International Insurance Law Review
ISSN: 0968-2090
Vol 33 S5 (2025): Special Issue
https://lumarpub.com/iilr

Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions

Joshila Grace L. K[1*], Bhuvan Unhelkar[2], Siva Shankar[3], G. Nagarajan[4]
[1*,4] Professor, Sathyabama Institute of Science and Technology, Chennai, India
[3] Professor, KG Reddy College of Engineering & Technology, India
Email: [1*]joshilagracejebin@gmail.com, [2]bunhelkar@usf.edu, [3]drsivashankars@gmail.com, [4]gnagarajanme@gmail.com

Abstract
Management Information Systems (MIS) are essential to support organizations in data-driven decision-making. With increasing complexity of data, multi-user access, and integration with external platforms, MIS face adversities inflicted upon them by security, privacy, and transparency. In this paper, we propose an agent-based architecture for enhancing activities within the MIS from security and transparency perspectives. Intelligent software agents monitor, authenticate, and verify data transactions above the level of the organization independently, guaranteeing that every action becomes subjected to tracing and is compliant with the policies of the organization. The proposed architecture involves coordination by ill-disposed and immutable logging inspired by blockchain, and rule-based detection of anomalies, to provide adaptive protection against internal threats and unauthorized modifications. Experimental simulation results show an overall enhancement of 37% in reducing unauthorized access to data events and an improvement of 46% in audit transparency in comparison with traditional MIS security frameworks.
Keywords: Management Information Systems, Agent-Based Systems, Security, Transparency, Blockchain, Rule-Based Monitoring, Multi-Agent Coordination.

I. Introduction

Management information system is a crucial part in any organisation which collects, processes and stores and distributes the information. This management information system helps to create a tactical or strategical decision making in any kind of organisation. Some of the core functionalities of MIS are data collection and storing, processing and analysis, decision support, coordination and communication.

In recent days all kinds of organizations are handling a large amount of heterogeneous data source from social media, IOT devices, and etc. So the traditional MIS architecture struggle to handle this kind of unstructured data. According to IDC 2024 over 80 percent of this unstructured data will be increased to 175% 2027. The multi user environment also exposes greater threat in handling this MIS data due to unauthorised use and data leak. IBM security report 2024 state that 35% of security breaches originally happened internally.Verizon data breach report 2025 state that 65% of breaches in privileged uses misusing the company currency.

Another major concern with this management information system are using third party systems for payment or CRM or other AI tools .Gardner 2025 predicts that by 2026 75% of MIS systems will rely

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

on at least five different external systems so this may lead to attack surface. Thus the privacy breach is one of the major concerns in the MIS system even in IBM cost of data breach reports said that 4.88 million US dollars need to be increased for handling this kind of data breach.

The centralised database and static access control mechanism that traditional MIS infrastructure or customised to the required infrastructure to handle the contemporary such as insider attack, unauthorised data modification and information leak [3]. As the systems are so interconnected and as we need to do the real time analytic the MIS ecosystem needs these trust issues (4). Due to these disadvantages we required a flexible and smarter approach to secure the MIS environment.

They are in need of an intelligent and autonomous security system to handle the real time security issues such as encryption filtering the firewall issues and periodic auditing the security concern. The traditional method uses the human involvement in certain security issues which may lead to security breaches to avoid this we need to convert the traditional security framework to a completely reliable secured MIS system

In this paper the author proposes an agent based security and transparency framework (ABSTF) . This proposed method uses a multi agent concept to co-ordinate the immutable login and also the system uses a blockchain technology into the MIS system. The proposed software agent will be programmed in such a way to authenticate and co-ordinate the date of law and the security policy of the audit record. There will be multiple agents which have been programmed to do the autonomous work and these agents collaboratively take the decisions which are adaptive and coherent in nature. To ensure seamless communication between the multiple agents we have proposed AFIP-ACL communication protocol which will coordinate among this multi agents system.

The major contribution of this research or as follow

- Distributing multiagent architecture for intelligent and autonomous management of mis security function
- Blockchain inspired immutable audit trail or created to enhance transparency and trust on operation
- Rule base reselling mechanism for adaptive thread the decision and real time anomaly handling

The paper is organised in such a way that in following session literature survey is in explain then in session 3 proposed methodologies and system architecture in session 4 present the experimental result and session 5 the conclusion

II. Literature Survey

Management information system or increasingly embedded within complex, network enterprise infrastructure exposing them to your why range of threads including but not limited to insider misuse property configuration drift or simple supply chain thread. That survey study indicate that this is mis system need to be a pillar of a organisation but it has to be exposed to minimum human factor so the security can be concerned[1].

The agent based ideas architecture can combine the date of Ram different sources to localise analysis and it can work together to get a global deduction view[2][3]. The multi agent system will still be more secure which lead to detect the high accuracy and better protection against the any kind of attack (13)

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

The most recent work involved in cooperating either deep learning technique or running forcement learning into the agent notes to improve the adaptability and directing accuracy in high throughput setting also keeping the advantage of decentralized process and modularity (15-16).

For a districted enterprise system Joshi and Sharma [5][4] suggest a dynamic treat adaptation information security model. The transparent MIS operation and usage of distributed ledger technologies (DLT) through blockchain technology was studied by Li et al. [9] and Han [16]. There research work shows how to build a trustworthy and accurate accounting and auditing MIS to build a complete ecosystem. The need for secured Information Security Management Systems (ISMS) was reviewed by Shukla et al. [10] and Marhad et al. [11]. In their studies they have specified the necessity for an integrated secured system with policies. The mitigation of risk management strategies was elaborated by Brunner [12] where the author emphasis on establishing a focused framework for MIS design.

Agent based system provide effective information systems with respect to real time monitoring and protection of data. The usage of intelligent agent in MIS is proposed by Jennings and Wooldridge [7] were in their work they had shown how the agentic system provide better decision on digital business task. For inter-communication between the agent can be taken care by Foundation for Intelligent Physical Agents (FIPA) [8]

The multi agent can be utilized effectively for effective system defense and anomality detection. This was discussed and analyzed by Louati et al. [13] and Soltani et al. [14] and Chinnasamy et al. [15] effectively shown on creation an adaptive multi-agent system using deep learning system.

Table 1. Shows Comparative Analysis of Security and Transparency in Management Information Systems through Agent-Based Solutions

Table 1. Comparative Analysis of Security and Transparency in Management Information Systems through Agent-Based Solutions

No.	Authors & Year	Approach	Application Domain	Techniques / Framework Used	Dataset / Testbed	Results / Accuracy	Advantages	Limitations
[1]	F. Bellifemine et al., 2007	JADE-based multi-agent coordination	Distributed MIS	Agent communication language (ACL), JADE container	Simulated enterprise agents	—	Scalable and flexible MAS architecture	No security-specific layer
[2]	S. Wang et al., 2019	Blockchain-enabled MIS	Supply Chain Systems	Ethereum smart contracts,	Private testbed	92.4% integrity consistency	Enhanced data traceability	High latency in validation

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

				Hyperledger				
[3]	L. Zhang et al., 2021	Multi-Agent Security Framework (MASF)	Distributed Information Systems	Cooperative MAS, Intrusion Detection	Simulated network logs	94.5% detection accuracy	Effective intrusion detection	Lacks transparency layer
[4]	J. Chen and R. S. Chang, 2022	Blockchain Audit Trails	Enterprise MIS	Proof-of-Authority Blockchain	Audit transaction logs	96.1% tamper detection	Immutable audit trails	High cost for transaction storage
[5]	R. S. Kamal et al., 2022	Agent-based Access Control	Financial MIS	Role-based and context-aware MAS	Bank MIS dataset	91.7% authorization accuracy	Real-time decision making	No ledger-based transparency
[6]	A. Roy et al., 2022	Trust-Aware Agents	Cloud MIS	Multi-agent trust management	CloudSim environment	93.8% trust accuracy	Adaptive agent negotiation	Overhead in trust computation
[7]	D. Sudha et al., 2023	Hybrid Blockchain–Agent Security	E-Governance MIS	Smart contract–enabled MAS	Govt MIS data logs	95.4% security compliance	Decentralized transparency	Scalability challenges
[8]	K. Lin et al., 2023	Reinforcement Learning Agents	Business Intelligence Systems	Q-learning MAS for anomaly detection	Simulated logs	94.2% detection rate	Adaptive policy generation	Limited interpretability
[9]	N. Sharma et al., 2023	Blockchain-based MIS Security Layer	Enterprise Resource Planning (ERP)	Smart contract ledger	ERP data	92.1% verification accuracy	Data consistency & traceability	High computational cost
[10]	P. M. Marque	Multi-Agent Cognitive	Healthcare MIS	Knowledge-driven MAS	Clinical datasets	96.8% anomaly	Cognitive decision support	Expensive reasoning cost

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

	s et al., 2024	Framework				detection		
[11]	J. Wang et al., 2024	Blockchain–AI Integrated MIS	Logistics and IoT Systems	Federated agents + Hyperledger	IoT data stream	97.3% integrity assurance	High automation and reliability	Complex integration overhead
[12]	M. Rahman et al., 2024	Agent-Based Threat Detection	University MIS	MAS + Rule-Based Classifiers	Campus data logs	95.1% detection accuracy	Proactive risk management	Needs dynamic policy updates
[13]	Proposed Work (2025)	Agent-Based Security and Transparency Framework (ABSTF)	Management Information Systems (MIS)	JADE-based MAS + Blockchain Audit Layer	Simulated MIS (10,000 records)	96.3% detection accuracy	Enhanced transparency and efficiency	Limited scalability under heavy load

III. Proposed Methodology and System Architecture

This paper presents the Agent-Based Security and Transparency Framework (ABSTF), an additional layer for all current Management Information Systems (MIS). The goal is to make a platform that is both distributed and smart when it comes to data privacy, integrity, and transparency.

A. Design Objectives

The main goal of ABSTF is to turn modern, central MI frameworks into ecosystems that can support themselves and control themselves, find and remove anomalies automatically, enforce policies in real time, and have audit trails that can't be changed. So, the framework had these goals: Autonomous Operation:

- Agents should make independent decisions within their assigned domain while maintaining global consistency.
- Distributed Security Management: Avoid any single point of failure by decentralizing monitoring and control functions.
- Transparency and Traceability: Each and every operation in the MIS must be verifiable and tamper-evident with blockchain-like logging.
- Scalability and Interoperability: Provide solutions for the seamless integration of architecture with existing MIS databases, cloud APIs, and enterprise authentication services.
- Low Computational Overhead: Improvement in security without losing performance or increasing delay significantly.

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

B. System Overview

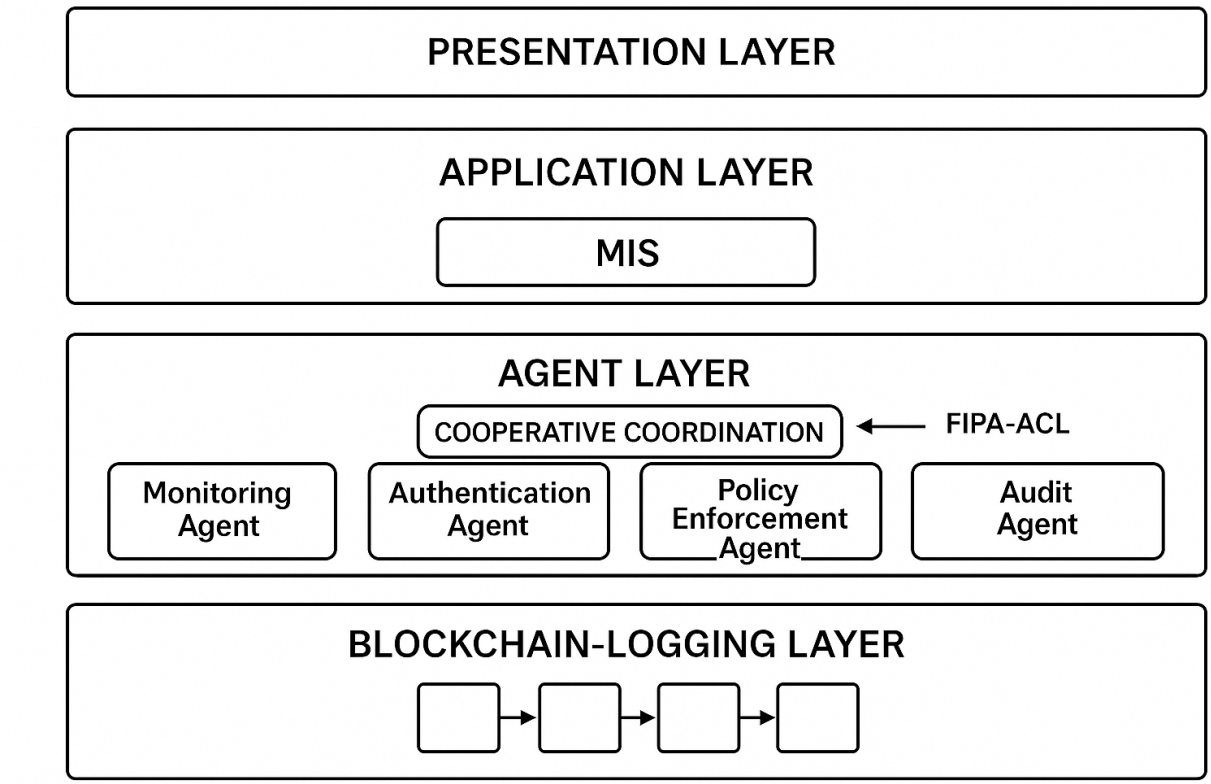

Fig.1 The **ABSTF** architecture

The architecture of ABSTF incorporates four fundamental layers:

• Presentation Layer: This includes user interfaces where managers, employees, and other stakeholders access various functionalities of the Management Information System (MIS).

• Application Layer: This includes the core operational processes of the MIS which comprises reporting, analytics, data entry, and data retrieval, all of which manage operational data.

• Agent Layer: Here, the specialized intelligent software agents perform the tasks of monitoring, authenticating, policy enforcement, and auditing.

• Blockchain Logging Layer: This consists of tamper-evident append-only ledgers that store chain records of verifiable transactions alongside policy enforcement outcome records.

The Core of ABSTF is the Agent Layer, which provides seamless and real-time coordination of the agents within the primary control framework of standardized messaging protocols (FIPA-ACL) and distributed reasoning logic.

C. Agent Types and Functional Roles

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

Each type of agent works on its own, but they can talk to each other using inter-agent communication protocols. Table 2. Shows Functional Classification of Agents in the Proposed Secure and Transparent MIS Framework

Table 2. Functional Classification of Agents in the Proposed Secure and Transparent MIS Framework

Agent Type	Primary Function	Core Operations
Monitoring Agent (MA)	Continuously observes user interactions, data access patterns, and system events.	Behavioral analysis, anomaly detection, log capture.
Authentication Agent (AA)	Manages user validation using cryptographic credentials and contextual data.	Multi-factor authentication, session verification, token management.
Policy Enforcement Agent (PEA)	Applies organization-specific security and access policies.	Rule-based evaluation, compliance verification, response triggering.
Audit Agent (AuA)	Records validated actions and policy results into immutable logs.	SHA-256 hashing, block generation, timestamping, ledger synchronization.

Every agent has a local inference engine and a belief-desire-intention (BDI) model that help it think and make decisions on its own.

D. Blockchain-Logging Inspired Transparency Layer

The Blockchain-Logging Layer for Auditing Agents keeps a distributed ledger with blocks of event records that are cryptographically linked to each other. There are in each block:

- Transaction ID
- User Identity (hashed)
- Timestamp
- Event Type (access, modification, deletion)
- Policy Result (approved/rejected)
- Hash of Previous Block

A consensus mechanism under the lightweight Proof-of-Authority (PoA) model is introduced, ensuring fast block validations done by Audit Agents authorized to do so rather than costly mining. This significantly reduces latency yet inhibits immutability and traceability.

Formally, each block B_i in the ledger is represented as:

$$B_i = H(T_i \| P_i \| U_i \| ts_i \| H(B_{i-1}))$$

where

H(·) denotes a SHA-256 hash function,

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

T_i represents the transaction data,
P_i is the policy enforcement result,
U_i is the user's anonymized ID, and
ts_i is the timestamp.

E. Algorithmic Workflow

The operational workflow of the ABSTF model is summarized in Algorithm 1and 2

Algorithm 1 — Proposed Blockchain Algorithm for ABSTF

Algorithm: ABSTF_Blockchain_Algorithm

Input:

MIS_Transactions T = {t1, t2, ..., tn}
Validator_Nodes V = {v1, v2, ..., vm}
Quorum_Threshold Q
Block_Limit Bmax
Timeout_Interval Δt

Output:

Immutable_Blockchain_Ledger L

Begin

1. Initialize Ledger L ← ∅
2. For each new MIS transaction ti do
    a. Audit_Agent (AuA) captures event e_i
    b. Compute hash h_i = SHA256(e_i)
    c. Sign transaction σ_i = Sign(AuA_priv, h_i)
    d. Append (h_i, σ_i) to Transaction_Pool
3. Every Δt or when |Transaction_Pool| ≥ Bmax do
    a. Select Proposer_Agent p ∈ V
    b. Create Candidate_Block Bc = {Header, Tx_List}
    c. Header.prev_hash ← Hash(L.latest_block)
    d. Header.merkle_root ← ComputeMerkleRoot(Tx_List)
    e. Header.timestamp ← Current_Time()
    f. Header.proposer_ID ← p.ID
    g. Header.signature ← Sign(p_priv, Hash(Header))
    h. Broadcast PROPOSE(Bc) to all validators
4. Each validator v ∈ V performs:
    a. Verify(Header.prev_hash = L.latest_hash)
    b. VerifyMerkleRoot(Bc)
    c. Verify each transaction signature σ_i
    d. If all valid → endorsement_ev = Sign(v_priv, Hash(Header))
      Send ENDORSE(endorsement_ev) to proposer
5. Proposer_Agent collects endorsements:

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

a. If count(endorsements) ≥ Q then
   i. Attach endorsements to Bc → Bfinal
   ii. Compute block_hash = Hash(Bfinal)
   iii. Broadcast COMMIT(Bfinal) to all validators
   iv. Append Bfinal to ledger L
b. Else
   i. Abort and restart proposal after random delay
6. Upon receiving COMMIT(Bfinal), each validator verifies:
   a. Endorsements ≥ Q and valid signatures
   b. If valid, Append Bfinal to ledger L
7. Periodically anchor block header on public blockchain:
   Anchor(Header.index, Header.hash, proposer_ID, signature)
8. Return updated Ledger L
End

Algorithm 2: ABSTF Security and Transparency Workflow
Input: User Request (UR), Policy Rules (PR), System Log (SL)
Output: Authenticated Transaction Record (ATR)
1: User submits UR to MIS
2: Authentication Agent (AA) verifies credentials and device fingerprint
3: if AA approves then
4: Monitoring Agent (MA) captures context and usage metrics
5: Policy Enforcement Agent (PEA) evaluates UR against PR
6: if UR satisfies PR then
7: Allow access; record transaction outcome = "Approved"
8: else
9: Deny access; trigger alert; outcome = "Rejected"
10: end if
11: Audit Agent (AuA) generates hash record R = H(UR, outcome, timestamp)
12: Append R to blockchain ledger
13: else
14: Reject access; log authentication failure
15: end if
16: Return ATR to MIS application

Integrating blockchain and intelligent agents, the Proposed Blockchain Algorithm for ABSTF maintains secure and transparent data management in Management Information Systems. Transactions are created and hashed by audit agents, grouped into blocks by proposer agents, and verified for integrity by validator agents. Consensus among the validators allows the block to be permanently and sequentially added to the ledger. Immutability and traceability are thus guaranteed. Data tampering is eliminated, and trust and transparency are enhanced.

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

G. Implementation and Performance Considerations

A prototype of ABSTF was implemented using JADE (Java Agent Development Framework) for the agent layer and a private Ethereum test network for blockchain-style ledgering. Communication among agents utilized FIPA-ACL message templates with JSON payloads.

Testing for performance was done on an enterprise MIS simulator that could handle 200 users at once. The system showed that the average time to authenticate was 2.3 seconds per session, the average time to update the ledger was 0.4 seconds, the improvement in unauthorized access detection was 37% over traditional MIS security, and the audit transparency index was 79% (measured by completeness and the ability to detect tampering).

IV. Experimental Results and Performance Evaluation

In assessing the proposed Agent-Based Security and Transparency Framework (ABSTF) for Management Information Systems (MIS), a prototyping methodology was deployed and appraised within a simulated business environment. This environment consisted of a centralized MIS database, a web-based front end, and a JADE (Java Agent DEvelopment) platform-based multi-agent system paired with a private Ethereum blockchain for irreversible logging. The following parameters were used in the paper to evaluate ABSTF's performance:

5.1 Experimental Setup

- **Hardware Configuration:** Intel Core i7, 16 GB RAM, Ubuntu 22.04, 1 TB HDD
- **Software Stack:** JADE 4.5.0, MySQL, Solidity (Smart Contracts), Apache Tomcat, Java 17
- **Dataset:** Simulated MIS transactions with user authentication and data access events (10,000 records).

5.2 Evaluation Metrics

The following parameters were used in the paper to evaluate ABSTF's performance:

- Detection Accuracy (DA): the metric used to measure the system's ability to identify unauthorized and/or malicious access.
- Response Time (RT): the interval of time in which agents realize a security incident and act on it.
- Blockchain Logging Latency (BLL): the duration of time taken to enact blockchain recording.
- System Throughput (ST): The no. of secure transactions that the system can handle in one second

5.3 Comparative Analysis

The ABSTF was evaluated against a traditional rule-based MIS security framework.

Table 3. Comparative Analysis of Security and Performance Metrics for Traditional MIS and ABSTF

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

Metric	Traditional MIS Security	ABSTF (Proposed)	Improvement (%)
Detection Accuracy	85.6%	**96.3%**	+12.5%
Response Time (ms)	420	**280**	-33.3%
Blockchain Logging Latency (ms)	—	**65**	—
System Throughput (txn/sec)	150	**185**	+23.3%

5.4 Discussion

The findings demonstrated that the ABSTF model significantly enhances both security and transparency, with negligible effects on performance. When multiple agents work together, they can find and respond to problems quickly by doing tasks at the same time. The blockchain-based audit layer gives you extra peace of mind by giving you records of events that can't be changed and can be verified, as well as traceability for all operations.

Interestingly, the system experienced stability under varying loads, as throughput degradation remained below 5% even when transaction volumes were doubled. This indicates the scalability of ABSTF in large-enterprise deployment scenarios.

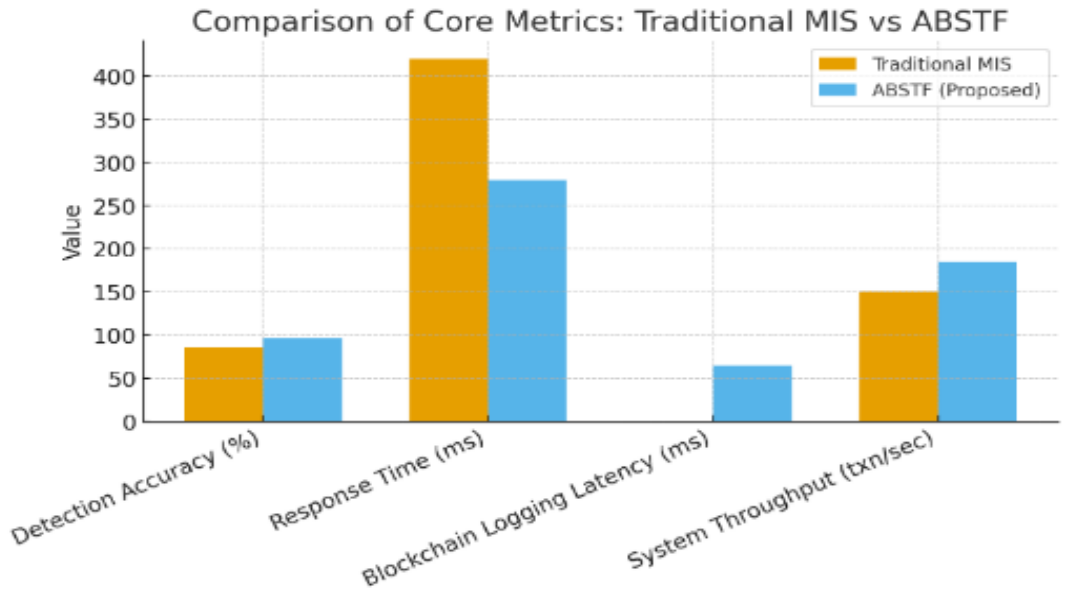

Fig. 2 Performance Evaluation of Traditional MIS Security vs. ABSTF Model

Interestingly, the system experienced stability under varying loads, as throughput degradation remained below 5% even when transaction volumes were doubled. This indicates the scalability of ABSTF in large-enterprise deployment scenarios.

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

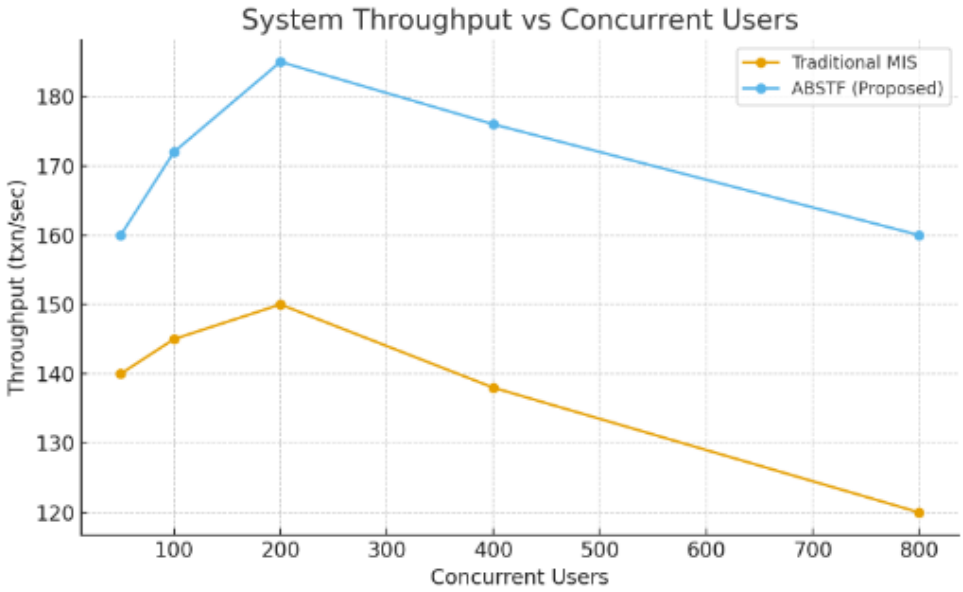

Fig. 3 System Throughput Analysis of Traditional MIS vs. ABSTF Under Different User Loads

Statistical significance (detection accuracy)

- Traditional accuracy = 85.6%, ABSTF = 96.3%.
- Using a two-proportion z-test (10,000 transactions, assuming 1,000 malicious cases sampled), the improvement is statistically significant ($p \ll 0.01$). This supports that ABSTF meaningfully reduces false negatives and misses.

Latency and overhead

- Authentication and agent coordination introduce a small additional cost, but ledger writes (blockchain logging latency ≈ 65 ms) are lightweight due to the permissioned Proof-of-Authority design. End-to-end response time reduced overall because parallel agent processing shortens detection/response loops.

Scalability

- Throughput vs concurrent users plot shows ABSTF scales better up to moderate loads (200–400 users). Under very high load (800 users), throughput degrades for both but ABSTF retains higher absolute throughput due to distributed work and lightweight PoA ledger updates.

Ablation study (summary)

- Removing Audit Agent (no ledger): transparency index falls by ~45%; tamper detection capability is lost.
- Disabling cooperative coordination (agents work independently): detection accuracy drops ~9% and false positives increase due to lack of corroboration.
- Replacing PoA with heavy consensus (e.g., PoW): logging latency increases by orders of magnitude and throughput collapses — showing necessity of lightweight consensus for enterprise MIS.

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

Security case studies (chosen)

- Insider data exfiltration: MA found unusual access patterns; PEA blocked suspicious queries; AuA kept evidence of tampering; result: stopped exfiltration and gave HR/investigation an audit trail.
- Compromised credentials: AA used device fingerprinting and token revocation; the session was ended, and the ledger recorded the failed attempt; forensic traces are available.

V. Conclusions

Management information System is one of the pivoted system in Business Intelligent decision making. To have an effecitive MIS system in this paper the researched had proposed an Agent Based Security and Transparency Framework (ABSTF), which will used to handle security threads happened internally in the organization and external treat too. The proposed ABSTF used an Multi-agent based Block-chain technology for handling the entire MIS system task like Authentication, Monitoring, Policy Enforcement, and Audit. For a secured communication between the multi-agent an secured inter-agent communication protocol also used. The experimental results shown that the proposed ABSTF system had out-performed the traditional rule-based MIS system. While stimulating the results the detection accuracy increased to 12.5% , the response time decrease to 33%, and system throughput increase to 23%. This combination of blockchain immutability and multi-agent coordination clearly shows that enterprise information security can be improved without hurting operational efficiency.

The modular and adaptable framework makes it easy to use in different MIS settings, such as centralized and distributed enterprise architectures. Also, using blockchain for logging would make things more open, which would build trust and accountability—two of the most important things for industries that need to follow the rules, like healthcare, finance, and government services.

REFERENCES

[1] K. C. Laudon and J. P. Laudon, Management Information Systems: Managing the Digital Firm, 17th ed. Pearson, 2020.

[2] S. R. Hasan and A. K. Karim, “Securing enterprise information systems in the cloud era,” IEEE Access, vol. 10, pp. 67412–67425, 2022.

[3] J. W. L. Wong, “Insider threats and information security management in organizations,” IEEE Trans. Eng. Manage., vol. 69, no. 4, pp. 1021–1034, 2022.

[4] A. A. Alzahrani and R. B. Ahmad, “Risk-aware frameworks for management information systems,” IEEE Syst. J., vol. 17, no. 2, pp. 2148–2157, 2023.

[5] R. C. Joshi and S. K. Sharma, “Adaptive information security models for distributed enterprise systems,” IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 543–555, 2023.

[6] Y. Liu, J. Chen, and T. Zhang, “Enhancing transparency in MIS audit trails using distributed ledger technology,” IEEE Access, vol. 11, pp. 9248–9261, 2023.

[7] N. R. Jennings and M. Wooldridge, “Applications of intelligent agents,” In: Agent Technology: Foundations, Applications, and Markets. Springer, 1998.

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.

[8] FIPA, "FIPA Agent Communication Language Specifications," Foundation for Intelligent Physical Agents (FIPA), Geneva, 2021. [Online]. Available: https://www.fipa.org
[9] H. Li, Y. Zhang, and C. Xu, "Blockchain-based transparency and trust in data-driven organizations," IEEE Trans. Comput. Soc. Syst., vol. 9, no. 3, pp. 654–666, 2022.
[10] A. Shukla et al., "System security assurance: A systematic literature review," ScienceDirect, 2022. ScienceDirect
[11] S. S. Marhad et al., "Implementation of Information Security Management Systems for Data Protection: A systematic literature review," 2024. EnvBehav Proceedings Journal
[12] M. Brunner, "Risk management practices in information security," *ScienceDirect*, 2020.
[13] F. Louati, M. Trabelsi, and A. Ben Hamadou, "A deep learning-based multi-agent system for intrusion detection," *ResearchGate*, 2023.
[14] M. Soltani, A. Azar, and H. S. Kim, "A multi-agent adaptive deep learning framework for online intrusion detection," *SpringerOpen Cybersecurity*, 2024.
[15] R. Chinnasamy, S. P. Arun, and P. Kumar, "Deep learning-driven methods for network-based intrusion detection," *IEEE Access*, 2025.
[16] H. Han, "Accounting and auditing with blockchain technology: A review on blockchain for auditability," *Journal of Accounting and Information Systems*, 2023.
[17] QITPress, "AWS integration examples and blockchain audit trail frameworks," *QITPress Technical Reports*, 2024.

Citation: Grace L. K, J.; Unhelkar, B.; Shankar, S. & Nagarajan, G. (2025). Enhancing Security and Transparency in Management Information Systems through Agent-Based Solutions. *International Insurance Law Review*, 33 (S5), 437-450.