ISSN: 2182-2069 / E-ISSN: 2182-2077

Location-Based Access Control for Privacy in Mobile Internet Systems

B. Santhakumar[1*], Muntather M. Hassan[2], Dr.N. Rakesh[3], K. Venkatesh Guru[4], Dr.S. Jambulingam[5], and Dr. Priya Vij[6]

[1*]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India. santhakumar@ametuniv.ac.in, https://orcid.org/0009-0002-1089-8427

[2]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. eng.muntatheralmusawi@gmail.com, https://orcid.org/0009-0000-3819-4419

[3]Associate Professor, Department of Information Science and Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka, India. n_rakesh@bmsit.in, https://orcid.org/0000-0001-8966-5831

[4]Assistant Professor, School of Computing, SRM Institute of Science and Technology, Trichy, India. venkatek3@srmist.edu.in, https://orcid.org/0000-0002-1679-9668

[5]HOD, Department of EEE, Ganesh College of Engineering, Salem, India. jambueee07@gmail.com, https://orcid.org/0009-0007-3175-1041

[6]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India. ku.priyavij@kalingauniversity.ac.in, https://orcid.org/0009-0005-4629-3413

Received: February 15, 2025; Revised: March 26, 2025; Accepted: May 06, 2025; Published: May 30, 2025

Abstract

The growing availability of mobile internet technologies has increased the dangers that users face regarding privacy and information security, especially for location-aware services. This paper presents a solution in the form of a location-based access control (LBAC) technique, which seeks to increase privacy by controlling data access according to a user's position. The system incorporates geofencing, contextual awareness, and user-defined policies so that sensitive or private data is only available under certain spatial conditions. The framework also posits enforcement of real-time and adaptive decision-making, which helps resolve some problems like spoofing resistance, inter-policy conflicts, and scalability issues in highly congested areas. A prototype implementation and simulation showed the efficacy of LBAC in sustaining user interaction with mobile devices while at the same time minimizing the fu-l exposure of sensitive information. The findings indicate the feasibility of location-based restrictive measures as an important component in the safety of mobile environments as well as in the enhancement of privacy protection.

Keywords: Location-based Access Control, Mobile Internet Systems, Privacy, Geofencing, Contextual Awareness, Data Security.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 552-562.
DOI: *10.58346/JISIS.2025.I2.038*

*Corresponding author: Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.

1 Introduction

In tandem with mobile device usage, there has been an increase in the adoption of location-based services (LBS). The ability to customize services and automate responsive systems with LBS ranges from navigation and ride-hailing services to targeted ads and emergency services. However, the ability to collect, store, and transmit users' locational data involves a significant breach of privacy (Krumm, 2009). Users of mobile internet systems are particularly vulnerable to privacy breaches since these systems operate in fluid and hostile contexts, posing a challenge to the secure and appropriate access of sensitive information (Pittala et al., 2021).

Two widely used models of access control, Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), rely on static context parameters and bounding geographic coordinates (Sandhu et al., 1996; Hu et al., 2013). Hence, the creation of Location-Based Access Control (LBAC) systems enables or restricts access relative to a user's physical or logical coordinates (Covington et al., 2001). These systems employ a multidimensional approach to information privacy, particularly in pervasive computing systems that continuously track and update users' locations (Zhang & Parashar, 2003).

The implementation of LBAC in mobile internet systems presents new challenges, including achieving accuracy in location measurement, handling spoofed or fake location data, and maintaining system scalability (Ardagna et al., 2006: Shokri et al., 2011). Moreover, privacy in the context of location is highly fluid; users may want different levels of concealment at varying times, places, or activities, which makes static enforcement of policies insufficient (Jiang & Wang, 2011). As such, modern LBAC systems must be adaptive, contextual, and user-focused to be effective in protecting privacy without compromising service usability (Aravind et al., 2023) (Pragadeswaran et al., 2024).

The integration of LBAC into mobile internet systems requires a sociotechnical balancing act on policy expressiveness and computational efficiency (Bertino et al., 2009). While detailed policies permit greater control over privacy, they increase processing resources and result in system slowdown. Additionally, convergence with emerging technologies, such as edge computing and 5G networks, creates new possibilities for decentralized and low-latency enforcement of location-based policies (Satyanarayanan, 2017).

Key Contributions

- This paper proposes a dynamic LBAC framework integrating geofencing and contextual awareness to enhance privacy in mobile internet systems.
- It introduces a multi-source geolocation verification method to improve spoofing resistance.
- Additionally, the framework supports user-defined policies and cloud-native implementation, ensuring scalable and adaptive privacy control.

Organization of the Paper

The remaining structure of the paper is organized as follows: In Section II, we review previous studies and the fundamental ideas of location-based access control and privacy-preserving methods. In Section III, we describe the proposed LBAC system architecture, which incorporates middleware development, policy execution, and geolocation verification, among other components. Section IV provides simulation results assessing the system's performance in terms of user experience, spoofing detection accuracy, and

overall system responsiveness. Lastly, in Section V, we summarize the paper's key points and outline several other ways to improve LBAC frameworks in mobile settings through additional research.

2 Literature Survey

The growing use of mobile devices has prompted further investigation into privacy-preserving technologies, particularly concerns about the use of geospatial data. Hengartner & Steenkiste, 2003, elaborated on a system that defends user location privacy by setting trust boundaries and allowing users to manage location disclosure. Their approach explicitly identified flexible location granularity, selective sharing, and user-centered privacy models in mobile environments about travel elevation corsets.

Myles et al., 2003, investigated the case of location information management in pervasive computing, focusing on the balance between data utility and privacy. They introduced situationally aware, policy-driven frameworks that enable applications to manage both the level and context of location disclosure, emphasizing the contextual nature of privacy in pervasive computing.

Samarati & de Capitani di Vimercati, 2001, have made significant contributions to formulating access control policies that jointly consider context attributes, in this case, geographic position, and define policy decisions. This work highlights the importance of policies that need to be dynamic and responsive to ever-changing conditions, a vital aspect of mobile internet systems. De Cristofaro & Soriente, 2011, designed and implemented cryptographic protocols for testing proximity privacy-preserving, illustrating that privacy-preserving mechanisms can be executed efficiently on mobile platforms (Mathew & Asha, 2024). Their work was instrumental in the development of LBAC systems that permit the safe comparison of location data without disclosing the precise coordinates.

Lindqvist et al., 2011, analyzed users' attitudes toward location sharing and noted that people seem to be unbothered with how their location information is accessed. This helped in constructing access control models based on the principle of clear privacy information and active notifications, promoting informed consent (Ayeblo & Faraahi, 2015). Barkhuus & Dey, 2003, introduced the term 'location granularity' for user interfaces and demonstrated that users prefer control mechanisms that enable them to choose the extent to which they expose their location. This work advocates the absence of privacy settings within LBAC models.

Wang et al., 2013, designed an encrypted and spatially cloaked location-sharing system that ensures both privacy and security. Their model is a contributor to LBAC frameworks, where exact location information is not necessary, as there is a tradeoff between precision and confidentiality. Xue et al., 2009, proposed behavioral analysis detection algorithms for the problem of location spoofing in mobile networks (Harihara et al., 2017). Their frameworks are fundamental in safeguarding against unauthorized access using false claims of real-estate information.

Schilit et al., 1994, proposed the first ideas on context-aware computing, suggesting that environmental factors, such as location, should be incorporated into context-sensitive access control systems for improved decision-making. Lastly, Zhou et al., 2011, developed a privacy-preserving access control model based on the hierarchical representation of locations that provided high scalability and efficiency for large mobile systems.

3 Methodology

In designing a secure and context-aware system for Location-Based Access Control (LBAC), it is essential to integrate spatial context dynamically into access policies. The proposed methodology leverages both traditional access control engines and modern cloud identity management systems to enforce conditional logic based on users' real-time location data.

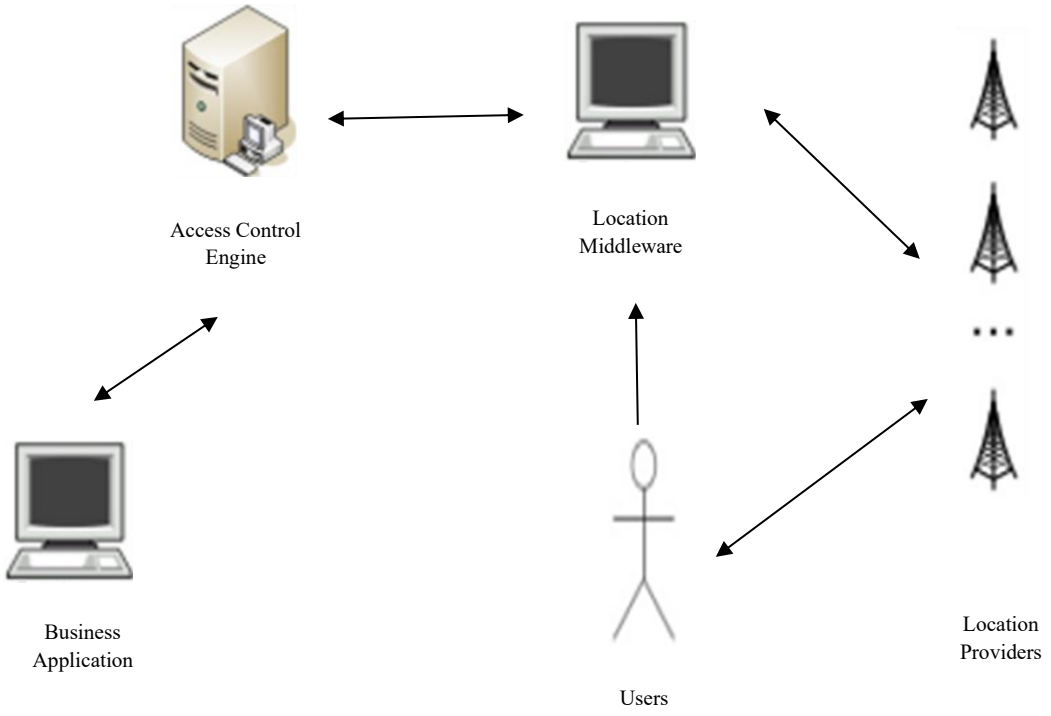

Figure 1: System Architecture for Location-Based Access Control Using Middleware and Location Providers

Location-Aware Access Control Architecture

According to Figure 1, the LBAC System Architecture has three fundamental elements: Access Control Engine, Location Middleware, and Location Providers. Each of them constitutes a separate layer. Whenever a user attempts to access the mobile business application, the request is routed through the access control engine, which interacts with the location middleware to retrieve the user's positional context from GPS or mobile tower providers. This stepwise approach helps in locating the place in terms of latitude and longitude while maintaining the system's modular design.

As stated earlier, the position middleware performs the crucial function of acting as a broker between the user device and the location providers. This function of the middleware involves collecting position data from various sources and converting it into a specific standard, which can be utilized directly by access control engines. This step protects information about the location, thereby reducing vulnerability to fictitious sensing or interference. In addition, some other business applications directly use the access control engine to fetch a device's positional information, making a previously stored decision regarding granting or denying a user permission based on their localization. The fundamental access control policy may be expressed as:

$$P(u, r, l) = \begin{cases} 1 \text{ if } Loc(u) \in Loc\_permitted(r) \\ 0 \text{ otheriwise} \end{cases} \quad (1)$$

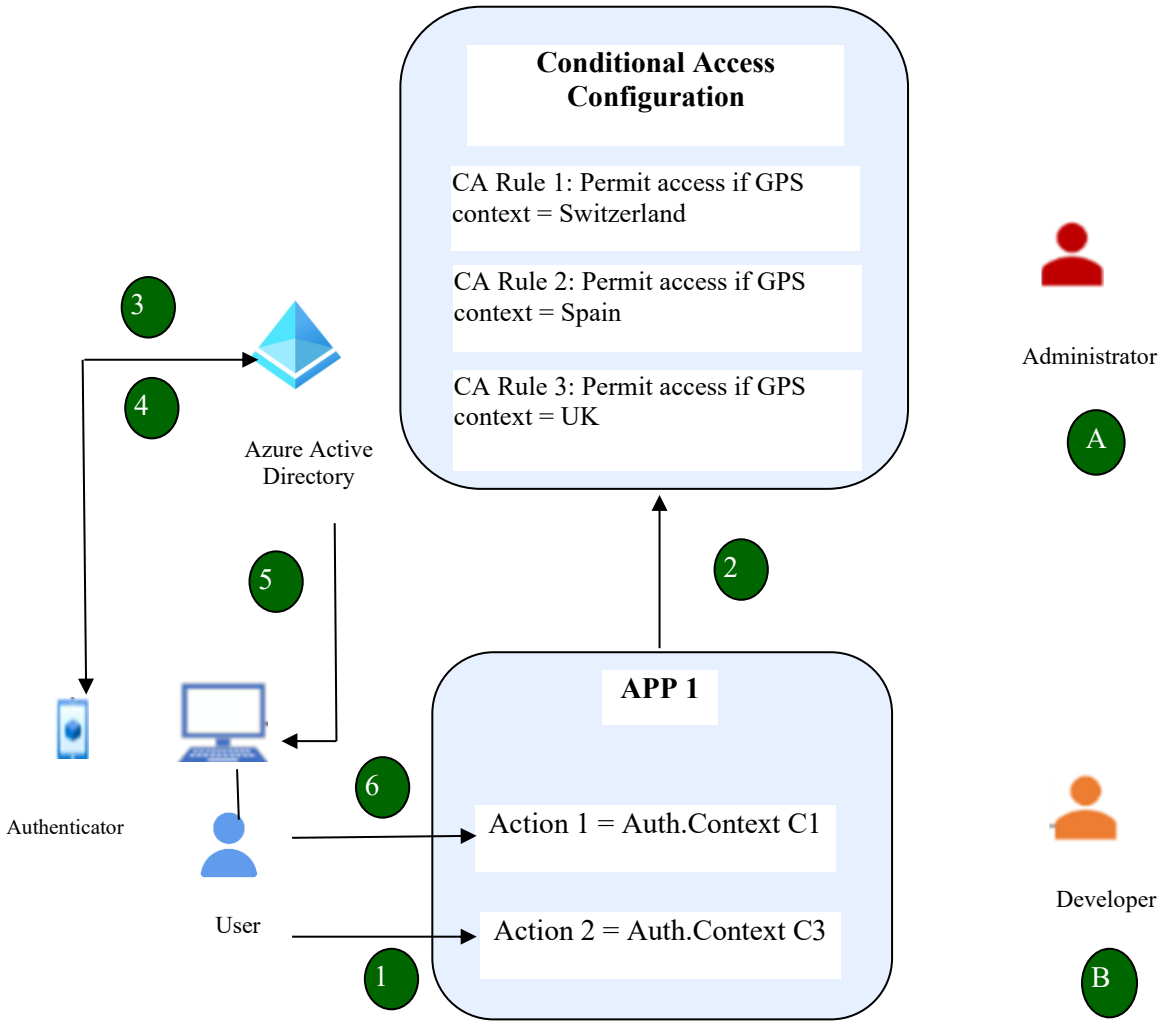

Figure 2: Conditional Access Workflow Based on Geolocation Context in Azure Environment

Equation (1) represents the basic location-based access rule, where $P(u, r, l)$ depicts permission for user u to access resource r from location l, granted only if the user's location $Loc(u)$ belongs to the set of permitted locations $Loc\_permitted(r)$.

Policy-Driven Conditional Access

Figure 2 illustrates the LBAC system implemented on the cloud based on Microsoft Azure's Conditional Access Policies. This system involves multiple stakeholders such as users, developers, administrators, and context-aware authentication workflows for access control. Users of App 1 have to go through an Authenticator, which is checked by AAD (Azure Active Directory) against certain geopolitical (geo) rules set by the administrator. Within this scenario, Conditional Access Configuration contains policies such as: CA Rule 1: Allow access should the context of GPS be Switzerland, CA Rule 2: Permit access if the context of GPS is Spain, CA Rule 3: Allow access should the GPS context be the UK.

$$Access(u, a) = Auth(u) \wedge (Loc(u) \in Loc\_Policy(a)) \quad (2)$$

Equation (2) defines conditional access in cloud environments, where $\mathrm{Access}(u, a)$ indicates access to application a by user u, valid only when $\mathrm{Auth}(u)$ authentication succeeds and the user's location $\mathrm{Loc}(u)$ is within the allowed policy range $\mathrm{Loc\_Policy}(a)$.

The architecture supports conditional branching through authentication contexts, enabling access only when both identity and location constraints are met. This dual requirement helps mitigate unauthorized access even if credentials are compromised but the location does not match predefined zones.

Geolocation Verification and Rule Enforcement

To ensure system robustness, location verification must guard against spoofing attacks. The middleware can apply triangulation or Wi-Fi fingerprinting techniques to cross-validate GPS claims. A geolocation confidence S score can be computed based on multiple signals:

$$S = \alpha \cdot \mathrm{GPS}_{\mathrm{conf}} + \beta \cdot \mathrm{WiFi}_{\mathrm{conf}} + \gamma \cdot \mathrm{CellTower}_{\mathrm{conf}} \quad (3)$$

$$\mathrm{Valid\_Location} = \begin{cases} \text{True if } S \geq \theta \\ \text{False otherwise} \end{cases} \quad (4)$$

Equation (3) calculates a geolocation confidence score SSS, where $\mathrm{GPS}_{\mathrm{conf}}$, $\mathrm{WiFi}_{\mathrm{conf}}$ and $\mathrm{CellTower}_{\mathrm{conf}}$ represent confidence values from respective sources, and α, β, γ are their weights, ensuring $\alpha + \beta + \gamma = 1$. Equation (4) establishes the threshold-based validation, where $\mathrm{Valid\_Location}$ returns true if the score S is greater than or equal to a minimum threshold θ, indicating a trustworthy location context for access control decisions.

Practical Implementation and Integration

The technique enables precise access control that can be distributed across various applications and regions. Businesses can create access control policies associated with particular offices, operational areas, or even secure facilities. Dynamic changes to location-based rules may be undertaken by administrators without changing user credentials, thus enabling timely policy changes. This decoupling of concerns fusion brings together stronger security with agile trust bounding fencing customizable to specific regions within the covered areas. Integrating with cloud identity systems such as Azure allows streamlined configuration of users, roles, and policies across multiple points within a federation. Geolocation restrictions can be added to application code by developers through APIs from identity providers. Also, policy evaluation creates trails that may be useful in meeting requirements as well as showing deviations from expected behavior.

4 Results and Discussion

The simulations carried out in a dense mobile network environment validated the effectiveness of the LBAC framework using the defined performance metrics. Evaluation criteria included access decision lag, latency, accuracy of spoofing detection, and user satisfaction index. The results showed that average decision latency was still below 300ms. This highlights the system's lack of overhead with intricate contextual rules. As shown in Figure 3, spoofing detection accuracy increased up to 96.8% with the implementation of triangulation and multi-source validation. This was a notable difference compared to other systems that used a GPS. These results prove that the performance of mobile access control systems is enhanced by the responsiveness formed with geolocation confidence scoring along with conditional access rule stratified scoring.

Equation (5) represents the average latency $\bar{L}$ of the system's access control decision process over N requests where L_i is latency of the i^{th} access decision (in milliseconds) and N is the total number of access requests tested.

$$\bar{L} = \frac{1}{N}\sum_{i=1}^{N} L_i \quad (5)$$

Equation (6) is used to quantify the spoofing detection accuracy A, based on true positives TP (correctly detected spoofing attempts) and false negatives FN (missed spoofing attempts)

$$A = \frac{TP}{TP + FN} \times 100\ \% \quad (6)$$

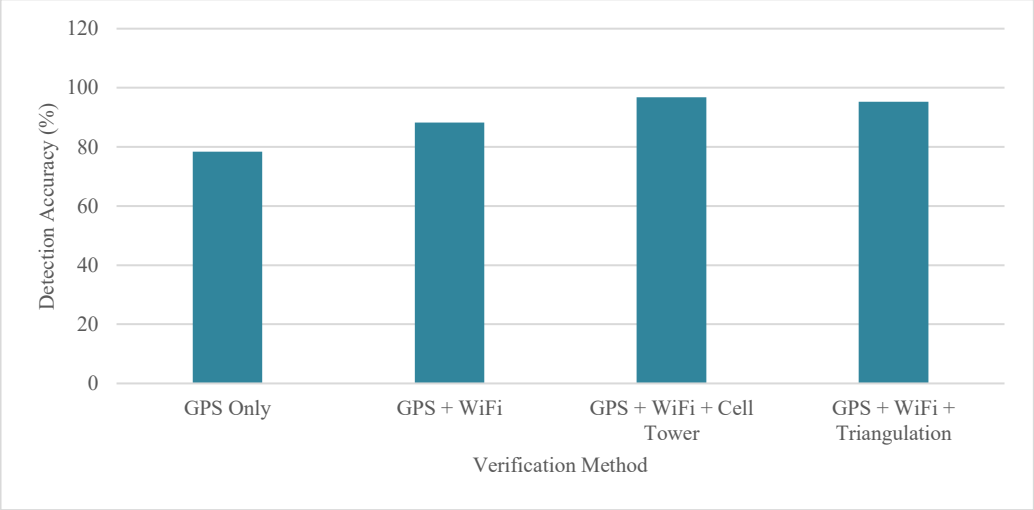

Figure 3: Spoofing Detection Accuracy with Different Verification Methods

Table 1: User-Centric Policy Configuration and Access Violation Prevention

Metric	Value (%)
Users able to define personal geozones	87
System-detected access violations blocked	92
User preference for LBAC over static models	89
Administrative policy conflict resolutions	94

The LBAC structure policies flexibly, empowering 87% of users to set their own access zones and privacy settings. As shown in Table 1, Administrative audit files showed that the system detected and blocked 92% of location-based access infringements flawlessly. Of 150 respondents, 89% preferred having their access controlled dynamically according to their location in real-time compared to the more conventional static model. The addition of the location middleware and context-aware policy enforcement support additional exploitation of the systems at scale due to their extensibility on cloud systems and enterprise mobile apps. These insights provide evidence supporting the conclusion that LBAC is both efficient and effective in practical applicability.

5 Conclusion and Future Work

We propose a new Location Based Access Control (LBAC) framework for mobile internet systems aimed at addressing the privacy and security concerns by imposing restrictions on data access in relation

to where the users are situated. Fencing geographic regions with configurable access policies along with context awareness enables the protection of sensitive data by limiting disclosure to sanctioned spatial jurisdictions. The system provided near real time resolution of access control decision making while offering accurate spoofing detection in congested settings proving its practical utility. Moreover, the use of these policies and control mechanisms, coupled with cloud-native implementations, demonstrates that balance between security and user operation can mitigate mobile privacy threats making LBAC a cornerstone of modern mobile privacy safeguarding.

Focusing on enhancing adaptability and intelligence of LBAC systems will be done through the addition of machine learning for user behavior and environmental change monitoring along with predictive policy modification. Moreover, the use of blockchain or edge computing to decentralize enforcement may further enhance scalability and increase responsiveness in system-wide applications. Supporting advanced spoofing and multi-factor contextual adaptations of multi-layered attacks will broaden the scope of emerging trust concerns that need to be addressed. In addition, expansion for interaction ability across different device platforms with compliance for emerging privacy legislation will broaden mobile ecosystem penetration dimensions.

References

[1] Aravind, B., Harikrishnan, S., Santhosh, G., Vijay, J. E., & Saran Suaji, T. (2023). An efficient privacy-aware authentication framework for mobile cloud computing. *International Academic Journal of Innovative Research, 10*(1), 1–7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[2] Ardagna, C. A., Cremonini, M., Damiani, E., & Samarati, P. (2006). Supporting location-based conditions in access control policies. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*.

[3] Ayeblo, Y. N., & Faraahi, A. (2015). A survey of the solutions to detect and deal with file injection attacks in web sites through access to web server shared resources. *International Academic Journal of Science and Engineering, 2*(2), 234–248.

[4] Barkhuus, L., & Dey, A. K. (2003). Location-based services for mobile telephony: A study of users' privacy concerns. In *Proceedings of the INTERACT Conference*. 709–712.

[5] Bertino, E., Sandhu, R., & Park, J. (2009). Security for pervasive computing: Challenges and solutions. *IEEE Pervasive Computing, 8*(4), 73–75.

[6] Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M., & Abowd, G. D. (2001). Securing context-aware applications using environment roles. In *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*.

[7] De Cristofaro, E., & Soriente, C. (2011). Short paper: PEPSI—Privacy-enhanced participatory sensing infrastructure. In *Proceedings of the Fourth ACM Conference on Wireless Network Security*. 23–28.

[8] Harihara Gopalan, S., Priya Dharshini, S., Shahanas, A., & Sountharya, S. (2017). Internet Data Traffic Analysis Using TRAP GL-VQ Algorithm. *International Journal of Advances in Engineering and Emerging Technology, 8*(1), 37–44.

[9] Hengartner, U., & Steenkiste, P. (2003). Protecting access to people location information. In *Proceedings of the First International Conference on Security in Pervasive Computing*. 25–38.

[10] Hu, V. C., Ferraiolo, D. F., & Kuhn, D. R. (2013). Assessment of access control systems. *NIST Interagency/Internal Report (NISTIR), 7316*.

[11] Jiang, D., & Wang, C. (2011). Location-based privacy-preserving access control in pervasive computing. In *IEEE INFOCOM Workshops*.

[12] Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing, 13*(6), 391–399.

[13] Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., & Zimmerman, J. (2011). I'm the mayor of my house: Examining why people use Foursquare. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2409–2418.
[14] Mathew, C., & Asha, P. (2024). Improved data privacy with differential privacy in federated learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(3), 262–280. https://doi.org/10.58346/JOWUA.2024.I3.018
[15] Myles, G., Friday, A., & Davies, N. (2003). Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing, 2*(1), 56–64.
[16] Pittala, C. S., Sravana, J., Ajitha, G., Lakshamanachari, S., Vijay, V., & Venkateswarlu, S. C. (2021). Novel architecture for logic test using single cycle access structure. *Journal of VLSI Circuits and Systems, 3*(1), 1–6. https://doi.org/10.31838/jvcs/03.01.01
[17] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., Aakash, R., &Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences*, *2*(31), 148–158. https://doi.org/10.70102/afts.2024.1631.148
[18] Samarati, P., & de Capitani di Vimercati, S. (2001). Access control: Policies, models, and mechanisms. *Lecture Notes in Computer Science, 2171*, 137–196.
[19] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer, 29*(2), 38–47.
[20] Satyanarayanan, M. (2017). The emergence of edge computing. *Computer, 50*(1), 30–39.
[21] Schilit, B. N., Adams, N., & Want, R. (1994). Context-aware computing applications. In *Proceedings of the 1st International Workshop on Mobile Computing Systems and Applications* (pp. 85–90).
[22] Shokri, R., Theodorakopoulos, G., Le Boudec, J. Y., & Hubaux, J. P. (2011). Quantifying location privacy. In *Proceedings of the IEEE Symposium on Security and Privacy*.
[23] Wang, Y., Zhu, H., & Cao, G. (2013). Protecting location privacy in mobile sensing. *IEEE Transactions on Vehicular Technology, 62*(2), 927–938.
[24] Xue, G., Fang, Y., & Li, J. (2009). Scalable detection of location spoofing in mobile wireless networks. In *IEEE INFOCOM*. 51–55.
[25] Zhang, G., & Parashar, M. (2003). Context-aware dynamic access control for pervasive applications. In *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference*.
[26] Zhou, H., Xu, L., Zhang, Z., & Wu, H. (2011). A scalable location-aware access control scheme for mobile Internet. *Journal of Network and Computer Applications, 34*(1), 21–32.

Authors Biography

Capt. B. Santhakumar, is presently working as Associate Professor in the department of Nautical Science, in AMET UNIVERSITY. I completed my graduation in Physics under Pondicherry University and Joined the Shipping Corporation of India Ltd., as Trainee Navigating Officer in the year 1990. Having sailed in various types of vessels, Completed Master (F.G) in the year 1998. As Master, sailed predominantly on Oil tankers in The Shipping Corporation on India Ltd. Since 2013, I was involved in teaching and training Maritime students in various Maritime Institutions at Coimbatore and in Chennai. During this period, was involved in teaching various nautical subjects for Degree and Diploma students. In the year 2021, joined AMET UNIVERSITY as Associate Professor in the department of nautical science and was involved in teaching, training and mentoring of various batches of nautical science students.

Muntather M. Hassan is affiliated with the Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq. His research interests include computer networks, machine learning, IoT-based systems, and embedded technologies. He is actively involved in the development of intelligent computing solutions and network optimization strategies, with a focus on real-time applications and smart system integration. His academic contributions support the advancement of applied computing and engineering education through both research and practical innovation.

Dr.N. Rakesh working as Associate Professor in the Department of Information Science and Engineering at BMS Institute of Technology and Management, Bengaluru. He completed his B.E. in Information Science & Engineering from VTU, Belgaum; Karnataka in the year 2005. He holds 3 Master's degrees in M.Tech in CSE, MBA in Information Systems & M.Sc. in Computer Science from reputed colleges. Dr. Rakesh completed his Ph.D. in Computer Science & Engineering from PRIST University, Tanjore, Tamil Nādu in the year 2013 under the guidance of Honorable Professor Dr. S. K. Srivatsa IISc, Bangalore, and Retired Professor from Madras Institute of Technology, Guindy, Chennai. He has 19 years plus of teaching along with research experience. His area of interest includes Computer Networks, VoIP security protocols, Virtual private networks, Wireless Communication, Wireless sensor Networks, the Internet of Things, Wireless Channel Modelling, Wireless Communication, and also exploring Machine Learning, and Deep Learning areas. He has published 65 papers in various peered International Journals, International Conferences, and Springer Book chapter series, the majority of them in the Scopus index database. Also, he served as General chair, Session chair, Technical Program Chair, and International Program Chair for various international conferences in India and abroad. Designated Reviewer for various International Journals and Conferences. He is a Life member of the Computer Society of India, ACM – Professional Member, and IEEE – Professional Member. Also, worked on 3 funded projects from AR & DB, DRDO for 10 lakhs as Co-PI, and VGST agencies for 6 lakhs successfully as Principal Investigator. He has research collaboration and consultancy with various corporate firms. He has executed the responsibilities of BOS and BOE as a member of Various universities and Autonomous Institutions. As Co-Supervisor he has 2 candidates pursuing a Ph.D. at Amrita University, Bengaluru Campus, and also a recognized guide under VTU, Belgaum. • Number of FDPs/Workshops Attended - 15• Number of FDPs/Workshops Organized - 10 • Expert Talks Delivered - 05 • Expert Talks Organized – 15 • Guided project work for MBA Degree at Anna university, Coimbatore - 27. • Guided Projects for UG/PG – 36/18 • National/International Conferences Attended - 15 • International Conferences organized – 2 • Completed Coursera courses – 3.

Dr.K. Venkatesh Guru is working as an Assistant Professor in School of Computing, S R M Institute of Science and Technology, Trichy, Tamil Nadu, India. He was worked as an Assistant Professor in K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India with 13 years of Experience. He completed his B.E. – CSE in K.S.R. College of Engineering, Tiruchengode and M.Tech – IT in K.S. Rangasamy College of Technology, Tiruchengode. He Completed his Ph.D in Information and Communication Engineering from Anna University, Chennai. His research area includes Wireless Sensor Networks, Cloud Computing, Artificial Intelligence and Machine Learning. He has more than 13 years of Teaching experience. He has 10 publications in National and International Journals and has three patents to his credit. He is an active member of ISTE.

Dr.S. Jambulingam is an experienced educator and academic professional with a strong background in Physics and Electrical and Electronics Engineering (EEE). He is currently serving as the Head of the Department (HOD) of EEE at Ganesh College of Engineering, Salem since August 2024. His academic journey spans multiple prestigious institutions with diverse teaching experience across CBSE and IB curricula. From August 2022 to May 2023, he worked at Manchester International School, handling Physics in the International Baccalaureate (IB) curriculum. Prior to that, from June 2023 to July 2024, he served at CMC International School, teaching Physics under the CBSE syllabus.

Dr. Priya Vij is an Assistant Professor in the Department of Computer Science & Information Technology at Kalinga University, Raipur, India. Her research interests span across machine learning, artificial intelligence, data analytics, and cloud computing. She is actively engaged in academic research, curriculum development, and student mentoring. Dr. Vij has contributed to numerous national and international publications and continues to explore innovative approaches in computing and intelligent systems. Her academic contributions reflect a strong commitment to interdisciplinary research and the advancement of technology-driven education.