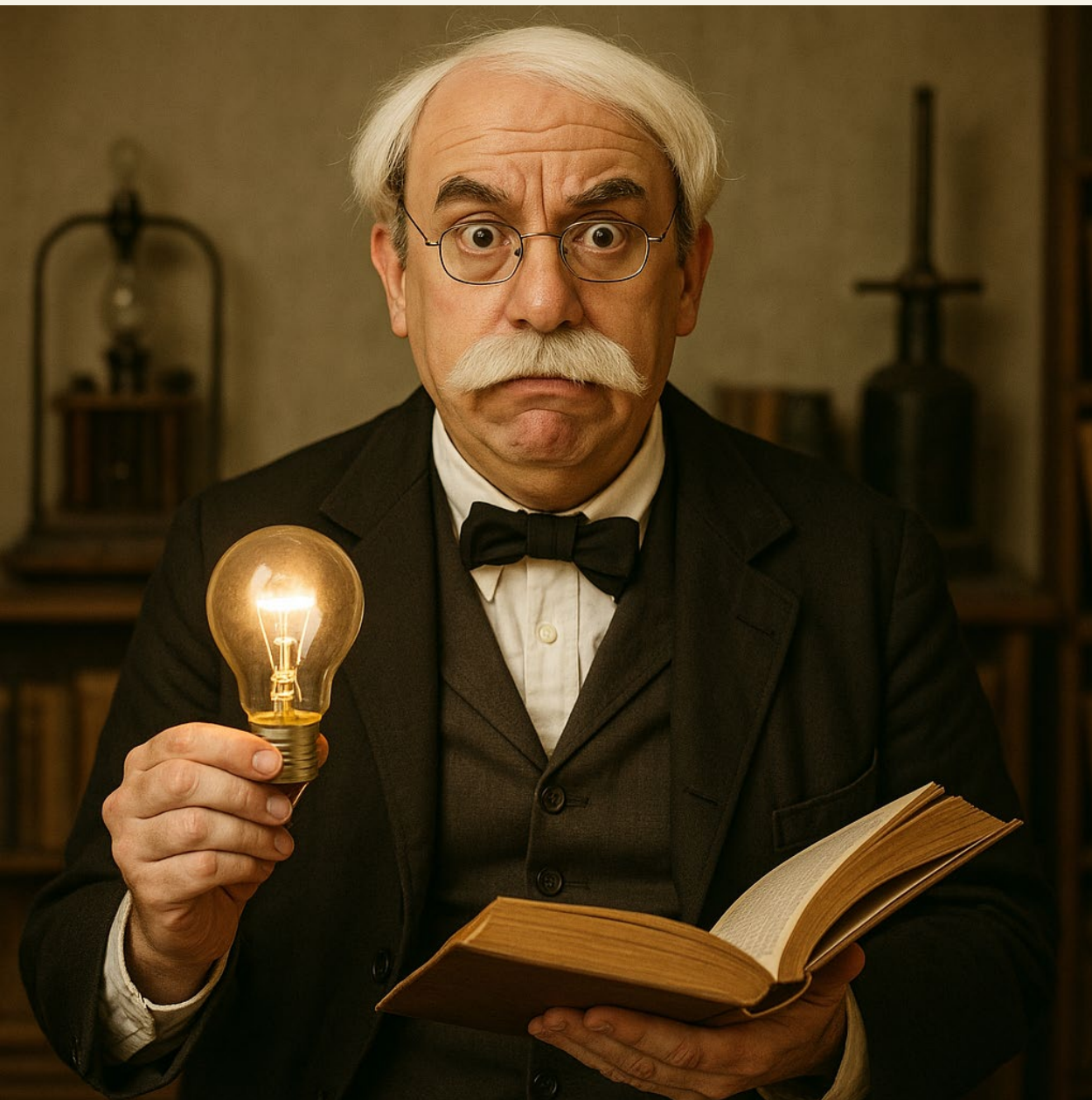# BALANCING TRUST AND ACCESSIBILITY: IMPLEMENTING RESEARCHER IDENTITY VERIFICATION IN SCHOLARLY PUBLISHING

Andy Heard

Sr. Director, IEEE Business Technology

Would you trust this person?

INTRODUCTION

Fictional reviewer accounts used to manipulate peer review

Spoofed emails to inject fictional reviewers

Stolen identities

Unwitting co-authors

Threats to Scholarly Integrity
Research fraud and identity manipulation undermine trust and cause reputational damage in academic publishing.

Traditional Trust Assumptions
Publishers historically relied on implicit trust, assuming good faith from authors and reviewers.

Balancing Security and Accessibility
Verification measures must deter fraud while remaining inclusive and user-friendly for legitimate researchers.

WHY THIS MATTERS

Risks of Weak Identity Checks

Minimal verification methods enable fraud like paper mills and fake peer reviews, causing retractions and loss of trust.

Impact on Scholarly Integrity

Fraudulent practices damage publisher reputation, waste resources, and harm credibility of research outputs.

Need for Balanced Verification

Stronger identity checks deter fraud while ensuring legitimate researchers retain access and inclusivity is maintained.

CORE PRINCIPLES

Inclusivity

Inclusivity ensures that all legitimate researchers can access verification without exclusion.

Proportionality

Verification efforts align with the risk level to avoid unnecessary burdens.

Privacy and Compliance

Privacy minimizes data collection and follows regulations like GDPR transparently.

Feasibility and Accountability

Verification is simple, scalable, integrated, and includes clear accountability for fraud.

THE TENSION BETWEEN TRUST AND FRICTION

Balancing Trust and Friction

Publishers must balance strong identity verification with minimizing participation barriers to maintain trust and accessibility.

Risks of Stringent Verification

Excessive verification steps can deter submissions and reduce inclusivity among participants.

Risks of Lax Verification

Weak verification processes increase fraud risk and threaten the integrity of publishing.

Risk-Proportionate Verification

Verification efforts should match risk level, applying rigorous checks for high-risk roles and streamlined checks for low-risk actions.
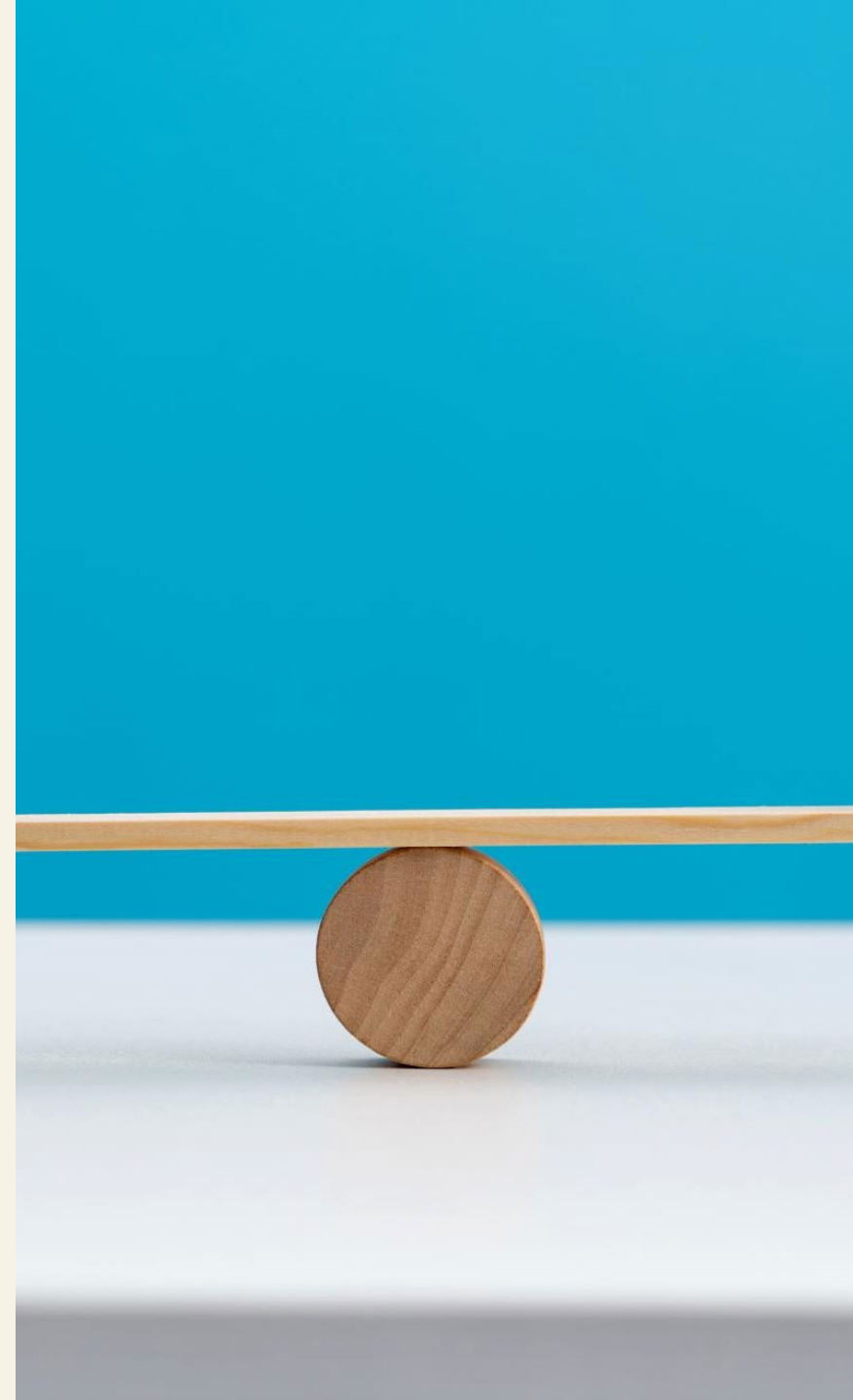
RECOMMENDATIONS AND IMPLEMENTATION

RECOMMENDATIONS OVERVIEW

Multi-step Verification

Introduce verification steps for authors, reviewers, and editors to enhance identity confirmation processes.

Flexible Credential Separation

Separate sign-in credentials from verification methods to provide adaptable and flexible identity checks.

Multiple Verification Routes

Offer diverse verification options such as institutional IDP, email, document checks, and manual fallback.

Continuous Monitoring and Improvement

Monitor outcomes to create feedback loops that improve verification processes inclusively and effectively.

RISK-BASED APPROACH

Proportionate Verification

Verification is matched to the risk severity of actions, ensuring appropriate security without excess burden.

Risk Assessment Framework

Assessment considers action severity and journal profile to identify risk levels for tailored checks.

Continuous Improvement Loop

Outcomes are evaluated with feedback used to refine and improve verification processes continuously.

PRACTICAL STEPS AND STRATEGIC BENEFITS

PRACTICAL IMPLEMENTATION FOR PUBLISHERS

Pilot Verification Processes

Start verification with reviewers and editors who have higher fraud risks to ensure integrity in publishing.

Industry Collaboration

Develop shared infrastructure like email validation services and trust markers for streamlined verification.

Clear Communication

Communicate benefits and purposes of verification clearly to researchers to build acceptance and reduce resistance.

Transparency and Consistency

Ensure transparent design and consistent user experience across platforms to enhance trust and usability.

CHALLENGES AND MITIGATIONS

User Experience Challenges

Identity verification can cause friction for legitimate users, leading to user inconvenience and drop-offs.

Inclusivity and Accessibility

Global inclusivity issues arise for users without institutional affiliations or access to standard verification methods.

Cost and Complexity Management

Shared services and standardized methods help reduce costs and simplify identity verification implementation.

Mitigation Strategies

Using familiar logins, remembering verification choices, and providing fallback options improves verification fairness and efficiency.

STRATEGIC BENEFITS

Publishers' Reputation Protection

Strengthened identity verification helps publishers safeguard their reputation and reduce costs related to fraud.

Researcher Confidence

Researchers benefit from a transparent and fair verification process that builds trust in scholarly work.
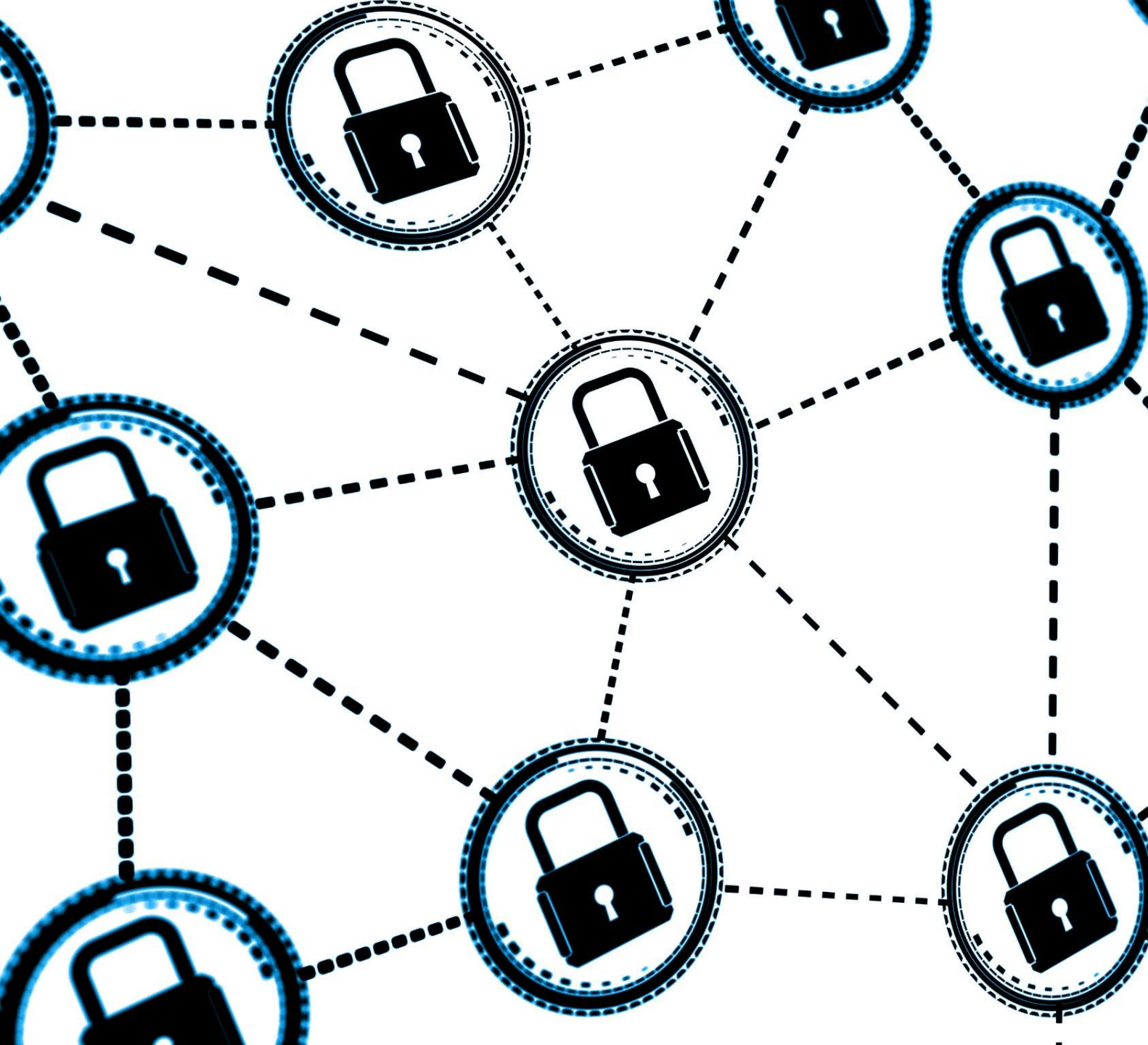
Community Trust

Enhanced identity verification fosters trust across the scholarly community, supporting academic record integrity.

Sustainability of Publishing

Verification strengthens long-term sustainability and integrity in academic publishing as a strategic priority.

CLOSING MESSAGE

Importance of Identity Verification

Identity verification is crucial for building and maintaining trust in scholarly publishing systems.

Collaborative Approach

Engaging stakeholders and sharing best practices fosters collaboration and continuous improvement.

Balance of Accessibility and Security

Verification must be proportionate and inclusive to preserve fairness and accessibility for all researchers.