RESEARCH ARTICLE

JENER Journal of Empirical and Non-Empirical Research
Volume 1, Issue 3, Page 993-1002| Article No. 121
DOI: 10.4898/jener.v1i3.a121
ISSN: 7895-9216
Journal homepage: https://jenerjournal.com
Journal email: editor@jenerjournal.com

JENER Journal
JENER Journal of Empirical and Non-Empirical Research

Accountability Gaps in AI-Driven Organizations: Examining the Diffusion of Responsibility in Algorithmic Decision-Making Systems

Bappy Ahmed[1] & Rashedul Alam[2]

[1]Department of Computer Science, International American University, Los Angeles, USA
[2]School of Business Administration, National University of San Diego, San Diego, USA

ARTICLE INFORMATION

Article history:
Published: November 14, 2025

Keywords:
Artificial Intelligence, Accountability, Organizational Governance, Decision-Making Systems, Algorithmic Responsibility

ABSTRACT

The integration of artificial intelligence (AI) into organizational decision-making has fundamentally reshaped how authority, responsibility, and accountability are structured within modern institutions. While AI systems offer substantial benefits in terms of efficiency, consistency, and predictive capability, they also introduce complex challenges related to responsibility and governance. This paper examines the emergence of accountability gaps in AI-driven organizations, focusing on how responsibility becomes diffused across multiple actors involved in algorithmic decision-making processes. Drawing exclusively on theoretical and scholarly perspectives available up to November 2025, the study explores the limitations of traditional accountability models when applied to distributed decision environments. It analyzes key contributing factors, including system complexity, lack of transparency, automation bias, and organizational reliance on algorithmic outputs. The research further evaluates the effectiveness of human-in-the-loop approaches and identifies their limitations in maintaining meaningful oversight. A conceptual framework of shared accountability is proposed to clarify the distribution of responsibility across developers, organizations, managers, and end-users. The findings suggest that accountability is not removed by AI but redistributed in ways that create ambiguity and risk. Without deliberate governance structures, organizations may face ethical, legal, and operational challenges. The paper concludes by emphasizing the need for adaptive accountability models that reflect the realities of AI-driven decision-making and ensure that responsibility remains clearly defined within increasingly complex systems.

1. Introduction

Artificial intelligence has moved from being a specialized technological tool to becoming a central component of modern organizational operations. Across industries, organizations are increasingly relying on AI systems to support, enhance, and in some cases replace human decision-making. These systems are used in areas such as recruitment, financial analysis, customer service, supply chain management, and risk assessment. The adoption of AI has enabled organizations to process large volumes of data, identify patterns, and generate insights at a scale that was previously impossible.

However, this transformation has also introduced new challenges. One of the most significant issues is the question of accountability. In traditional organizational settings, accountability is relatively straightforward. Decisions are made by individuals or groups, and responsibility can be traced through hierarchical structures. When something goes wrong, it is usually possible to identify who is responsible and hold them accountable.

In AI-driven environments, this clarity is often lost. Decision-making processes become more complex, involving interactions between humans and machines. AI systems may generate recommendations or make decisions based on data patterns that are not fully understood by human users. As a result, responsibility becomes distributed across multiple actors, including developers, managers, organizations, and end-users.

This distribution of responsibility creates what can be described as an accountability gap. In such situations, it becomes difficult to determine who is responsible for the outcomes of decisions influenced by AI systems. This gap raises important ethical, legal, and organizational questions.

1.1 Problem Statement

The central problem addressed in this paper is the emergence of accountability gaps in AI-driven organizations. These gaps occur when responsibility for decisions is diffused across multiple actors, making it difficult to assign accountability for outcomes.

1.2 Research Objectives

The objectives of this study are to:

- Examine traditional models of accountability in organizations
- Analyze how AI systems disrupt these models

- Identify the factors contributing to accountability gaps
- Propose a conceptual framework for shared accountability

1.3 Significance of the Study

Understanding accountability in AI-driven environments is essential for organizations seeking to adopt these technologies responsibly. Without clear accountability, organizations may face ethical dilemmas, legal challenges, and loss of stakeholder trust. This study contributes to the theoretical understanding of AI governance by providing a detailed analysis of accountability issues.

2. Literature Review

The concept of accountability has long been central to organizational theory, governance, and decision-making processes. Traditionally, accountability refers to the obligation of individuals or institutions to explain and justify their actions and accept responsibility for outcomes. This concept assumes that actions can be traced to identifiable actors and that decision-making processes are sufficiently transparent to allow evaluation. However, the rapid integration of artificial intelligence (AI) into organizational systems has fundamentally altered these assumptions, introducing new complexities that challenge traditional accountability frameworks.

2.1 Accountability in Traditional Organizational Theory

In classical organizational theory, accountability is closely linked to authority, hierarchy, and control. Organizations are designed with structured roles and responsibilities that ensure decision-making authority is clearly defined. Individuals in positions of power are expected to justify their decisions, and accountability flows through hierarchical chains.

Bovens (2007) conceptualizes accountability as a relationship between an actor and a forum in which the actor must provide explanations for actions and face consequences when necessary. This framework is built on three key elements: transparency, answerability, and enforceability. These elements depend on the assumption that decisions are made by identifiable individuals whose reasoning can be articulated.

Mintzberg (1980) further emphasizes that organizational structures play a critical role in maintaining accountability. In centralized systems, decision-making authority is concentrated, making accountability more straightforward. In decentralized systems, responsibility may be distributed, but it remains traceable due to clearly defined roles.

However, these traditional models rely on a key assumption: that decision-making processes are understandable and that responsibility can be assigned based on observable actions. This assumption becomes problematic in AI-driven environments where decisions are influenced by complex, often opaque systems.

2.2 The Transformation of Decision-Making in AI-Driven Systems

The integration of AI into organizational processes represents a shift from human-centered decision-making to hybrid or algorithmic systems. AI systems are capable of processing large volumes of data, identifying patterns, and generating recommendations or decisions that influence organizational outcomes.

This transformation introduces several challenges. First, AI systems operate based on algorithms that may not be fully understood by users. Second, decision-making processes become distributed across multiple actors, including developers, organizations, and end-users. Third, the reasoning behind decisions may not be easily interpretable, leading to reduced transparency.

The concept of algorithmic governance has emerged to describe how decisions are increasingly shaped by computational processes rather than human judgment. Unlike traditional governance models, which rely on institutional authority and human reasoning, algorithmic governance depends on data-driven models and automated systems.

While AI systems can improve efficiency and accuracy, they also create new forms of dependency. Organizations may rely heavily on algorithmic outputs, reducing the role of human judgment. This reliance can lead to situations where decisions are accepted without sufficient scrutiny, contributing to accountability gaps.

2.3 The Black Box Problem and Transparency Limitations

One of the most significant challenges associated with AI systems is the lack of transparency, often referred to as the "black box" problem. Pasquale (2015) highlights how complex algorithms operate in ways that are not easily interpretable by humans. This lack of transparency creates barriers to understanding how decisions are made.

Transparency is a fundamental requirement for accountability. Without access to information about decision-making processes, it becomes difficult to evaluate whether decisions are fair, accurate, or appropriate. In traditional systems, decision-makers can explain their reasoning, allowing for accountability to be enforced. In contrast, AI systems may produce outputs without providing clear explanations.

This issue is particularly critical in high-stakes domains such as finance, healthcare, and security. For example, AI models used in financial markets to detect systemic risk rely on complex deep learning architectures that process interconnected data across institutions (ALAM et al., 2025). While these models enhance predictive capabilities, their complexity makes it difficult to trace how specific decisions are generated.

The lack of explainability in such systems complicates accountability. If an AI system produces an incorrect prediction or recommendation, stakeholders may struggle to determine whether the issue lies in the data, the model, or its implementation.

2.4 Automation Bias and Human Dependence on AI

Automation bias is a critical factor influencing how individuals interact with AI systems. It refers to the tendency to trust automated systems and rely on their outputs, even when they may be incorrect. Glikson and Woolley (2020) suggest that trust in AI is shaped by perceptions of reliability, consistency, and performance.

Logg et al. (2019) introduce the concept of "algorithm appreciation," which describes the tendency of individuals to prefer algorithmic recommendations over human judgment. This preference is particularly evident in complex decision-making scenarios where human cognitive limitations are more pronounced.

While reliance on AI can improve efficiency, it also reduces critical evaluation. Individuals may accept AI outputs without questioning their validity, leading to overdependence on automated systems. This behavior contributes to accountability gaps because responsibility is effectively transferred from humans to machines.

In cybersecurity contexts, AI-based anomaly detection systems are used to identify insider threats and protect sensitive data (Imran et al., 2025). While these systems enhance security, they also create new forms of reliance. If an AI system fails to detect a threat, it becomes unclear whether responsibility lies with the system, the organization, or the individuals responsible for oversight.

2.5 AI in Financial Systems and Accountability Complexity

The application of AI in financial systems provides a clear example of how accountability becomes complex in algorithm-driven environments. AI models are widely used for tasks such as fraud detection, risk assessment, and financial forecasting.

Adversarial machine learning techniques have been developed to improve fraud detection in high-frequency financial transactions (Kowshik et al., 2025). These systems are designed to adapt to evolving threats, making them highly dynamic and difficult to interpret. While they enhance security, they also introduce challenges for accountability.

Similarly, AI-driven treasury management systems use data-driven approaches to optimize financial decision-making processes (Alam et al., 2024). These systems rely on large datasets and complex algorithms, making it difficult to trace how specific decisions are generated.

The use of AI in financial systems also raises regulatory concerns. As organizations increasingly rely on algorithmic decision-making, regulators must consider how accountability can be enforced. However, traditional regulatory frameworks are not always equipped to address the complexities of AI systems.

2.6 AI Security, Cyber Infrastructure, and Responsibility

AI plays a critical role in protecting financial infrastructure from cyber threats. Advanced AI systems can identify patterns, detect anomalies, and predict potential attacks (Alam & Fahad, 2022). These capabilities are essential for maintaining security in increasingly complex digital environments.

However, the use of AI in cybersecurity also introduces accountability challenges. If an AI system fails to prevent a cyberattack, determining responsibility becomes difficult. Organizations may argue that they relied on advanced technology, while developers may claim that the system functioned as intended.

Furthermore, AI-driven security systems are often integrated into broader organizational processes, making it difficult to isolate the source of errors. This integration creates a network of interdependencies that complicates accountability.

2.7 Generative AI and Expanding Decision Boundaries

The emergence of generative AI and large language models has expanded the role of AI in decision-making. These systems are capable of generating insights, recommendations, and even strategic decisions in various domains (Mahmud et al., 2025).

Generative AI systems often produce outputs that appear authoritative and credible. This can lead users to rely on them without verification, increasing the risk of automation bias. As these systems become more integrated into organizational processes, their influence on decision-making continues to grow.

This expansion raises important questions about accountability. If a generative AI system produces an incorrect or misleading output, it is unclear who should be held responsible. The system itself cannot be held accountable, and responsibility must be distributed among the actors involved in its use.

2.8 AI, Regulation, and Public Trust

AI systems also influence public trust, particularly in sectors such as finance and governance. Research has shown that AI-driven misinformation and deepfakes can undermine trust in institutions (Alam et al., 2023). When trust is compromised, organizations face challenges in maintaining legitimacy and credibility.

Regulatory frameworks are evolving to address these challenges. For example, efforts have been made to modernize financial regulations to account for the use of AI in counter-terrorism and fraud detection (Alam et al., 2023). However, these efforts are still in early stages and may not fully address accountability gaps.

The relationship between AI, regulation, and trust highlights the importance of accountability. Without clear accountability structures, organizations may struggle to maintain public confidence in their systems and decisions.

2.9 Synthesis of Literature and Research Gap

The existing literature provides valuable insights into the challenges of accountability in AI-driven environments. However, several gaps remain. First, much of the literature focuses on technical aspects of AI, such as performance and accuracy, rather than organizational implications. Second, existing accountability frameworks are primarily designed for human-centered systems and may not be suitable for AI-driven environments.

This study addresses these gaps by providing a comprehensive theoretical analysis of accountability in AI-driven organizations. It integrates perspectives from organizational theory, ethics, and AI governance to develop a conceptual framework that reflects the complexity of modern decision-making systems.

3. Methodology

This study adopts a conceptual and qualitative research approach, focusing on theoretical analysis rather than empirical data collection.

3.1 Research Design

The research design is based on an integrative framework that combines insights from organizational theory, ethics, and AI governance. This approach allows for a comprehensive examination of accountability in AI-driven environments.

The study does not rely on quantitative data or statistical analysis. Instead, it uses conceptual reasoning to explore how accountability is structured and how it is affected by the introduction of AI systems. This approach is appropriate for examining complex and evolving phenomena where empirical data may be limited or difficult to interpret.

3.2 Data Sources and Selection Criteria

The study relies on secondary data sources, including:

- Peer-reviewed academic journal articles
- Books and theoretical frameworks
- Conference papers and scholarly discussions

Sources were selected based on relevance to the following themes:

- Organizational accountability
- AI decision-making
- Ethics and governance
- Human-AI interaction

3.3 Analytical Approach

The analysis is conducted through thematic synthesis. Key themes related to accountability and AI are identified and examined in relation to each other. This approach allows for the development of a conceptual framework that integrates multiple perspectives.

The study focuses on understanding:

- How responsibility is distributed across different actors
- How AI systems influence decision-making processes
- How accountability gaps emerge

3.4 Limitations of the Methodology

As a theoretical study, this research has certain limitations. It does not provide empirical validation of the proposed framework. Additionally, the analysis is limited to existing literature and may not capture all aspects of real-world applications.

However, the conceptual approach provides valuable insights into the underlying mechanisms of accountability in AI-driven systems and serves as a foundation for future empirical research.

4. Findings

The findings of this study highlight the complex and multifaceted nature of accountability gaps in AI-driven organizations.

4.1 Structural Complexity of AI Systems

AI systems are composed of multiple components, including data inputs, algorithms, and decision outputs. Each component involves different actors and processes. This complexity makes it difficult to trace how decisions are made.

For example, data used to train AI systems may come from various sources, each with its own limitations and biases. Algorithms are designed by developers who make decisions about how the system operates. Organizations then implement these systems within specific contexts. Finally, users interact with the system and rely on its outputs.

This layered structure creates challenges for accountability because responsibility is distributed across multiple levels.

4.2 Diffusion of Responsibility Across Actors

One of the most significant findings is the diffusion of responsibility across different actors. In AI-driven systems, no single actor has complete control over the decision-making process.

- Developers may argue that they only created the system
- Organizations may claim they relied on technology
- Managers may state they followed system recommendations
- Users may assert they trusted the system

This diffusion creates ambiguity and makes it difficult to assign accountability.

4.3 Transparency and Explainability Challenges

The lack of transparency in AI systems limits the ability to understand decision-making processes. Even when organizations attempt to implement explainable AI techniques, explanations may be simplified or incomplete.

This creates a gap between technical processes and human understanding. Without clear explanations, it becomes difficult to evaluate decisions and assign responsibility.

4.4 Human-in-the-Loop Limitations

Human oversight is often proposed as a solution to accountability challenges. However, this study finds that human-in-the-loop approaches are not always effective.

Humans may:
- Lack the expertise to evaluate AI outputs
- Experience cognitive overload
- Rely on AI recommendations due to time constraints

As a result, human oversight may become symbolic rather than functional.

4.5 Organizational and Systemic Risks

Accountability gaps can lead to a range of risks, including:
- Ethical violations
- Legal liability issues
- Loss of stakeholder trust
- Operational inefficiencies

These risks highlight the importance of addressing accountability challenges in AI-driven organizations.

5. Discussion

The findings of this study indicate that accountability gaps in AI-driven organizations are not isolated issues but are the result of a broader transformation in how decision-making authority, responsibility, and control are structured. These gaps emerge from the interaction between technological complexity, organizational design, and human behavior. To fully understand their implications, it is necessary to examine how these dynamics reshape accountability across different levels of organizational activity.

5.1 Reconfiguration of Authority in AI-Driven Organizations

One of the most fundamental changes introduced by AI systems is the reconfiguration of authority. In traditional organizations, authority is formally assigned to individuals based on their roles and positions. Decision-making power is clearly defined, and responsibility can be traced through hierarchical structures.

In AI-driven environments, authority becomes partially embedded in technological systems. While humans retain formal control, AI systems increasingly influence the outcomes of decisions. Managers often rely on algorithmic outputs to guide their actions, which creates a form of shared authority between humans and machines.

This hybrid authority structure complicates accountability. When decisions are influenced by AI systems, it becomes difficult to determine whether responsibility lies with the human decision-maker or the system itself. Over time, repeated reliance on AI can lead to a gradual shift in perceived authority, where individuals defer to algorithmic outputs even when they retain formal responsibility.

5.2 Normalization of Algorithmic Dependence

As organizations integrate AI systems into their operations, dependence on these systems becomes normalized. Employees begin to treat AI outputs as standard inputs in decision-making processes, reducing the role of independent judgment.

This normalization is driven by several factors, including efficiency gains, perceived accuracy, and organizational expectations. AI systems are often presented as objective and data-driven, which increases trust and encourages reliance.

However, this reliance can lead to a reduction in critical evaluation. Individuals may accept AI recommendations without questioning their validity, particularly in high-pressure environments where time constraints limit decision-making capacity. This behavior reinforces automation bias and contributes to the diffusion of responsibility.

In financial contexts, for example, AI systems are used to detect systemic risks and predict market behavior (ALAM et al., 2025). While these systems provide valuable insights, their complexity can lead users to rely on outputs without fully understanding the underlying processes. This creates a situation where decisions are influenced by AI, but accountability remains unclear.

5.3 Diffusion of Responsibility and Organizational Behavior

The diffusion of responsibility is a well-established concept in organizational and social psychology. It refers to the tendency for individuals to feel less accountable when responsibility is shared among multiple actors. In AI-driven environments, this phenomenon is amplified by the presence of technological systems.

Responsibility is distributed across several layers:

Developers who design and train AI models

Organizations that deploy and integrate these systems

Managers who interpret outputs and make decisions

Users who interact with the system

Each of these actors contributes to the decision-making process, but none have complete control. As a result, accountability becomes fragmented. When errors occur, each actor may attribute responsibility to others, creating ambiguity.

This dynamic is particularly evident in systems designed for fraud detection and financial monitoring. Adversarial machine learning models used in high-frequency financial transactions are highly complex and continuously evolving (Kowshik et al., 2025). When such systems fail to detect fraud or generate incorrect outputs, it is difficult to assign responsibility to any single actor.

5.4 Transparency, Explainability, and Accountability

Transparency is a critical component of accountability, yet it remains a significant challenge in AI systems. The black box nature of many AI models limits the ability of users to understand how decisions are made.

Even when explainability techniques are applied, they often provide simplified representations of complex processes. This creates a gap between technical reality and human understanding. As a result, explanations may not fully capture the reasoning behind decisions, reducing their usefulness for accountability purposes.

In financial and cybersecurity applications, this lack of transparency is particularly problematic. AI systems used to protect sensitive data and detect insider threats operate based on complex anomaly detection algorithms (Imran et al., 2025). While these systems can identify unusual patterns, they may not provide clear explanations for their decisions.

This lack of explainability makes it difficult for organizations to evaluate the performance of AI systems and assign responsibility when issues arise.

5.5 Human-in-the-Loop Limitations and Cognitive Constraints

Human-in-the-loop systems are often proposed as a solution to accountability challenges. These systems involve human oversight in decision-making processes, with the expectation that humans will review and validate AI outputs.

However, this study finds that human oversight is not always effective. Several factors limit its effectiveness:

Cognitive limitations: Humans may not fully understand complex AI outputs

Time constraints: Rapid decision-making environments reduce the ability to critically evaluate outputs

Trust bias: Individuals may assume that AI systems are more accurate than they actually are

As a result, human oversight may become procedural rather than substantive. Individuals may approve AI-generated decisions without thorough evaluation, reducing the effectiveness of accountability mechanisms.

5.6 High-Risk Domains: Finance, Security, and Governance

Accountability gaps are particularly significant in high-risk domains where decisions have substantial consequences. These domains include finance, cybersecurity, and public governance.

Financial Systems: AI-driven financial systems are used for tasks such as risk assessment, fraud detection, and treasury management. These systems rely on large datasets and complex algorithms, making decision-making processes difficult to interpret.

The concept of an AI-powered treasury highlights how data-driven approaches are transforming fiscal management (Alam et al., 2024). While these systems improve efficiency, they also introduce risks related to accountability. Errors in algorithmic decision-making can lead to financial losses and regulatory challenges.

Cybersecurity and Infrastructure Protection: AI systems are increasingly used to protect financial infrastructure from cyber threats. These systems can identify patterns and predict potential attacks (Alam & Fahad, 2022). However, they are not infallible.

If an AI system fails to prevent a cyberattack, determining responsibility becomes complex. Organizations may argue that they relied on advanced technology, while developers may claim that the system functioned as intended. This ambiguity highlights the need for clearer accountability structures.

Regulation and Public Trust: AI systems also influence public trust in institutions. Research indicates that AI-driven misinformation and deepfakes can undermine trust in financial systems (Alam et al., 2023). When trust is compromised, organizations face challenges in maintaining credibility.

Regulatory frameworks are evolving to address these issues. However, traditional regulatory approaches may not be sufficient to address the complexities of AI-driven systems. This underscores the need for adaptive governance models.

5.7 Generative AI and Expanding Accountability Boundaries

The rise of generative AI and large language models has expanded the scope of AI in decision-making processes. These systems can generate insights, recommendations, and strategic outputs that influence organizational decisions (Mahmud et al., 2025).

Generative AI systems often produce outputs that appear authoritative, leading users to rely on them without verification. This behavior increases the risk of automation bias and further diffuses responsibility.

Unlike traditional AI systems, generative models can produce a wide range of outputs, making it difficult to predict their behavior. This unpredictability complicates accountability, as it becomes challenging to determine how decisions are generated.

5.8 Long-Term Organizational Implications

The persistence of accountability gaps can have significant long-term implications for organizations. These include:

Erosion of trust: Stakeholders may lose confidence in organizational decision-making

Legal risks: Ambiguity in responsibility can lead to regulatory challenges

Ethical concerns: Lack of accountability may result in unfair or biased outcomes

Operational inefficiencies: Unclear responsibility can hinder decision-making processes

If organizations fail to address these issues, they may face long-term consequences that affect their sustainability and competitiveness.

5.9 Synthesis of Discussion

The discussion highlights that accountability gaps in AI-driven organizations are the result of a complex interplay between technology, human behavior, and organizational structures. AI systems introduce new forms of decision-making that challenge traditional accountability frameworks.

The key insight is that accountability is not eliminated by AI but redistributed across multiple actors. This redistribution creates ambiguity and requires new approaches to governance and responsibility.

Addressing these challenges requires a comprehensive understanding of how AI systems operate and how they influence decision-making processes. Organizations must develop frameworks that account for the distributed nature of accountability and ensure that responsibility remains clearly defined.

6. Conceptual Framework: Expanded Shared Accountability Model

6.1 Introduction to the Framework

The increasing reliance on artificial intelligence (AI) in organizational decision-making requires a rethinking of how accountability is conceptualized and operationalized. Traditional accountability models are based on linear relationships between authority and responsibility, where decision-makers can be clearly identified and held accountable for outcomes. However, in AI-driven environments, decision-making processes are distributed across multiple actors and influenced by complex technological systems. This creates a need for a more comprehensive framework that reflects the multi-layered nature of accountability.

The proposed Shared Accountability Model addresses this need by conceptualizing accountability as a system of interconnected layers. Each layer represents a group of actors involved in the lifecycle of AI systems, from development to deployment and use. Rather than assigning responsibility to a single entity, the model emphasizes the distribution of accountability across multiple levels while maintaining clarity in roles and responsibilities.

6.2 Core Principles of the Model

The framework is built on four key principles:

- Distributed Responsibility: Accountability in AI systems is inherently distributed. Multiple actors contribute to decision-making processes, and responsibility must be shared accordingly. This principle recognizes that no single actor has complete control over outcomes.
- Traceability: Despite the distributed nature of accountability, it is essential to maintain traceability. Organizations must be able to track how decisions are made and identify the contributions of different actors.
- Transparency and Explainability: Transparency is critical for accountability. AI systems must provide explanations that allow users to understand how decisions are generated, even if full technical transparency is not achievable.
- Governance Integration: Accountability must be supported by governance mechanisms that define roles, responsibilities, and oversight processes. These mechanisms ensure that accountability is not only conceptual but also operational.

6.3 Layered Structure of the Shared Accountability Model

The framework consists of four primary layers, each representing a distinct group of actors and responsibilities.

6.3.1 Layer 1: Technical Development Layer

This layer includes developers, data scientists, and engineers responsible for designing and building AI systems. Their responsibilities include:

Selecting and preprocessing data
Designing algorithms and models
Ensuring system robustness and reliability
Identifying and mitigating bias

Accountability at this level is primarily technical. Developers are responsible for ensuring that AI systems function as intended and meet ethical and performance standards.

In financial systems, for example, developers design models for fraud detection and risk assessment (Kowshik et al., 2025). These models must be robust against adversarial attacks and capable of handling large volumes of data. Failures at this level can have significant downstream consequences, highlighting the importance of accountability in system design.

6.3.2 Layer 2: Organizational Implementation Layer

This layer includes organizations that deploy AI systems within their operations. Responsibilities at this level include:

Selecting appropriate AI systems for specific use cases
Defining the scope and purpose of system use
Establishing policies and guidelines
Ensuring compliance with regulatory requirements

Organizations play a critical role in shaping how AI systems are used. They determine the context in which systems operate and the extent to which they influence decision-making.

For instance, AI-driven treasury management systems are implemented to optimize financial decision-making processes (Alam et al., 2024). Organizations must ensure that these systems are used responsibly and that their outputs are aligned with organizational goals.

6.3.3 Layer 3: Managerial Decision Layer

Managers serve as the bridge between AI systems and organizational outcomes. Their responsibilities include:

Interpreting AI-generated outputs
Integrating recommendations into decision-making processes
Exercising judgment and oversight
Ensuring accountability for decisions

This layer is critical because it represents the point at which AI outputs are translated into actionable decisions. Managers must balance reliance on AI systems with their own expertise and judgment.

However, this layer is also vulnerable to automation bias. Managers may rely too heavily on AI recommendations, reducing their level of critical evaluation. This behavior can weaken accountability, as decisions may be attributed to the system rather than the individual.

6.3.4 Layer 4: User Interaction Layer

The user interaction layer includes employees and stakeholders who interact directly with AI systems. Their responsibilities include:

Using systems appropriately

Understanding system limitations

Reporting errors or inconsistencies

Providing feedback for system improvement

Users play an important role in maintaining accountability by ensuring that AI systems are used correctly. However, their ability to fulfill this role depends on their understanding of the system and the level of training they receive.

In cybersecurity contexts, for example, users rely on AI systems to detect insider threats (Imran et al., 2025). Their ability to interpret system outputs and respond appropriately is critical for maintaining security.

6.4 Cross-Layer Governance Mechanisms

In addition to the four layers, the framework includes cross-layer governance mechanisms that ensure coordination and accountability across all levels. These mechanisms include:

6.4.1 Transparency Protocols

Organizations must implement processes that provide visibility into how AI systems operate. This includes documentation, reporting, and explainability tools.

6.4.2 Audit and Monitoring Systems

Regular audits and monitoring are essential for identifying issues and ensuring compliance. These systems help track decision-making processes and evaluate system performance.

6.4.3 Ethical Guidelines

Ethical considerations must be integrated into all layers of the framework. This includes addressing issues related to fairness, bias, and transparency.

6.4.4 Regulatory Alignment

Organizations must ensure that their AI systems comply with relevant regulations. This is particularly important in high-risk domains such as finance and healthcare.

6.5 Integration with High-Risk Domains

The Shared Accountability Model is particularly relevant for high-risk domains where accountability is critical.

Financial Systems

AI systems used for systemic risk detection and financial forecasting operate in highly complex environments (ALAM et al., 2025). The framework ensures that accountability is maintained across all layers, from model design to decision implementation.

Cybersecurity

AI-driven security systems must be robust and reliable to protect critical infrastructure (Alam & Fahad, 2022). The framework emphasizes the importance of accountability at each stage of system development and use.

Generative AI Applications

Generative AI systems expand the scope of decision-making by producing insights and recommendations (Mahmud et al., 2025). The framework ensures that responsibility is clearly defined despite the increased complexity of these systems.

6.6 Strengths of the Framework

The proposed framework offers several advantages:

Comprehensive coverage: It addresses all stages of the AI lifecycle

Clarity: It defines roles and responsibilities at each layer

Flexibility: It can be adapted to different organizational contexts

Practical relevance: It provides a foundation for developing governance policies

6.7 Limitations of the Framework

Despite its strengths, the framework has limitations:

It is conceptual and may require empirical validation

Implementation may be resource-intensive

It may need adaptation for specific industries

6.8 Implications for Future Research

The framework provides a foundation for future research on accountability in AI-driven organizations. Future studies could:

Empirically test the framework in real-world settings

Explore industry-specific adaptations

Examine the role of regulation in shaping accountability

6.9 Synthesis of the Conceptual Framework

The Shared Accountability Model provides a structured approach to understanding accountability in AI-driven environments. By recognizing the distributed nature of responsibility and integrating governance mechanisms, the framework addresses the limitations of traditional models.

The key contribution of this framework is its ability to reconcile the complexity of AI systems with the need for clear accountability. It emphasizes that while responsibility is distributed, it must remain traceable and enforceable.

7. Conclusion and Recommendations

7.1 Conclusion

This study has examined the emergence of accountability gaps in AI-driven organizations and provided a comprehensive analysis of the factors contributing to these gaps. The findings demonstrate that accountability in AI environments is fundamentally different from traditional organizational contexts.

In traditional systems, accountability is based on clear relationships between authority and responsibility. However, in AI-driven environments, decision-making processes are distributed across multiple actors and influenced by complex technological systems. This creates ambiguity and challenges traditional accountability frameworks.

The study highlights that accountability gaps are not simply the result of technological limitations but are also influenced by organizational structures, human behavior, and governance practices. AI systems introduce new forms of complexity that require organizations to rethink how responsibility is assigned and enforced.

Importantly, the study emphasizes that AI does not eliminate responsibility. Instead, it redistributes responsibility in ways that are not always visible or clearly defined. Without deliberate efforts to address these challenges, accountability gaps may continue to grow as AI adoption increases.

7.2 Recommendations

To address accountability gaps, organizations should adopt a proactive and structured approach. The following recommendations are proposed:

- Develop Clear Accountability Frameworks: Organizations should define roles and responsibilities for all actors involved in AI systems. This includes developers, managers, and users.
- Enhance Transparency and Explainability: Efforts should be made to improve the transparency of AI systems. This includes providing explanations for decisions and ensuring that users understand system limitations.
- Strengthen Governance Mechanisms: Organizations should establish governance structures that oversee the development and use of AI systems. This includes policies, guidelines, and oversight committees.
- Promote Critical Engagement with AI: Employees should be trained to critically evaluate AI outputs rather than relying on them blindly. This can reduce automation bias and improve decision-making.
- Implement Continuous Monitoring and Auditing: AI systems should be regularly monitored and audited to identify potential issues. This helps ensure accountability and maintain system integrity.
- Align Ethical and Organizational Goals: Organizations should ensure that AI systems align with ethical principles and organizational values. This includes addressing issues related to fairness and bias.
- Encourage Interdisciplinary Collaboration: Addressing accountability gaps requires collaboration between technical experts, managers, and policymakers. Interdisciplinary approaches can provide more comprehensive solutions.

References

[1] Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13(4), 447–468.

[2] Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, 14(2), 627–660.

[3] Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation. *Organizational Behavior and Human Decision Processes*, 151, 90–103.

[4] Mintzberg, H. (1980). Structure in organizations. *Management Science*, 26(3), 322–341. Pasquale, F. (2015). *The Black Box Society*. Harvard University Press.

[5] ALAM, A., Kowshik, M., & Mahmud, A. (2025). Deep learning for early detection of systemic risk in interconnected financial markets: A U.S. regulatory perspective. *Journal of Computer Science and Technology Studies*, 7(9), 353–375. https://doi.org/10.32996/jcsts.2025.7.9.42

[6] Imran, M., Kowshik, M., & Mahmud, M. A. (2025). AI-based anomaly detection in cloud databases for insider threats. *Repository Universitas Muhammadiyah Sidoarjo*, 2(6). http://eprints.umsida.ac.id/16212/1/AI-BASED%20ANOMALY%20DETECTION%20IN%20CLOUD%20DATABASES%20FOR%20INSIDER%20THREATS.pdf

[7] Kowshik, M., Mahmud, A., & ALAM, A. (2025). Adversarial machine learning for robust fraud detection in high-frequency financial transactions. *Journal of Computer Science and Technology Studies*, 7(8), 314–335. https://doi.org/10.32996/jcsts.2025.7.8.35

[8] Kowshik, M., Rahman, L., & Nayem, M. (2024). Guardian of the vault: AI-driven solutions for protecting sensitive financial data in the US. *Repository Antispublisher*, 7(2). http://repository.antispublisher.my.id/id/eprint/1160/1/AJEBM_M%2BKOWS_Guardian%2Bof%2Bthe%2BVault.pdf

[9] Mahmud, M. A., ALAM, M. A., & Alam, M. K. (2025). Generative AI and large language models in financial applications. *Journal of Computer Science and Technology Studies*, 7(8), 1069–1088. https://doi.org/10.32996/jcsts.2025.7.8.122

[10] Mohammad Kowshik Alam, Md Asief Mahmud, & Md Saiful Islam. (2024). The AI-powered treasury: A data-driven approach to managing America's fiscal future. *Journal of Computer Science and Technology Studies*, 6(2), 236–256. https://doi.org/10.32996/jcsts.2024.6.2.25

[11] Mohammad Kowshik Alam, & Md Lutfur Rahman Fahad. (2022). The digital shield: AI's role in protecting US financial infrastructure. *Journal of Computer Science and Technology Studies*, 4(1), 112–133. https://doi.org/10.32996/jcsts.2022.4.1.14

[12] Mohammad Kowshik Alam, Md Lutfur Rahman Fahad, & Md Sabbir Hossen Shuvo. (2023). Regulating AI for counter-terrorism in financial systems. *Journal of Computer Science and Technology Studies*, 5(2), 66–87. https://doi.org/10.32996/jcsts.2023.5.2.6

[13] Mohammad Kowshik Alam, Md Lutfur Rahman Fahad, & Nayem Miah. (2023). AI-driven misinformation and trust in financial institutions. *Journal of Computer Science and Technology Studies*, 5(1), 133–160. https://doi.org/10.32996/jcsts.2023.5.1.13