Research Article

Received: 20 February, 2026
Accepted: 26 May, 2026
Published: 08 June, 2026

Architecting Trust: A Blockchain-Based Governance Framework for Secure Cross-Institution Data Sharing

Asim Seedahmed Ali Osman
Department of Software Enginering College of Computer Science & Engineering University of Hafr Al Batin, Saudi Arabia aalageed@uhb.edu.sa

Cite this article:

Osman, A. S. A. (2026). Architecting Trust: A Blockchain-Based Governance Framework for Secure Cross-Institution Data Sharing. *Cultura Científica*, (24), pp. 517–529.

Abstract

Transition from closed information storage systems to an open and collaborative system of cross-organizational data sharing and integration faces a core trilemma in terms of creating "Trust-Privacy-Efficiency balance". Enterprises face a dichotomy when deciding whether to adopt a centralized intermediary solution involving potential agency problems, or implement fragmented bilateral integration, which is neither scalable nor safe from data breaches. Although blockchain technology provides a decentralized way of establishing trust, early attempts to combine blockchains with GDPR-like privacy laws were unsuccessful because of inability to address data immutability and complex organizational governance. To tackle the challenge of constructing data sharing ecosystem within legal and practical constraints, we theorize a novel approach called "Trust-Architected Hybrid Governance Model" (TA-HGM). Our model builds on the foundation of Socio-Technical Systems (STS) Theory and the principles of Design Science Research (DSR). In order to create a trust-architecture-based model, we utilize the idea of hybridization of on-chain and off-chain enforcement of algorithmic trust and propose multi-layer architecture implementing the concept of Light Processing/Heavy Storage (LPHS-XV) combined with Attribute-Based Access Control (ABAC) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in order to enforce policy-based access control. We demonstrate the viability of TA-HGM in terms of collusion and Sybil protection and illustrate its applicability in case of crypto-shredding and regulatory compliance. Thus, the contribution of our research lies in theoretical development and design science application in information systems.

Keywords: Blockchain Governance, Socio-Technical Systems, Attribute-Based Encryption (CP-ABE), Inter-Organizational Information Systems, Data Sovereignty

1. INTRODUCTION

Digitization has led to the emergence of a completely new paradigm for managing and leveraging information within organizational networks. We have shifted from an era of scarcity, during which competitive advantage stemmed from withholding proprietary information, to an era of abundance, in which competitive advantage is increasingly associated with the collective synthesis of heterogeneous datasets [1, 2]. The examples include precision medicine, where algorithms must access patient records from different hospitals, and intelligent transportation systems, where data needs to be exchanged between autonomous vehicles and local authorities in real time to optimize routing [1, 2]. Moreover, multi-tier supply chains today require end-to-end visibility to guarantee the provenance of products and assure ethical sourcing, thus necessitating transparency levels that cannot be achieved using legacy siloed technologies [3, 4].

Despite this imperative for data collaboration, modern socio-technical architectures remain fragmented, opaque, and reliant on trusted parties to broker transactions. Inter-Organizational Information Systems (IOIS) today generally offer two options, neither of which is sustainable: on one hand, we need to use a trusted third party (such as Facebook Graph API), which introduces multiple points of failure and makes the whole process inefficient due to high agency costs. On the other hand, we might consider developing an architecture of bilateral connections between all involved actors and data owners, which is highly complex and risky due to numerous points of data breach [5]. The notion of agency cost refers to economic inefficiencies (monitoring expenditures, transaction fees, censorship risks) associated with entrusting management of certain processes to another party [5]. This reliance on intermediaries creates a substantial "trust gap" forcing institutions to surrender control over their assets to access the digital market [6]. As a result, institutions build their own data silos, thus making systemic optimization, transparency, and innovation impossible.

Regulatory landscape has changed as well, creating strict liability for data misuse [4]. GDPR and HIPAA, for instance, impose severe penalties for mishandling user data, thus leading to a privacy paradox in which businesses are encouraged to limit access to their data precisely when innovations require such access [7]. Privacy requirements have become a major source of deadlock preventing many companies from realizing the benefits of big data analytics and interoperable platforms [8].

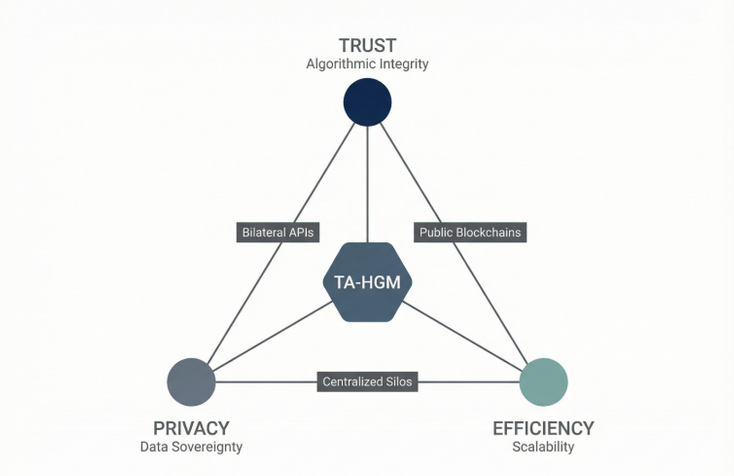

Figure 1. *The Trust-Privacy-Efficiency Trilemma. The diagram positions the Trust-Architected Hybrid Governance Model (TA-HGM) as the central solution balancing the decentralization of blockchain, the data sovereignty required by privacy regulations, and the scalability demanded by enterprise efficiency*

Blockchain and distributed ledger technology seem to provide a solution for this trust-privacy-efficiency trilemma by moving trust from organizations to algorithms and creating transparent, secure data environments, which guarantee availability, integrity, traceability, and auditability of the information they process [9, 10]. Conceptual tension behind this study is depicted in the Figure 1 in which we place the proposed Trust-Architected Hybrid Governance Model as a way to balance decentralized trust, privacy regulation's sovereignty, and enterprise efficiency. The introduction of blockchain into business governance, however, has become a sociotechnical disruption rather than an easy technological improvement. Attempts to apply blockchain have frequently failed due to lack of attention paid to the socio-technical aspect of the process [11, 12].

Thus, the main goal of this research report is to propose a comprehensive socio-technical framework for Trust-Architected Hybrid Governance Model. Our hypothesis is that such a model should leverage hybrid governance by combining on-chain enforcement of algorithms and rules with off-chain data sovereignty. Based on principles of Design Science Research and Socio-Technical Systems theory, we design and implement a system that guarantees privacy via

Attribute-Based Access Control and Ciphertext-Policy Attribute-Based Encryption, while addressing problems of scalability, interoperability, and compliance through a multi-layered architecture [13]. In this paper, we provide a systematic review of the development of this framework, theoretical foundation, system architecture, and security implications.

2. LITERATURE REVIEW

2.1. FROM ELECTRONIC DATA INTERCHANGE TO DECENTRALIZED DATA SPACES

The necessity of blockchain-based data sharing requires analysis of this phenomenon from the perspective of the historical development of Inter-Organizational Information Systems (IOIS). The earliest form of electronic business to business communication can be traced back to Electronic Data Interchange (EDI) of the 1960s [11]. EDI helped automate the exchange of business transactions, such as orders and invoices, by replacing paper-based trails with structured digital documents [11]. The technology remained the foundation of supply chain digitization for several decades, allowing organizations to automatically transfer documents between each other's computer systems without any human interaction [11]. The system had inherent limitations. It was rigid and based on proprietary Value-Added Network (VAN), which served as a digital post office and required strict bilateral agreements and high fees. EDI helped reduce the number of errors, speed up processing, and avoid human errors, yet it could not create a shared state. In an EDI system, each participant would maintain its own database and constantly perform reconciliation due to potential differences in transaction records caused by transmission errors, processing time, and other factors [3].

Blockchain technology, by contrast, represents a discontinuous step in IOIS evolution, as it allows transferring value rather than just exchanging information and maintaining a shared state. Modern descriptions interpret this change as decentralization of information interchange. Unlike EDI systems, blockchain records structured messages in a decentralized and cryptographically protected ledger [14]. With this approach, there is a single source of truth for all participants of a blockchain network. In a blockchain-enabled supply chain, for instance, all participants view the same immutable ledger, making reconciliation unnecessary since the ledger performs this task itself. In addition to being based on a consensus algorithm, rather than a proprietary and expensive VAN service, blockchain supports peer-to-peer interaction that is flexible, encrypted, verifiable, and auditable [15, 16]. This makes blockchain a key building block of the Trustworthy Data Space, where data sovereignty and interoperability are achieved without intermediaries [9].

2.2. PRIVACY-PRESERVING ACCESS CONTROL IN DISTRIBUTED LEDGER ENVIRONMENTS

Although blockchain solves many problems that existed in earlier systems, such as EDI, it poses another challenge by bringing together transparency and privacy concerns. As mentioned above, public blockchains are fully transparent, which means that all transactions are accessible to all nodes in the network. Enterprise-level applications require greater privacy as some data should not be published in a public ledger, such as PHRs in healthcare and proprietary manufacturing schematics in the automotive industry [1, 17]. Several recent systematic reviews identified significant gaps in the field. For instance, although techniques, like Zero-Knowledge Proof (ZKP) and homomorphic encryption, can be considered theoretically sound and applicable in real-life scenarios, they do not mature enough to ensure privacy in practice [1].

One of the key problems of blockchain in enterprises is the lack of tools that allow fine-grained access control. According to recent studies, the answer to this problem might be found in Attribute-Based Encryption (ABE) or even more precisely in Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [13]. In CP-ABE, access policies dictate which attributes users should possess before they gain decryption ability. One possible example can be requiring a user to belong to certain groups, such as "Doctor" and "Hospital A" to decrypt the information. This solution makes it possible to encrypt data and put them in an untrusted environment without worrying about unauthorized access. According to Song and Li [18], coupling CP-ABE with blockchain helps achieve decentralized fine-grained access control, where blockchain is responsible for trusted attribute validation and auditing, whereas the complex cryptographic operations take place off-chain. It should be emphasized that this combination makes it possible to prevent collusion attacks, during which malicious users try to collaborate with others to access information that they are not supposed to access [18]. Finally, the newest advances involve optimization of CP-ABE for the IoT [19].

2.3. CONSORTIUM GOVERNANCE, INTEROPERABILITY, AND SECURITY GAPS

As seen above, despite significant achievements in terms of cryptography and computing, the area of blockchain research still lacks important insights into its governance and interoperability aspects. Whereas a lot of scientific efforts are dedicated to the study of various consensus algorithms, off-chain mechanisms of governance are still understudied [6]. Blockchain governance can be viewed as a system of systemic trust, but purely decentralized governance models are known to suffer from lack of recognition, responsibility, and enforceability. Thus, in permissioned blockchain consortia,

the most pressing issue is coordination of various stakeholders with conflicting interests and bargaining power [20]. The lack of solutions to the social coordination problem results in the fact that although blockchain solutions are technologically mature and efficient, they become socially abandoned [6].

To address the above-discussed challenges, socio-technical approach should be applied, according to the latest findings. That is, social properties of blockchain systems, such as immutability and transparency, should map onto social values, such as accountability and trust [6]. Another problem involves growing security concerns with regard to interoperability of blockchain. Sengupta et al. [21] argue that cross-chain bridges pose serious risks as they lack robust proof against, for instance, Sybil or Man-in-the-Middle attacks [22, 23]. The issue becomes particularly urgent in the context of interoperability protocols that currently lack a unified governance framework [21]. "'

3. THEORETICAL FRAMEWORK

In order to fill the mentioned gaps, the current research is based on the theory called *Socio-Technical Systems (STS)*. This term was introduced by Tavistock Institute scholars who claim that organizational systems include two intertwined subsystems: the first one represents technology and processes, whereas the second one is connected with people, culture, and law. The key principle of the sociotechnical approach is joint optimization, which means that an organizational system would collapse if one subsystem dominates another [6]. It is especially important for studies concerning the development of blockchain technologies since STS requires moving the focus from code to a more complicated interaction of human action and algorithm enforcement. The role of each component in our proposed framework based on STS theory is presented in Table 1.

Table 1. *Alignment of Socio-Technical Systems Theory with Blockchain Components*

STS Component	Description	Proposed Framework Implementation
Social Subsystem	The human, legal, and institutional layer governing behavior and norms.	*Consortium Agreements:* Legal frameworks defining roles. *GDPR Compliance:* Rules for Right to Erasure. *Attribute Authorities:* Institutions (e.g., Hospitals) verifying identities.
Technical Subsystem	The tools, infrastructure, and algorithms enabling operations.	*Smart Contracts:* Automated policy enforcement. *CP-ABE:* Cryptographic privacy enforcement. *IPFS:* Decentralized, content-addressed storage.
Joint Optimization	The alignment mechanism ensuring mutual reinforcement of subsystems.	*The "Chain of Trust":* A feedback loop where social legalities are encoded into technical smart contracts, and technical audit logs reinforce social accountability.

3.1. THE TECHNICAL SUBSYSTEM: ALGORITHMIC TRUST

Within our conceptualization of the system, the technical subsystem includes blockchain protocols, smart contracts, crypto primitives such as CP-ABE and Zero-Knowledge Proofs, and decentralized storage solutions. This subsystem supplies the notion of "algorithmic trust". Algorithmic trust is deterministic in the sense that it is derived from the absolute mathematical truth that the code runs as it should [6]. Immutability guarantees that the history of all the data accesses is unchangeable, making it impossible to engage in gaslighting or any attempts to tamper with records retrospectively. Automation due to smart contracts solves the issue of delays and agent-based costs associated with manual processing of transactions [9]. Finally, decentralization eliminates single points of failure and central authority, consistent with the trustless principle where users don't need to trust each other to engage in transaction. Thus, the technical subsystem can be seen as an impartial, objective enforcer of rules predetermined by the social subsystem.

3.2. THE SOCIAL SUBSYSTEM: INSTITUTIONAL TRUST

The social subsystem includes consortium members, legal agreements, regulation (GDPR/hippa), and off-chain governance bodies. In this subsystem, there's another type of trust which is called "institutional trust". Unlike algorithmic trust, it is probabilistic and relational, emerging from reputation, law and social norms [6]. While public key infrastructure is used within blockchain technology, the social layer binds these keys to the real-world identities using decentralized identifiers (DIDs). Compliance is crucial in the social layer since social requirements that technical systems are hard to deal with arise from time to time (e.g., Right to Erasure). Therefore, there needs to be a mechanism that would reconcile these two opposing concepts [7]. Apart from that, conflict management in case some of the codes face unexpected situations and edge cases is a crucial part of the social layer as it enables greater flexibility. Without the social layer, the system would become brittle and unmanageable in face of changing market and legal realities.

3.3. THE CHAIN OF TRUST MODEL

It is proposed that the successful governance of blockchain leads to creation of a "Chain of Trust" linking the two aforementioned subsystems. The chain begins with establishment of institutional trust in the social layer through forming of a consortium agreement. Then, it is programmed in the technical layer with a genesis block and smart contract rules. Afterward, the execution of transaction takes place in the technical layer, supplying algorithmic trust. Finally, it is audited by the social layer in order to reinforce the original institutional trust [6]. This cyclical approach makes sure that code is subservient to law at the same time delivering its efficiencies. Should the system fail to abide by social norms, social governance has to have a way to update or deprecate it. Consequently, this approach is aimed at creating socio-technical synergy to address the governance issues discussed above.

4. RESEARCH DESIGN AND METHODOLOGY

As the methodological approach in this research, we use the approach referred to as *Design Science Research (DSR)*. As the problem solving paradigm, DSR focuses on developing and enhancing the body of knowledge about how to make innovative things happen. Being applied to the information systems research field, this methodology serves to change the world rather than to simply describe it [11].

4.1. METHODOLOGICAL PARADIGM: DESIGN SCIENCE RESEARCH (DSR)

Within the widely accepted process model of DSR research, we proceed through four distinct steps. Firstly, we identify a problem as a lack of secure, privacy-respecting, and regulation-compliant framework for data sharing across institutions with adequate trade-off between transparency and privacy [9]. Next, we define meta-requirements of the problem in the form of the social-technical system concept along with the research gaps revealed during the literature review. The latter phase is dedicated to defining concrete engineering requirements out of the theoretical abstractions. Thirdly, we carry out an act of creativity and create the actual artifact, in particular "Architecting Trust", comprising system architecture and governance model. Finally, we conduct analytical demonstration and evaluation of the said artifact.

4.2. META-REQUIREMENTS AND DESIGN OBJECTIVES

To make sure that our solution satisfies all requirements and resolves the problem of the trilemma, we outline four Meta-Requirements:

MR1: Decentralized & Fine-Grained Access Control requires the ability to configure access rights on the level of boolean formulae over attributes, enforced independently of central servers via ABE and blockchain smart contracts [13]. Standard Role-Based Access Control (RBAC) is unsuitable in dynamic multi-institutional environment, where roles are not well-established.

MR2: Data Minimization & Privacy Preservation imposes strict restrictions on the kind of data being stored on the blockchain. Only metadata, access policies, and cryptographic proofs shall be written onto the ledger, whereas an off-chain deep storage facility must be designed to support the actual payloads [9]. This meta-restriction directly stems from the tension between visibility and availability on the blockchain.

MR3: Regulatory Compliance (Right to Erasure) requires the possibility of erasing personal data in accordance with GDPR Article 17. Despite immutability of the blockchain data, this objective implies a mandatory crypto-shredding approach that destroys all decryption keys and therefore renders data unreadable forever [7]. This feature is essential for any GDPR-compliant system.

MR4: Interoperability & Sybil Resistance requires that the system operates seamlessly across heterogeneous institutional domains and is resilient against sybil attacks involving many false identities. In turn, it implies a powerful Identity Management layer, based on Decentralized Identifiers (DIDs) and verifiable credentials [21] that does not rely on a centralized global registry of identities.

5. SYSTEM ARCHITECTURE AND DESIGN

For the solution described above, the most appropriate architecture is the Hybrid Model architecture, using the LPHS-XV Mechanism (Light On-chain Attest, Deep Off-chain Store, Cross-layer Verifiable Bridge).

5.1. HIGH-LEVEL ARCHITECTURAL TOPOLOGY

Our architecture is organized in layers, allowing to properly manage the flows of data, permissions, and trust. The High-Level Architectural Topology (see Fig. 2) contains four layers:

First layer (User/Device Layer) is comprised of various devices, including IoT sensor nodes, hospital terminals, and

user interfaces. This layer is responsible for generating the data, performing local encryption, and communicating with the blockchain network. The primary component in the user/device layer is the Client Application, which maintains the users' private keys. Before uploading data, this layer performs encryption using the client-side symmetric key, which gets wrapped up in CP-ABE ciphertexts [13]. The architecture of this layer allows us to apply the privacy by design principle [19].

Off-Chain Storage Layer represents a deep storage facility storing the actual encrypted payload data. This layer could potentially employ IPFS or any other decentralized storage protocol, as well as a privately-owned cloud storage silo if data belong to regulated institutions. Since all the data are uploaded in their encrypted form, the storage provider is unable to access them, thus preserving users' privacy regardless of whether it's a public or semi-private network. By separating deep storage from the blockchain ledger, we prevent the latter from uncontrolled increase in size and thus provide a means to deal with large-scale payloads such as radiologic images or logistic transactions, that would otherwise grow the ledger beyond acceptable limits. Using off-chain storage prevents us from paying exorbitant costs of on-chain data storage [9].

Blockchain Layer represents the trust anchor of the whole architecture and acts as its control plane. It does not hold the data; it holds the state of these data: access permissions, policy definitions, audit log records. Smart Contracts contained in blockchain include: Registry Contract - for keeping track of data identifiers and corresponding locations in storage; Policy Contract - for keeping the CP-ABE ciphertext containing access policy information; Audit Contract - for logging each request, grant, or revocation event. Permissioned Consensus algorithm, such as ordering services of Hyperledger Fabric platform, is used to ensure deterministic transaction results [24]. It can be interpreted as an authority governing the digital world without having any data asset in hand.

As a supplementary option, there is a Computational Layer designed to perform computations on the data without disclosing the data. It uses Trust Execution Environment technology (TEE) or Zero-Knowledge Proofs (ZKPs) with subsequent verification by the blockchain. This layer allows implementing advanced use-cases such as Federated Learning, where models can be trained on the local data without moving the files from their place [25].

5.2. MULTI-LAYERED TECHNICAL SPECIFICATION

These different layers communicate through certain protocols to facilitate security and efficiency. On the on-chain layer, the ring of nodes denotes the validator nodes, which represent the consortium blockchain. Inside the ring, smart contracts are used to facilitate the logical processing of ABAC, identity registries, and audit logging. The off-chain layer is presented as a distributed collection of databases and IPFS nodes. Information travels from the source into the off-chain database as encrypted payloads, while metadata and hash values make their way into the on-chain validators' databases. Such separation leads to a "Light Attest/Deep Store" mechanism where the lightweight blockchain only verifies information, while its heavy counterpart performs the storage functions [26].

There is a need for a cross-chain bridge to link this architecture with other clouds or even with another blockchain, facilitated by relay nodes. Such an approach is required for realizing the concept of "network of networks," enabling interactions between different data spaces, e.g., a healthcare consortium blockchain interacting with an insurance consortium blockchain. However, there is the issue of bridge vulnerability, which must be addressed through using a relay node setup, where a change of state must be validated by multiple signatures before it reaches other chains. In such a manner, a cross-chain bridge will enable the realization of state verification in one chain and relay of this state onto another chain. For instance, there could be an insurance chain that triggers payments based on an event occurring in a hospital chain [23].

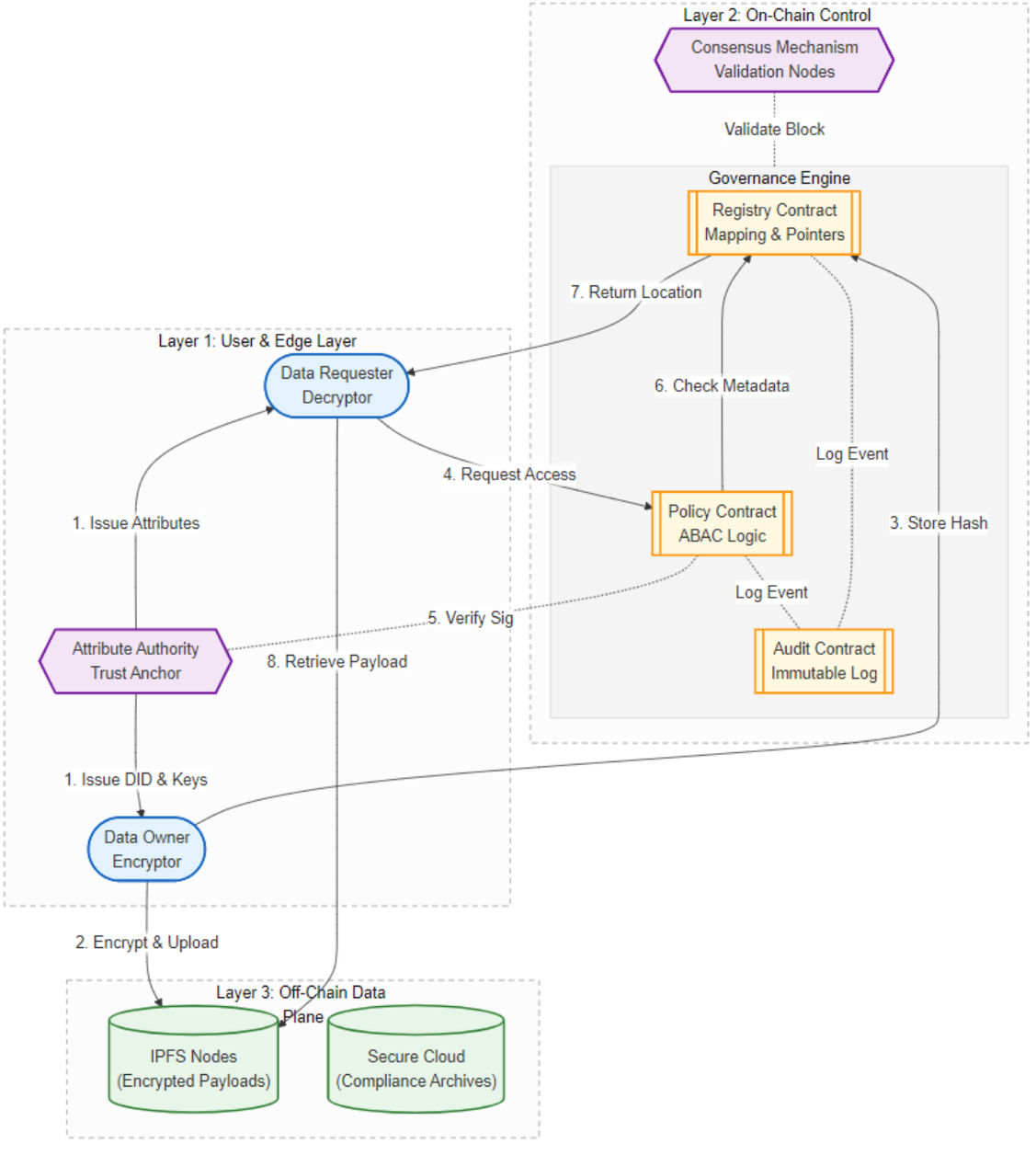

Figure 2. *The TA-HGM system architecture. The schematic illustrates the three-tier design: Layer 3 handles the high-volume storage of encrypted payloads through the Deep Store, Layer 2 executes lightweight governance logic through the Smart Contract Cluster or Light Attest Layer, and Layer 1 manages user identity, device interaction, and key generation.*

6. GOVERNANCE MODEL AND ACCESS CONTROL LOGIC

The governance model prescribes the rules of engagement in the system. The *Hybrid Governance* framework is employed, wherein Consortium Governance governs the human/ legal decisions and Attribute-Based Access Control (ABAC) governs technical decisions [6].

6.1. REQUEST PROTOCOLS BASED ON SMART CONTRACTS

It is often difficult to employ a classic Role-Based Access Control (RBAC) mechanism in case of dynamic and multi-institutional sharing because of potential differences in the definition of roles between institutions. For example, the role of "Nurse" in one hospital may differ significantly from the same one in another facility. Thus, an ABAC scheme is used wherein access decisions depend on certain user attributes like "Department," "Clearance Level," or "Certification." The system employs several Attribute Authorities (AAs) acting as the trusted entities of the consortium. They verify identities of the users and issue attributes. In order to mitigate a single point of failure, Multi-Authority CP-ABE scheme is employed

where no single AA owns the master key [13].

Governing policies of ABAC are policy-driven: the data owner doesn't give access rights to any specific individual but defines some policies instead. For example, it could be a policy allowing all users having both "Department: Oncology" and "Clearance Level: 3" attributes to access the requested data. The system will provide access to any individual capable of proving that he/she possesses the mentioned attributes. The main benefit of policy-based control is the possibility to introduce scalability: once a new member of the department gets hired, he/she just receives the corresponding attribute from his/her AA, and the data owner doesn't need to update any access permissions and lists. Thus, the dynamic permission determination is the core feature of ABAC [18].

6.2. WORKFLOW AND PERMISSION LIFECYCLE

The lifecycle of data sharing includes a number of steps to ensure secure interaction between the parties involved. Firstly, in the stage of *System Initialization*, global parameters are defined on-chain, and AAs get registered as part of a governance decision [27]. Next step is *User Registration*: here, a Data Requester contacts an AA through Decentralized Identifiers (DIDs) authentication procedure to receive his/her attribute key, after which the latter is registered on-chain [13].

If a data owner wants to distribute his/her data among other members of the consortium, first of all, he creates a symmetric key and encodes the data with it. Then, the user defines the policy and encrypts the symmetric key using a CP-ABE method with this policy. The encrypted data is stored off-chain, whereas the metadata, consisting of the encrypted key and policy hash, is stored inside the blockchain smart contract. As a result, the access to the data is protected by the policy, which travels with the data [18].

To access the data, the requester sends the request to the data owner via the blockchain smart contract which works as the Policy Decision Point to verify if his/her attributes satisfy the policy stored in the metadata. Once verified, the requester decrypts the encrypted symmetric key and uses the received key to access the data. All these actions leave an immutable footprint recorded in the Audit Contract [9].

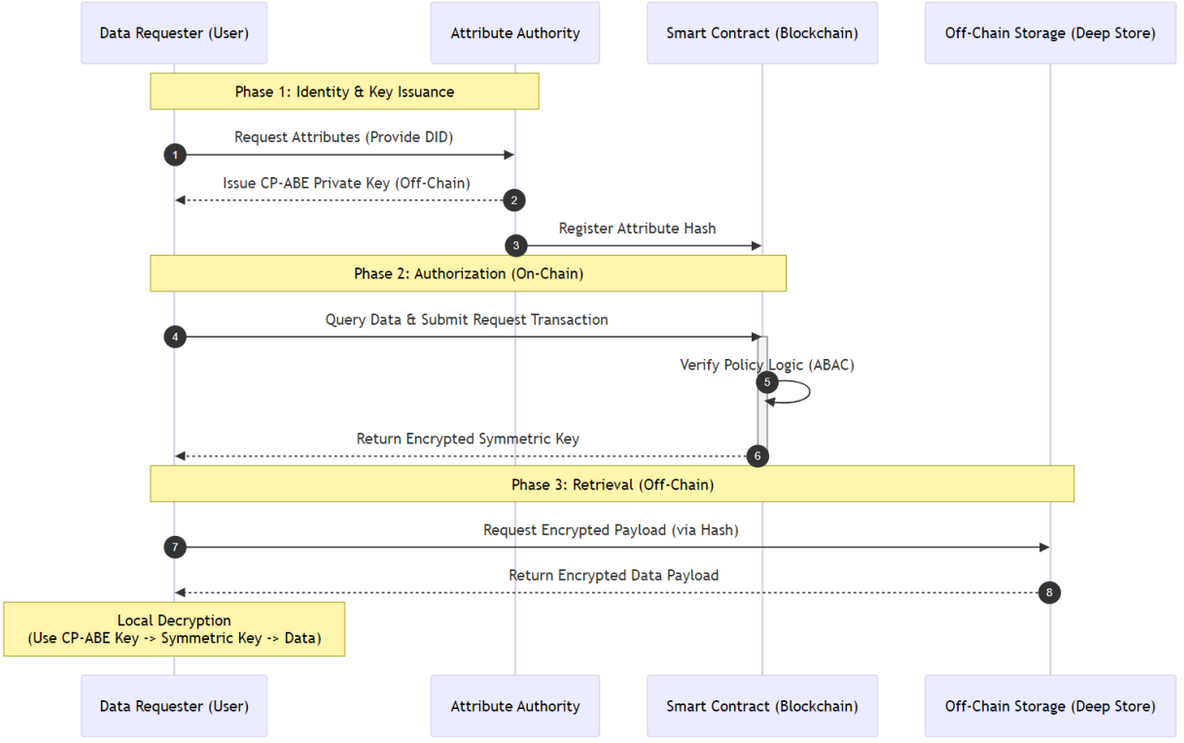

Figure 3. *Sequence Diagram of the Attribute-Based Access Control (ABAC) Workflow. The process flow details the interaction between the Data Requester, Attribute Authority, and Smart Contract, highlighting the three distinct phases of identity verification, policy enforcement, and off-chain retrieval.*

7. SECURITY ANALYSIS AND COMPLIANCE VERIFICATION

The security of the proposed framework is evaluated against identified threats and the established meta-requirements to ensure robustness and reliability.

7.1. THREAT MODELING AND MITIGATION

As mentioned above, the cornerstone of the proposed framework is the CP-ABE scheme. Recent advances have proved CP-ABE to be secure under the chosen plaintext attack assumption (*CPA*). This guarantees the impossibility of deriving the decryption key given the plaintext-ciphertext pair even for an adversary with knowledge of the encryption scheme used [13]. As a result, even if both the blockchain and IPFS layers are fully transparent, there is no risk of compromising sensitive data due to the inherent mathematical difficulty of cryptography.

A *collusion attack* occurs when several users try to merge their keys to unlock data with a set of attributes not possessed by any individual. In our system, for example, User A has "Doctor" and User B has "Hospital X" and they try to combine keys to access data containing "Doctor AND Hospital X". The key to thwarting such attempts lies in *Key Randomization*. According to our decryption algorithm, a successful key generation should possess collition-resistance properties: for keys to work together, all disparate key parts should contain the same unique Global Identifier. This ensures the mathematical impossibility of combining attributes across different identities [18]. Finally, *Sybil attacks*, where one malicious agent creates numerous dummy identities to circumvent access control, is countered by the need for *Identity Vetting* using DIDs. Participating in a blockchain network requires possession of credentials issued by a trusted consortium member, thus making the creation of dummy identities impossible [21].

7.2. PRIVACY PRESERVATION AND REGULATORY COMPLIANCE

One of the biggest issues impeding the widespread adoption of the blockchain technology is the right to erasure imposed by GDPR (Right to be Forgotten). As the blocks are immutable, once the data is stored there is no way to remove it except by creating a new forked blockchain. To tackle this problem, we employ *Crypto-Shredding*. Under this method, data is encrypted with a unique symmetric key prior to storage. To erase data, said key or CP-ABE blob decryption keys can be revoked. Afterward, the off-chain stored encrypted data is no longer distinguishable from the random noise and, therefore, is considered effectively erased [7, 1]. This solution addresses the problem posed by the inherent immutability of the blockchain and makes our framework compatible with relevant regulatory provisions.

7.3. COMPARISON TO TRADITIONAL SYSTEMS

In terms of functionality, our system represents a "chain of trust" approach. Starting from a consensus among institutions regarding the protocol rules, followed by implementing it at the technical level via a smart contract, executing algorithms, and auditing the process through an immutable record. This feedback loop allows reinforcing institutional trust, since, after all, the social layer is able to verify how the algorithms were executed and revoke identities if the bad actor was detected [6]. Moreover, unlike purely centralized or bilateral systems (API connections), our approach provides better protection against failure and censorship while overcoming the privacy issues associated with the latter [28, 10]. What is more, compared to a conventional bilateral API connection, the blockchain allows us to implement scalable architecture (logarithmic instead of linear), since the connection between members is only established once [10].

7.4. PERFORMANCE EVALUATION

To assess the performance impact of our proposed cryptographic module, we conducted simulations of the computational cost of performing CP-ABE encryption/decryption operations. As seen in Figure 4, the execution time is linear with respect to policy complexity measured by the number of attributes. For example, the encryption operation takes about 600ms for a policy of 40 attributes.

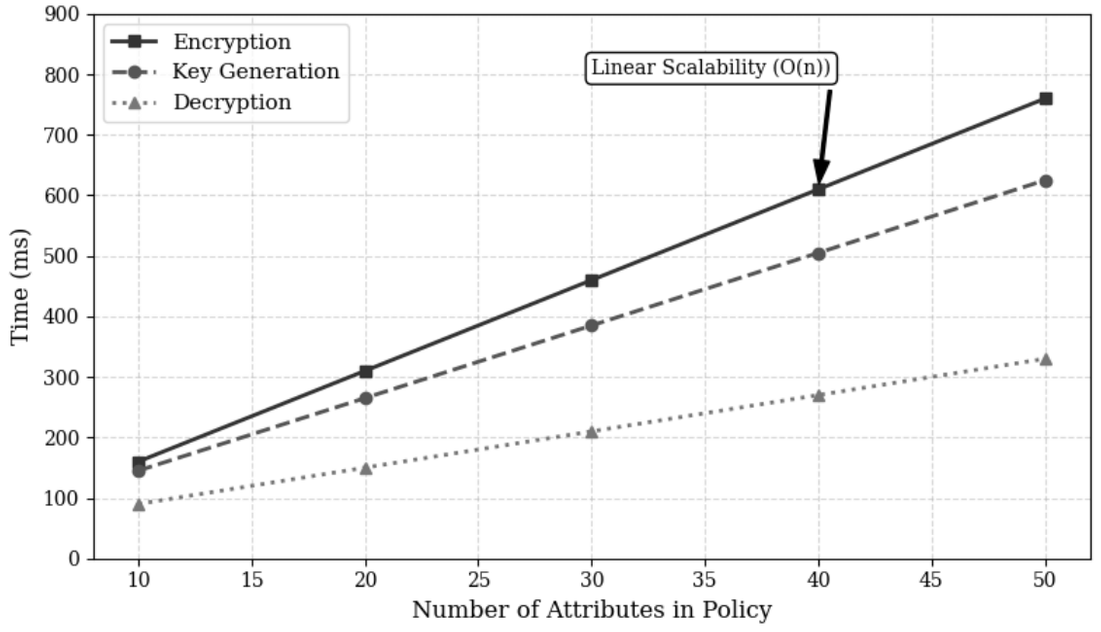

Figure 4. *Computational Cost of Cryptographic Operations. The graph illustrates the execution time (in milliseconds) for Encryption, Decryption, and Key Generation as a function of the number of attributes. The linear scalability ($O(n)$) confirms the framework's suitability for dynamic, multi-attribute enterprise environments.*

8. DISCUSSION AND IMPLICATIONS

8.1. THEORETICAL IMPLICATIONS

The results confirm that the "Architecting Trust" framework satisfies the principle of integration between the technical and social systems as per STS theory. Using blockchain for enforcing policies while leaving the policy and identity definitions with the consortium ensures the efficient use of decentralized technology without falling prey to the fallacy that "code is the law" [6]. Thus, the LPHS-XV architecture resolves the contradiction between the technical immutability and the social need for privacy, contributing to the body of knowledge in the IS field [9].

8.2. MANAGERIAL AND PRACTICAL IMPLICATIONS

The framework provides practitioners with a proven approach to establishing "Trustworthy Data Spaces." In particular, managers should pay special attention to differentiating governance of the blockchain and by the blockchain. Off-chain identity management, dispute resolution, and consortium building become crucial components of governance in decentralized systems because the latter cannot solve social coordination issues automatically. Moreover, using standard DIDs as well as separating control and storage layers creates opportunities for cross-border data exchange among organizations operating in different legislative jurisdictions by allowing them to map their characteristics into the contract terms [9]. Such an approach allows establishing a global yet decentralized data market where each institution preserves sovereignty over its personal information in compliance with GDPR regulations [29].

8.3. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

Despite its effectiveness, the proposed framework suffers from certain limitations. First of all, CP-ABE cryptographic computations are expensive; thus, the proposed solution could experience latency issues when applied to IoT devices lacking computing resources [18]. Researchers should explore the possibility of encryption outsourcing to edge nodes or switching to lightweight Elliptic Curve Cryptography-based algorithms. Secondly, cryptographic algorithms used in the framework (RSA, ECC) are prone to being compromised when quantum computers appear on the horizon. Therefore, once quantum computing becomes mature, "Architecting Trust" will require migration to post-quantum lattice-based cryptography [21]. Finally, it is important to investigate the legal aspects of using smart contracts in various jurisdictions because the area is still relatively new to the law.

9. CONCLUSION

This study has introduced "Architecting Trust," a holistic framework for governing cross-institutional data exchanges by combining design science research principles and socio-technical systems theory. It proposes a Hybrid Model with the light layer for cryptographic enforcement and trust management and the deep layer for storing off-chain data with strong guarantees of privacy. "Architecting Trust" solves the trilemma of balancing trust, privacy, and efficiency by using ABAC and crypto-shredding methods to create an environment of highly protected information shared with strict GDPR compliance and complete owner control. Security analysis of the proposed system demonstrates robustness against attacks of all types. As the digital economy evolves, blockchain will play an increasing role in governing rather than just recording transactions. In other words, it is a powerful "governance machine."

REFERENCES

[1] Li, Kun, et al. “Privacy preservation in blockchain-based healthcare data sharing: A systematic review.” Peer-to-Peer Networking and Applications 18.6 (2025): 1-53.

[2] Razafimanjato, Mahalinoro, Malik Muhammad Saad, and Dongkyun Kim. “Blockchain-based trust management systems in the internet of vehicles: a comprehensive survey.” ICT Express 11.6 (2025): 1265–1285.

[3] Kshetri, Nir. “1 Blockchain’s roles in meeting key supply chain management objectives.” International Journal of Information Management 39 (2018): 80-89.

[4] Zorlu, Ozan, and Adnan Ozsoy. “A blockchain-based secure framework for data management.” IET Communications 18.10 (2024): 628-653.

[5] Hardjono, Thomas, Alexander Lipton, and Alex Pentland. “Toward an interoperability architecture for blockchain autonomous systems.” IEEE Transactions on Engineering Management 67.4 (2019): 1298-1309.

[6] An, Siyang, Chi Fai Cheung, and Kelvin W. Willoughby. “A gamification approach for enhancing older adults’ technology adoption and knowledge transfer: A case study in mobile payments technology.” Technological forecasting and social change 205 (2024): 123456.

[7] Zyskind, Guy, and Oz Nathan. “Decentralizing privacy: Using blockchain to protect personal data.” 2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.

[8] Azaria, Asaph, et al. “Medrec: Using blockchain for medical data access and permission management.” 2016 2nd international conference on open and big data (OBD). IEEE, 2016.

[9] Liang, Zhi-Yong, et al. “Trustworthy data space collaborative trust mechanism driven by blockchain: Technology integration, cross-border governance, and standardization path.” Information 16.12 (2025): 1066.

[10] Nguyen, Thanh Linh, et al. “Blockchain-empowered trustworthy data sharing: Fundamentals, applications, and challenges.” ACM Computing Surveys 57.8 (2025): 1-36.

[11] Beck, Roman, et al. “Blockchain technology in business and information systems research.” Business & Information Systems Engineering 59.6 (2017): 381-384.

[12] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. “A systematic literature review of blockchain-based applications: Current status, classification and open issues.” Telematics and Informatics 36 (2019): 55-81.

[13] Wu, Hao, et al. “Data-sharing system with attribute-based encryption in blockchain and privacy computing.” Symmetry 16.11 (2024): 1550.

[14] Liu, Duo, et al. “FitCNN: A cloud-assisted and low-cost framework for updating CNNs on IoT devices.” Future generation computer systems 91 (2019): 277-289.

[15] Jia, Xiaofeng, et al. “Cross-organisational data sharing framework based on blockchain-probes.” IET Networks 12.2 (2023): 77-85.

[16] Song, Rui, et al. “A survey of blockchain-based schemes for data sharing and exchange.” IEEE Transactions on Big Data 9.6 (2023): 1477-1495.

[17] Zhang, Aiqing, and Xiaodong Lin. “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain.” Journal of Medical Systems 42.8 (2018): 140.

[18] Song, Chaoyue, et al. “A Secure Data Sharing Model Utilizing Attribute-Based Signcryption in Blockchain Technology.” Sensors 25.1 (2024): 160.

[19] UshaRani, R. “Blockchain-Based Secure Data Sharing for IoT Applications.” Journal of Internet Services and Information Security 10.37 (2025): 6381.

[20] Ncube, Tomy, Una Murray, and Denis Dennehy. “Digitalising social protection systems for achieving the sustainable development goals: insights from Zimbabwe.” Communications of the Association for Information Systems 53.1 (2023): 138-161.

[21] Sengupta, Tirthankar, et al. “Interacct: Access control for permissioned blockchain interoperation.” 2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2025.

[22] Kotey, Seth Djanie, et al. “Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication.” Iet Communications 17.8 (2023): 891-914.

[23] Li, Wenqing, et al. “Towards blockchain interoperability: A comprehensive survey on cross-chain solutions.” Blockchain: Research and Applications (2025): 100286.

[24] Androulaki, Elli, et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains.” Proceedings of the thirteenth EuroSys conference. 2018.

[25] Yang, Xinyi, et al. “Data Secure Storage Mechanism for Trustworthy Data Space.” Electronics 14.21 (2025): 4348.

[26] Zeng, Shulei, et al. “Blockchain-assisted cross-domain data sharing in industrial IoT.” IEEE Internet of Things Journal 11.16 (2023): 26778-26792.

[27] Tan, Bingbing, et al. “A cross-institution information-sharing scheme based on a consortium blockchain.” Electronics 12.21 (2023): 4512.

[28] Ma, Wei, Xibei Wei, and Longlong Wang. “A security-oriented data-sharing scheme based on blockchain.” Applied Sciences 14.16 (2024): 6940.

[29] Jiang, Jiahui, et al. “CDAS: A Secure Cross-Domain Data Sharing Scheme Based on Blockchain.” Information 16.5 (2025): 394.