Advanced Location-Driven Authentication Protocols in Mobile Computing Environments

Robina Safi[1], Farhan Nisar[2]
[1]Department of Computer Science, Abasyn University, Pakistan
[2]Department of Computer Science, Qurtaba University, Pakistan
*Correspondence: robinasafi223@gmail.com, farhansnisar@yahoo.com

Citation | Safi. R, Nisar. F, "Enhancing Teacher Resilience: Innovative Coping Strategies for Flood Vulnerabilities", IJIST Vol. 08 Issue. 01 pp 320-328, February 2026
Received| January 01, 2026 **Revised|** February 02, 2026 **Accepted|** February 05, 2026 **Published|** February 08, 2026.

Mobile devices have evolved into indispensable instruments of contemporary life, fundamentally transforming the manner in which individuals interact with digital services. The proliferation of smartphones has significantly streamlined access to internet-based applications, fostering unprecedented levels of connectivity and convenience. Modern smartphones are equipped with sophisticated technologies, including Location-Based Services (LBS) such as the Global Positioning System (GPS), enabling enhanced contextual awareness and spatial intelligence. While smartphones serve as seamless gateways to digital ecosystems, they simultaneously introduce critical security vulnerabilities, particularly in the domain of authentication. As primary repositories of sensitive and confidential information—Given the pervasive reliance on mobile technologies, ensuring robust authentication mechanisms has become a strategic imperative. Location-based authentication emerges as a promising paradigm that leverages geospatial data to validate user legitimacy. Authentication, being a foundational pillar of cybersecurity architecture, must therefore be reinforced through adaptive and context-aware mechanisms integrated within mobile platforms.

Keywords: GPS; Smartphones 4G/5G; authentication; location-based services; Security

Introduction:

This paper aims to conduct a comprehensive survey of existing methodologies that utilize location services for user authentication. It seeks to systematically examine, analyze, and synthesize the diverse approaches proposed in the literature, highlighting their strengths, limitations, and practical implications for enhancing mobile security infrastructures. tokens, smart cards; (c) what you are, e.g., biometrics like fingerprints, face recognition, palm recognition [1], as shown in Table 1

There are many existing systems that use location information to provide solutions for authentication and authorization problems. These systems require a setup, large infrastructures, and specially designed devices. Another commonly used method is biometrics, in which a user provides their identity using a physical feature.

We combine these two methods to implement our proposed approach. [2].

Table 1. Authentication methods and definitions

Methods	Procedure
Passwords	A secret combination of characters that can be used several times for login
One-time Passwords	Passwords that are to be used only once
Biometrics	Proves a user's identity by physical features like fingerprints, face recognition
Location-Based	The user located in a specific location is authorized.
Two-factor Authentication	A combination of two types of authentication methods
Smart cards	Tamper-resistant hardware that communicates with the computer directly.

Location-Based Authentication:

Authentication can be defined as the process of accurately identifying entities (i.e., users). Location-based authentication can be defined as a process of proving a user's identity and authenticity with the help of location detection. Location-based authentication has three factors: (a) the individual who wants to be authenticated must provide a sign of identification; (b) the user must have at least one human authentication factor that can be identified even at a distinct location; (c) the distinct location must have a mechanism to determine the presence of the user at that location.

Privacy Issues:

Privacy is defined differently by each individual, and it is difficult to define. Privacy is not limited to human beings; it can also apply to websites. According to the definition of location-based privacy by Beresford and F. Stajano, it is "the ability to prevent other parties from learning one's past or current location." Personal privacy can be categorized into four different types: (a) Information Privacy; (b) Bodily Privacy; (c) Privacy of Communication; (d) Territorial Privacy [2].

Some of the privacy-related issues are:

What determines when users are notified that their location-based system is turned on or off? Can it be an opt-in or opt-out approach?

Should the information stored be personally identifiable?

Should there be an information retention period?

Can users choose to what extent their information is personalized?

What legal laws apply to the users?

What level of disclosure is allowed?

Privacy Challenges: Security and privacy are considered the same by many people [2]. Security is the action, and privacy is the result of a successful action. The first challenge in

location-based systems is understanding location-based vulnerabilities, such as leaked personal information from services, including current location or any personal identification details, which can lead to significant problems for users and services in general.

A user's current location and some identifying details can help hackers track the movements of a user and, in some cases, gain access to the user's vehicles in the context of location-based services.

Usage of Location-Based Authentication in Services:

Location-based authentication systems are implemented in real time. Products like iPhone, Android, and Visa payment systems use this method for authentication. iPhone has recently launched a new method to provide security based on the location of the device. Different security tolerances can be applied depending on the device's location. For example, if the device is being used at home, it may not require a high level of security; similarly, if the device is used outside, it requires a higher level of security. Mobile phones can be provisioned with tokens, enabling applications to be authenticated through various methods such as over-the-air (OTA), Bluetooth, SMS requests, etc.

Launch Key is one of the leading providers in this field. It offers password-free logins securely using a phone, along with security policies, user provisioning, security fencing, analytics, and more. Its products can secure any internet-connected application. A mobile app can serve as an authenticator. If a service adopts these products, the user can log in without a password and receive real-time authorization.

Location-Based Authentication v/s Location-Based Services:

Program-level services that use location data to control specific features can be called location-based services. Location-based services can be used in social networking sites, vehicle tracking, mobile commerce, emergency services, and informational services. They generally rely on control-plane locating, GSM localization, or self-reported positioning protocols as locating methods. Typically, the service provider's infrastructure determines the user's location and responds to requests accordingly.

For example, when a user wants to locate the nearest eatery, the system must determine the user's location and match it with pre-existing information about eateries in that area.

Location-based authentication, in contrast, is used to authenticate users for login or access to certain resources based on location.

Current Approaches:

Recently, there has been significant research in this field, including discussions of privacy issues and the challenges faced by system designers in providing user interfaces that respect privacy. Many different methods have been proposed, but most require special devices and installations. Here we will discuss the various methods proposed in the field of location-based services. Internet connectivity and the availability of smartphones have enabled users to spend significant time online, irrespective of place and time. This has created a considerable challenge for service providers in authenticating users.

Generation of Questions:

One of the systems implemented generates authentication questions based on the user's location, tracked by smartphones. Location-based profiles are built for all users based on data periodically collected, such as the Wi-Fi access points the user connects to. This method was tested on 14 individuals, some in sets of two and others individually. The user is presented with two sets of questions: one based on the user's own data and the other chosen randomly [3].

This method implements an algorithm based on a Bayesian classifier to authenticate legitimate users. The first step in this implementation is to calculate the user's score for every

authentication session. Every incorrect option is penalized to prevent users from attempting to compromise the system. The following formulas are used: (1)

$$\text{Scoreq1} = (P \times \text{Lcorrect}) - (P \times (S - \text{Lcorrect}))$$
$$\text{Scoreq2} = ((P \times \text{Ocorrect}) - (P \times (S - \text{Ocorrect}))$$
$$\text{Scoreq3} = ((P \times \text{Tcorrect}) - (P \times (S - \text{Tcorrect})) \quad (1)$$

Here Lcorrect is the number of locations answered correctly Ocorrect is the number of locations ordered correctly, TcorrectT_{\text{correct}}Tcorrect is the number of correctly answered time ranges, and SSS is the number of selected locations [3].

OTP:

Another popular method used by many online services is the use of One-Time Passwords (OTP). Services such as banking, online transactions, and chatting websites use OTPs to authenticate users. Modern chatting applications like WhatsApp, Hike, and WeChat require the user to enter an OTP before accessing the application to ensure that only the authorized user with the given phone number can use it. A volatile password reduces the risk of passwords being stolen, shoulder surfing, phishing, etc. [4]. GPS is now precise, which helps implement this method without any significant issues. This method is comparatively easier to implement than other methods.

This approach requires only the built-in GPS and no special designs or interfaces, making it cost-effective. OTPs are generated based on time and location, which makes it difficult for hackers to determine the exact details. In case of a misjudgment where a legitimate user is denied access, SMS can be used as a fallback. The following procedure is followed (see Table 2 for notations):

$$\text{Skey (Pkey (IMSI}||\text{OTP))} \rightarrow \text{IMSI}||\text{OTP} \rightarrow \text{OTP} \rightarrow f(\text{OTP}) \rightarrow T, (x,y)$$

Table 2. Notations

PKey	Public key
SKey	Secret Key
IMSI	International Mobile Subscriber Identity
||	Concatenation

Policy Beacon:

A small device called a policy beacon is placed in an area to define a boundary within which the policy is in effect and can be used by mobile devices. If mobile devices are equipped with the policy beacon protocol, they will be able to sense the active policy beacons in that area. The footprint of the beacon's communication signal determines whether the device is within the vicinity or outside it. The Policy Beacon authentication mechanism checks the proximity of the policy beacon on a mobile device. If a device can be detected and verified, it is considered successful.

It has the following disadvantage:

Policy settings may affect the availability of functionality on mobile devices.

Two-Factor Authentication:

This method follows two-factor authentication, meaning it combines two different authentication mechanisms. Here, location and biometrics are combined. GPS tracking is used to determine the location of a particular user. GPS provides longitude and latitude coordinates and sends them to the local server for authentication [5]. A fingerprint is used as the biometric factor. A fingerprint identification algorithm is applied, and encryption is used for data exchange after authentication.

Drawbacks:

Location Registration:

This protocol has a two-level implementation. In the first level, a registration algorithm is used. Registration by users is allowed only once when the user joins the system. The next level is authentication, which is performed for every session, unlike the registration phase. In this protocol, two types of location information are used: static and dynamic. Static location information represents the standard/static location captured during registration and stored in a location-based ID database. This information does not change unless the user explicitly updates it. Dynamic location information is gathered when the user requests authentication. The authentication server sends challenges to the user when they attempt to access the system.

The user responds to the challenge by providing security credentials. Upon successful validation, the authentication server sends a location verification request to the location-based client application residing on the user's smartphone. The user is prompted to enter a PIN, which is then sent to the location-based ID database with encryption applied. The location authorization policy sends the result to the server, and finally, the authentication server authenticates the user [6].

Disadvantages of the protocol are:

The PIN can be stolen.

Security credentials provided by the user can also be stolen.

Best Approach:

As there are various methods to implement location-based authentication using smartphones, it is important to consider the advantages and disadvantages of each method. Another method is based on question generation [7]. However, the biggest disadvantage is that anyone can pretend to be the user and answer the questions. As proper identification details are not available, others can act as authorized users. Nevertheless, this method employs strong encryption techniques.

Typically, OTPs can be generated using physical It is assumed that all users are already registered with the application server. [8] We also assume that the mobile device clock and the application server clock are synchronized [9]. After the mobile device initiates the process and provides its location and time, the information is recorded on the server.

Phase I: Location and Time-Based Authentication:

Step 1: The mobile device is initiated by the user, then it sends the current time T0T_0T0, IMSI, and location LLL to the server [10]. Location L (X0, Y0), L (X_0, Y_0) L (X0, Y0) and time are sent to the application server, and the data is recorded in the database, as shown in Figure 1.

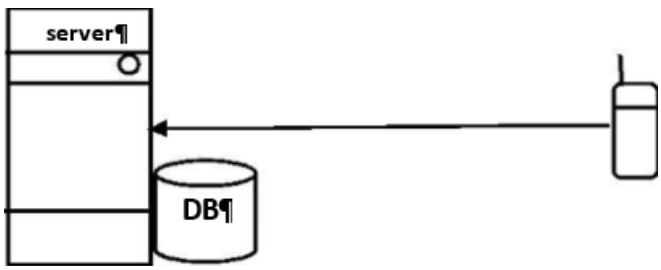

Figure 1. Mobile sends IMSI, Location L, and time t0, encrypted by public key, to the server

Mobile phone:

Step 2: After a time period, the new time T1T_1T1 and location L (X1, Y1) L (X_1, Y_1) L (X1, Y1) are sent by the mobile device to the application server, which stores them in the database.

Step 3: The server calculates the velocity of the mobile device using the following formula (2):

$$V=\sqrt{(X1-X0/T1-T0)^2 + (Y1- Y0 / T1- T0)^2} \quad (2)$$

Step 4: By referring to the statistics in [4], it is possible to predict the future moving direction and the future location of the mobile device.

Step 5: The distance ddd can be derived from Steps 3 and 4, as shown in (3):

$$d = Vt \times \Delta T \quad (3)$$

Based on the algorithm given in [4], a line is drawn through the two locations L(X0, Y0)L(X_0, Y_0)L(X_0, Y_0) and L1(X1, Y1)L_1(X_1, Y_1)L1(X_1, Y_1). The line has the formula y=ax+by = ax + by=ax+b. This equation is used to calculate aaa and bbb, as shown in (4):

$$a= \ Y1-Y0 \ / \ X1-X0, X1 \neq X0 \ (4) \ b= \ X1Y0 \ - X0Y1 \ / \ X1-X0$$

An equilateral triangle is constructed with one vertex at (X1, Y1) (X1, Y1) and its center located on line lll. The edge length of the equilateral triangle is ddd. The coordinates of the triangle's center (X, Y) (X, Y) (X, Y) are calculated using the formula shown in (5). Probable directions are then estimated, as illustrated in Figure. 2. Location and time will be encrypted using the public key, and

$$\frac{C\,X\,X\,1}{3\,d \quad X1\,X0}$$

$$3 \quad |\,X1\,X0\,|\cos(\arctan(|\,a\,|)) \quad \textbf{(5)}$$

Then, the encrypted data will be sent to the server. Upon receiving the encrypted message, the server decrypts it using the secret key [4].

In the next phase, a hash function is used to:

$$\frac{C\,Y\,Y\,1}{3\,d \quad Y1\,Y0}$$

$$6 \quad |\,Y1\,Y0\,|$$

sin (arctan (a)), Generate the OTP. If there is a failure to authenticate a legitimate user, an SMS is sent.[11] A circle is drawn to contain the equilateral triangle, sharing the same center (C_X, C_Y). This provides the predicted future location.

Step 6: By using the location received from the GPS and the current time, the OTP is generated when the user wants to log in to the application server.

Step 7: The OTP and IMSI are encrypted together using the public key and are sent to the server.

Step 8: The encrypted message received by the server is decrypted using the shared key. The location L (X, Y) L (X, Y) L (X, Y) is extracted by the server along with the OTP from the message. Time is extracted from the inverse function (f).

Step 9: The server then checks whether the location coordinates (X, Y) (X, Y) (X, Y) are within the tolerance distance. If the coordinates match, the user is authenticated; otherwise, access is denied.

Phase II: Supplementary SMS-Based Mutual Authentication

In cases where the coordinates are not within the tolerance distance, or if Phase I fails, [12] SMS-based authentication is used to ensure that a genuine user can log in.

Step 1: The user is assumed to be already registered in the system before requesting login. A smart card is inserted into the mobile phone, which allows the user to request and receive the OTP. As the user already has an account, they also possess the password.

Step 2: Meanwhile, the system selects two large prime numbers and computes modulo (p).

Step 3: When the user requires an OTP, they insert the smart card into the mobile phone, enter account details, the password, and a large prime number less than p−1p-1p−1. The system acquires the timestamp.[13] An XOR operation is performed, and value CCC is calculated. The device then sends the message M (timestamp, account details, C)

M(\text{timestamp}, \text {account details}, C) M (timestamp, account details) via SMS to the server.

Step 4: If the timestamp has already been used [14], the request is terminated. The account details entered by the user are matched with those in the authentication database. The server then selects another prime number (y) less than p−1 and sends it to the device via SMS.

Step 5: The device checks whether the sent timestamp matches the stored timestamp. If not, an error message is generated [15][16].

Step 6: The mobile device computes the OTP.

Step 7: The OTP is input to the server.

Step 8: The server verifies whether the received OTP and timestamp match the stored OTP and timestamp.

Step 9: If both fields match, the user is authenticated.

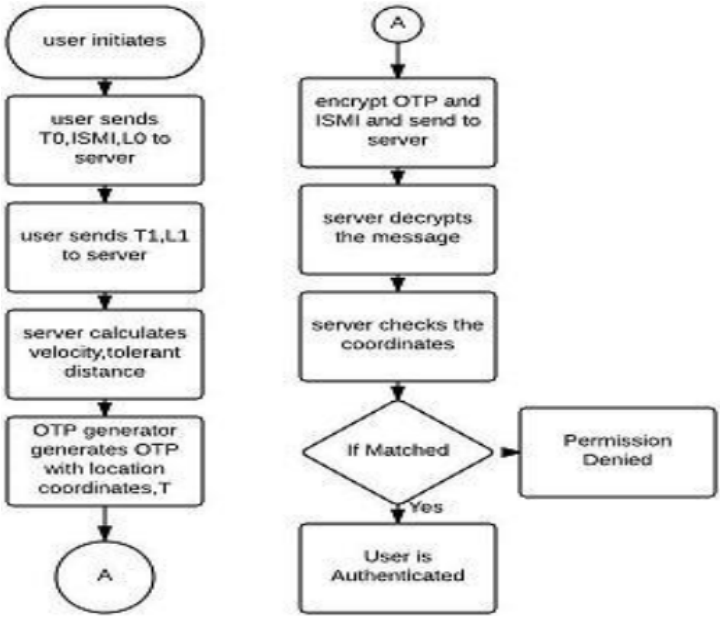

Figure 2. Phase I Flow Chart

Advantages:

The OTP mechanism is a highly effective method for authenticating users based on location. The advantages of this method are:

Due to its volatile nature, it is difficult for hackers to obtain the information.

It provides not only time-dependent but also location-dependent OTPs, making it nearly impossible for a hacker to predict the exact location [17]; the OTP cannot be reused.

To improve precision, the method uses developed statistical techniques.

Table 3. Mobile encrypted by public key, to the server

	Traditional Authentication System	OTP system
Inputting Accounts and Passwords	Required	Not necessary
User Behaviour Dependent	No	Yes
Passwords Lifetime	Permanent	Volatile
Vulnerability to being Attacked	High	Low

Different Implementations of OTP:

Time-Based Mechanism: An OTP, once generated, [18][19] is valid for a specific period of time.

Event-Based Mechanism: An OTP, once generated, is valid for a certain period of time only if specific conditions are met.

Time and Event-Driven Mechanism: A combination of both time-based and event-based mechanisms.

Security Conditions:

The event condition specified in the above-described OTP approach is the tolerant area. Mimicking the user's velocity and exact behavior is extremely difficult.[20][21] Table 4 provides a comparative view of the security value of the OTP method relative to existing methods.

Table 4. Security Comparison

Protocol	Kerberos	S/KEY OTP	Best approach protocol (OTP)
Replay Attack	√	√	√
Eavesdropping Attack	Ŏ	√	√
Dictionary Attack	×	√	√
Brute Force Attack	×	Ŏ	√
Man-in-the Middle Attack	×	×	√
User Impersonation Attack	Ŏ	√	√

Notations: √-satisfies, ×-not satisfied, ŏ-partially satisfied

Conclusion:

Location-based authentication systems have helped reduce security and privacy concerns. The Europay, MasterCard, and Visa (EMV) Chip Authentication Program has been using these protocols. Most of these protocols are time-constrained. .

We also reviewed the application of these protocols in real-time environments. Location-based authentication systems offer significant advantages over traditional password systems, and the reasons for this are discussed in detail throughout this paper.

References:

[1] D. Jaros and R. Kuchta, "New location-based authentication techniques in the access management," *Proc. - 6th Int. Conf. Wirel. Mob. Commun. ICWMC 2010*, pp. 426–430, 2010, doi: 10.1109/ICWMC.2010.62.

[2] Amit Kumar Tyagi, N.sreenath, "Future Challenging Issues in Location based Services," *Int. J. Comput. Appl.*, vol. 114, no. 5, p. 3, 2015, [Online]. Available: https://www.ijcaonline.org/archives/volume114/number5/19978-1921/

[3] Y. Albayram, M. M. H. Khan, A. Bamis, S. Kentros, N. Nguyen, and R. Jiang, "A location-based authentication system leveraging smartphones," *Proc. - IEEE Int. Conf. Mob. Data Manag.*, vol. 1, pp. 83–88, Oct. 2014, doi: 10.1109/MDM.2014.16.

[4] W. Bin Hsieh and J. S. Leu, "Design of a time and location based One-Time Password authentication scheme," *IWCMC 2011 - 7th Int. Wirel. Commun. Mob. Comput. Conf.*, pp. 201–206, 2011, doi: 10.1109/IWCMC.2011.5982418.

[5] Shraddha Ghogare, "Location Based Authentication: A New Approach towards Providing Security," *Int. J. Sci. Res.*, vol. 2, no. 4, 2012, [Online]. Available: https://www.researchgate.net/publication/290317536_Location_Based_Authentication_A_New_Approach_towards_Providing_Security

[6] F. Zhang, A. Kondoro, and S. Muftic, "Location-based authentication and authorization using smart phones," *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012*, pp. 1285–1292, 2012, doi: 10.1109/TrustCom.2012.198.

[7] D. Denning and https://independent.academia.edu/DDenning, "Geo-Encryption Using GPS to Enhance Data Security," Jan. 01, 2003. Accessed: Feb. 22, 2026. [Online]. Available: https://www.academia.edu/127773158/Geo_Encryption_Using_GPS_to_Enhance_Data_Security

[8] Hsien Chou Liao, Yun Hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users," *Inf. Technol. J.*, vol. 7, no. 1, 2008, [Online]. Available: https://www.researchgate.net/publication/26557016_A_New_Data_Encryption_Algorithm_Based_on_the_Location_of_Mobile_Users

[9] V. F. Stefano Rinaldi, "Machine learning-based spreading factor optimization in LoRaWAN networks," *Front. Comput. Sci*, vol. 7, 2025, doi: https://doi.org/10.3389/fcomp.2025.1666262.

[10] Arshad Farhad, Muhammad Ali Lodhi, "LSML-SF: a lightweight stacked ML approach for spreading factor allocation in mobile IoT LoRaWAN networks," *Front. Artif. Intell.*, vol. 9, 2026, doi: https://doi.org/10.3389/frai.2026.1704369.

[11] D. Son, A. Helmy, and B. Krishnamachari, "The effect of mobility-induced location errors on geographic routing in mobile ad hoc and sensor networks: Analysis and improvement using mobility prediction," *IEEE Trans. Mob. Comput.*, vol. 3, no. 3, pp. 233–245, Jul. 2004, doi: 10.1109/TMC.2004.28.

[12] M. Hussain, "An authentication scheme to protect the location privacy of femtocell users," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2014, pp. 652–657, 2014, doi: 10.1109/AICCSA.2014.7073261.

[13] L. Hua and J. Dai, "A location authentication scheme based on adjacent users," *PIC 2014 - Proc. 2014 IEEE Int. Conf. Prog. Informatics Comput.*, pp. 158–162, Dec. 2014, doi: 10.1109/PIC.2014.6972316.

[14] M. H. Chen and C. H. Chen, "Secondary user authentication based on mobile devices location," *Proc. - 2010 IEEE Int. Conf. Networking, Archit. Storage, NAS 2010*, pp. 277–281, 2010, doi: 10.1109/NAS.2010.56.

[15] J. Torres, J. M. Sierra, and A. Izquierdo, "A realistic approach on password-based mutual remote authentication schemes with smart-cards," *Proc. 2007 Inaug. IEEE-IES Digit. Ecosyst. Technol. Conf. DEST 2007*, pp. 334–338, 2007, doi: 10.1109/DEST.2007.371994.

[16] H. Jin, L. Tu, G. Yang, and Y. Yang, "An improved mutual authentication scheme in multi-hop WiMax network," *Proc. 2008 Int. Conf. Comput. Electr. Eng. ICCEE 2008*, pp. 296–299, 2008, doi: 10.1109/ICCEE.2008.155.

[17] W. Su, S. J. Lee, and M. Gerla, "Mobility prediction in wireless networks," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 1, pp. 491–495, 2000, doi: 10.1109/milcom.2000.905001.

[18] Lei Mu, Geng-Sheng Kuo, and Ningning Tao, "A Novel Location Algorithm Based on Dynamic Compensation Using Linear Location Prediction in NLOS Situations," pp. 594–598, Sep. 2006, doi: 10.1109/vetecs.2006.1682893.

[19] P. Hoyer, "OTP and Challenge/Response algorithms for financial and e-government identity assurance: current landscape and trends," *ISSE 2008 - Secur. Electron. Bus. Process. Highlights Inf. Secur. Solut. Eur. 2008 Conf.*, pp. 281–290, 2009, doi: 10.1007/978-3-8348-9283-6_29.

[20] W. Diffie, W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

[21] F. Nisar, M. Ameen, M. Touseef Irshad, H. Hadi, N. Ahmad, and M. Ladan, "XGBoost-Driven Adaptive Spreading Factor Allocation for Energy-Efficient LoRaWAN Networks," *Front. Commun. Networks*, vol. 6, p. 1665262, doi: 10.3389/FRCMN.2025.1665262.