**Journal of Administrative and Economic Sciences** • Vol 18, Issue 1 (2025) • p 439-462



# Recommendations for a More Economically Viable and Secure Crowdsensing Environment

**Mohannad Alswailim**

Department of Management Information Systems, College of Business and Economics, Qassim University • P.O. Box 6640, Buraidah 51452 • Saudi Arabia

Malswailim@qu.edu.sa

**Abstract:**

This scientific paper examines crowdsensing security and economic issues. The study focuses on Artificial intelligence (AI), blockchain, and cryptography. By analyzing their effects, this paper shows how these technologies increase crowdsensing security and economic sustainability. AI-enabled algorithms improve crowdsensing data processing and decision-making. AI methods help stakeholders make educated decisions by extracting key insights from crowdsourcing data. Data integrity, trustworthiness, and privacy in crowdsensing platforms depend on blockchain technology. By securing conversations and sensitive data, encryption improves security. This article emphasizes crowdsensing system economics, including cost-effectiveness, scalability, and revenue creation. AI in data analysis helps generate market insights, improve service quality, and drive innovation. Blockchain technology enables transparent, auditable transactions, providing new revenue streams. In conclusion, integrating AI, blockchain, and encryption, is critical for tackling crowdsensing security and economic concerns. The findings offer recommendations for stakeholders, researchers, and policymakers on how to properly harness these technologies in order to ensure secure and economically sustainable crowdsensing ecosystems.

**Keywords:** Crowdsensing, Security, Economic viability, Artificial intelligence, Blockchain, Cryptography.

## 1. Introduction

Crowdsensing has evolved as a disruptive paradigm that harnesses the pervasiveness of mobile devices and the collective strength of individuals to gather data about the physical environment on a previously unimagined scale [1], [2]. This novel technique opens the door to a wide range of applications, including environmental monitoring, urban planning, healthcare, transportation management, and others. However, crowdsensing system deployment demands careful consideration of both security and economic factors [3], [4].

Due to the engagement of a diverse and frequently anonymous crowd of individuals, security is a significant problem in crowdsensing [5], [6]. It is critical to ensure the privacy, integrity, and confidentiality of the obtained data in order to develop confidence and preserve the credibility of crowdsensing platforms [7], [8]. Furthermore, the danger of hostile attacks, data alteration, and unauthorized access is substantial and must be addressed [9], [10].

On the other side, economic feasibility is critical to the long-term success and widespread adoption of crowdsensing [11]. Because crowdsensing systems create massive amounts of data, efficient processing, storage, and analysis are critical in order to extract relevant insights [12]. Creating economically sustainable crowdsensing systems that can attract and retain stakeholders requires optimizing resource allocation, lowering costs, and researching income generation options [13].

To overcome these obstacles and fully realize the promise of crowdsensing, the integration of multiple modern technologies is required. AI tools such as machine learning and data analytics offer efficient processing and analysis of crowdsourced data, allowing stakeholders to make educated decisions and get important insights. With its decentralized and immutable nature, blockchain technology provides a safe and transparent foundation for maintaining data integrity, trust, and privacy [14], [15], [16]. Cryptography techniques improve communication security and protect sensitive data in crowdsensing situations.

We investigate the complex interaction between security and economic elements in crowdsensing situations in this research. We investigate the integration of artificial intelligence, blockchain, and encryption technologies, as well as the implications for improving security while encouraging economic viability [17], [18], [19], [20]. We hope to provide insights and recommendations for stakeholders, researchers, and policymakers to successfully exploit these technologies and develop secure and economically viable crowdsensing ecosystems by investigating these complex elements.

This paper is organized as follows: Section 2 provides an outline of crowdsensing's technological foundations, as well as the roles of AI, blockchain, and encryption in this context. Section 3 focuses on crowdsensing security concerns, while Section 4 investigates the economic ramifications of these technologies. Section 5 focuses on the use of AI in crowdsensing, followed by Section 6 recommendations for security and economic developments. Section 7 discusses future directions and problems, and Section 8 highlights the important findings and implications for future research and

practical implementation. The main aspected coved by in this paper are illustrated in Figure 1.

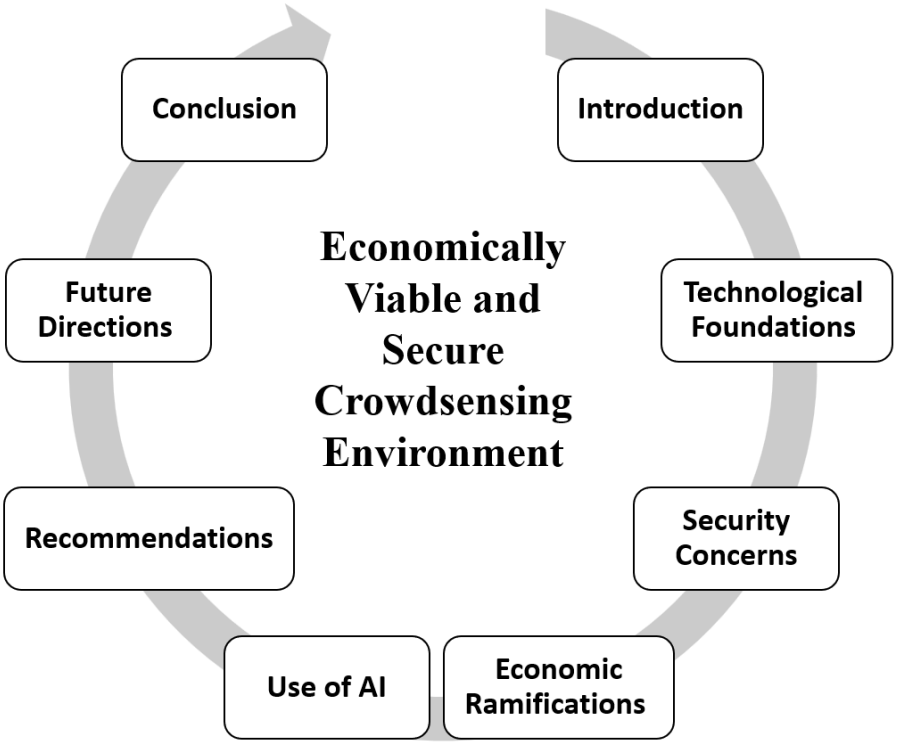


**Figure 1.** Illustration of the structure of the paper

## 1. Technological Foundations of Crowdsensing

### 1.1. Overview of crowdsensing and its key components

Crowdsensing, an influential paradigm, uses human intelligence to acquire physical data [21]. This system requires mobile devices with GPS, accelerometers, cameras, and microphones to be widely available [22]. These sensors help users record their environment, behaviors, and interactions. Crowdsensing data is valuable and applicable across fields [23]. Volunteers provide data for crowdsensing, creating a network for large-scale, real-time data collection [24]. The data includes location-based data, environmental data (air quality, noise levels), user-generated content (reviews, ratings), and social interactions [25]. A wide range of data helps understand the tangible domain and apply it to urban planning, transportation management, healthcare, and disaster response [26]. Mobile devices used by participants, a central server or cloud infrastructure, and apps or services that exploit the data make up crowdsensing platforms [27]. Participants can install specialized mobile apps or communicate data through pre-existing apps. After that, the data is processed, aggregated, and made available for analysis or application-specific use on the central server or cloud architecture [28]. The general architecture of a crowdsensing environment is illustrated in Figure 2.

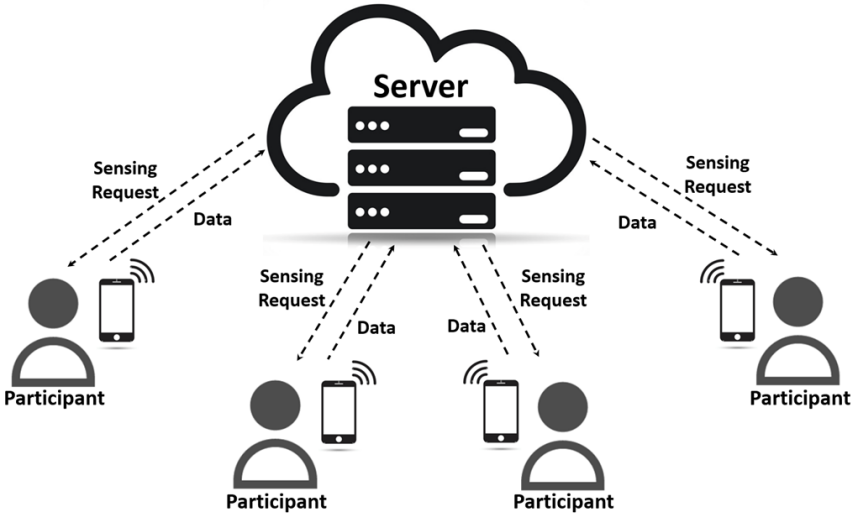


**Figure 2.** The general architecture of a crowdsensing environment

### 1.2. Role of AI in enhancing data analysis and decision-making in crowdsensing

AI is crucial for crowdsensing data processing and decision-making [29]. AI methods enable stakeholders to gain valuable insights from crowdsensing's massive data sets [30]. Machine learning algorithms like classification, clustering, and regression may identify patterns, predict trends, and make recommendations from historical data [31]. Crowdsensing can use AI algorithms for many purposes. In transportation management, AI may use crowdsensed traffic data to predict congestion and suggest the best routes [31]. AI can analyze crowdsourced health data to find disease epidemic patterns in healthcare [32]. AI-driven data analytics can use customer preferences and past data to provide tailored services and suggestions [33] . AI could improve crowdsensing platforms' data processing efficiency and capacity [34]. Data interpretation requires less manual labor with automated data processing and analysis. AI algorithms can adapt and learn from new input, improving insight precision and relevance [35].

### 1.3. Blockchain technology for ensuring data integrity, trust, and privacy

Blockchain technology's ability to protect crowdsensing platform data has received attention recently [36]. Blockchain is a decentralized ledger system that records and validates transactions across nodes [37]. Visible, immutable, and decentralized, the technology ensures crowdsensed data security and authenticity [38]. Blockchain technology can help crowdsensing solve problems [39]. It first preserves data integrity by creating an immutable record of data from several sources. Every data entry is cryptographically related to the previous one, creating an immutable sequence. Immutability protects crowdsensing data from illicit tampering. Blockchain technology also boosts crowdsensing platform participant confidence. Blockchain is decentralized because it eliminates a single authority for data validation and verification. The blockchain consensus mechanism verifies and validates participant data to ensure trustworthiness. Trust promotes crowdsensing ecosystem growth by encouraging participant collaboration. Blockchain technology also improves crowdsensing anonymity. Encrypting data before storing it on the blockchain allows parties to retain data control. Data is only accessible to authorized entities, ensuring privacy and

confidentiality. Smart contracts, autonomous contractual agreements with blockchain-based rules, can be used in crowdsensing systems. Smart contracts automate and verify agreement execution, enhancing openness and fairness. These methods can be used in the crowdsensing ecosystem to build explicit incentivization plans, recompense participants for their valuable contributions, and promote secure transactions.

### 1.4. Cryptography techniques for secure communication and data protection

In crowdsensing, cryptography is crucial for communication security and data protection. Cryptographic protocols ensure data privacy, integrity, and authenticity and validate transaction participants' identities [40]. Crowdsensing systems use encryption to protect data during transmission and storage. Data encryption converts original data into an unreadable format for unwanted parties. The decryption key is needed to decipher encrypted data [41]. Encryption prevents illegal access and protects data even if intercepted. Secure key exchange methods offer secure communication channels among crowdsensing platform participants. The above methods ensure encryption key exchange, ensuring that only authorized entities can access and decipher data [42]. Digital signatures are cryptographic methods used in crowdsensing to guarantee data authenticity. Digital signatures are created using a participant's private key. This identity verifies that the data comes from the source and has not been altered. Digital signatures ensure non-repudiation, so people cannot deny their involvement or contributions [43]. Homomorphic encryption, a growing cryptographic technique, allows calculations on encrypted data while ensuring data confidentiality. Crowdsensing platforms can use this technology for privacy-preserving data processing [44]. Homomorphic encryption encrypts sensitive data, allowing computations without decryption. Then, the calculations can be decrypted to reveal important findings while protecting the data. Cryptography in crowdsensing systems protects data, prevents tampering, and builds confidence [45].

## 2. Security Considerations in Crowdsensing

### 2.1. Data Privacy and Confidentiality

Ensuring the protection of personal and sensitive information collected from participants is of utmost importance in the context of crowdsensing [46] , [47]. In order to safeguard data privacy, it is imperative for crowdsensing platforms to incorporate robust encryption methodologies, such as symmetric or asymmetric encryption, to uphold the secrecy of the data throughout both storage and transmission processes [48] [49]. Furthermore, it is possible to employ secure data transmission protocols such as Secure Sockets Layer and Transport Layer Security (SSL/TLS) to establish encrypted connections between the devices of participants and the crowdsensing platform [50]. This measure effectively prevents illegal access or interception of data. In addition, the use of secure storage technologies, such as encrypted databases or secure cloud storage, can provide an additional level of safeguarding for the data of participants [51]. In order to bolster data privacy, it is possible to employ anonymization techniques to eliminate personally identifiable information from the data that has been gathered. Various techniques, such as generalization, randomization, and k-anonymity, can be utilized to

anonymize data points, thereby safeguarding the privacy of individuals and preventing their direct identification from the information collected by crowdsensing.

### 2.2. Data Integrity and Tampering Prevention

For crowdsensed data to be reliable, data integrity is crucial [52]. Crowdsensing platforms can use several methods to reduce data tampering hazards. One method is to use digital signatures in data acquisition. Digital signatures use public-key cryptography to verify data authenticity [53]. Participants can authenticate their data contributions by adding their private keys, and the crowdsensing platform can verify data fidelity using the matching public keys. Checksums or hash functions can also ensure data integrity [54]. The above functions use data to produce different values. Comparing the received data to the computed checksum makes tampering detection easy. Blockchain technology can improve crowdsensing data fidelity. A decentralized and immutable blockchain ledger stores crowdsensed data, making data modification unlikely since it would require altering many distributed copies of the blockchain.

### 2.3. User Authentication and Access Control

User authentication is crucial to crowdsensing platform security. Participants and platform users can be authenticated using robust authentication methods like Two-Factor Authentication (2FA) or biometric authentication [55]. The 2FA requires a password and a temporary verification code sent to a mobile device, increasing security [56]. Biometric authentication systems like fingerprint or facial recognition use physiological traits to validate user identities, boosting platform security. Access control rules limit data access based on user roles and permissions. The crowdsensing environment can assign permissions to users depending on their roles using Role-Based Access Control (RBAC) [57]. This ensures that only authorized users can access, change, or retrieve data for their jobs. Additional monitoring and auditing protocols for user activities can help identify unauthorized behavior or access attempts [58]. The crowdsensing platform monitors and records user actions using sophisticated logging and SIEM technologies. This allows the platform to quickly detect and resolve security issues.

### 2.4. Malicious Behavior Detection and Prevention

Crowdsensing platforms should detect and address malicious behavior. Anomaly detection can identify outliers in crowdsensed data. Advanced machine learning methods like clustering or classification models can be trained to find data patterns and abnormalities [59]. This helps detect data manipulation and malicious activity. In addition, reputation systems can assess persons' credibility and dependability [60]. Reputation scores, based on participants' accuracy and consistency, identify those with negative reputations. This identification allows further analysis of their contributions, reducing the impact of incorrect or malicious data. Data validation can verify crowdsensed data's coherence, legitimacy, and authenticity [61]. The algorithms can discover data outliers, timestamp or location anomalies, and data that clashes with other reputable sources. The software can identify and remove malicious data using data validation methods, ensuring the integrity and quality of crowdsourced information [62].

### 2.5. Secure Communication and Trust Establishment

Data integrity and confidentiality during crowdsensing transmission require secure communication methods. Participants' devices can connect to the crowdsensing platform securely using SSL/TLS. The above protocols use encryption to protect data during transmission, reducing the possibility of eavesdropping [63]. Building trust between participants and the crowdsensing platform is crucial to ecosystem integrity and security [64]. Open and clear communication about security, privacy, and data management helps build trust in the platform. Consistent and timely security, vulnerability, and incident response updates can enhance participant confidence in the platform. Crowdsensing platforms might use impartial third-party certifications or audits to generate credibility [65]. These certifications show that the platform follows industry-leading practices and security criteria, giving participants confidence in its security. Additionally, comprehensive and user-friendly privacy rules must outline data collection, usage, retention, and disclosure methods. Participants must have full visibility and control over their data, including the ability to participate or not. By giving people control and being transparent, the platform can build trust and participation [66].

### 2.6. Incident Response and Recovery

It is imperative for crowdsensing platforms to establish a comprehensive incident response plan in order to efficiently address and manage security breaches or occurrences [67]. The proposed approach aims to establish unambiguous protocols and accountabilities in order to identify, address, and restore operations following instances of security breaches [68]. When faced with a security incident, the initial course of action is to segregate the impacted systems or compromised data in order to minimize the consequences and mitigate any additional harm [69]. The process entails the disconnection of compromised devices or networks from the crowdsensing platform, followed by a comprehensive investigation to ascertain the origin and magnitude of the breach.

It is imperative to swiftly inform the individuals who have been impacted by the security incident, ensuring that they receive pertinent details regarding the nature of the breach, the dangers involved, and recommended measures to safeguard their personal information [70]. Effective communication and a transparent approach in the context of incident response are crucial in preserving the trust and confidence of individuals involved in the platform. Upon resolving the immediate issues, it is imperative for the platform to undertake a post-incident study in order to ascertain the underlying cause of the breach and then implement requisite measures to mitigate the likelihood of future occurrences of a similar nature. This process may encompass the remediation of vulnerabilities, the augmentation of security controls, or the revision of security policies and procedures. Regular security audits and vulnerability assessments can proactively detect possible vulnerabilities and facilitate prompt remedy. Through the implementation of a clearly defined incident response strategy and the ongoing enhancement of security measures, crowdsensing platforms can proficiently alleviate the consequences of security incidents, safeguard the data of participants, and uphold the integrity and reliability of the crowdsensing ecosystem.

In the context of crowdsensing, it is imperative to address these security aspects in order to safeguard the confidentiality and privacy of participants' data, uphold the accuracy and reliability of the acquired information, and cultivate a sense of trust and confidence in the platform. By including robust security protocols, utilizing encryption and authentication systems, detecting and mitigating malicious activities, ensuring safe communication channels, and establishing a complete incident response strategy, stakeholders can establish a secure and dependable crowdsensing ecosystem.

## 3. Economic Implications of Crowdsensing Technologies

### 3.1. Cost Efficiency and Resource Optimization

Cost-effectiveness and resource optimization are crowdsensing technology' main economic benefits. Using sophisticated sensors or experienced staff to do surveys might be expensive [71] . Crowdsensing uses cellphones and other linked devices to avoid expensive infrastructure investment. Through users' devices and collective sensing talents, crowdsensing can capture large amounts of data at a lower cost than conventional methods. This strategy is cost-effective and allows businesses and researchers to efficiently obtain and analyze enormous amounts of data, enabling broad applications in multiple sectors. Crowdsensing optimizes resources by using existing infrastructure and resources. Instead of buying more traffic sensors, transportation authorities can use GPS data from participants' smartphones to monitor traffic congestion and improve network efficiency. Optimization reduces costs and improves resource allocation, benefiting both public and commercial sectors.

### 3.2. New Business Opportunities and Revenue Generation

Crowdsensing technology may create new revenue streams. Organizations can use crowdsourced data to get insights and make smart decisions. Offering data-driven services or selling aggregated and anonymized data to interested parties can generate revenue [72] [73]. Crowdsensing data can reveal consumer preferences, behavior, and purchase habits in retail. This data can help retailers improve shop layouts, personalize marketing, and offer geographic specials. Organizations may improve customer experiences, sales, and revenue by using crowdsensed data. By providing infrastructure, tools, and services, crowdsensing platforms can become successful businesses. These platforms provide data gathering frameworks, analytics tools, and data management services allowing corporations and academics to use crowdsensing without building their own infrastructure. Crowdsensing platforms might charge fees or use a subscription model to generate revenue and value.

### 3.3. Job Creation and Economic Growth

Crowdsensing technology can create new jobs and boost the economy. Crowdsensing projects require platform administrators, data analysts, quality assurance specialists, and project managers [74], [75]. Demand for crowdsensing services and information has created jobs in various fields. Crowdsensing technology can also boost economic growth by encouraging innovation and entrepreneurship. Crowdsensed data and easy access to platforms allow individuals and organizations to create creative apps, services, and products. An entrepreneurial environment can boost economic growth, investment,

and a competitive crowdsensing technology industry. Additionally, crowdsensing data can benefit academics, the academic community, and policymakers. Crowdsensed data can inform legislation, urban planning, and industry innovation. Thus, these phenomena can boost economic and social progress.

### 3.4. Social and Environmental Impact

Crowdsensing technology can improve society and the environment, boosting the economy. Crowdsensing efforts can solve social problems and improve quality of life by leveraging individual strengths. Crowdsensing could improve healthcare industry monitoring of public health trends, illness outbreaks, and environmental elements that affect well-being. This data could help authorities and healthcare professionals make evidence-based decisions, allocate resources more efficiently, and provide targeted solutions. Crowdsensing improves public health and lowers healthcare costs, improving economic stability and social well-being. Crowdsensing could support environmental sustainability activities. Crowdsensing collects air quality, noise, and waste management data. This helps people make informed decisions and promotes eco-friendly practices. This phenomenon can help conserve resources, reduce pollution, and enhance environmental management, resulting in long-term economic benefits and a more sustainable global ecology.

In conclusion, crowdsensing technology has major economic effects. Cost efficiency, resource optimization, new business prospects, and revenue generation are the benefits. Crowdsensing boosts economic growth, job creation, and innovation and entrepreneurship. It also improves social and environmental conditions, contributing to economic stability and a sustainable future. Crowdsensing technologies can boost the economy and society.

## 4. Artificial intelligence (AI) Integration in Crowdsensing

### 4.1. Data Processing and Analysis

AI is crucial for crowdsensed data processing and analysis. AI solutions are needed to manage and gain insights from crowdsensing's massive data sets from multiple sources.

AI algorithms can preprocess and clean raw data from many participants. These tasks include noise reduction, outlier detection, and data integration. AI methods can improve crowdsensed data quality and reliability, improving future analysis and decision-making. AI also enables machine learning and data mining to identify patterns, trends, and correlations in crowdsensing data. These methods can expose hidden insights, construct prediction models, and enable real-time decision-making. In transportation planning, AI systems can use crowdsensed traffic data to predict congestion patterns, improve traffic flow, and suggest alternative routes.

### 4.2. Intelligent Task Allocation and Resource Management

Crowdsensing systems using AI can efficiently allocate work and manage resources. AI algorithms can be used to assign work to crowdsensing campaign participants based on their skills, location, and availability [76]. AI algorithms can match activities with the right participants by analyzing participant profiles, historical data, and contextual

information. This approach optimizes data collection efficiency and accuracy. Intelligent task allocation strategies reduce redundancy and maximize resource efficiency by assigning participants to tasks. Additionally, AI can help crowdsensing programs manage resources efficiently. If a region needs more data coverage, AI systems can dynamically route participants there. Adaptive resource management ensures crowdsensed data collecting adapts to changing needs and priorities [77].

### 4.3. Intelligent Quality Control and Validation

The quality and reliability of crowdsensed data must be considered before use. Crowdsensing with AI enables intelligent quality control and validation processes. AI systems can analyze crowdsensed data in real time [78]. This includes identifying erroneous or inconsistent data points, guaranteeing data integrity, and detecting malicious or manipulated contributions. Crowdsensing solutions can reject untrustworthy data using AI, ensuring the use of only high-quality data for analysis and decision-making. To verify crowdsourcing data, AI-driven validation methods might compare it to ground truth or reference data. AI algorithms can compare crowdsensing and official monitoring station air quality values for environmental monitoring. This ensures data uniformity and reliability [79].

### 4.4. User Experience Enhancement

AI in crowdsensing technologies also prioritizes user experience. Personalization using AI algorithms can improve crowdsensing by adapting to each user's preferences, skills, and environmental circumstances. AI can adjust task frequency and type based on past performance and feedback. Personalization improves crowdsensing participant engagement, satisfaction, and retention. AI-driven recommendation systems can also suggest relevant tasks or interests, motivating and engaging users. Crowdsensing platforms leverage AI to create a tailored and engaging user experience, encouraging persistent participation and a sense of community.

### 4.5. Ethical Considerations and Bias Mitigation

AI in crowdsensing requires ethical considerations and prejudice reduction. The development and implementation of AI algorithms for data processing, analysis, and decision-making must prioritize fairness, openness, and accountability. AI models must not promote biases or discriminate against specific groups or communities. To eliminate biases and encourage fair and inclusive crowdsensing participation and representation, data collection methods, algorithm design, and model training must be carefully considered.

Additionally, AI algorithm openness and explainability boost stakeholder and participant confidence. It's crucial to explain how AI is used in crowdsensing, decision-making, and data processing. This is essential to address privacy concerns and promote transparency.

In conclusion, crowdsensing with AI has many benefits. AI helps with data processing and analysis, task allocation and resource management, quality control and validation, user experience, and ethical considerations. Crowdsensing can completely harness the value of crowdsourced data by using AI methods, improving analysis, decision-making,

and user experiences. To responsibly and effectively use AI in crowdsensing, a balance must be struck between using AI and addressing ethical problems [80].

## 5. Recommendations for Security and Economic Advancements in Crowdsensing

### 5.1. Security and Privacy Measures

In order to guarantee the efficacy and extensive acceptance of crowdsensing technologies, it is imperative to implement solid security and privacy protections. The subsequent suggestions can contribute to the improvement of security in crowdsensing:

- Data Encryption and Anonymization: The implementation of robust encryption methodologies is important in order to safeguard crowdsensed data throughout its transmission and storage processes. Furthermore, it is imperative to implement anonymization techniques that effectively eliminate any personally identifiable information from the collected data in order to safeguard the privacy of the participants.
- Access Control and Authentication: Utilize robust access control measures to effectively limit unwanted access to crowdsensing platforms and associated data. The implementation of multi-factor authentication methods is recommended in order to authenticate the identity of participants and users of the platform.
- Secure Data Aggregation: Use robust data aggregation methodologies that maintain the confidentiality of data while enabling insightful analysis. Various strategies, such as differential privacy and homomorphic encryption, can be employed to safeguard the privacy of individual contributions while facilitating precise data analysis.
- Threat Detection and Response: Develop and deploy resilient mechanisms for identifying and addressing security vulnerabilities, including but not limited to instances of data manipulation, impersonation, or deliberate disruption of service. Utilize real-time monitoring techniques and anomaly detection algorithms to swiftly detect and address possible security breaches.

### 5.2. Incentive Mechanisms

In order to foster extensive involvement and active participation in crowdsensing endeavors, the implementation of efficient incentive structures is of utmost importance. The subsequent suggestions can facilitate the promotion of economic progress in the field of crowdsensing:

- Financial Incentives: Offer financial rewards or compensation to participants for their contributions to crowdsensing campaigns. This can include monetary incentives, gift cards, or discounts on products or services.
- Gamification: One potential approach to enhance the engagement and enjoyment of participants in crowdsensing is to incorporate gamification components. The aforementioned features encompass leaderboards, badges, and virtual awards, which serve to acknowledge and exhibit the accomplishments of participants.
- Reputation Systems: The implementation of reputation systems that monitor and incentivize participants according to the caliber and dependability of their contributions. In order to allocate resources more efficiently, it may be

advantageous to grant participants who possess a favorable reputation preferential access to jobs of greater value or other advantages.

- Collaborative Incentives: Promote collaboration among participants through the use of incentives that encourage collaborative successes or the pursuit of shared goals. An illustration of this concept involves the provision of incentives to participants, which are contingent upon the collective accomplishments of a group or community in successfully attaining predetermined objectives related to crowdsensing.

### 5.3. Collaboration and Partnerships

In order to optimize the capabilities of crowdsensing technologies, it is imperative to foster collaboration and establish partnerships among relevant parties. The subsequent suggestions have the potential to enhance collaboration and foster economic progress in the field of crowdsensing.

- Public-Private Partnerships: Promote synergistic partnerships across public institutions, corporate companies, and academia to use their collective knowledge, assets, and data. Collaborative alliances of this nature have the potential to foster groundbreaking resolutions, facilitate the utilization of common resources, and provide financially viable frameworks that promote long-term sustainability.
- Data Sharing and Open Application Programming Interfaces (APIs): Promote the practice of data sharing across crowdsensing platforms, academics, and pertinent organizations by means of open APIs. The aforementioned statement serves to enhance interoperability, foster innovation, and facilitate the creation of value-added services.
- Standardization and Best Practices: The objective is to provide universally accepted standards and optimal approaches for crowdsensing activities, encompassing methodology for data collecting, formats for data representation, and guidelines for ensuring privacy. The process of standardization plays a crucial role in enabling the interchange of data, promoting comparability and interoperability. This, in turn, enhances collaboration and promotes the effective exploitation of crowdsensed data, resulting in improved efficiency.
- Collaboration with Regulatory Bodies: It is imperative to actively collaborate with regulatory agencies, legislators, and legal experts in order to guarantee that crowdsensing efforts adhere to relevant laws and regulations. Engaging in collaborative efforts with regulatory organizations can effectively mitigate apprehensions pertaining to data protection, privacy, and ethical considerations.

| Topic | Recommendations |
|---|---|
| Security and Privacy Measures | • Implement data encryption and anonymization to protect crowdsensed data.<br>• Utilize access control and multi-factor authentication to limit access.<br>• Employ secure data aggregation methods like differential privacy.<br>• Develop threat detection and response mechanisms for security vulnerabilities. |

| Topic | Recommendations |
|---|---|
| Incentive Mechanisms | • Provide financial rewards, gift cards, or discounts for participant contributions.<br>• Incorporate gamification elements to enhance engagement.<br>• Implement reputation systems to reward reliable contributions.<br>• Promote collaborative incentives for achieving shared goals. |
| Collaboration and Partnerships | • Foster public-private partnerships to leverage collective resources.<br>• Encourage data sharing and open APIs for improved interoperability.<br>• Establish standards and best practices for crowdsensing activities.<br>• Collaborate with regulatory bodies to ensure compliance with laws and regulations. |

**Table 1:** Strategic Recommendations

Table 1 provides a concise overview of strategic recommendations aimed at enhancing security and fostering economic growth within the realm of crowdsensing technology. By applying the aforementioned recommendations, the enhancement of security and privacy in the context of crowdsensing can be achieved, hence facilitating economic progress. The use of this approach will facilitate the development of trust, promote active involvement, and unleash the whole capabilities of crowdsensed data in diverse industries, ultimately resulting in enhanced decision-making processes, increased creativity, and bolstered economic expansion.

## 6. Future Directions and Challenges

### 6.1. Advancements in Artificial intelligence (AI) and Machine Learning

The forthcoming developments in AI and machine learning approaches will bring about notable progress in the field of crowdsensing. These technological developments will facilitate the use of more advanced data analysis techniques, predictive modeling algorithms, and decision-making capabilities. AI algorithms are expected to exhibit enhanced intelligence and efficiency, enabling the real-time analysis of extensive crowdsensed data and the derivation of practical insights. Moreover, the use of deep learning and neural networks would augment the capacity to discern intricate patterns and generate precise forecasts using data gathered from crowdsensing.

### 6.2. Edge Computing and Mobile Devices

The future of crowdsensing will be influenced by the widespread adoption of edge computing and the advancing capabilities of mobile devices. Edge computing facilitates the execution of data processing and analysis in close proximity to the origin of the

data, hence diminishing latency and enabling prompt decision-making in real-time. Mobile devices will maintain their pivotal significance in the field of crowdsensing, as they function as the principal instruments for data collection utilized by participants. Future developments will prioritize the enhancement of data processing and analysis capabilities on mobile devices, with the aim of enabling more efficient and energy-conscious crowdsensing applications.

### 6.3. Integration with Internet of Things (IoT)

The integration of crowdsensing and IoT will present novel opportunities and complexities. IoT devices have the capability to function as sensors, enabling them to gather data from the surrounding physical world. This data can then be utilized to actively participate in crowdsensing initiatives. The integration of IoT devices with crowdsensing platforms will facilitate the collecting and analysis of data in a seamless manner. This integration will contribute to a more thorough understanding of intricate systems and environments. Nevertheless, it is imperative to acknowledge and tackle certain obstacles in order to effectively harness the capabilities of crowdsensing enabled by IoT. These problems encompass data interoperability, device heterogeneity, and scalability.

### 6.4. Ethical and Privacy Concerns

The rise in popularity of crowdsensing will necessitate a heightened focus on ethical considerations and privacy problems. The acquisition and application of individualized information give rise to issues regarding the granting of consent, the ownership of data, and the safeguarding of participant confidentiality. Future research should prioritize the development of comprehensive privacy frameworks, the establishment of transparent data handling practices, and the provision of individuals with autonomy over their personal data. In addition, it is imperative to acknowledge and mitigate potential biases inherent in crowdsensing data and algorithms in order to uphold principles of fairness and prevent instances of discrimination.

### 6.5. Sustainability and Energy Efficiency

Future crowdsensing attempts will prioritize sustainability and energy efficiency as crucial factors to be taken into account. The environmental impact of data collecting, processing, and transmission can be substantial as the size of crowdsensing expands. This is mostly due to the increased energy consumption involved. Future research should investigate energy-efficient methods for data collection, optimization algorithms, and sustainable strategies for deployment. The utilization of renewable energy sources and the integration of energy-conscious design principles can effectively reduce the environmental impact of crowdsensing applications.

### 6.6. Data Fusion and Cross-Domain Integration

The integration and fusion of data from various sources and domains holds significant potential for advancing the field of crowdsensing in the future. The integration of crowdsensed data with data from many domains, including social media, satellite images, and government statistics, can yield more profound insights and facilitate a more thorough study. Nevertheless, it is imperative to acknowledge and tackle the

obstacles associated with data integration, interoperability, and data quality. The future trajectory should prioritize the advancement of resilient data fusion methodologies, the establishment of standardized data formats, and the creation of frameworks to facilitate collaboration across different domains.

### 6.7. Trust and Social Acceptance

The success of crowdsensing projects will depend significantly on the establishment of trust and social acceptance. It is imperative to acknowledge and prioritize the resolution of issues pertaining to the exploitation of data, breaches of privacy, and biases inherent in algorithms. In the forthcoming trajectory, it is imperative to prioritize the incorporation of openness, accountability, and user-centric design principles. The establishment of open conversation and active involvement of participants and stakeholders in the decision-making process can contribute to the cultivation of trust and promotion of social acceptance towards crowdsensing technology.

### 6.8. Regulatory and Legal Frameworks

The significance of regulatory and legal frameworks will grow in tandem with the advancement of crowdsensing. Future research should prioritize the establishment of explicit principles and standards pertaining to the protection of data, privacy, and ethical considerations within the context of crowdsensing. Engaging in partnerships with regulatory organizations, legislators, and legal experts can facilitate the compliance of crowdsensing efforts with legal frameworks and ethical standards.

| Topic | Summary |
|---|---|
| Advancements in AI and Machine Learning | AI and machine learning will improve real-time data analysis and forecasting in crowdsensing, leveraging deep learning for enhanced pattern recognition. |
| Edge Computing and Mobile Devices | Adoption of edge computing and mobile device advancements will enable real-time, efficient, and energy-saving crowdsensing applications. |
| Integration with Internet of Things (IoT) | Crowdsensing and IoT integration will enhance data gathering and analysis but faces challenges with interoperability and scalability. |
| Ethical and Privacy Concerns | As crowdsensing grows, addressing privacy, consent, data ownership, and bias becomes critical for ethical practices. |
| Sustainability and Energy Efficiency | Emphasis on sustainability will lead to energy-efficient crowdsensing methods and the use of renewable energy sources. |
| Data Fusion and Cross-Domain Integration | Combining crowdsensed data with other sources will offer deeper insights but requires overcoming data integration and quality challenges. |

| Topic | Summary |
|---|---|
| Trust and Social Acceptance | Building trust and acceptance involves addressing data exploitation and privacy breaches through transparent and participatory practices. |
| Regulatory and Legal Frameworks | Establishing clear regulatory standards is essential for aligning crowdsensing with data protection and ethical guidelines. |

**Table 2:** Core Directions and challenges for the future development of crowdsensing technology

Table 2 concisely captures the core directions and challenges for the future development of crowdsensing technology. In summary, the potential of crowdsensing in the future is highly promising, owing to the progress made in AI, edge computing, integration of IoT, and data fusion. Nevertheless, it is imperative to successfully tackle the difficulties pertaining to ethics, privacy, sustainability, and trust. By adopting and actively addressing these prospective avenues, crowdsensing has the potential to further alter the processes of data gathering, analysis, and decision-making, hence facilitating significant breakthroughs across diverse fields.

## 7. Conclusion

The concept of crowdsensing has emerged as a prominent and effective method for collecting and analyzing data, offering substantial prospects in various domains including smart cities, healthcare, environmental monitoring, and transportation. The usage of collective intelligence and the active involvement of individuals enhances the capture of comprehensive and current data, hence enabling the discovery of insights and solutions that were previously unattainable. This study investigates the key components of crowdsensing, including its benefits, challenges, and recommendations related to security, economic development, and future directions. The benefits of crowdsensing are easily evident as it allows users to actively engage in decision-making processes that are driven by data. The concept of crowdsensing allows for the efficient and cost-effective collection of data on a broad scale, facilitated by the widespread use of mobile devices and advancements in connectivity. The application of crowdsensed data has the potential to yield significant insights that can inform policy development, enhance urban planning approaches, foster environmental sustainability, and enable the delivery of customized services. However, the successful deployment of crowdsensing is accompanied by some challenges that need to be adequately resolved to ensure its success and sustainability in the long run. In order to ensure the integrity of participant data and foster confidence in the system, it is imperative to adopt stringent protocols that effectively address issues pertaining to security and privacy. The advancement of the economy relies on the existence of effective incentive mechanisms that successfully motivate individuals to actively participate and make significant contributions. The facilitation of resource, expertise, and data sharing necessitates the formation of

collaboration and partnerships among stakeholders. Furthermore, the future trajectory of crowdsensing will be shaped by various other factors, including developments in artificial intelligence, the integration of edge computing and internet of things, and ethical considerations. In brief, crowdsensing is an innovative approach to data collection and analysis that has the potential to greatly influence decision-making processes and drive advancements across several industries. By following the suggested recommendations outlined in this scientific publication, relevant stakeholders can overcome challenges and maximize the benefits of crowdsensing in terms of security enhancement, economic advancement, and future planning. The continuous progress, collaborative endeavors, and adoption of ethically and ecologically sound approaches will support the gradual growth and significant influence of crowdsensing in promoting an intelligent and data-driven global community.

**References:**

[1] J. Liu, H. Shen, H. S. Narman, W. Chung, and Z. Lin, "A Survey of Mobile Crowdsensing Techniques: A Critical Component for The Internet of Things," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 3, p. 18:1-18:26, Jun. 2018, doi: 10.1145/3185504.

[2] L. Wang, D. Zhang, Y. Wang, C. Chen, X. Han, and A. M'hamed, "Sparse mobile crowdsensing: challenges and opportunities," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 161–167, Jul. 2016, doi: 10.1109/MCOM.2016.7509395.

[3] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 32–39, Nov. 2011, doi: 10.1109/MCOM.2011.6069707.

[4] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, and P. Bouvry, "A Survey on Mobile Crowdsensing Systems: Challenges, Solutions, and Opportunities," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2419–2465, 2019, doi: 10.1109/COMST.2019.2914030.

[5] I. J. Vergara-Laurens, L. G. Jaimes, and M. A. Labrador, "Privacy-Preserving Mechanisms for Crowdsensing: Survey and Research Challenges," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 855–869, Aug. 2017, doi: 10.1109/JIOT.2016.2594205.

[6] Z. Wang *et al.*, "When Mobile Crowdsensing Meets Privacy," *IEEE Commun. Mag.*, vol. 57, no. 9, pp. 72–78, Sep. 2019, doi: 10.1109/MCOM.001.1800674.

[7] J. Xiong *et al.*, "A Personalized Privacy Protection Framework for Mobile Crowdsensing in IIoT," *IEEE Trans. Ind. Inform.*, vol. 16, no. 6, pp. 4231–4241, Jun. 2020, doi: 10.1109/TII.2019.2948068.

[8] Z. Wang *et al.*, "Personalized Privacy-Preserving Task Allocation for Mobile Crowdsensing," *IEEE Trans. Mob. Comput.*, vol. 18, no. 6, pp. 1330–1341, Jun. 2019, doi: 10.1109/TMC.2018.2861393.

[9] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling Privacy-Preserving Incentives for Mobile Crowd Sensing Systems," in *2016 IEEE 36th*

*International Conference on Distributed Computing Systems (ICDCS)*, Jun. 2016, pp. 344–353. doi: 10.1109/ICDCS.2016.50.

[10] J. W. Kim, K. Edemacu, and B. Jang, "Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey," *J. Netw. Comput. Appl.*, vol. 200, p. 103315, Apr. 2022, doi: 10.1016/j.jnca.2021.103315.

[11] D. Li, S. Wang, J. Liu, H. Liu, and S. Wen, "Crowdsensing From the Perspective of Behavioral Economics: An Incentive Mechanism Based on Mental Accounting," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9123–9139, Oct. 2019, doi: 10.1109/JIOT.2019.2928035.

[12] M. H. Cheung, F. Hou, and J. Huang, "Delay-Sensitive Mobile Crowdsensing: Algorithm Design and Economics," *IEEE Trans. Mob. Comput.*, vol. 17, no. 12, pp. 2761–2774, Dec. 2018, doi: 10.1109/TMC.2018.2815694.

[13] B. Liu, W. Zhou, T. Zhu, H. Zhou, and X. Lin, "Invisible Hand: A Privacy Preserving Mobile Crowd Sensing Framework Based on Economic Models," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4410–4423, May 2017, doi: 10.1109/TVT.2016.2611761.

[14] "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 03, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8306424

[15] J. An, D. Liang, X. Gui, H. Yang, R. Gui, and X. He, "Crowdsensing Quality Control and Grading Evaluation Based on a Two-Consensus Blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4711–4718, Jun. 2019, doi: 10.1109/JIOT.2018.2883835.

[16] X. Tao and A. S. Hafid, "ChainSensing: A Novel Mobile Crowdsensing Framework With Blockchain," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2999–3010, Feb. 2022, doi: 10.1109/JIOT.2021.3094670.

[17] Y. Chen and H. Wang, "IntelligentCrowd: Mobile Crowdsensing via Multi-Agent Reinforcement Learning," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 5, no. 5, pp. 840–845, Oct. 2021, doi: 10.1109/TETCI.2020.3042244.

[18] D. Chatzopoulos, S. Gujar, B. Faltings, and P. Hui, "Privacy Preserving and Cost Optimal Mobile Crowdsensing Using Smart Contracts on Blockchain," in *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, Oct. 2018, pp. 442–450. doi: 10.1109/MASS.2018.00068.

[19] Z. Chen, C. Fiandrino, and B. Kantarci, "On blockchain integration into mobile crowdsensing via smart embedded devices: A comprehensive survey," *J. Syst. Archit.*, vol. 115, p. 102011, May 2021, doi: 10.1016/j.sysarc.2021.102011.

[20] W. Wang *et al.*, "BSIF: Blockchain-Based Secure, Interactive, and Fair Mobile Crowdsensing," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3452–3469, Dec. 2022, doi: 10.1109/JSAC.2022.3213306.

[21] D. Belli, S. Chessa, B. Kantarci, and L. Foschini, “Toward Fog-Based Mobile Crowdsensing Systems: State of the Art and Opportunities,” *IEEE Commun. Mag.*, vol. 57, no. 12, pp. 78–83, Dec. 2019, doi: 10.1109/MCOM.001.1900003.

[22] K. Abualsaud *et al.*, “A Survey on Mobile Crowd-Sensing and Its Applications in the IoT Era,” *IEEE Access*, vol. 7, pp. 3855–3881, 2019, doi: 10.1109/ACCESS.2018.2885918.

[23] W. Zamora, C. T. Calafate, J.-C. Cano, and P. Manzoni, “A Survey on Smartphone-Based Crowdsensing Solutions,” *Mob. Inf. Syst.*, vol. 2016, p. e9681842, Dec. 2016, doi: 10.1155/2016/9681842.

[24] D. E. Boubiche, M. Imran, A. Maqsood, and M. Shoaib, “Mobile crowd sensing – Taxonomy, applications, challenges, and solutions,” *Comput. Hum. Behav.*, vol. 101, pp. 352–370, Dec. 2019, doi: 10.1016/j.chb.2018.10.028.

[25] H. Vahdat-Nejad, E. Asani, Z. Mahmoodian, and M. H. Mohseni, “Context-aware computing for mobile crowd sensing: A survey,” *Future Gener. Comput. Syst.*, vol. 99, pp. 321–332, Oct. 2019, doi: 10.1016/j.future.2019.04.052.

[26] “Sensors | Free Full-Text | Crowdsensing in Smart Cities: Overview, Platforms, and Environment Sensing Issues.” Accessed: Feb. 03, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/18/2/460

[27] “The Emergence of Visual Crowdsensing: Challenges and Opportunities | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Feb. 03, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7982609

[28] S. Chen, M. Li, K. Ren, and C. Qiao, “Crowd Map: Accurate Reconstruction of Indoor Floor Plans from Crowdsourced Sensor-Rich Videos,” in *2015 IEEE 35th International Conference on Distributed Computing Systems*, Jun. 2015, pp. 1–10. doi: 10.1109/ICDCS.2015.9.

[29] P. Grubitzsch, E. Werner, D. Matusek, V. Stojanov, and M. Hähnel, “AI-Based Transport Mode Recognition for Transportation Planning Utilizing Smartphone Sensor Data From Crowdsensing Campaigns,” in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, Sep. 2021, pp. 1306–1313. doi: 10.1109/ITSC48978.2021.9564502.

[30] Z. Zhou, H. Liao, B. Gu, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, “Robust Mobile Crowd Sensing: When Deep Learning Meets Edge Computing,” *IEEE Netw.*, vol. 32, no. 4, pp. 54–60, Jul. 2018, doi: 10.1109/MNET.2018.1700442.

[31] A. Alharam, H. Otrok, W. Elmedany, A. B. Bakht, and N. Alkaabi, “AI-Based Anomaly and Data Posing Classification in Mobile Crowd Sensing,” in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sep. 2021, pp. 225–229. doi: 10.1109/3ICT53449.2021.9581443.

[32] J. Xiong, M. Zhao, M. Z. A. Bhuiyan, L. Chen, and Y. Tian, “An AI-Enabled Three-Party Game Framework for Guaranteed Data Privacy in Mobile Edge

Crowdsensing of IoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 922–933, Feb. 2021, doi: 10.1109/TII.2019.2957130.

[33] Y. Zhang and B. Kantarci, "Invited Paper: AI-Based Security Design of Mobile Crowdsensing Systems: Review, Challenges and Case Studies," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, Apr. 2019, pp. 17–1709. doi: 10.1109/SOSE.2019.00014.

[34] L. Xiao, Y. Li, G. Han, H. Dai, and H. V. Poor, "A Secure Mobile Crowdsensing Game With Deep Reinforcement Learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 1, pp. 35–47, Jan. 2018, doi: 10.1109/TIFS.2017.2737968.

[35] M. E. Barachi, F. Kamoun, J. Ferdaos, M. Makni, and I. Amri, "An artificial intelligence based crowdsensing solution for on-demand accident scene monitoring," *Procedia Comput. Sci.*, vol. 170, pp. 303–310, Jan. 2020, doi: 10.1016/j.procs.2020.03.044.

[36] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019, doi: 10.1016/j.future.2018.11.046.

[37] Z. Ning *et al.*, "Blockchain-Enabled Intelligent Transportation Systems: A Distributed Crowdsensing Framework," *IEEE Trans. Mob. Comput.*, vol. 21, no. 12, pp. 4201–4217, Dec. 2022, doi: 10.1109/TMC.2021.3079984.

[38] J. Hu, K. Yang, K. Wang, and K. Zhang, "A Blockchain-Based Reward Mechanism for Mobile Crowdsensing," *IEEE Trans. Comput. Soc. Syst.*, vol. 7, no. 1, pp. 178–191, Feb. 2020, doi: 10.1109/TCSS.2019.2956629.

[39] "CrowdBLPS: A Blockchain-Based Location-Privacy-Preserving Mobile Crowdsensing System | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 03, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8926541

[40] S. Subramani, S. M, K. A, and S. K. Svn, "Review of Security Methods Based on Classical Cryptography and Quantum Cryptography," *Cybern. Syst.*, vol. 0, no. 0, pp. 1–19, 2023, doi: 10.1080/01969722.2023.2166261.

[41] W. Diffie and M. E. Hellman, "New Directions in Cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, 1st ed., vol. 42, New York, NY, USA: Association for Computing Machinery, 2022, pp. 365–390. Accessed: Feb. 14, 2024. [Online]. Available: https://doi.org/10.1145/3549993.3550007

[42] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Gener. Comput. Syst.*, vol. 129, pp. 77–89, Apr. 2022, doi: 10.1016/j.future.2021.11.011.

[43] D. R. Ibrahim, J. S. Teh, and R. Abdullah, "An overview of visual cryptography techniques," *Multimed. Tools Appl.*, vol. 80, no. 21, pp. 31927–31952, Sep. 2021, doi: 10.1007/s11042-021-11229-9.

[44] O. Goldreich, “On the foundations of cryptography,” in *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, New York, NY, USA: Association for Computing Machinery, 2019, pp. 411–496. Accessed: Feb. 14, 2024. [Online]. Available: https://doi.org/10.1145/3335741.3335759

[45] A. M. Qadir and N. Varol, “A Review Paper on Cryptography,” in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, pp. 1–6. doi: 10.1109/ISDFS.2019.8757514.

[46] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, “Security, Privacy, and Incentive Provision for Mobile Crowd Sensing Systems,” *IEEE Internet Things J.*, vol. 3, no. 5, pp. 839–853, Oct. 2016, doi: 10.1109/JIOT.2016.2560768.

[47] G. Xu, H. Li, S. Liu, M. Wen, and R. Lu, “Efficient and Privacy-Preserving Truth Discovery in Mobile Crowd Sensing Systems,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3854–3865, Apr. 2019, doi: 10.1109/TVT.2019.2895834.

[48] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. S. Shen, “Enabling Strong Privacy Preservation and Accurate Task Allocation for Mobile Crowdsensing,” *IEEE Trans. Mob. Comput.*, vol. 19, no. 6, pp. 1317–1331, Jun. 2020, doi: 10.1109/TMC.2019.2908638.

[49] X. Wang, Z. Liu, X. Tian, X. Gan, Y. Guan, and X. Wang, “Incentivizing Crowdsensing With Location-Privacy Preserving,” *IEEE Trans. Wirel. Commun.*, vol. 16, no. 10, pp. 6940–6952, Oct. 2017, doi: 10.1109/TWC.2017.2734758.

[50] L. Pournajaf, D. A. Garcia-Ulloa, L. Xiong, and V. Sunderam, “Participant Privacy in Mobile Crowd Sensing Task Management: A Survey of Methods and Challenges,” *ACM SIGMOD Rec.*, vol. 44, no. 4, pp. 23–34, May 2016, doi: 10.1145/2935694.2935700.

[51] Y. Wang, Z. Yan, W. Feng, and S. Liu, “Privacy protection in mobile crowd sensing: a survey,” *World Wide Web*, vol. 23, no. 1, pp. 421–452, Jan. 2020, doi: 10.1007/s11280-019-00745-2.

[52] S. Bhattacharjee and S. K. Das, “Information Integrity in Participatory Crowd-Sensing via Robust Trust Models,” in *Mobile Crowdsourcing: From Theory to Practice*, J. Wu and E. Wang, Eds., in Wireless Networks. , Cham: Springer International Publishing, 2023, pp. 251–273. doi: 10.1007/978-3-031-32397-3_10.

[53] R. K. Sahoo, S. K. Pradhan, and S. Sethi, “Ensuring Data Integrity in Mobile Crowdsensing Environment Using Fuzzy Logic,” in *Intelligent Systems*, S. K. Udgata, S. Sethi, and X.-Z. Gao, Eds., in Lecture Notes in Networks and Systems. Singapore: Springer Nature, 2022, pp. 223–237. doi: 10.1007/978-981-19-0901-6_22.

[54] H. Zhang, S. Bagchi, and H. Wang, “Integrity of Data in a Mobile Crowdsensing Campaign: A Case Study,” in *Proceedings of the First ACM Workshop on Mobile Crowdsensing Systems and Applications*, in CrowdSenSys ’17. New York, NY, USA: Association for Computing Machinery, Nov. 2017, pp. 50–55. doi: 10.1145/3139243.3139255.

[55] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, “Two-factor authentication: is the world ready? quantifying 2FA adoption,” in *Proceedings of the Eighth European Workshop on System Security*, in EuroSec ’15. New York, NY, USA: Association for Computing Machinery, Apr. 2015, pp. 1–7. doi: 10.1145/2751323.2751327.

[56] D. Wang, Q. Gu, H. Cheng, and P. Wang, “The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes,” in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, in ASIA CCS ’16. New York, NY, USA: Association for Computing Machinery, May 2016, pp. 475–486. doi: 10.1145/2897845.2897916.

[57] C. Blundo, S. Cimato, and L. Siniscalchi, “Managing Constraints in Role Based Access Control,” *IEEE Access*, vol. 8, pp. 140497–140511, 2020, doi: 10.1109/ACCESS.2020.3011310.

[58] J. P. Cruz, Y. Kaji, and N. Yanai, “RBAC-SC: Role-Based Access Control Using Smart Contract,” *IEEE Access*, vol. 6, pp. 12240–12251, 2018, doi: 10.1109/ACCESS.2018.2812844.

[59] A. M. Alajlan and M. M. Almasri, “Malicious behavior detection in cloud using self-optimized dynamic kernel convolutional neural network,” *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 5, p. e4449, 2022, doi: 10.1002/ett.4449.

[60] M. Senthil Raja and L. Arun Raj, “Detection of Malicious Profiles and Protecting Users in Online Social Networks,” *Wirel. Pers. Commun.*, vol. 127, no. 1, pp. 107–124, Nov. 2022, doi: 10.1007/s11277-021-08095-x.

[61] Y. Sun, A. K. Bashir, U. Tariq, and F. Xiao, “Effective malware detection scheme based on classified behavior graph in IIoT,” *Ad Hoc Netw.*, vol. 120, p. 102558, Sep. 2021, doi: 10.1016/j.adhoc.2021.102558.

[62] M. Rabbani *et al.*, “A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies,” *Entropy*, vol. 23, no. 5, Art. no. 5, May 2021, doi: 10.3390/e23050529.

[63] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, “Secure and Efficient Data Communication Protocol for Wireless Body Area Networks,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 94–107, Apr. 2016, doi: 10.1109/TMSCS.2016.2525997.

[64] D. Naylor, R. Li, C. Gkantsidis, T. Karagiannis, and P. Steenkiste, “And Then There Were More: Secure Communication for More Than Two Parties,” in *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, in CoNEXT ’17. New York, NY, USA: Association for Computing Machinery, Nov. 2017, pp. 88–100. doi: 10.1145/3143361.3143383.

[65] K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015, doi: 10.1016/j.adhoc.2015.01.006.

[66] A. Meena Kowshalya and M. L. Valarmathi, “Dynamic trust management for secure communications in social internet of things (SIoT),” *Sādhanā*, vol. 43, no. 9, p. 136, Jul. 2018, doi: 10.1007/s12046-018-0885-z.

[67] S. Ossenbühl, J. Steinberger, and H. Baier, “Towards Automated Incident Handling: How to Select an Appropriate Response against a Network-Based Attack?,” in *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, May 2015, pp. 51–67. doi: 10.1109/IMF.2015.13.

[68] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, “How can organizations develop situation awareness for incident response: A case study of management practice,” *Comput. Secur.*, vol. 101, p. 102122, Feb. 2021, doi: 10.1016/j.cose.2020.102122.

[69] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, “How integration of cyber security management and incident response enables organizational learning,” *J. Assoc. Inf. Sci. Technol.*, vol. 71, no. 8, pp. 939–953, 2020, doi: 10.1002/asi.24311.

[70] N. H. Ab Rahman and K.-K. R. Choo, “A survey of information security incident handling in the cloud,” *Comput. Secur.*, vol. 49, pp. 45–69, Mar. 2015, doi: 10.1016/j.cose.2014.11.006.

[71] J. Liu, X. Shen, W. Liu, Z. Lv, R. Liu, and D. Li, “Decision Analysis under Behavioral Economics—Incentive Mechanism for Improving Data Quality in Crowdsensing,” *Mathematics*, vol. 11, no. 10, Art. no. 10, Jan. 2023, doi: 10.3390/math11102288.

[72] J. Liu, Y. Yang, D. Li, X. Deng, S. Huang, and H. Liu, “An Incentive Mechanism Based on Behavioural Economics in Location-Based Crowdsensing Considering an Uneven Distribution of Participants,” *IEEE Trans. Mob. Comput.*, vol. 21, no. 1, pp. 44–62, Jan. 2022, doi: 10.1109/TMC.2020.3002586.

[73] D. Li, L. Qiu, J. Liu, and C. Xiao, “Analysis of Behavioral Economics in Crowdsensing: A Loss Aversion Cooperation Model,” *Sci. Program.*, vol. 2018, p. e4350183, Apr. 2018, doi: 10.1155/2018/4350183.

[74] J. Liu, S. Huang, D. Li, S. Wen, and H. Liu, “Addictive Incentive Mechanism in Crowdsensing From the Perspective of Behavioral Economics,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 5, pp. 1109–1127, May 2022, doi: 10.1109/TPDS.2021.3104247.

[75] C. Jiang, L. Gao, L. Duan, and J. Huang, “Economics of Peer-to-Peer Mobile Crowdsensing,” in *2015 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2015, pp. 1–6. doi: 10.1109/GLOCOM.2015.7417152.

[76] L. Atzori, R. Girau, S. Martis, V. Pilloni, and M. Uras, “A SIoT-aware approach to the resource management issue in mobile crowdsensing,” in *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, Mar. 2017, pp. 232–237. doi: 10.1109/ICIN.2017.7899418.

[77] H. R. Arkian, A. Diyanat, and A. Pourkhalili, “MIST: Fog-based data analytics scheme with cost-efficient resource provisioning for IoT crowdsensing applications,” *J. Netw. Comput. Appl.*, vol. 82, pp. 152–165, Mar. 2017, doi: 10.1016/j.jnca.2017.01.012.

[78] F. Restuccia, N. Ghosh, S. Bhattacharjee, S. K. Das, and T. Melodia, “Quality of Information in Mobile Crowdsensing: Survey and Research Challenges,” *ACM Trans. Sens. Netw.*, vol. 13, no. 4, p. 34:1-34:43, Nov. 2017, doi: 10.1145/3139256.

[79] T. Luo, J. Huang, S. S. Kanhere, J. Zhang, and S. K. Das, “Improving IoT Data Quality in Mobile Crowd Sensing: A Cross Validation Approach,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5651–5664, Jun. 2019, doi: 10.1109/JIOT.2019.2904704.

[80] J. Ren, Y. Zhang, K. Zhang, and X. (Sherman) Shen, “SACRM: Social Aware Crowdsourcing with Reputation Management in mobile sensing,” *Comput. Commun.*, vol. 65, pp. 55–65, Jul. 2015, doi: 10.1016/j.comcom.2015.01.022.