femington

Int. J. Artif. Intell. Agent Syst. (2026) 1(1):1–11
Article ID: IJAIAS-2026-795

Formalizing Trust: A Modal Logic Approach to Trust Management in Distributed Systems

Ujjwal Yadav
y-ujjwal12@yahoo.com
Independent Researcher

Abstract

Trust is a core concept in secure and cooperative distributed systems. However, the dynamic, context-dependent nature of trust poses challenges to its formalization and enforcement. In this paper, we offer a framework for trust management in a modal logic-based setting. In particular, we offer a rigorous method to model belief, knowledge, and delegation among agents. In multi-agent systems, we study how modal operators can represent fundamental aspects of trust, such as permissions, obligations, and authority propagation. Our framework improves the specification and verification of trust-based decisions, enabling reasoning through modal logic to formalize trust relationships. The system were proposed can induce both monotonic and non-monotonic inferences, thus providing flexibility in inducing or revoking trust. The framework is demonstrated to be wide-ranging, robust, and useful in policy specification, access control, and automated trust negotiation. The proposed work promotes transparent, verifiable, and intelligent trust management mechanisms in distributed and decentralized systems.

Keywords

• Trust Management • Modal Logic • Distributed Systems • Role-Based Access Control (RBAC) • Context-Aware Authorization • Temporal Reasoning

1. Introduction

Trust constitutes a foundational pillar in secure and cooperative distributed systems, serving as a critical enabler for authorization, delegation, and decision-making processes. The establishment and maintenance of trust determine the effectiveness of interactions among autonomous agents and the robustness of system-wide operations. However, the dynamic and context-dependent nature of trust presents significant challenges for formalization, monitoring, and enforcement. Trust is inherently influenced by temporal, spatial, and situational variables that evolve unpredictably, leading to frequent invalidation of previously held assumptions or authorizations [1, 2].

Traditional systems often assume static credentials throughout a session, overlooking the fact that contextual information such as user location, device status, environmental variables, or network conditions may change within seconds, rendering previous authorization decisions obsolete. Rigid credential-based systems are ill-equipped to address this volatility, resulting in increased vulnerability to policy violations, security breaches, and operational inconsistencies [3].

In environments where contextual factors evolve rapidly, authorization mechanisms must adapt by continuously reassessing session validity. Static validation models, which verify credentials only at the time of session initiation, are insufficient for supporting dynamic contexts and evolving risk landscapes. A comprehensive trust management framework must incorporate continuous evaluation, reactive adaptation,

and predictive reasoning about possible future states. The ability to proactively enforce security policies based on anticipated changes in trustworthiness is critical for sustaining secure interactions in decentralized and heterogeneous systems [4].

Existing trust management frameworks predominantly focus on credential verification, policy enforcement, or probabilistic trust scoring without offering rigorous formal reasoning capabilities. While reputation-based and statistical models provide adaptability, they often lack explainability, verifiability, and formal guarantees essential for high-assurance systems. Logic-based approaches, on the other hand, offer a pathway for specifying and verifying trust properties with mathematical rigou [5, 6]; however, a comprehensive integration of modal logic capable of expressing temporal evolution, conditional dependencies, and dynamic revocation remains largely underexplored.

Modal logic, with its intrinsic ability to reason about possible worlds, state transitions, and evolving truths, presents a powerful yet underutilized tool for trust modelling [7, 8]. By enabling formal representation of beliefs, obligations, permissions, and authority propagation across time and context, modal reasoning offers significant advantages in designing trust management systems that are both adaptive and verifiable [9, 10].

This work introduces a modal logic framework for trust management in distributed systems, facilitating explicit modelling of belief, knowledge, permissions, and delegation under evolving contextual conditions. Formalizing trust relationships through modal reasoning enhances the ability to specify, verify, and dynamically enforce trust-based policies across decentralized and dynamic environments. Moreover, this framework establishes a foundation for the development of intelligent, transparent, and verifiable trust management systems suited to modern architectures, including mobile ad hoc networks, peer-to-peer infrastructures, IoT ecosystems, and federated identity platforms. By bridging the gap between theoretical rigor and practical applicability, modal logic-based trust management approaches offer promising solutions to longstanding challenges in secure distributed computing, thereby enabling more resilient, explainable, and future-proof security architectures.

2. Related Work

Trust management in distributed systems has been extensively studied across multiple disciplines, including computer security, distributed computing, formal methods, and artificial intelligence. Early frameworks such as the PolicyMaker and KeyNote systems [1, 3] laid foundational work in expressing flexible security policies and delegating trust in a decentralized fashion. These systems emphasized the need for distributed authorization schemes independent of centralized identity authorities, setting the stage for scalable trust infrastructures.

Building on these foundations, logic-based approaches to trust were proposed to provide formal semantics for reasoning about authorization, delegation, and revocation. The BAN logic [11] played a seminal role in formalizing authentication protocols through belief logic, influencing later work on protocol verification and trust propagation. More expressive systems, such as Binder [5] and SecPAL [6], extended the logical framework to accommodate practical policy specifications and interoperability among heterogeneous systems.

Modal logic has also played an important role in formalizing reasoning in distributed and multi-agent systems. Modal epistemic logics, such as those discussed by Fagin et al. [7] has been utilized to capture agents' knowledge, belief, and uncertainty. The application of modal logic to security and trust management, although comparatively limited, has demonstrated significant promise.

In addition to logical models, reputation-based trust evaluation has been widely adopted, particularly

in peer-to-peer (P2P) systems and open environments. Models such as EigenTrust [12], PeerTrust [13], and PowerTrust [14] offer mechanisms for quantifying trustworthiness based on transaction history and community feedback. However, these systems typically rely on statistical aggregation and machine learning techniques, limiting formal verifiability and explainability of trust decisions.

Formal verification tools such as TLA+ [15], Alloy [16], and SPIN [17] have enabled the rigorous specification and analysis of security properties in distributed systems. Although highly successful for system-level verification, these tools have not been widely adapted to model dynamic trust relationships. Logic programming frameworks, particularly Datalog [18], have been employed in trust management systems like Cassandra and have shown effectiveness in expressing fine-grained trust rules, albeit without dynamic temporal reasoning.

Emerging approaches have begun exploring the fusion of modal, temporal, and epistemic logics with trust frameworks. Research in dynamic logic and belief revision [19] opens additional avenues for formalizing adaptable and context-sensitive trust mechanisms. This work contributes to this evolving body of literature by integrating modal logic into trust management frameworks for distributed systems, aiming to combine the expressiveness of formal reasoning with the dynamic, volatile nature of trust relationships. Compared to probabilistic and reputation-based models, the proposed approach emphasizes transparency, explainability, and formal verifiability. Unlike prior logic-based frameworks, the current model leverages modal operators to encode trust delegation, belief evolution, context-aware revocation, and policy dynamics in distributed settings.

3. Problem Scope

To ensure clarity and manageability, the proposed framework focuses initially on a constrained context. The scope of application is restricted to role-based access control (RBAC) systems, specifically those adhering to the Role-based Trust-management (RT) framework [18]. In such systems, authorization decisions depend exclusively on determining principal membership within defined roles, simplifying the complexity of trust evaluation. Further narrowing the focus, the current work addresses only temporal contextual inputs. The validity of credentials and contextual claims is treated as time-dependent, without consideration of other dynamic attributes such as location, device state, or environmental conditions. Several factors motivate this restriction. Temporal context frequently influences access control scenarios, including time-based employee privileges, certificate expiration, and emergency response activation. Additionally, the theoretical foundations for reasoning about time, such as temporal modal logics, are well-established and offer a mature basis for formal modeling [20].

Concentrating on temporal dynamics provides an opportunity to establish a solid and extensible theoretical framework capable of handling time-sensitive trust relationships. Although the initial model excludes other types of contextual inputs, the underlying principles are designed to accommodate future generalizations. Incorporating additional context modalities such as spatial, organizational, or behavioral dimensions would entail the extension of the modal logic framework, leveraging established advances in multi-modal logic systems [11]. Limiting the scope to RBAC and temporal contexts facilitates the development of formal definitions, reasoning mechanisms, and correctness proofs, which are essential prerequisites for practical implementation. A rigorous foundation in this specialized domain serves as a stepping stone toward constructing scalable and adaptable trust management solutions applicable to broader distributed and decentralized systems.

4. Instantiation of RT^R

Extending the RT framework to incorporate contextual inputs necessitates a formal instantiation of Role-based Trust Management with Contextual Reasoning (RT^R) [18]. The proposed instantiation models contextual conditions as time-invariant propositions, allowing the system to reason about access control decisions in the face of dynamically evolving environmental, situational, or state-based inputs. This enables a more nuanced and adaptive decision-making process that can reflect the real-time state of systems and entities involved in a given process.

Let $P = \{p_0, p_1, p_2, \dots\}$ denote a countable set of primitive proposition symbols, where each p_i represents a specific contextual condition. These conditions can range from environmental states, such as critical reactor temperature or system load, to operational states, such as the presence of personnel in restricted areas or the health status of patients in a hospital. Each proposition p_i is a discrete, measurable condition that can change over time, and the formal structure provided ensures that the dynamic nature of these conditions is well-supported by the framework. In practical terms, this might include sensor readings, user actions, or any other input that can affect the security or operational requirements of the system.

To ensure semantic consistency and facilitate interoperability across different stakeholders in a distributed system, it is crucial that all participants share a common interpretation of the symbols. This is especially important when credentials are exchanged across federated trust systems, where multiple organizations might rely on different contextual conditions to determine access rights [1]. By using standardized propositions and ensuring their uniform interpretation, the system guarantees a consistent basis for decision-making.

The set of well-formed propositional formulas F is defined inductively as follows:

- The symbols $\top$ (truth) and $\bot$ (falsehood) are elements of F, providing the foundational elements for the lattice.
- Each primitive proposition p_i is an element of F, representing basic contextual information.
- Negations $\neg p_i$ are elements of F, enabling the system to model conditions where the negation of a contextual proposition is required (e.g., ensuring access only when certain conditions are not met).
- Conjunctions $f_i \wedge f_j$ are elements of F for $f_i, f_j \in F$, allowing the system to combine multiple conditions to form more complex reasoning about access control. This conjunction operation reflects the need for multiple conditions to be satisfied simultaneously.

The restricted set of operations (excluding disjunction and other complex operations) serves two important purposes. First, it helps maintain decidability within the system, ensuring that reasoning about access control remains computationally feasible even as the complexity of the system increases. Second, the simplicity of the set ensures that the system remains robust and predictable, even in the face of large-scale deployment where performance and reliability are critical. The lack of disjunctions prevents the system from becoming overly complex and ensures that reasoning remains grounded in clear, understandable conditions.

Based on these definitions, a complete lattice $(K, \sqsubseteq)$ is established, where $K = F$ and the ordering relation $\sqsubseteq$ is defined by set inclusion over primitive propositions contained within each formula. This ordering relation provides a clear hierarchy, where more general formulas (those including a larger set of propositions) are considered "larger" or more inclusive, while more specific formulas (those containing

fewer propositions) are considered “smaller.” The bottom element $\bot$ represents absolute falsehood, while the top element is represented by the conjunction $\top \wedge p_0 \wedge p_1 \wedge \ldots$, which represents a formula where every possible condition holds true, thus enabling the maximal level of access.

The aggregation operators required by RT^R, specifically $\oplus$ and $\otimes$, are instantiated as logical conjunctions ($\wedge$). These operators preserve associativity and monotonicity, which are important properties when working with lattices and ensuring that reasoning about access control remains consistent and predictable. The use of conjunction as the aggregation operator reflects the need for multiple conditions to hold true simultaneously for a particular access decision to be made.

Credential issuance within this model binds principal roles to contextual formulas. For instance, consider a hospital H issuing a credential that grants a doctor access to emergency resources conditioned upon being on call. This condition can be represented as:

$$H.e \leftarrow A, p_c$$

where p_c denotes the proposition "on-call status is active." This example demonstrates how role-based trust can be adapted to context-specific situations, where a doctor’s ability to access critical resources is not only dependent on their role but also on the real-time status of the on-call condition.

Federated trust arrangements among entities, such as hospitals and emergency services, can be captured through hierarchical role delegations conditioned on contextual conjunctions. For example, a federation F may define its member hospitals with credentials of the form:

$$F.m \leftarrow H, \top$$

indicating that a hospital in the federation can delegate certain trust properties without conditions. However, external authorities, such as a police department P, may issue credentials that require more stringent conditions, such as:

$$P.r \leftarrow F.m.e, p_a \wedge p_n$$

where p_a and p_n denote propositions corresponding to specific conditions, such as "accident activity is occurring" and "unstabilized patients are present," respectively. These credentials are issued under the context of both the federation’s trust and the particular emergency conditions, ensuring that access is only granted under the appropriate circumstances [5].

Through this instantiation, RT^R supports the precise and expressive modeling of authorization policies that adapt to evolving contextual realities. By leveraging propositional logic and role-based delegation, the system provides a structured and verifiable approach to making access control decisions. This allows organizations to implement fine-grained access control policies that consider both the roles of participants and the dynamic conditions under which they operate. Additionally, the model’s simplicity and formal structure enable easier validation and enforcement of these policies, promoting greater trust and security in distributed systems.

Moreover, as RT^R supports temporal reasoning and the use of evolving conditions, it is possible to incorporate additional elements such as time-based constraints, user activity monitoring, and more sophisticated event-driven decisions. These features further enhance the adaptability of the system, allowing it to react to real-time conditions in a way that is both efficient and secure. As distributed systems grow in complexity, such a model becomes increasingly valuable, ensuring that access control remains both secure and responsive to the dynamic nature of the real world.

5. Role of Modal Logic

Modal logic provides a natural and rigorous framework for reasoning about trust in distributed systems, particularly in environments characterized by dynamic and context-dependent information [7]. In modal logic, reasoning occurs over a universe of states, where each formula is evaluated relative to a particular state. This state-centric approach aligns with trust management scenarios, in which authorization decisions depend critically on the evolving contextual conditions.

Temporal modal logic extends traditional logical systems by introducing operators that capture properties over time, such as necessity ($\Box$) and possibility ($\Diamond$) [10, 19]. These operators enable explicit reasoning about how contextual states evolve and how trust-related properties persist or change across state transitions. For example, policies can express not only current access rights but also conditions under which access may eventually be granted or revoked based on future events.

To illustrate the practical use of these operators, consider a healthcare scenario: a policy may state that a doctor's access to a patient's record is necessarily revoked after discharge, expressed as $\Box(\text{discharged} \rightarrow \neg\text{access})$. Conversely, an emergency protocol might allow access if a future emergency is declared, captured as $\Diamond\text{emergency} \rightarrow \text{access}$. These examples show how modal logic naturally captures temporal constraints that are essential for context-sensitive trust management [2, 20].

The dynamics of contextual information such as location changes, sensor readings, or operational statuses necessitate reasoning mechanisms capable of anticipating and managing state evolution. Static logical frameworks are insufficient in this regard, as they fail to account for the fluidity inherent in real-world environments. Modal logic, by contrast, inherently models transitions between states through accessibility relations, offering a mathematically sound approach for capturing potential futures and evaluating policy robustness under uncertainty [4].

In the instantiation of RT^R, modal logic enables the specification of policies that are sensitive to temporal progression and context change. Trust delegations, obligations, and permissions can be expressed as modal propositions, providing a structured means for encoding complex trust behaviors. Furthermore, the incorporation of modal reasoning facilitates meta-level inquiries, such as verifying whether certain access rights necessarily or possibly hold under all admissible evolutions of the system state.

By integrating modal logic with trust management frameworks, a pathway is established toward developing trust systems that are both adaptable to contextual volatility and formally verifiable. This integration strengthens the ability to enforce dynamic security policies, conduct formal proofs of correctness, and support automated reasoning about trust in decentralized and heterogeneous environments [15, 16].

6. Discussion

The integration of modal logic into trust management frameworks, such as RT^R, represents a significant step forward in addressing several critical challenges inherent in dynamic and distributed environments. Modal logic, by enabling formal reasoning over contextual state changes, facilitates the construction of trust systems that are not only resilient but also transparent, verifiable, and adaptive. This is especially important in environments where the context is constantly evolving, and decisions regarding access control must account for both past events and future possibilities [19, 20].

One major advantage of the modal logic approach is its ability to reason not only about current access control decisions but also about potential future scenarios. This forward-looking perspective allows for policies to be evaluated under various assumptions about the evolution of context, empowering system

designers to preemptively identify vulnerabilities, inconsistencies, or gaps in the trust model. Such foresight can lead to more robust and adaptable systems, as the potential effects of various environmental changes, such as the introduction of new security threats or changes in system conditions, can be anticipated and mitigated. This ability to model and reason about the future is particularly valuable in environments characterized by high volatility and uncertainty, such as mobile networks, Internet of Things (IoT) ecosystems, and emergency response infrastructures, where conditions can shift rapidly and unexpectedly [2, 8].

Furthermore, modal logic can be particularly effective in modeling complex multi-agent systems where various stakeholders, each with distinct roles and responsibilities, interact with one another under dynamically changing conditions. By reasoning about these interactions, the system can ensure that trust decisions are made in a way that is consistent with both current and potential future contexts. For instance, in a distributed health care system, modal logic can ensure that access to sensitive medical data is only granted when specific conditions such as a patient's consent or a doctor's on-call status are met, while also accounting for potential future states, such as the evolution of the patient's health condition [6].

However, despite these advantages, the adoption of modal reasoning in trust management systems introduces new challenges, primarily in terms of computational complexity and scalability. Modal logics, particularly those involving temporal operators, often lead to state space explosions when naively applied. This is due to the need to model and reason about an exponentially growing number of possible future states as the system evolves over time. Consequently, as the system scales and the number of agents and contextual factors increases, the complexity of the reasoning process can grow rapidly, potentially rendering the system computationally intractable for large-scale deployments [15, 17].

To address these challenges, efficient reasoning algorithms and practical optimization strategies are essential. Advances in algorithmic techniques, such as heuristics, approximation methods, and incremental reasoning, could help mitigate the computational overhead associated with modal logic-based reasoning. Additionally, the development of lightweight modal reasoning engines and context abstraction mechanisms represents a promising direction for overcoming scalability limitations. By abstracting and simplifying certain contextual elements, the system can focus on the most critical aspects of decision-making, thus improving performance without sacrificing the flexibility and expressiveness that modal logic provides.

Moreover, future work should explore hybrid models that combine the strengths of modal logic with other reasoning paradigms, such as probabilistic reasoning or machine learning techniques. Such hybrid approaches could enhance the system's robustness under uncertainty, particularly in environments where the available information is incomplete or noisy. By integrating probabilistic models, for example, the system could better handle cases where context is uncertain or imprecise, while still maintaining formal verifiability through the modal logic foundation. This would enable the development of more sophisticated trust management systems capable of adapting to a wide range of uncertain, dynamic, and distributed environments [12–14].

Furthermore, the extension of RT^R through modal logic paves the way for a new generation of trust management systems that are not only capable of meeting the demands of highly dynamic environments but also of providing formal guarantees regarding the evolution and enforcement of trust relationships. These guarantees are crucial for ensuring the security, privacy, and integrity of distributed systems, especially in applications where trust is paramount, such as financial systems, healthcare, and critical infrastructure. By leveraging the power of modal logic, RT^R can offer a more comprehensive framework for modeling trust that accounts for both static and dynamic factors, ensuring that access control decisions are not only based on current conditions but also consider potential future scenarios and uncertainties [3, 4].

The ability to reason about time, possibility, and necessity also opens up new opportunities for advanced applications of trust management systems in areas such as multi-party negotiations, dynamic access control in cloud computing, and automated compliance monitoring. These areas often involve complex, evolving interactions between multiple entities with varying levels of authority and access requirements. Modal logic provides a flexible and expressive tool for capturing these interactions and ensuring that decisions regarding trust, access, and authorization remain consistent with both current and anticipated conditions.

In conclusion, while the modal logic extension of RT^R offers significant promise for enhancing trust management in dynamic environments, further research is required to address its challenges in computational complexity and scalability. The development of efficient reasoning mechanisms, hybrid models, and lightweight engines will be critical for making this framework viable for large-scale, real-world applications. As these challenges are addressed, the potential of modal logic to transform trust management systems will become increasingly evident, making it a key enabler of the next generation of secure, adaptive, and transparent distributed systems.

Table 1: Comparison of Trust Management Approaches

Approach	**Strengths**	**Limitations**
Credential-Based Systems	Simplicity, widespread adoption	Poor adaptability to context changes
Reputation-Based Models	Dynamic trust adjustment based on history	Lack of formal guarantees and explainability
Logic-Based Frameworks (Static)	Formal specification and verification capabilities	Inflexibility under dynamic contexts
Modal Logic-Based RT^R	Context-aware reasoning, temporal adaptability, formal proofs	Computational complexity, scalability challenges

Future work should also investigate hybrid models that combine probabilistic reasoning with modal logic to enhance robustness under uncertainty while maintaining formal verifiability [12, 13]. By enabling deeper insights into the evolution and enforcement of trust relationships, the modal logic extension of RT^R establishes a foundation for next-generation trust management systems capable of meeting the demands of highly dynamic and decentralized environments.

7. Conclusion and Future Work

This work presents a formal framework for trust management in distributed systems by integrating modal logic into the role-based trust management paradigm RT^R. By modeling trust relationships through modal operators, the proposed system captures the dynamic, context-sensitive nature of trust and facilitates rigorous reasoning about trust propagation, delegation, and revocation across evolving states [9–11].

The use of modal logic enables the explicit specification of contextual changes and future state transitions, strengthening the verifiability, adaptability, and transparency of authorization policies. Compared to traditional credential-based and reputation-based models, the RT^R framework offers

significant advantages in expressiveness and formal assurance, supporting advanced trust scenarios in decentralized and dynamic environments [1].

7.1 Limitations

Despite the conceptual strengths, certain limitations of the proposed framework must be acknowledged:

- **Computational Complexity:** Modal reasoning, especially with temporal operators, can lead to exponential growth in state space, posing challenges for scalability [15, 17].
- **Idealized Assumptions:** The current model assumes perfect synchronization of contextual inputs and reliable communication among distributed agents, which may not hold in adversarial or fault-prone environments [4].
- **Absence of Probabilistic Reasoning:** Trust evaluations in highly uncertain environments often require probabilistic or fuzzy extensions, which are not currently integrated into the framework [12–14].
- **Limited Contextual Scope:** The present instantiation focuses solely on temporal contexts, excluding spatial, behavioral, or organizational factors that could enrich trust evaluations.

Recognizing these limitations is essential for guiding the evolution of the framework toward broader applicability and robustness.

7.2 Future Work

Several promising research directions emerge from this foundation:

- **Scalability Enhancements:** Development of optimized algorithms for modal reasoning, leveraging context abstraction and symbolic model checking techniques [16].
- **Probabilistic Extensions:** Integration of probabilistic and fuzzy logic elements into the RT^R framework to better model trust under uncertainty and incomplete information [12].
- **Multi-Context Reasoning:** Extension of the modal logic framework to accommodate diverse contextual inputs beyond temporal factors, such as location, device health, or organizational state.
- **Prototype Implementation:** Construction of a prototype trust management system based on RT^R to evaluate performance, scalability, and practical applicability in real-world distributed environments [18].
- **Empirical Validation:** Deployment and testing in case studies such as peer-to-peer networks, blockchain-based infrastructures, and federated identity systems to empirically assess effectiveness and guide iterative refinement [3, 5].

By advancing along these directions, modal logic-based trust management frameworks can be established as a core technology for building secure, explainable, and adaptive systems in future decentralized environments.

References

[1] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In *Proceedings 1996 IEEE Symposium on Security and Privacy*, pages 164–173. IEEE, 1996.

[2] T. Sylla, L. Mendiboure, M. A. Chalouf, and F. Krief. Blockchain-based context-aware authorization management as a service in iot. *Sensors*, 21(22):7656, 2021.

[3] Matt Blaze, Joan Feigenbaum, and Angelos D Keromytis. The role of trust management in distributed systems security. In *Secure internet programming*, pages 185–210. Springer, 1999.

[4] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems (TOCS)*, 8(1):18–36, 1990.

[5] John DeTreville. Binder, a logic-based security language. In *Proceedings 2002 IEEE Symposium on Security and Privacy*, pages 105–113. IEEE, 2002.

[6] Moritz Y Becker, Cedric Fournet, and Andrew D Gordon. Secpal: Design and semantics of a decentralized authorization language. In *Proceedings of the 2006 IEEE Computer Security Foundations Workshop*, pages 3–15. IEEE, 2006.

[7] Ronald Fagin, Joseph Y Halpern, Yoram Moses, and Moshe Y Vardi. *Reasoning about knowledge*. MIT press, 2004.

[8] S. Xiong, A. Payani, R. Kompella, and F. Fekri. Large language models can learn temporal reasoning. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 10452–10470, August 2024.

[9] Z. Chu, J. Chen, Q. Chen, W. Yu, H. Wang, M. Liu, and B. Qin. Timebench: A comprehensive evaluation of temporal reasoning abilities in large language models. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 1204–1228, August 2024.

[10] F. Berto. *Topics of thought: The logic of knowledge, belief, imagination*. Oxford University Press, 2022.

[11] A. Giannakidou and A. Mari. *Truth and veridicality in grammar and thought: Mood, modality, and propositional attitudes*. University of Chicago Press, 2021.

[12] Sepandar D Kamvar, Markus T Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. *Proceedings of the 12th International Conference on World Wide Web*, pages 640–651, 2003.

[13] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):843–857, 2004.

[14] Rui Zhou and Kai Hwang. Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Transactions on Parallel and Distributed Systems*, 18(4):460–473, 2007.

[15] Leslie Lamport. *Specifying systems: The TLA+ language and tools for hardware and software engineers*. Addison-Wesley, 2002.

[16] Daniel Jackson. *Software abstractions: logic, language, and analysis*. MIT press, 2012.

[17] Gerard J Holzmann. The model checker spin. *IEEE Transactions on Software Engineering*, 23(5): 279–295, 1997.

[18] Ninghui Li, John C Mitchell, and William H Winsborough. Design of a role-based trust-management framework. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 114–130. IEEE, 2003.

[19] M. Sahyudi and E. R. Susanto. Analisis implementasi sistem keamanan basis data berbasis role-based access control (rbac) pada aplikasi enterprise resource planning. *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, 5(1):105–116, 2025.

[20] Y. A. Marquis. From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts. *Journal of Engineering Research and Reports*, 26(5):138–154, 2024.