES

[1] Ananda Kumar J. S , S.Muni Kumar, M. Nagaraju Naik1 “Study on Securely Digitalizing Crime Records by using RSA Algorithm” IJCSE Research Paper Vol.-7, Special Issue, 6, March 2019.
[2] Bharath D R , Cibiya N E , Divya M N , Dheekshitha S , Lynsha Helena Pratheeba HP,”Implementation of Blockchain for Police Complaint Management” International Journal of Research Publication and Reviews, Vol 4, March 2023

DOI: 10.17148/IJARCCE.2024.134195

[3] Chandramohan Dhasarathan,Vengattarama Thirumal Ponnurangam, "Grid Based Authentication for Online Crime Reporting System" IJCSMC, Vol. 4, Issue. 3, March 2015.
[4] "Cryptography and Network Security" by William Stallings : Seventh Edition.
[5] R.Manmadha Reddy , Neeraj Nishad, MOHD.Saif, M.Vijayalakshmi, "Police complaint management system using blockchain technology" JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY,HYDERABAD
[6] "The Twofish Encryption Algorithm" - March 1999 by Bruce Schneier ,Chris Hall , John Kelsey David Wagner, Doug Whiting
[7] The Twofish Encryption Algorithm: A 128–Bit Block Cipher 14 April 1999 By Bruce Schneier ,Chris Hall , John Kelsey David Wagner, Doug Whiting.
[8] https://www.techtarget.com/searchsecurity/definition/Twofish.
[9] https://profiletree.com/protecting-user-data-and-secure-storage-techniques.
[10] https://www.geeksforgeeks.org/what-is-data-encryption/?ref=lbp