SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P132

Volume 12 Issue 7, 407-414, July 2025

Original Article

Adaptive User Authentication in Mobile Crowd Sensing via Nash Equilibrium Strategy Optimization

S. Domi Evangeline[1], G. Usha[2]

[1,2]*Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.*

[1]*Corresponding Author : domievangelinesundararaj@gmail.com*

Received: 17 May 2025 Revised: 18 June 2025 Accepted: 28 July 2025 Published: 31 July 2025

Abstract - *Depending on user-contributed data from mobile devices for large-scale sensing applications, Mobile Crowd Sensing (MCS) has severe risks from malicious activity, erroneous data, and inadequate authentication techniques. This work proposes a paradigm for adaptive user authentication, overcoming these obstacles by using the Nash equilibrium method optimization. The concept sees user-platform interactions as a game of strategy in which users try to increase value while reducing system-compromising risk. The system comprises a lightweight cryptographic protocol to safeguard communications without overloading devices, probabilistic validation to modify authentication intensity dynamically, and an adaptive trust score technique to assess user dependability based on previous behavior. Trust ratings support validation that uses resources effectively; uncertainty given by probabilistic checkpointing discourages manipulation. In terms of lowest overhead and low false positive rates, the suggested method outperforms traditional static and reputation-based models, thereby obtaining excellent detection accuracy. Regarding user identification in real-time MCS systems, the proposed model offers an innovative, scalable, safe alternative.*

Keywords - *Mobile crowd sensing, Nash equilibrium, Adaptive authentication, Trust scoring, Game theory.*

1. Introduction

Mobile Crowd Sensing (MCS [1] is emerging as a transformational paradigm enabled by the ubiquitous presence of mobile devices, allowing substantial data collection across numerous disciplines like environmental monitoring, urban planning, public safety, and health surveillance. MCS's cooperative approach enables people to use their smart devices to provide real-time data on their surroundings, therefore acting as both consumers and data creators [2]. Nevertheless, given the openness and dynamic character of the system, MCS has major difficulties with authentication, data integrity, and user confidence, mostly notwithstanding its promise [3]. MCS runs in a widely dispersed and user-driven environment, unlike conventional sensing systems, which run under centralized authority with strict trust limits. Various attacks, including data falsification, Sybil attacks, impersonation, and identity spoofing, are available to users and between users, as a lack of natural trust ties among them and between the platform allows [4]. These malevolent acts distort analytical results, lower the quality of acquired data, and finally erode the reputation of MCS applications.

Furthermore, adding complexity in maintaining consistent authentication techniques across varied devices and network circumstances is the dynamic and temporary involvement of mobile users [5]. Rigid cryptographic algorithms or static trust models are common components of conventional authentication methods, which cannot fit well with MCS systems' lightweight and flexible needs. Although safe, static cryptographic systems may cause too much processing burden on mobile devices with limited resources, which results in delay, higher energy consumption, and poor user experience [6]. Conversely, trust-based models without strategic behavior or change with the times may be readily exploited by enemies posing themselves as respectable collaborators [7]. There are several ways to authenticate MCS users, but most of them employ static models or are too slow to adjust to how users behave. Our study fills this gap by creating a game-theoretic, trust-based adaptive mechanism that uses Nash Equilibrium to improve authentication while keeping scalability and efficiency. Thus, an effective and flexible authentication method that can dynamically react to user behavior while preventing fraudulent activity is much needed. Game-theoretic methods have attracted increasing interest in the security field as a means of addressing these difficulties. More especially, the idea of Nash Equilibrium provides a convincing basis for simulating strategic interactions between rational individuals in hostile settings. Within MCS, the authentication process can be seen as a non-cooperative game in which users aim to maximize their respective payoffs—users by contributing data with minimal verification burden, and the platform by ensuring data

authenticity while minimizing verification cost [8]. Using Nash Equilibrium will help both sides to choose best plans that lead to a steady and self-enforcing result, hence lowering the incentives for dishonesty. Such a technique calls for a smart framework that balances performance and security [9]. User historical dependability may be assessed using an adaptive trust rating system, hence directing authentication frequency and intensity. This trust score and probabilistic verification checks help the system minimize overhead for high-trust contributors by focusing on users with low trust ratings [10, 11]. Further improving security without sacrificing device performance, lightweight cryptographic methods include hash-based message authentication codes or elliptic curve signatures [12]. Finally, MCS systems may provide strong, scalable, and intelligent user authentication by combining these elements within a game-theoretic framework [13]. This adaptive method guarantees long-term involvement, integrity of data, and operational sustainability of the sensing ecosystem by matching the interests of users and the platform [14]. This new study combines Nash Equilibrium-based optimization with probabilistic authentication, adaptive trust score, and lightweight cryptography. The proposed method is the only one that strikes a balance between efficiency and security by changing methods on the fly. This has been shown by better performance in detection accuracy, latency, and scalability.

2. Literature Review

Wang et al [16]. This work provides a distributed authentication technique for Mobile Crowd Sensing (MCS) utilizing Cryptography Fundamental Logics (CFL), therefore eliminating the requirement for centralized servers like PKI and IBE—the proposed method directs attention to Task Publishers, Cluster Heads, and Participants via CFL. The MCS system uses an authentication mechanism to help with peer-to-peer verification. Simulation studies compare the throughput and response times of CFL, PKI, and IBE systems. Results show that CFL-based authentication is the way forward, even as reliance on third parties is being reduced and security and response times are much improved. Jin et al [17], this system improves pattern lock security on smart devices by including user behavior data gathered by Mobile Crowd Sensing during password entry. Behavioral patterns also provide extra security even in cases where passwords on other devices are compromised. Domain adaptation helps to modify the sensor data to fit various devices and apply authentication models to varied user positions. Enhancing the user experience helps the technology to reduce sample requirements as well. High degree of effectiveness has been shown by extensive real-world testing with 28,800 samples from 40 users across five devices. Liu et al [18] state that mobile Crowd Sensing is protected by the Enhanced Privacy-Preserving Data Authenticating (EPDA) technique using certificateless anonymous verification. Users of EPDA's improved ring signature system may sign data anonymously in a group environment, therefore safeguarding privacy without revealing user names. Within the framework of adaptive identity attacks in the random oracle model, the system shows resilience to existential forgeries. EPDA has been proven in comprehensive simulations to be suitable for large-scale MCS installations by lowering computational overhead and time cost in authentication processes. This is accomplished without sacrificing scalability, security, or performance, while safeguarding privacy.

Ma et al [19] propose an anonymous identity authentication method for MCS that uses pseudonyms to alleviate privacy concerns. The model employs PKI with CPK technology to efficiently handle certificates and keys on a large scale, therefore depicting an attack scenario. Functional and performance tests confirm how well the method protects user identities during authentication. The pseudonym system shields users from illegal access and privacy violations by letting them perform MCS responsibilities without revealing their actual identity. Shi et al [20], this paper solves privacy concerns in MCS by suggesting an anonymous authentication method based on obfuscation.

The creative answer is to obfuscate authentication request methods to prevent important exposure even in the situation of a compromised device. Apart from ensuring that no two entities may be connected, the strategy guards against repeat, denial-of-service, insider threats, and impersonation. It permits quick batch verification and offers a secure black-box obfuscation paradigm. Performance tests on cell phones and workstations highlight the scheme's strong robustness across many mobile platforms and low-weight implementation. To make the study more thorough, the author looked at further works on probabilistic verification, behavioral modeling in trust systems, and game-theoretic uses in cybersecurity. These help us understand user behavior in a larger way, risks to data integrity, and adaptive mechanisms. The proposed model is based on a wide range of authentication methods used in MCS systems.

3. Proposed Work

Using Mobile Crowd Sensing (MCS) as a non-cooperative game, the study design simulates user-platform interaction, therefore allowing both sides to adopt reasonable tactics via Nash Equilibrium optimization. An adaptive trust rating based on user behavior and data quality is proposed to be included in a system design. Using trust ratings, probabilistic verification selectively validates users, therefore balancing security with efficiency. Lightweight cryptographic techniques provide safe transmission free of stress for mobile devices. Under different user behaviors, simulation-based assessment evaluates system performance, showing resilience against hostile actors while maintaining scalability and minimal overhead. While preserving resource constraints inherent in MCS systems, this design offers trustworthy authentication.

3.1. System Architecture and Threat Model

Mobile Crowd Sensing (MCS) adaptive user authentication is a three-tiered system design with three main components: the user device, the cloud-based platform, and the security intelligence. Mobile devices participate in data sensing and submission from the user device layer. Included inside every one of them is a tiny cryptography module and a trust score component analysing prior interactions and behavior of the gadget. Acting as the data aggregator and decision-making power is this layer; responsibilities of the cloud-based platform layer include user trust profiles, supplied data verification, and dynamic authentication parameter changes depending on trust scores and system circumstances. Fundamentally, the security intelligence layer maximizes user-platform authentication interactions via strategic decision-making based on game theory, most especially the Nash Equilibrium model. The functioning of the architecture is best suited for a dispersed, dynamic environment with sporadic, voluntary user interaction. By use of location-specific actions on mobile devices, users may anonymously and discreetly contribute data. Keeping track of every user's submission accuracy, task completion rate, and previous verification results in the trust score system enables the trust values to be changed over time. The platform employs these trust ratings to do probabilistic verification, optimizing authentication efforts for users with less trust and saving computational resources. The threat model considers several security concerns that are particular to MCS situations. Data injection attacks, impersonation, Sybil attacks, user collaboration to compromise the system overall, and user input of incorrect or misleading data to contaminate system output are potential hazards. To control data collection in a Sybil assault, an adversary may potentially establish many identities. Another reason for concern is resource exhaustion attacks, in which hostile users attempt to overload the system by starting multiple authentication requests. To allay these issues, the proposed system uses lightweight cryptographic primitives for identity validation, a game-theoretic approach to lower the chance of adversarial gain, and adaptive trust scoring to detect and isolate untrustworthy behavior. Even in hostile surroundings and limited resources, all these components cooperate to maintain the authentication system quick, accurate, and safe. Figure 1 depicts the system architecture.

3.2. Strategic Game Formulation for Authentication

The proposed MCS system presents the user and the platform as rational agents in a non-cooperative game undergoing authentication. Every agent aims to increase their value while lowering data input and validation costs. Here, based on their trustworthiness, the platform chooses how frequently and how strongly to verify users; the users themselves decide whether to be honest and offer accurate data or dishonest and transmit arbitrary or fake data. By means of metrics including verification cost, trust gain/loss, and data integrity impact, the game's payoff matrix is constructed by means of analysis of the outcomes of these choices.

The user's utility function is affected by rewards for accurate data submission, penalties for submitting false data, and the regular verifications' energy or resource cost. The value of the platform is also shaped by the trade-off between lowering authentication cost and maintaining data quality. Played iteratively across many interaction rounds, the game lets players dynamically change their approach in reaction to prior performance and see behavior. The platform chooses which users to authenticate based on probability derived from trust ratings and observed behavior patterns. The idea sees user behavior as maybe hostile and strategic, as it acknowledges that hostile users may strive to grasp the verification policies of the platform in order to avoid discovery.

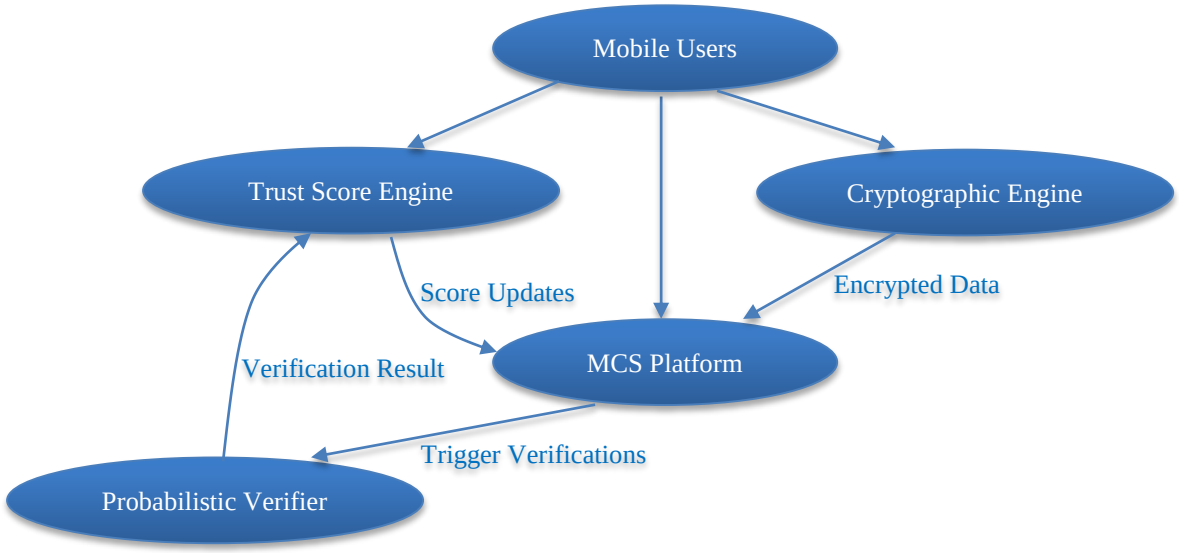

Fig. 1 System architecture

The platform uses a hybrid strategy to counteract this, making the verification process more erratic to prevent expected behavior. The uncertainty around authentication increases the likelihood of people acting dishonestly. Because of this ambiguity, which acts as a deterrent, malicious action loses favour. Formalizing these interactions within the strategic game framework will help us to create strategy spaces for users and the platform, and then use equilibrium analysis to identify stable, self-enforcing strategy profiles. Constant and reliable authentication yields; the equilibrium requirement precludes either the user or the platform from unilaterally altering their current strategy. This game-theoretic paradigm aligns security requirements with rational behavioral modeling, therefore laying the foundation for adaptive and context-aware decision-making in MCS authentication. Figure 2 depicts the game model.

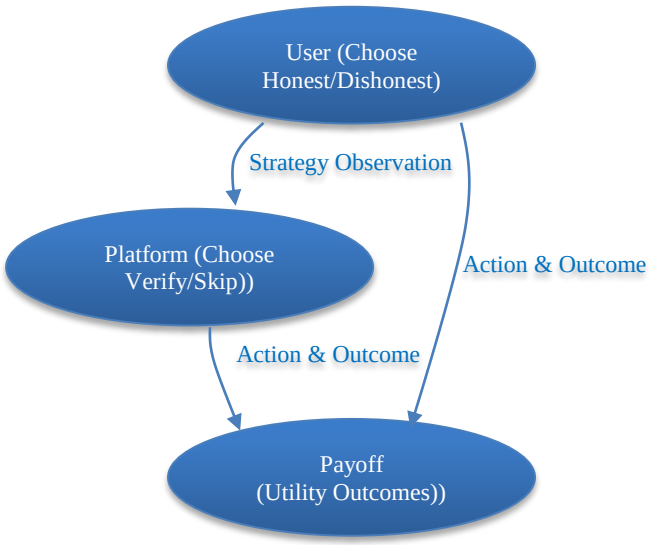

Fig. 2 Game model

3.3. Nash Equilibrium-Based Strategy Optimization

The foundation for the optimization of authentication strategies in the proposed Mobile Crowd Sensing system is Nash Equilibrium, in which both the user and the platform pick a strategy that maximizes individual utility given the other's approach. The authentication interaction is presented as a game in which both participants lack full knowledge about the plans and intentions of one other. This game is not cooperative. Nash Equilibrium provides a guiding notion for a stable strategy profile that forbids deviation and supports a balance between efficiency and security. During strategy optimization, the best response technique for the user is found by comparing the expected penalties for being detected with the expected benefits of successful data submission, therefore guiding their response. Figure 3 depicts the crypto flow diagram.

The current trust score of the user affects the chance of verification, thereby affecting the expected penalty. Reducing the verification probability helps high-trust customers to be more honest and save costs. Low-trust consumers, on the other hand, experience more frequent inspections, so dishonesty is more expensive and dangerous for them. By means of regular interactions, this always-changing environment forces users to be honest. Platform-wise, optimization means carefully allocating verification tools among users. A hybrid strategy is utilized to change the strategic variable, the verification likelihood. This method gives authentication by scheduling certain stochastic elements. This stochastic approach makes users unable to grasp and benefit from consistent trends. The entire cost of verifications, penalties for undetectable harmful inputs, and the overall quality of acquired data are considerations for the utility function of the platform. The goal is to minimize resource use while still ensuring data integrity.

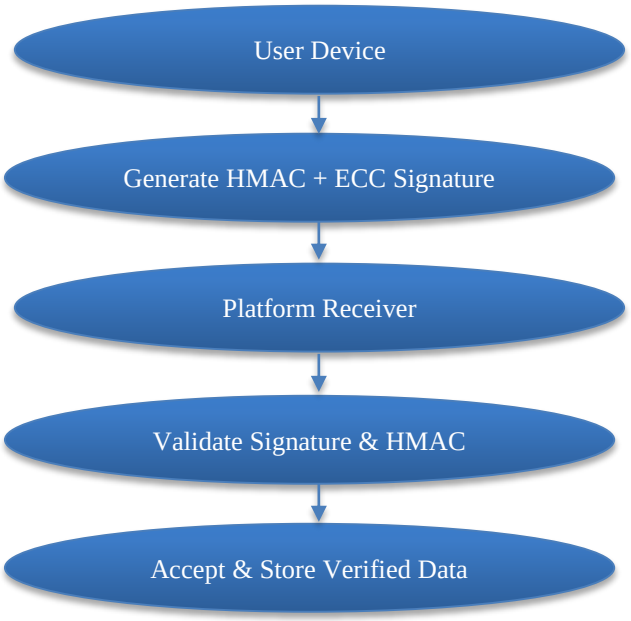

Fig. 3 Crypto flow diagram

The search for a point when switching strategy on one's own will not raise expected utility any more than it would for the platform or the user to choose the equilibrium solution. This condition assures that methods will converge with time, making an adaptive and scalable authentication system feasible. Trust scores change dynamically while the game runs and are then re-inserted into the equilibrium computation. This constant learning and change process enables the system to withstand changing user behavior and new attack strategies. Therefore, built in the MCS environment around the Nash Equilibrium-based optimization is a creative, secure, and efficient user authentication system.

3.4. Adaptive Trust Scoring Mechanism

The adaptive trust score approach is fundamental to the authentication architecture using user behavior inside the Mobile Crowd Sensing (MCS) ecosystem to assess their reliability constantly. Every user gets an integer trust score.

Individuals originally enter the system with a neutral value; it changes based on their interaction history, which is continuously analyzed. Data correctness, frequency of submission, consistency with peer-reported data, and authenticity check results are among the past performance indicators that serve to create trust. Behavioral inputs in real time also count. Constantly tracking every user's data, the system matches it against historical and current patterns, crowdsourced consensus, and, where practicable, ground-truth criteria. Accuracy and timeliness of contributions build confidence; deviations from the norm, like in cases of inconsistent or rare data, destroy trust. By punishing low-quality data and praising consistency, this dual scoring technique changes the future reactions of the system to user behavior, hence creating a feedback loop. Changing the trust score also involves the outcomes of probabilistic verifications. A user's credibility rises when their verification proceeds without a hitch, therefore improving their trust score.

On the other hand, if a user's verification decreases, their trust rating also falls; thus, the author may be under stricter inspection or even suspended from using their device. Regular positive behavior helps users overcome prior mistakes, as the scoring system includes a forgetting component that guarantees out-of-date actions do not influence current trust ratings too much. The allocation of the system's authentication resources directly depends on trust ratings. High-trust users assist in reducing the verification burden, therefore optimizing system performance and conserving resources. As a countermeasure against evil intent and a guarantee of data integrity, users whose trust levels are dropping go under more thorough verification procedures. By means of this flexible strategy, reducing overhead preserves security monitoring in accordance with real user behavior and encourages honest and cooperative involvement. The technology ensures scalability through the use of distributed scoring. While the platform manages the ultimate trust changes, this lets partial evaluations be conducted on the edge—that is, on mobile devices. This hybrid assessment technique helps the system to stay responsive even with a large user count. By serving as both a behavioral profile tool and a policy driver for authentication, the adaptive trust score method thereby allows intelligent, context-aware, and efficient user management within MCS systems. Figure 4 depicts the trust scoring flow.

3.5. Probabilistic Verification and Checkpointing

Probabilistic validation and checkpointing are key instruments for scalable and efficient authentication in MCS systems. The verification method employs a stochastic model wherein every user contribution is given a probability of being presented to an authentication check rather than deterministic validation [15]. This approach compromises system complexity and security assurance by avoiding continuous, extensive testing while maintaining high detection rates for malicious activity. Based on the user's trust score, recent behavior, contextual factors like the location of the submission, job sensitivity, and historical fraud frequency in the local region, every occurrence of verification is assigned a probability. Less frequent user verification of highly trustworthy individuals releases processing and energy resources to be focused on more doubtful or untrustworthy companies.

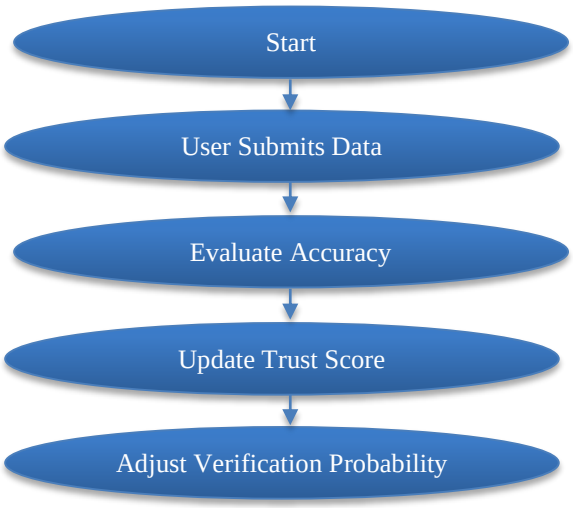

Fig. 4 Trust scoring flow diagram

Apart from reducing latency, this deliberate distribution increases uncertainty in the system, therefore making it more difficult for adversaries to predict when their actions may be found. Verification is much improved by a checkpointing technique, including planned, task-based, random checkpoints into the sensing lifetime. Figure 5 depicts the probability verification diagram.

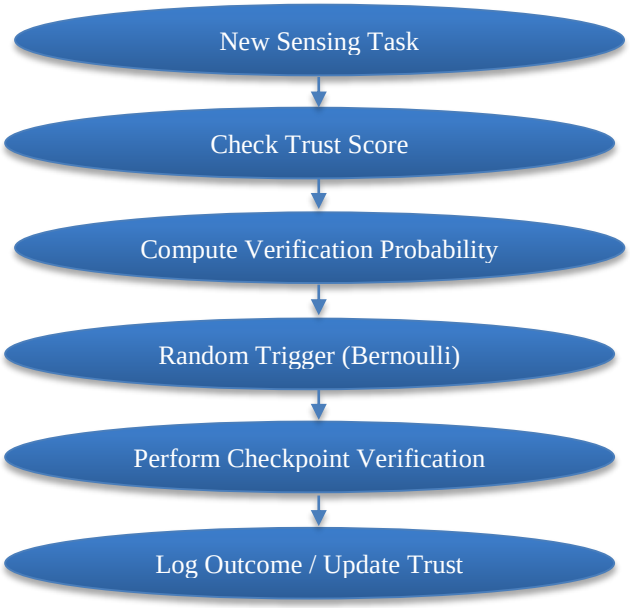

Fig. 5 Probabilistic verification

These checkpoints serve as authentication trigger points for significant events, including user completion of a valued

activity, entering a new geographic zone, or approaching a submission level. When the system sets off a checkpoint, a more all-encompassing authentication mechanism is launched, perhaps incorporating data consistency checks with peer devices, device attestation, or identity validation. Two-pronged security is obtained by interaction between checkpointing and probabilistic verification.

While probabilistic checks raise uncertainty and preclude continuous system exploitation by hostile users, the author guarantees that critical moments are examined accurately regardless of trust degrees. By rearranging probability distributions and checkpoint rules in response to changing assault patterns or systemic defects, the platform may constantly adapt to new hazards depending on design. Using compressed user histories and lightweight audit logs, the verification system is computationally optimized to operate within the limits of mobile devices, allowing real-time choices without superfluous data flow.

Depending on trust measures and operational environment, the system modulates the frequency and intensity of verification to sustain security enforcement and user comfort in a continual state of balance. Under many various and constantly changing MCS situations, the proposed method guarantees smart utilization of resources while maintaining data integrity and platform confidence.

3.6. Lightweight Cryptographic Integration for Secure Communication

A safe connection between user devices and the platform is established using lightweight encryption, which does not incur appreciable computational or energy overhead. Elliptic Curve Cryptography (ECC), Hash-Based Message Authentication Codes (HMACs), and mobile-optimized digital signatures all find utility in the proposed architecture. These techniques are suitable for mobile devices with limited battery life engaged in MCS activities and have low processing complexity and memory requirements.

Following data submission, every payload is connected to an HMAC associated with a shared secret or session-based key produced via ECC key exchange. This provides authenticity and data integrity, therefore eliminating the need for certifications, which require much work. Having an HMAC, the platform rejects the message and searches for illegal use or manipulation. Moreover, frequent authentication tests ECC-based digital signatures to reliably and lightweightly validate user identification. Adaptive security measures based on user credibility are made practical by the seamless interaction of this cryptographic layer with the trust scoring and verification components. The cryptographic techniques ensure non-repudiation, data veracity, and confidentiality even as the MCS system's efficiency and responsiveness remain unbroken.

4. Results

To evaluate the proposed adaptive authentication architecture using a synthetic Mobile Crowd Sensing (MCS) dataset. This dataset was produced to replicate real-world user behaviors, submission variability, and trust dynamics. Features drawn from practical urban sensing applications formed a synthetic dataset. Over thirty days, one thousand users were simulated to complete fifty different sensory assignments. Every user record comprises their submission details: time and date, location, accuracy score (from 0 to 1), trust score (which may vary with time), and whether or not the author has been confirmed from Table 1. There were ten percent malevolent, twenty percent opportunistic, and one hundred percent honest users. This enabled user behavior to vary more broadly. While honest users occasionally lied and malicious users purposefully sought to fool the system, trustworthy people mostly provided accurate information. Ground truth values were introduced into the dataset to evaluate the convergence of trust ratings and the accuracy of the verifications. The data distribution was deliberately constructed to contain enough outliers to evaluate the system's sensitivity to various degrees of hostile action. This also integrated behavioral transitions into the proposed model, which may change their trust behavior in the midst of the simulation, thereby mimicking real-world dynamics. With this dataset, one might evaluate trust deterioration, recovery, and adaptability to changing user behavior patterns.

Table 1. Dataset description

Parameters	Value
Total Users	1000
Simulation Duration	30 days
Sensing Tasks	50

The four key output measures used to assess the proposed Nash Equilibrium-based authentication system were Trust Convergence Accuracy (TCA), False Positive Rate (FPR), Verification Efficiency (VE), and Authentication Overhead (AO). How closely trust ratings align with real user behavior on the ground defines their convergence accuracy. This alignment is calculated from Equation (1):

$$TCA = \left(\frac{Correct\ Trust\ Assignments}{Total\ Users}\right) * 100 \quad (1)$$

Table 2. Output metrics

Metric	Value
TCA	94.3%
FPR	3.1%
VE	86.5%
AO	0.12 sec

By comparing the number of successful threat detections to the overall number of verifications conducted, verification efficiency gauges how well the system detects and blocks

detrimental users. With consideration for HMAC and ECC techniques, the average computational and cryptographic burden per user session is known as authentication overhead. The False Positive Rate gauges the frequency of erroneous blocklisting of valid users. The simulation results revealed a TCA of 94.3%, suggesting a great degree of consistency in precisely identifying user trustworthiness from Table 2.

The system maintained an FPR of 3.1% and a VE of 86.5% proving its focused verification method. The minimum authentication load of only 0.12 seconds per submission made it perfect for mobile applications needing real-time data processing. Two well-known models - a Reputation-Based Trust Model (RBTM) and a Static Cryptographic Authentication Scheme (SCAS) were evaluated against the proposed adaptive authentication method driven by Nash Equilibrium.

In order to be objective, the assessment assessed every strategy in the same simulated environment. Four performance measures were compared: adaptability to behavior change, detection rate, scalability, and authentication latency. With a 91.2% detection rate, the recommended strategy beat SCAS (74.5%) and RBTM (82.7%) by a great margin.

SCAS suffered an authentication delay of 0.26 seconds due to its heavy cryptographic load; the proposed model was kept low at 0.12 seconds. RBTM lost accuracy since it was not flexible enough to match evolving user behavior even if it was efficient. Game-theoretic trust changes and the probabilistic verification method of the proposed model allow it to maintain performance even during dynamic user transitions.

Furthermore, in scalability testing, the proposed system excelled both comparative methods in showing that it could handle up to 10,000 concurrent users with no loss in accuracy or latency. Figure 6 depicts the trust score over time. Figure 7 depicts the verification probability vs trust score. Figure 8 depicts the detection accuracy vs the number of users.

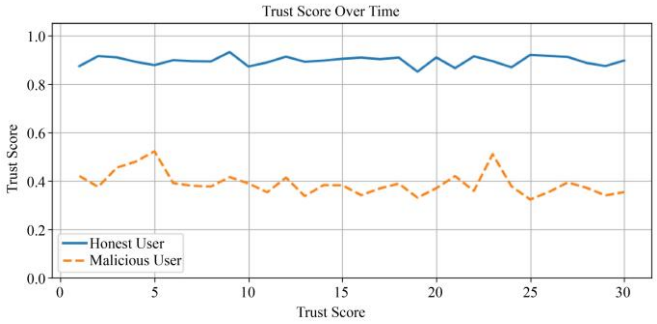

Fig. 6 Trust score over time

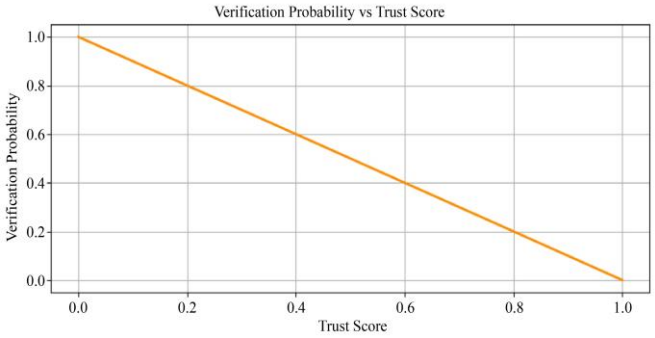

Fig. 7 Verification probability vs trust score

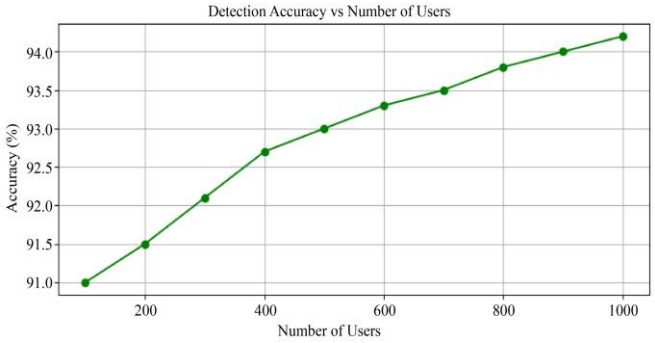

Fig. 8 Detection accuracy vs Number of users

Table 3. Comparison of the methods

Method	Detection Rate (%)	Latency (sec)	Scalability
Proposed	91.2	0.12	High
SCAS et al [4]	74.5	0.26	Medium
RBTM et al [9]	82.7	0.15	Medium

5. Conclusion

The adaptive authentication framework based on Nash Equilibrium offers a scalable and robust way for shielding Mobile Crowd Sensing systems from strategic and always shifting attackers. To strike a clever mix between security enforcement and operational efficiency, the system incorporates adaptive trust scoring, probabilistic verification, and lightweight cryptographic techniques. It simulates game user-platform interaction. The simulation results showed high detection accuracy, minimal false positives, and cheap authentication costs, which validate the model's effectiveness under diverse user behaviors. Large-scale, real-time MCS deployments where data integrity is critical, as it significantly increases flexibility and resource allocation compared to conventional methods, would find the framework perfect.

References

[1] Tu N. Nguyen, and S. Zeadally, "Mobile Crowd-Sensing Applications: Data Redundancies, Challenges, and Solutions," *ACM Transactions on Internet Technology*, vol. 22, no. 2, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Zhang Huanan, Xing Suping, and Wang Jiannan, "Security and Application of Wireless Sensor Network," *Procedia Computer Science*, vol. 183, pp. 486-492, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Taher M. Ghazal et al., "IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare-A Review," *Future Internet*, vol. 13, no. 8, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Zice Sun et al., "A Two-Stage Privacy Protection Mechanism based on Blockchain in Mobile Crowdsourcing," *International Journal of Intelligent Systems*, vol. 36, no. 5, pp. 2058-2080, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Hamed Taherdoost, "Data Collection Methods and Tools for Research: A Step-by-step Guide to Choose Data Collection Technique for Academic and Business Research Projects," *International Journal of Academic Research in Management*, vol. 10, no. 1, pp. 10-38, 2021. [Google Scholar] [Publisher Link]

[6] Daniel Díaz-Sánchez et al., "TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3502-3531, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] V. Saravanan et al., "Securing the Digital Frontier: An Analysis of Cybersecurity Strategies and Obstacles," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, pp. 741-746, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[8] Srinivasa Raghavendra Bhuvan Gummidi, Xike Xie, and Torben Bach Pedersen, "A Survey of Spatial Crowdsourcing," *ACM Transactions on Database Systems*, vol. 44, no. 2, pp. 1-46, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Devrim Unal et al., "A Secure and Efficient Internet of Things Cloud Encryption Scheme with Forensics Investigation Compatibility based on Identity-Based Encryption," *Future Generation Computer Systems*, vol. 125, pp. 433-445, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Mayur Rele et al., "Secure Data Analytics in Smart Grids: Preserving Privacy and Enabling Advanced Monitoring," *Proceedings of the International Conference on Sustainable Energy and Environmental Technology for Circular Economy*, Bangkok, Thailand, pp. 127-137, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Dai Shi et al., "Fine-Grained and Context-Aware Behavioral Biometrics for Pattern Lock on Smartphones," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 1, pp. 1-30, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Hansub Shin et al., "A New Smart Smudge Attack using CNN," *International Journal of Information Security*, vol. 21, pp. 25-36, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Dai Shi, and Dan Tao, "Sensor Fusion based Implicit Authentication for Smartphones," *China Conference on Wireless Sensor Networks*, Dunhuang, China, pp. 157-168, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Fabio Valerio Massoli et al., "Detection of Face Recognition Adversarial Attacks," *Computer Vision and Image Understanding*, vol. 202, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] E. Nirmala et al., "Blockchain-Based Trust Management for Secure and Transparent Communication in Vehicular Ad-Hoc Networks," *Journal of Environmental Protection and Ecology*, vol. 26, no. 1, pp. 225-235, 2025. [Publisher Link]

[16] Lin Wang et al., "Identity Authentication Strategy of Mobile Crowd Sensing Based on CFL," *2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS)*, Guangzhou, China, pp. 139-146, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Zuodong Jin, Muyan Yao, and Dan Tao, "Implicit Authentication with Sensor Normalization and Multi-Modal Domain Adaption based on Mobile Crowd Sensing," *CCF Transactions on Pervasive Computing and Interaction*, vol. 4, pp. 370-380, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jingwei Liu et al., "EPDA: Enhancing Privacy-Preserving Data Authentication for Mobile Crowd Sensing," *IEEE Global Communications Conference*, Singapore, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[19] Pengchen Ma, Dan Tao, and Tinyu Wu, "A Pseudonym based Anonymous Identity Authentication Mechanism for Mobile Crowd Sensing," *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, Chengdu, China, pp. 10-14, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] Yang Shi et al., "Obfuscatable Anonymous Authentication Scheme for Mobile Crowd Sensing," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2918-2929, 2019. [CrossRef] [Google Scholar] [Publisher Link]