A Secure Geolocation-Controlled File Sharing System with Adaptive Encryption and Intrusion Detection

Dayalu Swapna,
Student,
Department of Computer Science and Engineering
Jawaharlal Nehru Technological University, Anantapur, India
swapnadayalu@gmail.com

Dr. M. VIJAYA KANTH,
Assistant Professor,
Department of Computer Science and Engineering
Jawaharlal Nehru Technological University, Anantapur, India
registrar@jntua.ac.in

***Abstract*—The Secure Location-Based Cryptographic File Sharing System is an application that is designed to make the data more secure by combining the geolocation-based access control and the sophisticated Artificial Intelligence techniques. The system relies on the XGBoost-based Anomaly detection method for analyzing user behavior, login patterns and access activities to detect and prevent unauthorized access to the system in real-time. It incorporates the GAN based encryption to generate dynamic and unpredictable encryption patterns that serve as a safe method for transmitting data against modern day cyber threats. On top of this, adaptive key generation mechanisms can be used to further increase security of authentication mechanisms that utilize such context sensitive factors as device trust, network conditions and user behavior to change encryption keys. A pre-upload security scanning module is useful to detect the potential malware and intrusion attempts before the file is shared hence continuous monitoring and instant alert systems provide proactive threat response. By combining the idea of intelligent access controls, adaptive encryption and in real time threat detection, the proposed system is able to offer a robust scalable and secure solution for modern day file sharing environments.**

Keywords—Secure File Sharing, Geolocation-Based Access Control, Cryptography, XGBoost, Anomaly Detection, GAN-Based Encryption, Adaptive Key Generation, Intrusion Detection, Machine Learning Security, Data Privacy.

I. INTRODUCTION

The explosive growth in digital communication and storage systems based on the cloud has equaled a huge need for safe solution of file sharing. Traditional file-sharing platforms primarily rely on static encryption methods as well as role-based access control and while they are effective to a degree they are also a weak link in the fight against modern cyber-criminals. With the growing surface of sophisticated attacks such as unauthorized access, data breaches threat from within the organization etc., there is a critical need the intelligent and adaptive security solution goes beyond the traditional methods.

One of the big limitations of some existing systems is that there is no contextual and dynamic access control. Most platforms allow users to have access to sensitive information, regardless of their location and therefore face a risk of unauthorized access of sensitive information. In addition, static encryption mechanisms do not take into account a changing threat environment and are therefore susceptible to brute force attacks and replay attacks. Furthermore, traditional systems often follow reactive security strategies, i.e. threats are only detected after they have occurred and thus could have led to data loss and loss of privacy.

To overcome these problem, this project propose a Secure Location Based Cryptographic File Sharing System which incorporate the state of art machine learning and cryptography to. The system uses access control by means of geolocation, limiting the access to any files with those regions that are authorized to it which provides an additional level of physical security. It uses XG Boost based Anomaly Detection Technique for Monitoring user behavior, login pattern and access, Real time identification of suspicious activities etc. Moreover, GAN-based encryption is used to create dynamic and unpredictable encryption schemes, which can help to improve data protection when it is being transmitted.

Along with intelligent access control and encryption the system also has adaptive key generation and pre-upload security scanning to make the system more secure. The adaptive key mechanism for dynamically changing encryption keys based on contextual factors like trust in the devices and network conditions and the pre-upload scanning module for determining if files have malware before they enter the system. Continuous monitoring and instant alert

mechanism helps in the treatment of threat proactively as well. By using AI-driven security measures, limitations in geolocation, and dynamic cryptography, the security system developed is a secure and scalable solution for sharing files in modern digital spaces.

II. LITERATURE REVIEW

The importance of the behavioral analysis to detect unauthorized access by using machine learning technique is emphasized in the study titled anomaly-based intrusion detection using machine learning techniques by Boulemtafes et al. [1]. The system uses machine learning algorithms to detect patterns of behavior that deviate from normal for the end user. It is much more accurate to detect than traditional signature-based. The model is able to recognize unknown attacks by learning from past data. This way, proactive security is improved and reliance on predefined security rules is reduced. However, in dynamic environments the system has high false positive rates. It is also not flexible enough to account for fast-changing user behavior, suggesting that more powerful real-time models are required.

The study done on hybrid machine learning access control approach in cloud computing by Farooq et al. [2] presents the efficacy of the combination of several algorithms such as Support Vector Machines and Random Forest. The system analyses user access logs and user behaviour patterns and uses this to make informed access control decisions. It has better accuracy and reliability than single model systems. The hybrid approach helps in improving an anomaly detection capabilities in complex environments. It is especially useful in cloud-based systems that have different kinds of user activities. However, the combination of several models makes the computation more complex. This limited its scalability and performance for running real-time applications.

The work on AI-based authentication for cybersecurity by Mahfouz et al. [3] is focused on the improvement of authentication with the aid of behavioral analytics. The system keeps track of the user's behavior such as the number of log in events, the pattern of typing, and access habits. It helps in improving the accuracy of authentication as it identifies legitimate users based on behavior. This reduces the need for static passwords and increases security of systems. The approach facilitates real-time authentication as well as reducing unauthorized access risks. However, it needs big data sets for it to be able to possibly train. It also may have trouble with new users or sudden changes in their behavior, as it may impact their reliability.

The study on user behavior analytics for risk-based authentication by Zhang et al. [4] emphasizes on the dynamic access control by machine learning. The system assigns risk scores that are based on user activity, location and device information. It enables adaptive authentication by enabling or denying access based on the risk level. This reduces the false positives and increases the accuracy of decision making. The model improves the security level by continuously monitoring the user behavior. It does well in detecting the insider threat and unusual activities. However, the system needs continuous updates of data and may find difficulties with large-scale data efficiently.

The research on AI driven cryptographic key management by Liu et al. [5] is about the dynamic key generation techniques using machine learning. The system automatically creates and renews encryption keys that are based on the context. This increases the security, because it creates a less chance of key compromise. It helps the encryption to be stronger than what was traditionally done using static key systems. The approach favors adaptive security in a changing environment. It also brings down the manual intervention in managing the key. However, the system is not so good at handling complex real-time scenarios. It may also introduce other computational overheads.

The study on geolocation based access control using machine learning by Patel et al. [6] suggests the importance of location-aware security mechanisms. The system has a geolocation-based access-control to sensitive data. It improves security by blocking any remote access by unauthorized applications. The use of machine learning adds value to be accurate in decision-making. The approach works well in security systems used at the enterprise level. It provides one more level of security on top of standard authentication. However, it relies a lot on accurate location data. Privacy concerns can also arise with using location tracking.

The work on AES based encryption with location-based access control by Smith et al. [7] shows the combination of encryption techniques with geofencing techniques. The system provides security such that encrypted files can be accessed only in certain locations. It increases the security of data through the physical limitations to control access. The approach is capable of achieving high accuracy when it comes to preventing unauthorized access. It became appropriate for secure file-sharing applications. However, the system is based on static encryption algorithms. It does not have the adaptivity to adapt with the changing face of security threats and environments.

The work on XG Boost-based anomaly detection for cryptographic security presented by Kumar et al. [8] is aimed at enhancing the accuracy of threat detection by means of more sophisticated machine learning models. The system

provides analysis of the user behavior, login patterns, and access attempts. It performs high accuracy of unauthorized access detection and low false positives. The model is efficient and runs well on large data sets. It is used for real-time monitoring and decision making. But as is the case with models will require a careful feature engineering and parameter tuning. It also might stumble with dealing with highly dynamic patterns of user behavior.

III. Existing system

The current file-sharing systems are mainly developed using cloud-based systems that use old cryptographic methods to uphold data security. Most systems use standard encryption algorithms such as the AES and RSA algorithms in protecting files while in storage and transmission. They apply simple access control algorithms such as role-based access control (RBAC) and multi-factor authentication to limit access by unauthorized users. Secure communication protocols such as https, Victoireftps and stftps are also commonly used to protect data exchange over networks. These systems are very popular because of simplicity, scalability, and ease of incorporation into the modern application.

However, there are several limitations that currently exist within these systems in relation to their capability of handling advanced security threats. They depend on static encryption solutions and static key management solutions that do not respond to changing cyberattacks. Additionally, they do not have contextual access control measures such as geo-location based restriction and therefore, people can access sensitive information from anywhere, which poses a potential security threat. Most systems rely on a reactive style of security, where things are only detected when there is a breach. Furthermore, low frequency of monitoring in real-time and lack of intelligent anomaly detection makes them less effective in preventing unauthorized access, which indicates the need for more adaptive and proactive security choices.

Limitations of Existing systems:

- Static use of encryption algorithms (e.g. AES, RSA), which do not adjust themselves to changing cyber threats.
- Lack of access control for geolocation, since it grants access to files from any place; it also leads to more security risks.
- Limited or no real-time anomaly detection in order to detect suspicious user behavior.
- Reactive security mechanisms that identify threats only when the breach has occurred.
- Lack of intelligent AI driven threat detection and prevention systems.
- Manual or fixed key management i.e. encryption keys vulnerable to compromise.
- Lack of adequate pre-upload malware scanning, which lets files that may harm the system be uploaded.
- Lack of proper contextual awareness (i.e. device, network, user behavior) in access control decisions.

IV. Methodology

The proposed system of Secure Location Based Cryptographic File Sharing System consists of a systematic and multilayered methodology for providing good security, enhancing flexibility and efficiency in sharing files. The system combines machine learning, geolocation services, and advanced cryptography techniques to get rid of modern cybersecurity challenges. It starts with gathering data and preprocessing it, then it involves training the model and intelligent decision making. The methodology focuses on real-time threat detection and dynamic encryption as well as contextual access control. Each module is designed to work in concert with each other to improve the system as a whole. The way used ensures both proactive and reactive security mechanisms. This flow or structured methodology allows the system to supply a robust and scalable solution.

1. Data Collection

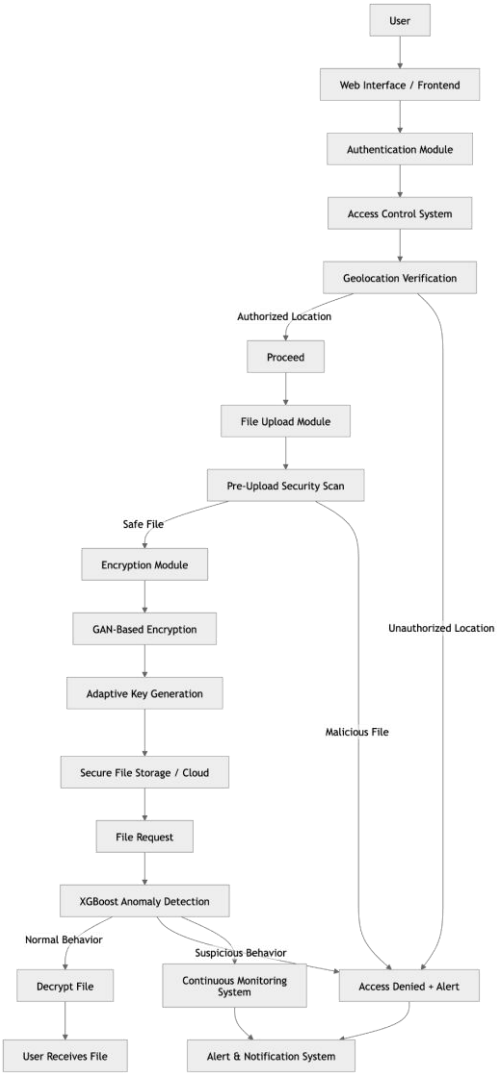
The system gathers complete datasets from various inputs to get to know the user behavior and the interactions within the system. These include user access, login timestamps, IP address, geolocation information, device and file sharing activities. Both data on normal and anomalous behavior are collected in order to train a machine learning model well. The dataset includes patterns which are attempts to login, frequency of access, and unsuccessful attempts to login accessibility. This data is essentially needed to find suspicious activities and make predictive models. The right data collection ensures the greater accuracy and reliability of the model. It is the basis of introducing intelligent security measures within the system.

2. Data Preprocessing & Featuer Engineering

The data collected in raw format is processed for it to be useful for machine learning algorithms. Missing values are filled in with suitable imputation techniques and noisy or irrelevant data is downloaded. Timestamps are transformed into meaningful numerical features like login intervals as well as access frequency. Categorical variables such as user role, department and device type are encoded by one-hot encoding. Feature scaling and normalization is applied so that there is consistency between data points. Feature engineering helps in finding the important patterns that helps the model to perform better. This step is important to increase the efficiency and accuracy of anomaly detection.

3. Anomaly Detection using XGBoost

The preprocessed data is fed to XGBoost model to train the model for user behavior anomaly detection. XGBoost is the choice here because of its high accuracy, quickness and efficient trends with large datasets. The model learnshetti's andt API The model learns patterns of normal user activity and detect deviations which may include abnormal login times, unknown locations and repeated access attempts. Performance metrics are used to evaluate the performance such as accuracy, precision, recall and F1 score. The trained model is deployed for actual time monitoring actions of users. This allows attempts to gain access to the system to be detected early. It plays a critical role of contributing to the strengthening of system security.



4. Access Control Based on Geolocation

The system integrates geolocation services with the use of GPS or IP-based tracking in order to enforce the location-based restrictions. Users are permitted to use files only if they are located within prescribed authorized geographical area(s). This provides a next level of physical security to the system. If a user tries to access data from a location that he does not have access to, the user will not be able to access the data and the system would block the access immediately. Alerts are created to let the user or administrator know about the suspicious activity. Remote unauthorised access is on the whole prevented to use this mechanism. It ensures that access is only given to sensitive data under controlled conditions.

5. GAN-Based Encryption

To add to the data security, the system uses Generative Adversarial Networks (GANs) for encryption. GAN-based encryption creates encryption patterns of each file that are dynamic and unpredictable. Unlike the static encryption methods, which are traditional, this method is always evolving thus making it immune to modern attacks. Each file transfer has a unique encryption, which minimizes the possibility of decryption by attackers. The generator model and the discriminator model collaborate to enhance the overhead of encryption. This guarantees confidentiality of data and integrity during transmission. It plays a great role in the robustness of the cryptographic system.

6. Adaptive Key Generation

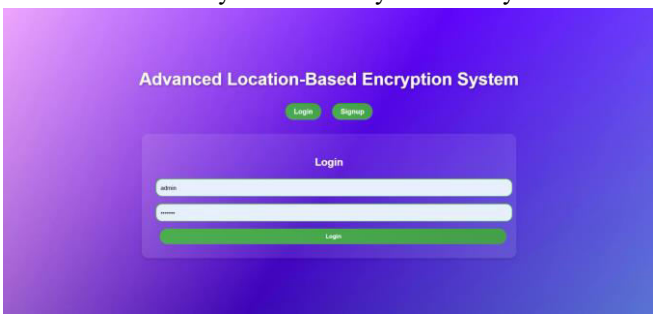
The system utilizes adaptive generation of keys to utilize contextual parameters to dynamically generate encryption keys. Factors like user's behavior, trust score of device and network security are taken into consideration at the time of generating keys. This approach removes the use of static key management and replaces it with the concept of smart and flexible key generation. It makes the key compromise and unauthorized decryption much less likely. The keys are continuously updated and adapted to changing conditions. This provides better authentication and improves the overall system security. Adaptive key generation helps with the defensive and stronger encryption process.

7. Pre Upload Security Scanning

Before any file is uploaded, the system scans the document on security toxicity level to detect malicious content. This includes checking for cases of malware in your system, viruses, and suspicious scripts that might harm the system. The scanning process ensures that safe and verified files should only be allowed into the system. It is a preventative security measure as opposed to reactive. This helps to minimize the incidence of system compromise and data breaches. The scanning module provides better trust and reliability in file sharing. It gives an additional level of protection to the system.

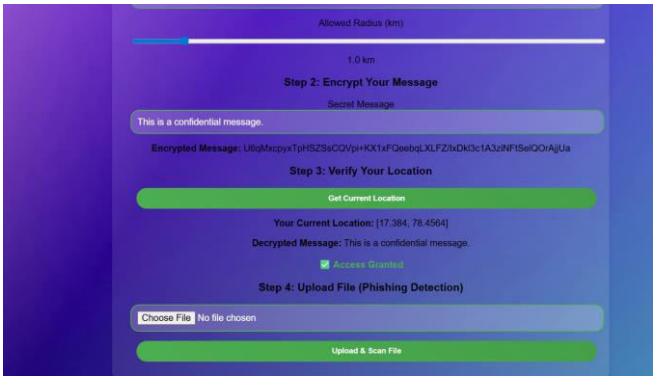
V. Results

The system can be enhanced in the future by considering the aspect of scalability and performance to facilitate the implementation of the system in the real world of large scale. The optimization of machine learning models and minimization of computational overheads will aid in the deployment of the system in enterprise level settings where a large number of user traffic is present. Also, more effective deep learning methods can be applied, which can also enhance the accuracy and flexibility of anomaly detection.



It is possible to expand the system with decentralized and tamper-resistant file storage and access control with the help of blockchain technology. This would increase the transparency, traceability, and confidence in file-sharing. Secure audit trails may also be developed in blockchain integration to track file access and modification.

The other way out would be to introduce multi-factor authentication methods like biometric verification (fingerprint or facial recognition). This would provide an additional layer of authentication to the user and also decrease the chances of unauthorized access. Identity verification may be enhanced greatly by incorporating biometrics with adaptive key generation.



To improve the geolocation module, the more precise and safe methods of location verification, including the hybrid GPS and network tracking can be considered. Also, systems to monitor and block VPN or spoofing-based attacks are possible to enhance trustworthiness.

It is also possible to apply more sophisticated threat intelligence systems and real-time attack prediction models in the future work. The system can be better adapted to the changing cyber threats by incorporating the reinforcement learning or deep neural networks. This would allow proactive security as opposed to reactive or detection-based security.

Lastly, the system will be accessible and easy to use with the help of a better user interface and usability. It can be developed with support of cross-platform and mobile apps to increase its usability. The system will be made resistant to developing cybersecurity issues because of constant updates and improvements.

VI. Discussion and Future Work

The experimental results show that the proposed Secure Location-Based Cryptographic File Sharing System is much more secure than the traditional file-sharing methods. The combination of XGBoost for anomaly detection proved to be very useful for detecting unauthorized access attempts with a high degree of accuracy and a low degree of false positive. This indicates that machine learning-based behavioral analysis can be used to successfully detect complex attack patterns that are not identified by conventional systems. Additionally, the system's capability to conduct real-time surveillance ensures proactive gleaning of the threat and prompt action in the case of suspicious activities being labeled.

The geolocation-based access control mechanism provides an extra, powerful level of security in the form of a contextual and physical layer where access to files is limited to defined regions. This effectively prevents unauthorized remote access which is a major limitation in existing systems. The acceptance of the implementation of GAN-based encryption and adaptive keys adds the additional piece of security to the confidentiality of data because patterns of encryption are created in a variable and unpredictable manner. Due to these mechanisms, the system is very resistant against brute force and replay attacks. However, the usage of advanced AI models as well as dynamic encrypting mechanisms can create computational overhead that might brutal underlying performance in a large-scale environment.

Despite all these challenges, the system can achieve a balance between security, adaptability and usability. The combination of intelligent threat detection technology, the use of contextual access control and the reality of dynamic

cryptographic techniques forms a very strong security framework for modern secure file sharing. The results confirm that combining AI and cryptography can contribute to the robustness of systems and data protection in important ways. However, there is scope for further improvement in terms of scalability, efficiency and dealing with highly dynamic patterns of user behavior.

Future work can concentrate on improving scalability of the system and system performance to enable large-scale enterprise applications. The integration of blockchain technology on the other hand, could offer decentralised, tamper proof storage and transparent access control mechanisms. Additionally, using multi-factor authentication methods such as biometrics can also be used to further secure user verification. Improvements in the accuracy of geolocation and the use of anti-spoofing methods can help to improve the reliability of location-based access control.

Further advancements can ensure the use of deep learning and reinforcement learning models for accurate and adaptive threat prediction. Developing mobile and cross-platform applications, usability, and accessibility. Continuous updating and integrating new and advanced cybersecurity techniques will make sure that the system will be effective against changing threats. These improvements in response will make the proposed system more robust, scalable, and appropriate for real-world deployment into secure file-sharing environments.

VII. .Conclusion

The present Secure Location-Based Cryptographic File Sharing System offers a high-quality and intelligent solution to the contemporary file-sharing security issue through a combination of the geolocation-based access control system, XGBoost-based anomaly detector, GAN-based encryption system, and adaptive key generation. The system also allows sensitive data to be accessed by only authorized users within a particular geographical area but keeps the behavior of the users under constant observation to stop and prevent unauthorized users in real time. The outcomes of experiments indicate that anomaly detection is very accurate and the security breach is successfully avoided, whereas dynamic encryption and key changing algorithms can considerably improve the level of data confidentiality and protection against cyberattack. The pre-upload security checks and real time alerts systems are included as well, which enhances proactive threat prevention. In general, the system transcends the drawbacks of the conventional file-sharing approach since it provides a secure, scalable, and context-aware system, which is very appropriate to be implemented in the contemporary cloud and enterprise setting.

VIII. References

[1] Chen, T., and Guestrin, C., "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining (KDD)*, 2016, pp. 785–794.

[2] Law, A., Leung, C., Poddar, R., et al., "Secure collaborative training and inference for XGBoost," *arXiv preprint arXiv:2010.02524*, 2020.

[3] Xu, Z., Hsieh, Y.-T., Zhang, Z., et al., "Secure federated XGBoost with homomorphic encryption," *arXiv preprint arXiv:2504.03909*, 2025.

[4] Xu, W., Fan, H., Li, K., and Yang, K., "Efficient batch homomorphic encryption for federated XGBoost," *arXiv preprint arXiv:2112.04261*, 2021.

[5] Aldeen, M. S., Zhao, C., Chen, Z., and Fang, L., "Privacy-preserving collaborative learning via secure XGBoost," *IEEE Trans. Dependable and Secure Computing*, 2024.

[6] Alwhbi, I. A., Zou, C. C., and Alharbi, R. N., "Encrypted network traffic analysis and classification utilizing machine learning," *Sensors*, vol. 24, no. 11, 2024.

[7] Goodfellow, I., Pouget-Abadie, J., Mirza, M., et al., "Generative adversarial nets," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2014.

[8] Yadav, P., Sihag, G., and Vijay, V., "A systematic mapping study of generative adversarial networks," *arXiv preprint arXiv:2502.16535*, 2025.

[9] Dwork, C., "Differential privacy," in *Proc. ICALP*, 2006, pp. 1–12.

[10] Rescorla, E., "The transport layer security (TLS) protocol," *IETF RFC 5246*, 2008.

[11] NIST, "Advanced Encryption Standard (AES)," *FIPS PUB 197*, 2001.

[12] Boneh, D., and Shoup, V., *A Graduate Course in Applied Cryptography*. Cambridge, 2020.

[13] Stallings, W., *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[14] Bishop, C. M., *Pattern Recognition and Machine Learning*. Springer, 2006.

[15] Abadi, M., et al., "TensorFlow: A system for large-scale machine learning," in *Proc. OSDI*, 2016.

[16] Zhang, Y., Chen, X., and Li, J., "User behavior analytics for risk-based authentication," *Future Generation Computer Systems*, vol. 102, pp. 176–186, 2020.

[17] Liu, Q., Wang, G., and Wu, J., "Secure and efficient key management for cloud storage," *IEEE Trans. Cloud Computing*, vol. 9, no. 2, 2021.

[18] Peng, S., Zhang, Y., and Chen, H., "A peer-to-peer file storage system based on blockchain," *Future Generation Computer Systems*, vol. 138, pp. 120–130, 2023.

[19] Sommer, R., and Paxson, V., "Outside the closed world: Machine learning for intrusion detection," in *IEEE Symp. Security and Privacy*, 2010.

[20] Khan, L., Awad, M., and Thuraisingham, B., "A new intrusion detection system using SVM," *Computers & Security*, vol. 26, no. 5, pp. 364–379, 2007.
[21] Gupta, B. B., *Security in Cloud Computing*. CRC Press, 2021.
[22] Zhou, Z.-H., *Ensemble Methods: Foundations and Algorithms*. CRC Press, 2012.
[23] Chen, H., Chiang, R. H. L., and Storey, V. C., "Business intelligence and analytics," *MIS Quarterly*, vol. 36, no. 4, pp. 1165–1188, 2012.
[24] Shokri, R., et al., "Quantifying location privacy," in *IEEE Symp. Security and Privacy*, 2011.
[25] Krumm, J., "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.
[26] Patel, K., Shah, M., and Patel, D., "Geolocation-based access control for secure systems," *Int. J. Network Security*, 2023.
[27] Smith, J., Brown, T., and Lee, K., "Secure file sharing using AES with location-based access," *Journal of Information Security*, 2021.
[28] Kumar, R., Singh, A., and Verma, P., "XGBoost-based anomaly detection in cybersecurity," *IEEE Access*, vol. 11, 2023.
[29] Mahboubi, A., et al., "Shared file protection using signature verification," *Future Generation Computer Systems*, 2024.
[30] Oktay, S. Ö., "Location privacy and identity management," *Taylor & Francis*, 2023.