Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 5, July : 2023

CRIME INFORMATION SECURITY BASED ON AES ENCRYPTION

Ms Kannika D, Student, Dept. Of Information Science, National Institute of Engineering, Mysuru.
Dr P. Devaki, Professor, Dept. Of Information Science, National Institute of Engineering, Mysuru.

Abstract
In the current system, individuals submit necessary information for passport applications either online or offline at the passport seva center. The final step in obtaining a passport requires the Police department to issue a police clearance certificate. During this process, local police stations conduct background checks to verify the applicants. Once completed, the data is encrypted using a hashing algorithm and stored in the database. However, due to potential tampering by influential individuals, the data's security is not entirely reliable. To address this issue, our project implements a higher level of security by encrypting the data using the AES technique and storing it in the AWS S3 service. Considering the rising instances of terrorist activities, it has become crucial to monitor unknown individuals traveling to other cities and renting houses locally. By maintaining a record of criminal and terrorist activities based on Aadhaar numbers in our application, we can conduct background checks before providing a house for rent and promptly inform the respective police station. Furthermore, in criminal investigations, we employ natural language processing concepts to identify potential matches between previous case summaries and the current case summary. By comparing and analysing these summaries, we can determine the percentage of similarities, aiding in the identification of criminals involved in the crime.

Keywords: AES Encryption, QR code image, AWS S3 service.

I. Introduction:

The police department has embraced digital transformation, transitioning its operations and processes to the digital realm. This new e-governance approach aims to address criticisms and expedite the issuance process. While the police department maintains a high level of security for crime-related records, there is a potential vulnerability where influential individuals or others with access to the records could manipulate them, compromising data accuracy. To tackle this issue, a novel solution has been implemented, harnessing cutting-edge technologies such as efficiency, user-friendliness, and privacy protection. To secure crime investigation data, the implementation utilizes AES encryption and the AWS S3 service, ensuring a more robust storage and retrieval system through a web-based platform. This application has been introduced to facilitate seamless and rapid communication among police officers within different divisions of the department. Given the rise in terrorist activities and the influx of unknown individuals relocating locally, a comprehensive system based on Aadhar No. has been established to manage criminal and terrorist information. This system allows for background checks to be conducted with the respective police station before renting or leasing a property, enabling the sharing of crucial information.

AES encryption: The AES Encryption algorithm, a symmetric block cipher with a block size of 128 bits, employs keys of 128, 192, and 256 bits to transform individual blocks. After encrypting these blocks, they are combined to create the ciphertext. AES is built upon a substitution-permutation network (SP network), which comprises interconnected operations, including input substitutions, specific output replacements, and bit shuffling. In this tutorial, we will explore the notable features of AES, a widely adopted encryption algorithm globally.

QR code: A QR code differs from a barcode in that it encodes data in two dimensions (horizontally and vertically), allowing it to store significantly more information than a one-dimensional barcode. In fact, while a barcode is limited to 20 alphanumeric characters, a QR code can accommodate thousands of characters. Consequently, a QR code proves useful for sharing various forms of content, such as multimedia, landing pages, or even entire e-books. Yet, QR codes possess capabilities beyond mere information storage—they can actually trigger specific actions on a phone. For instance, a theatre company might offer a QR code that not only redirects users to their website for show times and ticket details, but also automatically adds upcoming show dates, times, and venues to the user's phone calendar.

AWS Storage Services: AWS provides a diverse range of storage services that can be tailored to meet your specific project requirements and use cases. These storage services offer distinct provisions for handling highly sensitive data, frequently accessed data, as well as less frequently accessed data. You have the flexibility to select from various storage types, including object storage, file storage, block storage services, backups, and data migration options. All these options are encompassed within AWS Storage Services.

AWS Simple Storage Service (S3): Among the aforementioned services, AWS Simple Storage Service (S3) stands out as the primary object storage service offered by AWS. It is widely regarded as the go-to choose for AWS users due to its exceptional features such as high availability, robust security, and seamless integration with other AWS Services. AWS S3 caters to diverse use cases, ranging from mobile/web applications to big data and machine learning, among many others.

II. Literature:

[1]. Enhance efficiency and security of the Sri Lanka police department by digitizing it:
By KYAPYA, A.N SENARTHN, R.P. D.T. As the primary law enforcement organization of Sri Lanka, the police department plays a vital role in maintaining the public peace, preventing crime, terrorism, and upholding the law. Being a developing country, the police department is constantly moving forward with new technologies to manage operations efficiently and quickly respond to challenges and opportunities. However, in comparison to developed countries the police department is still lagging behind when it comes to modern technologies. The main issues that the police department faces include lack of coordination among departments, duplicate of data, delayed services, unauthorised data modification, lack of data analysis, and prediction, and corruption. This paper proposes 4 main improvements that help to overcome these issues and challenges: Improve the current police clearance certificates system to provide digital certificates that can verify authenticity, integrity, and provide efficient delivery and good user experience to applicants. Implement a blockchain network to securely store confidential data with transparency and integrity. I'm building a machine learning system that can predict where crimes will happen and what they'll do based on data from a CCTV system. Basically, the system is made up of 3 people: me, the applicant, a cop, and a verifier. I'm using Reacts for the front-end and the NodeJS/ExpressJs for the backend. I'm using MongoDB in the cloud for the database. First, I want you to fill out the application form with the info you need and submit it for verification. Then, the authorities will check your info and run a background check on you. After that, the next step is to get the police certificate.

[2]. Smart FIR: E-FIR data through block chain within smart cities:

By nazir D. khan: An e-FIR is a simple document filed to police stations by the victim or by someone on their behalf when they are involved in a cognizable crime like murder, kidnapping rape, theft etc. The database of e-FIRs stored in the police station's database is centralized and the record of the crime can be compromised. In addition, there is a risk of false registration of e-FIR due to the centralized nature of the database. Data integrity and transparency in e-FIR databases are therefore of utmost importance. In this paper, we address the issues of data integrity in e-FOR and false registration attached to police stations in the centralized database using a consensus based distributed blockchain solution. In particular, we use a smart contract-based intelligent framework to explore how the Ethereum blockchain can be used to provide integrity to the data stored in the local database. The framework is connected to the Ethereum blockchain via Web3 remote procedure call (RPC). Several simulations have been conducted to assess the performance of this framework Our results suggest a compromise between different levels of hashing algorithm security for the offense data and the number of transactions stored on the blockchain ledger in a single block. The proposed intelligent framework leverages the advantages of the blockchain technology to address an important challenge: how to provide intelligent integrity to e-FIR data stored in a centralized database of the police station in the context of a fully connected digital cities (smart cities) interoperability scenario? The vision is to decentralise the authorities' hold on e-FIR data in the central database of the police stations among various entities to ensure transparency. In this paper, our proposed novel framework is mainly twofold: An intelligent system to provide e-FIR data integrity via distributed blockchain ledger using smart contract that is tamper-resistant and fraud-resistant. Dealing with false e-FIR registration by collecting both the user's and the admin's credentials on the blockchain for audit purposes.

[3]. E- FIR Using E- governance:

By Kirti marmat, Anand more: This feature is created for the public to interact with the police better. The e-FIR system is designed to help the public interact with the police indirectly and to improve the facility of E-governance. E-FIR System with E-Portal: The E-portal website is specially designed to bring together information from various sources in a unified manner. Typically, each information source has its own dedicated area on the website for displaying information. Many crimes are witnessed by the people but they are scared to complain in the police stations because of fear, lack of time, and insensitivity. Because of this fear, many cases are not registered. Many cases are not properly investigated because of lack of proof, evidence, and lack of cooperation from the public. In this study, the main objective is to create an online system that can be easily accessed by the police departments, the public and the administrative departments, and to achieve electronic transparency at various levels, such as disclosure, reporting, transparency, accountability, etc. The primary objective is to increase the interaction between the police and the citizens without going to the nearest police station. This will help in reducing the crime rate, saving the time of the people, increasing the interaction between the government and the citizens, and will help in building an information society. The objective of the present study is to create an electronic first refusal (E-FIR) system with better facilities using e-governance, and to achieve transparency. The present study goes beyond all the limitations of the existing system, provides proper security, reduces manual work, reduces workload, and mental conflict for users, and makes it easy for them to file an FIR from anywhere, anytime.

[4]. Optimization of police resource allocation based on community public security risk prediction:

Making sure police resources are used wisely based on a community's public security risk prediction. Residential communities are at the heart of modern urban governance, with social security management being at the heart of it. The safety of residential communities is connected to the safety of the whole society, and this is reflected in the number of crimes in the community. A scientific and fair assessment of the residential community's public security situation, early warning and preventing

public security risks can help make police resources more efficient and improve the effectiveness of public security departments' work. This paper proposes a simple mechanism for community police resource allocation that can be easily implemented. It's a reference for community police work and aims to help make comprehensive social security governance more effective.

III. Conclusion:

The importance of ensuring security in information technology applications is widely recognized. In recent years, significant efforts have been made to enhance security measures, including advancements in AES encryption, QR codes, and the AWS S3 service. However, despite these improvements, various security vulnerabilities have emerged within these applications, rendering the achieved progress somewhat ineffective and resulting in perceived wastage of time and resources.

References

[1] W. Damayantha HANK, "Citizens Acceptance of Online Services in Sri Lanka Police: Study on Police Clearance Online System", 13th International Research Conference General Sir John Kotelawala defense university, pp.352-361, 2021. http://ir.kdu.ac.lk/handle/345/3006.

[2] "Refworld | Sri Lanka: Police reports, including records of arrest or detention, extracts of complaints, and police clearance certificates; procedures for an individual to obtain a copy of police reports; prevalence of fraudulent police reports", Refworld, 2021.https://www.refworld.org/docid/571f154b4.html.

[3] Online: January, 2019] Urban Population Growth statistics by UN; https:// population.

[4] Pal, Om & Alam, Bashir & Thakur, Vinay & Singh, Surendra. (2019). Key management for blockchain technology. IExpress. 7. 10.1016/j.icte.2019.08.002.

[5] B. Kaur, L. Ahuja and V. Kumar, "Crime Against Women: Analysis and Prediction Using Data Mining Techniques," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 194-196, doi: 10.1109/COMITCon.2019.8862195.

[6] S. Sathyadevan M. S. Devan and G. S. Surya "Crime analysis and prediction using data mining" 2014 First International conference on Networks & Soft Computing (ICNSC) pp. 406- 412 2014.

[7] P. Bhagya Divya, S. Shalini, R. Deepa, Baddeli Sravya Reddy, “Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras”, International Research Journal of Engineering and Technology (IRJET), December 2017.

[8] S. Gao, H. Wang, F. Xu, J. Song and K. Jia, "Real-time Human Action Detection for Elderly Monitoring System," 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), 2019, pp. 1191-1196, doi: 10.1109/CYBER46603.2019.9066751.