Grenze International Journal of Engineering and Technology, January Issue

Location-based AES Encryption and XGBoost Classification in a Hybrid Access Control System

Ramkumar Devendiran[1], Gogineni Veda Sri[2], Mutya Veda Phanindra Kashyap[3] and Vineeth Jermiah Cotton[4]
[1]Assistant Professor Senior Grade, School of Computer Science & Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India-522237
Email: ramkumar.d@vitap.ac.in
[2-4]M. Tech Student, CSE, VIT-AP University, Amaravati, Andhra Pradesh, India-522237;
Email: vedasri.gogineni@gmail.com, mutya.kashyap@gmail.com, jermiahcotton03@gmail.com

***Abstract*— In order to improve cybersecurity, this project offers a strong multi-factor access control system that combines machine learning-based decision-making, geolocation-based validation, and AES encryption. Access is only provided to users who are physically present in designated office zones, as confirmed by IP-based geolocation. To ensure confidentiality, messages are encrypted in CBC mode using AES. We create behavioral access records and train an XGBoost classifier to predict access permissions based on user role, department, login frequency, and other factors in order to further impose intelligent access control. The system handles security issues such location spoofing, brute-force attacks, and illegal access while achieving high accuracy and interpretability. For a more intelligent, context-aware access control system, our solution shows how well classical encryption works when combined with real-time data analytics and artificial intelligence.**

***Index Terms*— Cybersecurity, role-based access, location-aware security, behavioral analytics, IP tracking, encrypted messaging, access prediction, smart authentication, real-time validation, access control, AES encryption, geolocation, machine learning, XGBoost.**

I. INTRODUCTION

Data security and user authentication are now top priorities for businesses in a variety of sectors in the digital age. Password-based authentication and other traditional security measures are no longer adequate to prevent unwanted access to sensitive data. In order to improve security, this research presents a sophisticated access control system that integrates machine learning algorithms, geolocation-based authentication, and encryption approaches [1]. Only authorized staff will be able to decrypt and examine sensitive data thanks to the proposed system, which limits access to encrypted messages depending on the user's physical location. This solution attempts to reduce common security risks like data breaches and unauthorized access by utilizing the power of AES encryption and real-time geo-location [2].

By guaranteeing that users may only access sensitive data while they are inside a predetermined geographic radius, like an office location, geolocation-based authentication provides an additional degree of security [3]. By integrating geolocation services, this project makes it possible to verify a user's position in real time and provide or refuse access to encrypted data. Even in the case that login credentials are obtained, the system is built to prevent unwanted access by basing access decisions on the user's proximity to specified office locations.

Grenze ID: 01.GIJET.12.1.540_1

The technology offers a more flexible and safer substitute for conventional access control methods by combining location verification with AES encryption, shielding company data from numerous dangers [5].
To further improve security measures and anticipate access patterns, the project also uses machine learning methods, including XGBoost. Through the analysis of user behaviour, including years of service, access attempts, and frequency of logins, the system is able to anticipate and identify unusual trends that may point to fraudulent activity [4]. By using machine learning, the access control system is guaranteed to continuously adjust to changing security requirements. In order to reduce the danger of unwanted access and protect sensitive data, this project intends to offer a complete solution that integrates encryption, geolocation, and machine learning to build a strong, dynamic, and secure access control system for contemporary enterprises [6].

II. LITERATURE SURVEY

Significant progress has been made in the field of location-based encryption systems, with numerous studies concentrating on improv-ing security and privacy in networked and mobile environments. Using encryption methods like AES to protect user privacy and se-cure communication when using location-based services is one important area of research. For example, Alkady et al. (2020) used homomorphic encryption to safeguard users' location data in an effective privacy-preserving approach designed for location-based services on VANET systems [7]. In a similar vein, Farouk et al. (2021) suggested a location query strategy that protects privacy by using completely homomorphic encryption, guaranteeing that searches over encrypted data do not jeopardise efficiency or privacy [8]. These strategies demonstrate the increasing focus on incorporating encryption methods to protect private user information in real-time applications.
Integrating location-based services with secure communication protocols is another crucial area of research in this field. An oblivious transmission protocol based on ElGamal encryption was investigated by Bahrak and Jannati (2017), who made sure that users' location privacy was maintained throughout data exchange in VANET networks [9]. Additionally, with an emphasis on protecting communica-tion in the Internet of Things (IoT), You et al. (2018) looked into the application of AES-128 encryption in low-power communication contexts like LoRaWAN [10]. Their research highlights the need for low-power encryption techniques that can protect low-resource devices without sacrificing functionality or energy economy. These studies demonstrate how AES and related encryption methods can be used to protect sensitive location-based data in a variety of networked settings.
Recent research has concentrated on integrating location privacy and security in healthcare and other crucial industries, in addition to encryption-based techniques. In order to improve data integrity and privacy, especially in situations where user location and medical data overlap, Khandare et al. (2020) looked into integrating AES and DES encryption in medical information systems [12]. Their re-sults demonstrate how crucial strong encryption techniques are for safeguarding patient information and making sure location-based services are safe and adhere to privacy laws. In sensitive applications like healthcare, this line of research highlights the growing sig-nificance of encryption for preserving the integrity and authenticity of location-based services as well as for protecting privacy.
Enhancing access control, more studies in this area look into combining location-based encryption with machine learning models. Chandramohan and Arputharaj [1] introduced a hybrid approach to cloud security, which used location-based encryption algorithms to dynamically restrict access. Ahmed et al. [6] raised the stake for integration between geolocation and decision intelligence by building a RoLAWAN-based geofencing system for remote energy monitoring. Their method proved that contextual location can be an effi-cient security layer in constrained environments. Portnoi and Shen [13] came up with Loc-Auth, a location-and-attribute-based-encryption combination for safe authentication. Their study presented a new perspective on applying environmental context to guar-antee user authenticity.
Alongside encryption, privacy frameworks have changed over time. Geo-indistinguishability is a differential privacy method created for location-aware systems; Andrés et al. [15] showed it serves the purpose of masking a user's location so as to prevent the tracing of the location with extreme sise.] Yang et al. [19] further contributed by developing a PPQS consisting of a set of protocols to secure and coordinate outsourced location services on the cloud. Upadhyaya and Vivek [17] proposed an edge-based protocol that provides real-time location services with a trade-off between latency and confidentiality. As a result, the security architectures are becoming more intelligent, flexible, and context-aware. Unlike before, encryption is now combined with real-time access controls and predictive ana-lytics. The modern access control systems are based on this synergy of artificial intelligence, geolocation, and cryptography [20].

A. Inference of the Literature Survey

The literature review emphasises how crucial it is becoming to incorporate strong encryption methods, including AES and homomor-phic encryption, into location-based services in order to protect user privacy and data security. Numerous studies highlight the necessi-ty of secure communication protocols in networked and mobile contexts, especially in industries like VANET systems, IoT, and healthcare. According to the study, encryption guarantees data integrity and efficiency in low-power and resource-constrained devices in addition to protecting location privacy [11]. Furthermore, the investigation of privacy-preserving schemes in communication sys-tems and location enquiries highlights the necessity of adaptive encryption techniques that may strike a balance between security, pri-vacy, and performance in a variety of applications. These results highlight how important encryption is for building trust and protect-ing private data in real-time applications.

III. PROPOSED METHODOLOGY

A. Location-Based Access Control

The first step in the suggested methodology is to put in place a location-based access control system. Using GPS or IP-based geoloca-tion, the system will confirm the user's present location. The system will compare the user's location with pre-specified office loca-tions[13]. Access to the encrypted message will be provided only if the user is within a certain radius of an office. This enhances data security and privacy by guaranteeing that private data can only be accessed from designated areas. Furthermore, the system offers an easy-to-use method of managing access control by providing real-time feedback regarding whether the user is in an authorised location.

B. Data Security with AES Encryption

Sensitive messages are encrypted in the second stage using the Advanced Encryption Standard (AES). The symmetric-key encryption technique AES guarantees a high degree of security for data that is sent. To further improve security, the secret message will be en-crypted using a randomly generated key and the CBC (Cypher Block Chaining) method[14].

The ciphertext will be encoded in Base64 to securely store and send the encrypted data, making it easier to manage across various communication systems. The system uses AES to make sure that the data cannot be decrypted without the right key, even if it is intercepted.

C. Decryption Process Upon Location Verification

The third phase of the approach entails a decryption process that is initiated when the user's location has been successfully verified. The system uses the AES key to decrypt the message once the user is within the permitted range.

To guarantee that the message is de-crypted correctly, the decryption process makes use of the initialisation vector (IV) of the CBC mode. This method preserves a high degree of anonymity and stops unwanted access by guaranteeing that only people in approved physical locations can access the en-crypted data. Sensitive messages cannot be decrypted outside of specified zones due to this location-based restriction.

D. User Interface and engagement

A smooth engagement with the location-based access control and encryption systems will be made possible by the user interface (UI). Users will be able to engage with the location verification system, enter secret messages, and start the encryption process through the user interface[15].

Real-time feedback on the encryption's progress and the user's location verification will be given by the user inter-face. Additionally, notifications will be shown if the user is within the permitted decryption radius. This guarantees openness, aids users in comprehending the access control systems, and makes the complete procedure simple and easy to utilise.

E. Scalability and Adaptability:

The suggested methodology will be made to be both scalable and flexible enough to accommodate various settings and situations. The system can be expanded to function with dynamic locations or numerous geographical areas, even though it is currently made for stat-ic office locations. The location-based access control feature of the system can be tailored to a number of use cases, including protect-ing private communications for professionals who are constantly on the go or for remote teams. Because the encryption and decryp-tion procedures are simple and adaptable to larger data volumes, the system can be used in a variety of settings.

IV. WORKFLOW

A. User Input and Office Location Configuration

The process starts when the user logs into the system's user interface and is asked to enter the secret messages they want to encrypt. Users will be asked to provide their office locations by inputting their geographic coordinates (latitude and longitude) in addition to the message. The system then keeps track of these office locations for future use[17]. The user is also prompted to indicate the permitted radius that decryption can occur within. The location-based access control system, which makes that encrypted messages can only be viewed from particular geographic regions, depends on this configuration.

B. Message Encryption Process

Users encrypt the message they want to secure after configuring the office locations and radius. The secret message is encrypted using a special AES encryption key that is generated by the system. To protect the secrecy of data, the AES encryption algorithm runs in CBC mode. After that, the Base64 format is used to encrypt the message, making it safe for transmission or storage. This procedure offers a high degree of protection for sensitive data by guaranteeing that, even in the event that it is intercepted, it cannot be decrypted without the decryption key.

C. Location Verification

The procedure checks the user's location after the message has been encrypted. The system employs geolocation tech-nology (either via IP or GPS) to ascertain the user's present location when they click the "Get Current Location" button in the user interface. The system's predefined office locations are then compared with this geolocation data. The sys-tem accepts the user's present location as legitimate and allows access to decode the message if it is within a certain radius of any office location[16]. To guarantee that only authorised locations can view the encrypted communication, access is restricted if the location is deemed invalid.

D. Message Decryption

The system decrypts the encrypted message after verifying the user's location. The system decrypts the message using the same AES key that was used to encrypt it. To ensure that the message is decrypted correctly, the AES decryption procedure uses the same initiali-sation vector (IV) that was used during encryption. The system verifies that location-based access control has been effectively imple-mented by showing the user the original message after it has been decrypted. Only when the user is inside the permitted radius of an office location will the decrypted message be visible.

E. System Feedback and Access Logs

Giving the user feedback regarding the progress of their request is the last stage of the workflow. A success message and the decrypted message appear on the screen if access is approved. The system will show an error message stating that the user is outside the permit-ted location range if access is refused. For auditing and monitoring purposes, the system also records every access attempt, along with the time, location, and request status (approved or rejected) [18]. This improves the system's security and traceability by guaranteeing that any attempts at unauthorised access are documented.

V. DATA ACQUISTION

A. XGB Model Data Preprocessing

The first data preprocessing step for the XGB classifier model was turning raw timestamp data into useful information like the last login and access hours. To identify access patterns, these characteristics were taken from the initial login and access timestamps. Fur-thermore, one-hot encoding was used to transform categorical variables such as department and user role into numerical format for the model. Both numerical and categorical variables were included in the final dataset, which was then divided into features (X) and the target variable (y), which was the 'access_granted' column. The data was divided into training and test sets for the model training phase once all missing values had been addressed.

B. Access Data Dataset

The project's access data is made up of fictitious entries that depict organisational access attempts. User job, department, years of ser-vice, access time, number of access attempts, last login time, frequency of logins, and whether access was granted or denied are among the features included in the dataset. The model predicts whether

access should be given based on timestamps for both login and access, which are essential for comprehending user behaviour patterns[19]. The XGB model is trained in a realistic setting thanks to the randomly generated dataset, whose values reflect typical behaviour inside an organisation. The data simulates different staff access attempts during a 31-day period in March 2025.

C. User Information Gathered

Geographical coordinates and the locations of each user's office are the main types of user data for the location-based encryption sys-tem. Through the application interface, users enter the latitude and longitude of their offices, and the system uses geolocation technol-ogy (GPS or IP) to get their current location in real time. To make sure that decryption is only permitted if the user is within a prede-termined radius, this location data is saved and compared with established office locations. For security reasons, user interactions are also recorded, including the encrypted message input and the status of the access attempt (allowed or denied). This information guar-antees that the project's location-based access control and encryption systems operate as intended.

D. System Architecture

The proposed project's system design centres on an intuitive user interface (UI) created with flask that allows users to engage with the program. The user interface is made to enable users to recover their current position and enter a secret message for verification[14]. The geolocation module uses the user's IP address to retrieve the current location after the user has entered the necessary information. The database's pre-defined office locations are then compared to this one. The system then encrypts the message using AES encryp-tion and stores it safely for future access if the user is within the permitted radius.

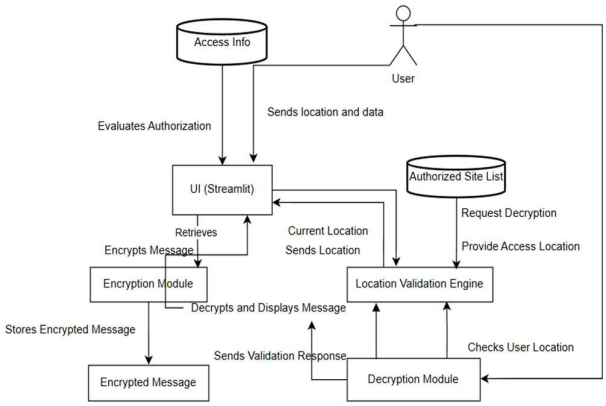

Fig 1. System Architecture

After the message has been decrypted, users engage with the system once more and ask for access. After receiving this request, the decryption module compares the user's position to the pre-established office locations to confirm their location once more. The system decrypts the message and shows it to the user if the user falls within the permitted range[7]. By integrating geolocation validation and cryptographic security, the architecture makes sure that sensitive data is only available when the user is in a certain geographic place. In order to provide a strong, multi-layered security system, the application also makes use of historical access data to forecast possible access permissions.

VI. Results and Discussion

The project's outcomes show how well location-based authentication and AES encryption work together to protect private communica-tions. The system successfully encrypts a message and makes sure that only users who are within a predetermined radius of particular office locations are able to access it. The geographic proximity-based access control method functions as planned, denying access to users who are beyond the specified range[16]. Because only authorised users within the office limits may decrypt the communication, the model also demonstrates the effectiveness of encryption in maintaining data security and secrecy. A strong security framework is ensured by combining AES encryption with geolocation, providing an extra degree of security over conventional password-based solu-tions.

The initiative emphasises a number of important conclusions from the conversation. While location-based authentication adds an add-ed degree of protection, it is not infallible and can still be subject to some sorts of attacks, such as IP spoofing. However, the solution greatly lowers the risk of unauthorised access by integrating AES encryption and combining it with other user-specific criteria like historical access data[2]. To further increase the security measures, future developments can include adding multi-factor authentication (MFA) and improving the geolocation accuracy. All things considered, the research demonstrates how encryption and geolocation can be used to produce a very safe system that can instantly protect important data.

TABLE I: XGBOOST MODEL PERFORMANCE METRICS

Metric	Denied (0)	Granted (1)	Macro Avg	Weighted Avg
Precision	0.95	0.95	0.95	0.95
Recall	0.96	0.93	0.95	0.95
F1-Score	0.95	0.94	0.95	0.95
Support	786	614	1400	1400
Overall Accuracy	-	-	-	0.95

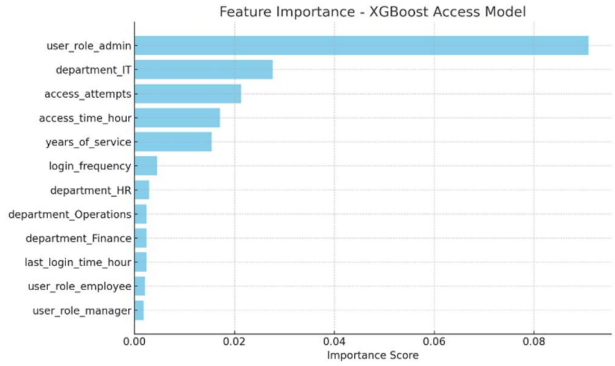

Figure 2: Feature Importance in Access Prediction using XGBoost

VII. CONCLUSION

To sum up, this project presents a hybrid access control system that integrates AES encryption, geolocation-based authentication, and machine learning to secure sensitive data. By combining real-time location verification with an XGBoost classifier trained on user be-havior data including department, access frequency, and login history, the system makes intelligent, context-aware decisions about access rights [4]. This approach not only ensures data confidentiality but also adds a dynamic behavioral layer to traditional security models. The proposed framework significantly reduces the risk of unauthorized access and illustrates a practical application of predic-tive analytics in cybersecurity. It establishes a strong foundation for future work in adaptive, multi-factor access control systems.

REFERENCE

[1] Chandramohan, P., & Arputharaj, K. (2021). Enhanced algorithm to improve the security level in cloud computing using location-based encryption. International Journal of Engineering Research & Technology (IJERT), 10(3), 125–129.

[2] Kwak, J., Kim, J., & Chong, S. (2018). Proximity-aware location-based collaborative sensing for energy-efficient mobile devices. IEEE Transactions on Mobile Computing, 17(4), 867-880.

[3] Anand, R., & Maitra, S. (2021). Quantum resource estimation for FSR based symmetric ciphers and related Grover's attacks. Pro-gress in Cryptology–INDOCRYPT 2021, 22nd International Conference on Cryptology in India, 2021.

[4] Proceedings of the International Conference on Advanced Intelligent Systems, 2019.

[5] Mohamed, N. N., Othman, H., Isa, M. A. M., Noor, N. A. M., & Hashim, H. (2017). A secure communication in location-based services using AES-256 encryption scheme. 2017 IEEE Symposium on Computer Applications and Industrial Electronics, 2017.

[6] Ahmed, S. T., Annamalai, A., & Chouikha, M. (2024). A scalable and energy-efficient LoRaWAN-based geofencing system for remote monitoring of vulnerable communities. IEEE Access, 12, 48540-48554.

[7] Alkady, Y. H., & Rizk, R. Y. (2021). Privacy-preserving location-based services query scheme based on fully homomorphic en-cryption. Journal of Theoretical and Applied Information Technology, 99(16), 4098-4121.

[8] Bahrak, B., & Park, J. (2014). Coexistence decision making for spectrum sharing among heterogeneous wireless systems. IEEE Transactions on Wireless Communications, 13(10), 5520-5531.
[9] Khandare, N. B., Dalvi, O., Nikam, V., & Pandit, A. (2020). Enhancing privacy and security in medical information with AES and DES. International Conference on Intelligent Computing and Communications, 2020.
[10] Jagadeesan, J., Chelliah, B. J., Nyapathy, N., & Tiwari, N. (2021). Reversible data hiding in encrypted images using AES data encryption technique. Turkish Journal of Computer and Mathematics Education, 12(6), 3803-3808.
[11] You, I., Tsai, K. L., Huang, Y. L., Leu, F. Y., & Huang, Y. L. (2018). AES-128 based secure low power communication for Lo-RaWAN IoT environments. IEEE Access, 6, 45325-45334.
[12] El-Rahman, S. A., Mansour, A. E., Jamel, L., Alohali, M. A., Seifeldin, M., & Alkady, Y. H. (2025). C-HIDE: A steganographic framework for robust data hiding and advanced security using coverless hybrid image encryption with AES and ECC. IEEE Access, 13, 41367-41381.
[13] Portnoi, M., & Shen, C.-C. (2015). Location-aware sign-on and key exchange using attribute-based encryption and Bluetooth beacons. arXiv preprint arXiv:1504.07192.
[14] Bohli, J. M., Dobre, D., Karame, G. O., & Li, W. (2014). PrivLoc: Preventing location tracking in geofencing services. arXiv pre-print arXiv:1404.4744.
[15] Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., & Palamidessi, C. (2013). Geo-indistinguishability: Differential privacy for location-based systems. Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS '13), 901–914.
[16] Jin, H., & Papadimitratos, P. (2020). Resilient privacy protection for location-based services through decentralization. arXiv pre-print arXiv:2001.07583.
[17] Upadhyaya, S. K., & Vivek, S. (2022). Revisiting a privacy-preserving location-based service protocol using edge computing. Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22), Article 70.
[18] Yang, X., Yin, F., & Tang, X. (2017). A fine-grained and privacy-preserving query scheme for fog computing-enhanced location-based service. Sensors, 17(7), 1611.
[19] Yang, G., He, Y., Zhang, J., & Zheng, D. (2022). Privacy-preserving query scheme (PPQS) for location-based services in out-sourced cloud. Security and Communication Networks, 2022, Article ID 9360899.
[20] M. Portnoi and C.-C. Shen, “Loc-Auth: Location-Enabled Authentication Through Attribute-Based Encryption,” in *Proceedings of [Conference/ArXiv]*, 2014.