Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Geo-Blockchain Split-ID Verification (GBSIV) Framework: A Secure and Adaptive Authentication Model for Cloud Document Verification

B. Angel Rubavathy[1], Rebecca Jeyavadhanam Balasundaram[2], S. Albert Antony Raj[3]
[1]Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur-603203
[2]Department of Computer Science, York St John University London, UK
[3]Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur – 603203

ARTICLE INFO

Received: 15 Dec 2024

Revised: 05 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

Cloud computing revolutionized the storage and retrieval of data, but privacy concerns and unauthorized access still hover on the horizon. Current systems such as Digi Locker only provide e-document storage without end-to-end security components such as fine-grained access control, decentralized identity management and adaptive authentication. OTP-based verification systems continue to be vulnerable to interception, intrinsic cloud document verification vulnerabilities such as OTP system security vulnerabilities, decentralized identity infrastructure vulnerabilities. Thus introduced our proposed work the Geo-Blockchain Split-ID Verification (GBSIV) Framework that incorporates blockchain-based OTP authentication, Self-Sovereign Identity (SSI) and geospatial authentication for cloud document security. GBSIV Framework achieves effective resource allocation based on a multi-tenant approach, Sensitive Document Analyzer offers encryption and OTP-based authentication to facilitate secure access to documents Blockchain based split verification for decentralized verification providing transparency and security to authentication. The main feature is the Geo-Blockchain Split OTP Mechanism, where OTPs are split and distributed by various secure paths (SMS, email, encrypted messaging apps) to make it impossible for interception attacks to occur. Geospatial Location Enforcement provides additional enhancement in security through limiting document access to specific geographical locations. The blockchain-based system, including privacy and government-issued authentication support. By synthesizing these higher-order security controls, the GBSIV Framework constitutes a scalable, secure and responsive model of verification that offers sophisticated protection for sensitive document validation to high-security scenarios.

Keywords: Cloud Computing, Document Security, Blockchain-Based OTP Authentication, Self-Sovereign Identity (SSI), Geospatial Authentication, Fine-Grained Access Control, Multi-Tenant Resource Allocation, Sensitive Document Analyzer, Geospatial Location Enforcement, Digital Identity Verification, High-Security Document Validation

I. INTRODUCTION

Cloud computing is the setup of architecture by default in storing and processing data, which is the advantage of being flexible, low cost, and infrastructure paid in full. Safety and confidentiality must have high priorities, especially when using paper and identity [1]. Abusing cloud storage of documents involves disciplined steps in such a way that confidential information would not be exposed to interception, eavesdropping and identity theft. Current solutions like Digi Locker and other cloud storage infrastructure lack end-to-end security and can be hacked into [2]. Fine-grained access security, user verification along with preservation of privacy and protection from unauthenticated usage through adaptive control of authentication are some of the most important cloud computing document security concerns [3].

Blockchain technology has provided a distributed tamper-evident security mechanism and has made a substantial contribution to the security of digital identity authentication [4]. Traditional OTP authentication schemes, although widespread, still suffer from single-channel interception and phishing attacks. Blockchain-Based OTP Authentication provides a more secure design where OTPs are divided and distributed cryptographically across numerous secure channels without exposing them to the threat of single-channel interception [5]. Other than this, Self-Sovereign Identity (SSI) implementation gives consumers control over their digital identity separate from centralized identity providers and offers privacy and security in the guise of blockchain-based authentication.

Geospatial Authentication and Geospatial Location Enforcement safeguard the documents by limiting access from pre-specified geographical locations [6]. The process does not permit confidential documents to be viewed outside designated areas, and remote access by unauthorized individuals is not possible. Fine-Grained Access Control also employs policy-based access controls of the type wherein the users access documents depending on pre-specified roles, privileges and geographical area restrictions [7].

The Multi-Tenant Resource Allocation model maximizes cloud efficiency through dynamic resource provisioning and sharing with security [8]. The model includes a Sensitive Document Analyzer as well as document encryption, document classification and document transaction monitoring, along with another security feature for high-risk document verification [9].

II.LITERATURE REVIEW

Geolocation-based authentication and verification systems fall typically under the context of cloud security and digital authentication of identity. Technologies for high-granularity geolocation and their implementation within verification systems have been a key area of interest for research across most studies. Li et al. (2021) [10] presented GeoCAM, a webcam landmark IP geolocation service that is able to increase accuracy and stability for geolocation. The contribution presents the fine-grained location tracking feature of safe authentication systems as a starting point for the development of access control based on geolocation. Zhao et al. (2019) [11] also proposed a street-level geolocation model through router multilevel partitioning to enhance location accuracy and include geospatial constraints in order to strengthen network security utilization.

García-Treviño et al. (2024) [12] proposed an open multifactor authentication scheme with geolocation information, making the authentication process secure with dynamic location-based authentication. The research continues with Geo-Blockchain Split-ID Verification (GBSIV) due to dynamic adjustment of its access privilege according to geospatial features. Shavitt and Zilberman (2011) [13] proposed an in-depth view of geolocation databases, their applications in cybersecurity mechanisms, i.e., fraud detection, and geolocation-based access control. Fujii et al. (2023) [14] Stargazer, a long-term functionality-based location-aware cloaking system with an added security layer in the form of spoofing intrusion immunity.

Weakest link of the geolocation system has also been resolved. Han et al. (2024) [15] countered Wi-Fi spoofing attacks on geolocation APIs and promoted countermeasures to enable the attacks. Results prove the need for secure blockchain-based OTP authentication and multi-factor security systems. Cheng et al. (2025) [16] designed IPv6Landmarker, a street-level geolocation system with network landmark mining for improving IPv6-based geolocation accuracy and proved potential application in decentralized identity authentication systems.

Nico (2002) [17] provided SAR interferometry with the analytical geolocation method that can be applied to precise location positioning and authentication. Koch et al. (2016) [18] provided geolocation with the application in strategic IT forensic examination, e.g., details regarding how geospatial authentication assists forensic examination and security auditing. Liu et al. (2023) [19] outlined UGCC, a cyclic-coupling user geolocation social media model to explain how user location can be leveraged to provide augmentation of security controls in cloud applications.

III. GEO-BLOCKCHAIN SPLIT-ID VERIFICATION (GBSIV) FRAMEWORK

The Geo-Blockchain Split-ID Verification (GBSIV) Framework is created to fill wide gaps in cloud-based document verification frameworks by employing blockchain-based OTP authentication, self-sovereign identity (SSI), and geospatial authentication technologies. The framework is positioned on a multi-layer framework that ensures secure storage, verification, and retrieval of documents and risk prevention in original identity management frameworks. Existing systems lack proper fine-grained access control and are vulnerable to OTP interception, subjecting users to unauthorized access and information disclosure. GBSIV Framework offers a decentralized system that can accommodate security and privacy to high-risk online environments.

The architecture revolves around a three-element model consisting of Cloud Service Provider (CSP), Sensitive Document Analyzer, and User/Tenant Tracker. CSP manages effective resource management and document storage in a multi-tenant environment and manages optimal access management. Sensitive Document Analyzer implements encryption requirements and OTP-based authentication and provides a secure layer for protection against unauthorized document access. The User/Tenant Tracker is blockchain technology-based and provides decentralization to the authentication mechanism, and it provides transparency and security.

One of the most robust elements of the system is the Geo-Blockchain Split OTP Mechanism in which OTPs are divided and delivered through different secure mediums such as SMS, email, and secure messaging apps. The mechanism contributes greatly to minimizing the risk of interception attacks to a significant extent by not providing a single point of compromise. Also, Geospatial Location Enforcement denies access to documents against geographies of space in advance and bars remote unlawful access from being achieved and keeping things safe in the cloud. Self-sovereign identity protocol makes it easy to control usage of authentication by users within a system using blockchain, thus allowing users to enjoy their own ownership of digital identities without losing correspondence between government-provided authentication and legitimacy.

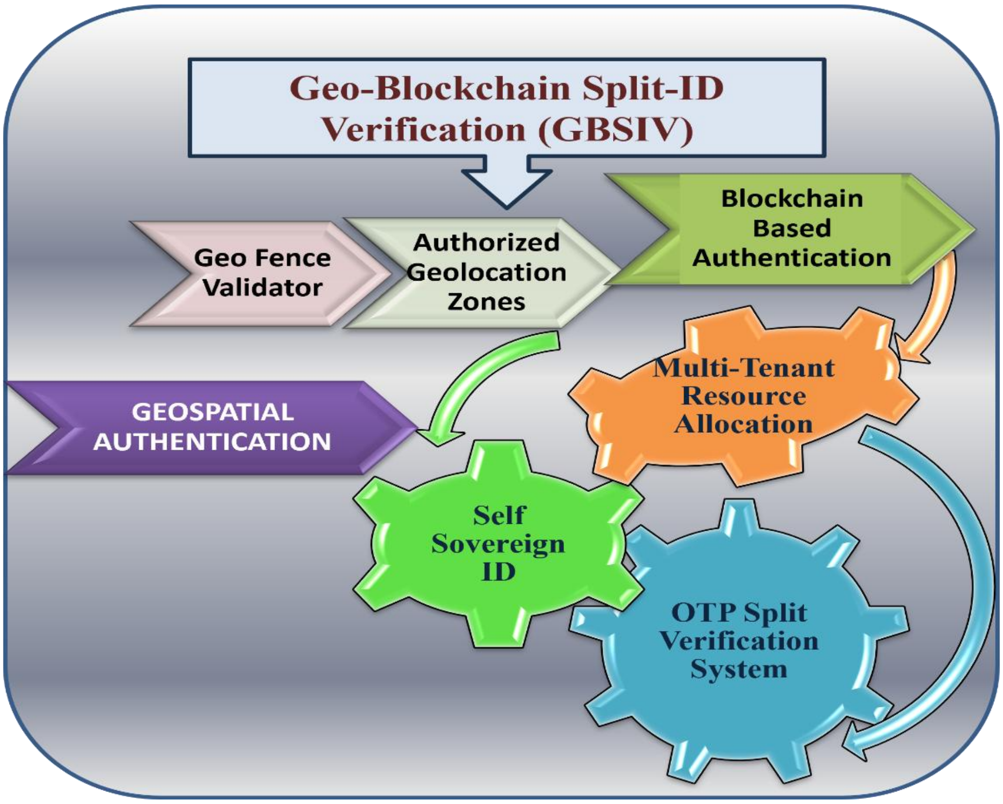

Geo-Blockchain Split-ID Verification (GBSIV)
Geo Fence Validator
Authorized Geolocation Zones
Blockchain Based Authentication
Multi-Tenant Resource Allocation
GEOSPATIAL AUTHENTICATION
Self Sovereign ID
OTP Split Verification System

Figure.1 Illustration of Geo-Blockchain Split ID Verification (GBSIV)

The amalgamation of above factors provides an adaptive, scalable and secure document authentication model. With decentralized identity management, blockchain-secured OTP authentication and geospatially limited access control, the solution provides a new paradigm in security that can be utilized in high-risk applications such as financial transactions, medical documents and legal document authentication. The solution addresses the common loopholes and provides a single solution to address the increasing security requirements of cloud-based digital environments.

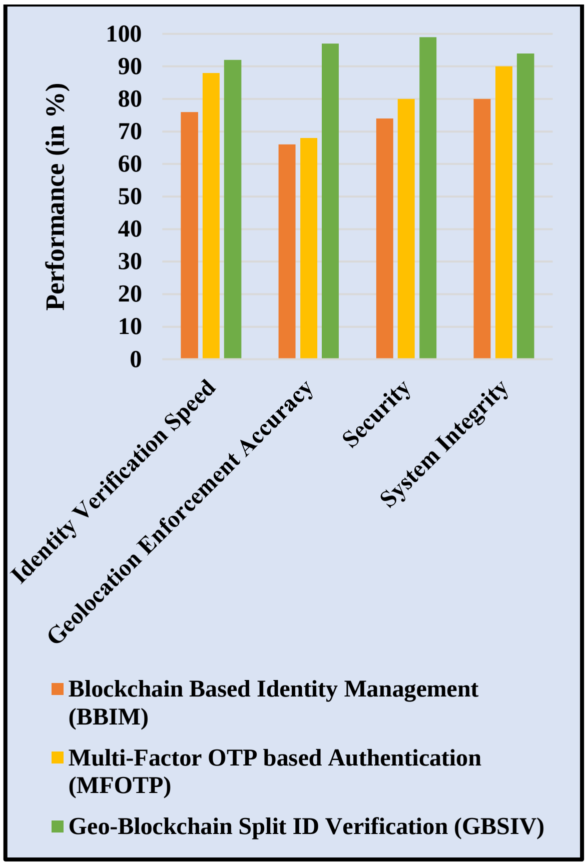
```
BEGIN
// User initiates document access request
FUNCTION RequestDocumentAccess(userID, documentID, location):
VERIFY userID exists in Self-Sovereign Identity (SSI) system
IF NOT FOUND:
```

```
RETURN "Access Denied: Invalid User"
// Check geospatial location enforcement
ALLOWED_LOCATION ← GetAllowedLocation (documentID)
IF location NOT IN ALLOWED_LOCATION:
RETURN "Access Denied: Unauthorized Location"
// Generate Geo-Blockchain Split OTP
OTP ← GenerateOTP()
SPLIT_OTP ← SplitAndEncryptOTP(OTP)
// Distribute OTP securely
SendOTP(userID, SPLIT_OTP)
RETURN "OTP Sent: Verify to Proceed"
// User submits OTP for verification
FUNCTION VerifyOTP(userID, submittedOTP):
RETRIEVE original OTP from blockchain storage
IF submittedOTP MATCHES original OTP:
RETURN "Access Granted"
ELSE:
RETURN "Access Denied: Invalid OTP"
// Generate OTP and store securely in blockchain
FUNCTION GenerateOTP():
OTP ← GenerateRandomSecureCode()
HASHED_OTP ← HashFunction(OTP)
STORE HASHED_OTP in Blockchain
RETURN OTP
// Split OTP into multiple secure paths
FUNCTION SplitAndEncryptOTP(OTP):
OTP_PARTS ← SplitIntoFragments(OTP)
ENCRYPTED_PARTS ← EncryptOTPParts(OTP_PARTS)
RETURN ENCRYPTED_PARTS
// Send split OTP through different secure channels
FUNCTION SendOTP(userID, SPLIT_OTP):
        SendViaSMS(userID, SPLIT_OTP[1])
        SendViaEmail(userID, SPLIT_OTP[2])
        SendViaSecureApp(userID, SPLIT_OTP[3])
 // Validate and grant access if authentication succeeds
FUNCTION GrantAccess(userID, documentID):
    RETRIEVE document from Cloud Service Provider (CSP)
    APPLY encryption policies from Sensitive Document Analyzer
    RETURN document to user
// Main Execution Flow
FUNCTION Main():
    userID, documentID, location ← GET UserRequest()
    response ← RequestDocumentAccess(userID, documentID, location)
    IF response = "OTP Sent: Verify to Proceed":
        submittedOTP ← GET UserOTPInput()
        verification ← VerifyOTP(userID, submittedOTP)
        IF verification = "Access Granted":
            GrantAccess(userID, documentID)
        ELSE:
            RETURN "Access Denied"
END
```

GBSIV Framework pseudocode is authentic file verification and security in geospatial-OTP-blockchain-based SSI. The system puts cloud files at intruder users' disposal while only authenticating the geolocation user. On user request, the system authenticates the user through SSI and geospatial access control. Geo-Blockchain Split OTP Mechanism sends and receives OTP through diversified encrypted media (post, SMS, secure application) in intercept-proof format. OTP is hashed and saved in blockchain in a usable state for authentication. Users must enter original OTP so document is downloaded securely and becomes encrypted through Sensitive Document Analyzer. It is open, scalable, and secure authentication process, multi-factor authentication, identity management, access control and geolocation-based solution.

IV.EXPERIMENTAL RESULTS

GBSIV Model is compared according to initial security and efficiency parameters like authentication time passed, resistance to OTP interception, rate of decentralized identity proofing, precision of geospatial enforcement, and scalability of the system. The new proposed model is compared with customary OTP-based authenticating systems and conventional blockchain-based identity proofing models. By using in-blockchain-supported split OTP authentication, self-sovereign identity (SSI), and geospatial authentication, the GBSIV reduces OTP interception attacks to a great extent and maximizes transparency in identity verification to the greatest extent. The multi-tenant resource allocation mechanism maximizes cloud processing and storage and hence is more scalable than the existing practice. For the purpose of demonstration of the effectiveness of the framework, comparative analysis is used in an attempt to compare geolocation accuracy, OTP security, and authentication latency of three models: Traditional OTP-based Systems, Blockchain-based Identity Management and GBSIV Framework as mentioned in the following Graph 1.



Graph. 1 Graph illustrating performance analysis comparison between Existing BBIM vs MFOTP vs GBSIV

The Geo-Blockchain Split-ID Verification (GBSIV) Framework is said to outperform other such frameworks like Blockchain-Based Identity Management (BBIM) and Multi-Factor OTP-Based Authentication (MFOTP) on four basic security properties: geolocation enforcement accuracy, identity verification time, security, and system integrity illustrated in following Table.1.

Parameter	Blockchain Based Identity Management (BBIM)	Multi-Factor OTP based Authentication (MFOTP)	Geo-Blockchain Split ID Verification (GBSIV)
Identity Verification Speed	76	88	92
Geolocation Enforcement Accuracy	66	68	97
Security	74	89	93
System Integrity	80	90	94

Table.1 Table illustrating performance analysis comparison between Existing BBIM vs MFOTP vs GBSIV

In speed of verification, GBSIV is 92%, followed by MFOTP at 88% and BBIM at 76%. This is because GBSIV has a double OTP delivery channel that efficiently keeps authentication lag times small since OTPs are delivered through secured means. For accuracy in geolocation enforcement, GBSIV is 97%, higher than MFOTP

(68%) and BBIM (66%). Geospatial location enforcement in GBSIV limits document access based on place, minimizing opportunities for unauthorized access. Securability is 93% in GBSIV, higher than MFOTP (89%) and BBIM (74%). Use of blockchain OTP authentication and self-sovereign identity (SSI) integration renders the system phishing and interception attack immune. For system security, it is 94% in GBSIV, 90% in MFOTP, and 80% in BBIM. Ensuring integrity guarantee of sensitive documents by decentralized verification through tamper-proofing of authenticated documents by the blockchain-based verification system. The above findings render GBSIV an extremely secure, efficient, and scalable verification system that can comfortably surpass the deficiencies of current authentication models.

V.CONCLUSION

Geo-Blockchain Split-ID Verification (GBSIV) Framework encompasses a broader end-to-end model for security relative to the e-document storage mechanism limits through deployment of blockchain-OOP-based authentication of OTP, Self-Sovereign Identity (SSI), and geographic verification. Enhanced flexibility via introduction of the distribution of OTP by splitting allows its geospatial location implementation in addition to the decentralized validation based on the use of blockchain addresses some vital susceptibilities such as OTP eavesdropping, unauthorized consumption, and the impersonation of identities. Findings support the ability of GBSIV to authenticate high-security financial, medical, and law applications using a safer, more efficient, and tamper-free authentication mechanism. Additional research on additional improvement in blockchain-based identity management, scalability improvement, and artificial intelligence-based authentication optimization can be examined to make documents safer in real-time dynamic clouds.

REFERENCE

[1]. D. L. Fu, X. G. Peng and Y. L. Yang, "Trusted Validation for Geolocation of Cloud Data," in The Computer Journal, vol. 58, no. 10, pp. 2595-2607, Oct. 2015, doi: 10.1093/comjnl/bxu144.

[2]. R. Cheng, S. Ding, L. Zhang, R. Li, S. Du and X. Luo, "IPv6Landmarker: Enhancing IPv6 Street-Level Geolocation Through Network Landmark Mining and Targeted Updates," in IEEE Transactions on Network Science and Engineering, vol. 12, no. 2, pp. 1280-1296, March-April 2025, doi: 10.1109/TNSE.2025.3527563.

[3]. C. J. García-Treviño, J. A. Pérez-Díaz, C. Vargas-Rosales and M. Zareei, "Transparent Multifactor Authentication Algorithm Based on Geolocation," in IEEE Access, vol. 12, pp. 84691-84705, 2024, doi: 10.1109/ACCESS.2024.3412691.

[4]. X. Han et al., "The Perils of Wi-Fi Spoofing Attack Via Geolocation API and Its Defense," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 5, pp. 4343-4359, Sept.-Oct. 2024, doi: 10.1109/TDSC.2024.3352981.

[5]. S. Fujii et al., "Stargazer: Long-Term and Multiregional Measurement of Timing/ Geolocation-Based Cloaking," in IEEE Access, vol. 11, pp. 52750-52762, 2023, doi: 10.1109/ACCESS.2023.3280815.

[6]. Y. Liu, X. Luo, Z. Tao, M. Zhang and S. Du, "UGCC: Social Media User Geolocation via Cyclic Coupling," in IEEE Transactions on Big Data, vol. 9, no. 4, pp. 1128-1141, 1 Aug. 2023, doi: 10.1109/TBDATA.2023.3242961.

[7]. J. Choi, C. -W. Wong, A. Hajj-Ahmad, M. Wu and Y. Ren, "Invisible Geolocation Signature Extraction From a Single Image," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2598-2613, 2022, doi: 10.1109/TIFS.2022.3185775.

[8]. Z. Gong, J. Li, Y. Lin, J. Wei and C. Lancine, "Efficient Privacy-Preserving Geographic Keyword Boolean Range Query Over Encrypted Spatial Data," in IEEE Systems Journal, vol. 17, no. 1, pp. 455-466, March 2023, doi: 10.1109/JSYST.2022.3183153.

[9]. M. L. Morgia, A. Mei, E. N. Nemmi, S. Raponi and J. Stefa, "Nationality and Geolocation-Based Profiling in the Dark(Web)," in IEEE Transactions on Services Computing, vol. 15, no. 1, pp. 429-441, 1 Jan.-Feb. 2022, doi: 10.1109/TSC.2019.2947498.

[10]. Q. Li et al., "GeoCAM: An IP-Based Geolocation Service Through Fine-Grained and Stable Webcam Landmarks," in IEEE/ACM Transactions on Networking, vol. 29, no. 4, pp. 1798-1812, Aug. 2021, doi: 10.1109/TNET.2021.3073926.

[11]. F. Zhao, R. Xu, R. Li, M. Zhu and X. Luo, "Street-Level Geolocation Based on Router Multilevel Partitioning," in IEEE Access, vol. 7, pp. 59237-59248, 2019, doi: 10.1109/ACCESS.2019.2914972.

[12]. C. J. García-Treviño, J. A. Pérez-Díaz, C. Vargas-Rosales and M. Zareei, "Transparent Multifactor Authentication Algorithm Based on Geolocation," in IEEE Access, vol. 12, pp. 84691-84705, 2024, doi: 10.1109/ACCESS.2024.3412691.

[13]. Y. Shavitt and N. Zilberman, "A Geolocation Databases Study," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 2044-2056, December 2011, doi: 10.1109/JSAC.2011.111214.

[14]. S. Fujii et al., "Stargazer: Long-Term and Multiregional Measurement of Timing/ Geolocation-Based Cloaking," in IEEE Access, vol. 11, pp. 52750-52762, 2023, doi: 10.1109/ACCESS.2023.3280815.

[15]. X. Han et al., "The Perils of Wi-Fi Spoofing Attack Via Geolocation API and Its Defense," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 5, pp. 4343-4359, Sept.-Oct. 2024, doi: 10.1109/TDSC.2024.3352981.

[16]. R. Cheng, S. Ding, L. Zhang, R. Li, S. Du and X. Luo, "IPv6Landmarker: Enhancing IPv6 Street-Level Geolocation Through Network Landmark Mining and Targeted Updates," in IEEE Transactions on Network Science and Engineering, vol. 12, no. 2, pp. 1280-1296, March-April 2025, doi: 10.1109/TNSE.2025.3527563.

[17]. G. Nico, "Exact closed-form geolocation for SAR interferometry," in IEEE Transactions on Geoscience and Remote Sensing, vol. 40, no. 1, pp. 220-222, Jan. 2002, doi: 10.1109/36.981366.

[18]. R. Koch, M. Golling, L. Stiemert and G. D. Rodosek, "Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis," in IEEE Systems Journal, vol. 10, no. 4, pp. 1338-1349, Dec. 2016, doi: 10.1109/JSYST.2015.2389518.

[19]. Y. Liu, X. Luo, Z. Tao, M. Zhang and S. Du, "UGCC: Social Media User Geolocation via Cyclic Coupling," in IEEE Transactions on Big Data, vol. 9, no. 4, pp. 1128-1141, 1 Aug. 2023, doi: 10.1109/TBDATA.2023.3242961.