Blockchain-Based Secure Data Sharing Framework: Dual Validation Through Content Validity and Thematic Analysis

Azman Azmi[1], Farashazillah Yahya[2]*, Nur Afrina Azman[3]
Faculty of Computing and Informatics, Universiti Malaysia Sabah, Malaysia[1, 2]
School of Mathematical, Physical and Computational Sciences, University of Reading, United Kingdom[3]

***Abstract*—Blockchain technology applied to digital government services platforms has introduced new possibilities for secure data sharing for public sector agencies. However, the verification and validation of critical security factors remain underexplored, leading to inconsistent security factors for implementations and theoretical gaps. This study addresses this issue by conducting a double validation analysis of security factors relevant to blockchain-based data sharing in e-government applications using thematic analysis and content validity index. Drawing from an extensive literature review, 54 security items from nine factors were evaluated by a panel of six domain experts using the methodological triangulation. The results indicate that key factors of confidentiality, integrity, availability, decentralisation, interoperability, transparency, auditability, and governance exhibit strong content validity and themes for thematic analysis. Immutability factors are outside the Universal Agreement (UA) scale and require further refinement. The validated framework contributes to both academic and practical domains by offering concrete fundamentals for secure system design and policy formulation. Future research directions include operational testing of validated factors and exploration of user-centric verification.**

***Keywords*—Blockchain; content validity; data sharing; e-government; thematic analysis**

I. Introduction

Recent years have witnessed a growing academic interest in integrating digital emerging technologies to support public sector services, potentially affecting the business and the citizens [1], [2]. Integrating social, legal, technological, and economic dimensions has demanded an increasing complexity of security and data protection, requiring a comprehensive approach in this digital era [3]. The widespread digitisation of services and the proliferation of data-driven e-government systems have created the demand for secure data sharing. The current trend of utilising decentralised platforms in public sectors is increasing to ensure reliability in sharing sensitive information, necessitating mechanisms that ensure data security [4]. Secure data sharing integration in information systems between government agencies in a seamless information sharing addresses new security challenges for data sharing. The transaction involves data sharing between agencies and entities [5], [6].

An increasing number of incidents and attacks have shown increasing threats to data sharing. MyCERT Cyber Incident Quarterly Summary report released on 10 June 2025 showed 195 data breach incidents reported in Q1 2025 compared to 151 in Q4 2024. This shows an increase in incidents by 29% [7]. Interest in blockchain technology for government data sharing security has grown rapidly, but the literature still lacks clear validation of the security factors for secure data sharing. Most existing studies present conceptual frameworks or technical models without rigorous empirical validation, leaving gaps in practical applicability [8], [9], [10]. However, employing a qualitative approach allows for deeper exploration of recurring themes, perspectives, and concepts among domain experts; the research is moving towards accuracy and credibility [11].

To address these limitations, this study applies methodological triangulation using thematic analysis and content validity assessment to examine and refine a set of security factors for blockchain-based e-government data-sharing applications. By engaging subject matter experts and utilising established validation techniques, the research seeks to deliver a robust and empirically grounded framework. The findings aim to advance both theoretical understanding and practical implementation by providing a validated framework that enhances the security and reliability of blockchain-enabled public services, while also guiding future system design, policy formulation, and research in the fields of information systems, government administration, and cybersecurity.

II. Background

A. Blockchain in E-Government: Opportunities and Challenges

Blockchain technology has gained traction in e-government initiatives due to its potential to enhance transparency, decentralisation, and provide immutability [12], [13], [14]. Studies by [15] and [16] highlight its use in digital identity management, public records, and inter-agency data sharing. Blockchain can reduce the reliance on central authorities due to its decentralised nature. This in turn will mitigate risks which are associated with single-point failures [17]. However, challenges remain, including privacy and data integrity [18], [19], [20], which hinders widespread adoption in public sector environments.

B. Blockchain-Based Data Sharing Security

Data sharing security is a cornerstone for trusted and effective e-government systems. Blockchain offers mechanisms such as smart contracts, cryptographic hashing, and distributed

*Corresponding author.

consensus to ensure data confidentiality and integrity. The authors in [21], [22] emphasise the role of blockchain in enabling trustworthy data exchange across organisational boundaries. Despite these advancements, the literature reveals a lack of standardised security factors frameworks tailored to the unique needs of e-government, particularly in multi-jurisdictional contexts.

Data sharing environments are inherently vulnerable to a wide range of security threats that may compromise confidentiality, integrity, and availability. Therefore, it is essential to systematically identify these threats and evaluate their potential consequences to inform the development of effective security solutions. Prior research has extensively addressed this domain, with initiatives such as the Open Web Application Security Project (OWASP) providing comprehensive classifications of common security attacks and MyCERT Cyber Incident Quarterly Summary report Q2 2025 (SR-031.082025) release on 6 August 2025 showed 103 data breach incidents reported in Q2 2025 compared to 195 in Q4 2024, a decrease of incidents by 47.18%. Data breach incidents reported in Q1 2025 are 29% higher compared to 151 in Q4 2024 [7]. The following threat categories in Table I are identified for the data sharing security by OWASP Top 10 [23] and the literature:

TABLE I. DATA SHARING THREATS

Threats	Issue
False Data Injection Attacks (FDIA)	Unauthorised actors exploit system vulnerabilities to inject malicious code or commands, compromising data integrity and confidentiality. False data injection attacks (FDIA) pose a significant threat to the microgrids by corrupting information exchange among controller units [24].
Broken Authentication and Access Control	Centralised authentication and access control systems are prone to single-point failure, security threats, and privacy and scalability issues [25].
Data Breaches	Unauthorised disclosure, leakage, or theft of sensitive data, resulting in compromised confidentiality and potential legal and reputational consequences.
Insider Threats	Malicious or inadvertent actions by authorised personnel (e.g., employees or contractors) leading to data misuse, exposure, or unauthorised access.
Insecure Data Handling	Improper practices in data storage, transmission, or disposal that may result in accidental exposure, leakage, or loss of sensitive data.
Non-Compliance with Data Protection Regulations	Failure to adhere to relevant legal, regulatory, and industry standards exposes organisations to legal risks, penalties, and reputational damage.
Exposing the contents of the sensitive files to sharing parties	Sensitive data is exchanged between organisations, and we require auditability and traceability of actions taken to assure compliance with signed legal agreements. In study [26], conflict resolution may require exposing the contents of the sensitive files to this party.
Single point of infrastructure failure	The Blockchain uses a Peer-to-Peer network, where all the nodes share their resources with each other. This will also increase the Blockchain availability; if one of the nodes goes down, others are available. The blockchain operators are unknown, and the objective of the network is not clear; through validation control, they can exclude and compromise some nodes that affect their network availability [27].
Lack of standardisation and an interoperable system	In a nationalised healthcare infrastructure, a lack of standardisation and interoperable Electronic Health Records has led to medical errors, diminishing the well-being of patients [28].

C. Security Factors in Blockchain-Based Data Sharing System

Several theories on the origin of data-sharing security factors have been identified in [29]. Nine blockchain-based data-sharing security factors have been critically identified: confidentiality, integrity, availability, transparency, auditability, decentralisation, immutability, interoperability, and governance, as in Fig. 1. The description reviews also presented solutions which emerged in various industries, as an understanding of blockchain's ability to overcome constraints that have been discussed in previous literature [29]. As a continuation of the literature synthesis, a content validity was conducted in this study.

D. Validation of the Theoretical Framework

Given the fact that valid and reliable factors are needed to theoretically design and evaluate blockchain-based data sharing security factors. Validity is the extent of accuracy with which the sub-factors of the target main security factors.

1) Thematic analysis: A powerful approach used in research. Research involving the analysis of qualitative data widely uses this methodology qualitative (Mohd Noor et al., 2025; Proudfoot, 2023). Patterns, themes and meaning which are embedded in the data could be uncovered by researchers when this method is used as an inductive approach. This will allow a deeper understanding to be facilitated based on the event [31], [32]. Thematic analysis is being used by [33] on blockchain-related agri-food business news and expert opinions from the Ovid database's Agricola section, while [34] applied a thematic network analysis approach for blockchain adoption effectiveness. The weakness of the research by [34] is that it used collected data from secondary sources, where there were no in-depth interviews with the targeted audience that were conducted to gain further understanding of the behavioural elements that impact the application of blockchain in supply chain management. Both researchers agreed that there is a need to conduct further empirical research that investigates various other perspectives

2) Content validation: A widely used method in the research validation process. Preliminary evidence of the validity of the instrument can be provided through this approach. Previous research using Aiken's V with Content Validity Index (CVI) has established a robust quantitative process validation [10]. Another approach by [35] adopted a two-stage content validation using Content Validity Ratio (CVR) and Content Validity Index (CVI), both are quantitative

methodologies. However, both studies restricted the range of methodological approaches, which did not incorporate quantitative and qualitative analysis.

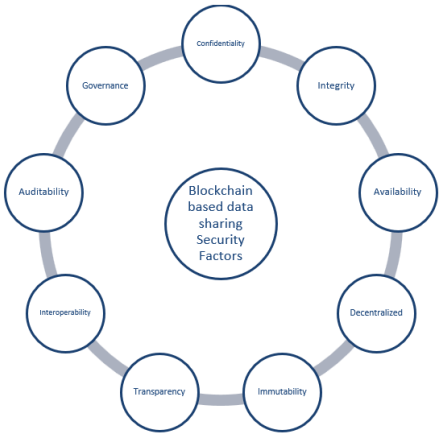

Fig. 1. Blockchain-based data sharing security factors.

III. Methodology

A. Research Design

This research applied methodological triangulation, as shown in Fig. 2. Methodological triangulation is a technique defined as the combination of two or more methods in a study [11], [36]. The study employs a double validation method using thematic analysis for qualitative data analysis and a content validity approach to empirically assess the relevance and clarity of security factors associated with blockchain-based data sharing in e-government applications. By using triangulation and drawing on multiple viewpoints, this research is moving towards accuracy and credibility as it involves several sources, confirmation, and processes of data collection.

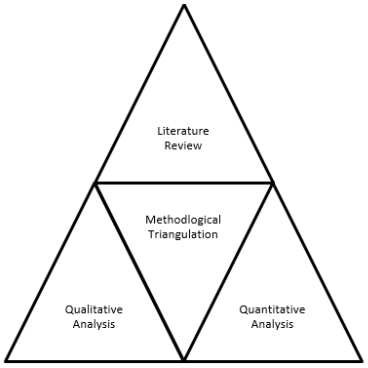

Fig. 2. Methodological triangulation methodology.

B. Instrument Development

The generation of items during questionnaire development requires considerable pilot work to refine wording and content. To assure content validity, items is generated from a number of data sharing security factors and subfactors that were compiled through an extensive literature review [29], [37], focusing on blockchain applications in public sector data sharing. 54 sub-factors were translated into an open-ended questionnaire and measurable items. The items were categorised under nine key factors: confidentiality, integrity, availability, decentralised, immutability, transparency, auditability, interoperability and governance. The instrument has gone through a test by an undergraduate student studying computer science.

C. Expert Panel Selection

A group of subject matter experts was assembled, comprising IT professionals from various backgrounds and industries in government information system security practice, to ensure robust validation. Selection criteria included:

- Minimum of ten years of experience in the Information Technology field, focusing on e-government information systems.
- Prior involvement in data and information security-related projects.
- Different types of government departments and agencies diversity to capture contextual variations.
- Government or Industry expert in Blockchain Technology or Data Security.

A total of six (6) experts participated in the validation process, as mentioned in Table II.

TABLE II. Expert Panel Information

No	Expert Initial	Domain	Expertise Area	Experience	Institution
1	Expert 1	Government	Information Security	> 15 years	Public University
2	Expert 2	Government	Information Security	> 15 years	Public University
3	Expert 3	Government	Blockchain, Cyber Security	> 15 years	Federal Government
4	Expert 4	Government	Blockchain, Network Security	10 - 15 years	State Government
5	Expert 5	Government	Blockchain, Fintech	10 - 15 years	State Government
6	Expert 6	Industry	Blockchain, Database, Information Security	10 - 15 years	Private Sector

D. Expert Interview

Data were collected from experts' review using interviews and questionnaire methods. The interview is done face-to-face with each and every single expert. Each session takes about two to three hours to complete. Subsequently, the results obtained were compared to identify similar answering patterns [38].

E. Thematic Analysis

Thematic analysis is a popular qualitative research approach that focuses on recognising, examining, and interpreting patterns or themes found in a dataset. A systematic, multi-step process has been used to enhance the rigour and replicability of the analysis, often culminating in a conceptual model that explains the research findings [39]. Qualitative thematic analysis was performed using Atlas.ti. The information security and blockchain technical experts all reviewed and coded data in the coding process.

1) Key stages of thematic analysis: Six key stages for thematic analysis are defined by [39], [30] [40], [41] using Fig. 3:

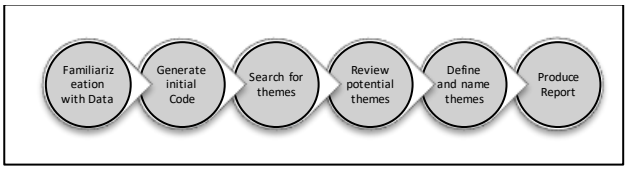

Fig. 3. Six key steps in conducting thematic analysis.

The thematic analysis process adopted in this study is characterised as systematic, as it follows a structured and sequential approach to the interpretation of qualitative data. While a clearly defined analytical framework enhances transparency and provides logical progression from raw data to codes and themes, each stage of the process inevitably relies on the researcher's interpretive judgement, which influences how meanings are constructed and prioritised. In this research, the systematic nature of the analysis facilitates consistency and allows the analytical decisions made to be traced and does not entirely eliminate potential bias. By maintaining an explicit audit trail and adhering. Nevertheless, given the complex and context-dependent nature of expert perspectives, alternative interpretations are possible, and therefore, the findings should be viewed as one plausible interpretation rather than a definitive account.

The first step is to get familiar with the transcript data. The transcript will be read several times to ensure that all terms used and explanations are well understood. The interpretation of the transcript is noted. The second step is identifying and labelling significant features of the data that are relevant to the main factors and sub-factors. The coding framework will be generated for further analysis. The next step is to search for themes. In this research, themes are determined by the main factor used in the Blockchain-based data sharing. In step 4, reviewing the theme includes the sub-factors in the main theme that have been determined before. In step 5, each theme is clearly defined and named, giving a clarification on each theme represented in relation to the factors and subfactors. In the final step, a report of the themes is presented to show the findings and implications for the factors in the research field.

F. Content Validation Procedure

Content Validity Index (CVI) can be categorised into two types, the I-CVI (item level) and S-CVI (scale level). The definition and formula were based on the recommendation by Lynn(1986), Davis (1992), Polit & Beck(2006) and Poliy et al. (2007), as cited in [42]. The instrument designed is subjected to the expert to evaluate the CVI for item (I-CVI) and scale (S-CVI) that have S-CVI/Ave and S-CVI/UA. To quantify the expert level agreement, we use the Item level of CVI on the relevance of each individual item in the measurement instrument. Each item will be rated by an expert on a 4-point ordinal scale for relevance. The 4-point scale is used to avoid a "neutral" middle point, forcing clearer judgments [42]. To calculate the I-CVI, each of the items rated as 3 (quite relevant) or 4 (highly relevant) by the experts will be counted and divided by the total number of experts shown in the formula below:

$$\text{I} - \text{CVI} = \frac{\text{No. of experts rating item as 3 or 4}}{\text{Total no. of experts}} \quad (1)$$

Scale-level Content Validity Index (S-CVI), which extends the item-level CVI (I-CVI) to the *entire instrument*. It shows overall content validity across all items. There are two main approaches: S-CVI/Ave and S-CVI/UA. S-CVI (Scale-level CVI) is used to summarise how well the *whole set of items* in an instrument reflects the construct. S-CVI/Ave (Average method). The average of the I-CVI values for all items in the instrument:

$$S - CVI/Ave = \frac{\sum I-CVI}{N} \quad (2)$$

where, N = total number of items and $\sum$ I-CVI = Sum of sub-factors in a main factor.

The S-CVI/Ave provides a mean proportion of agreement across all sub-factors in the main factors. It is more lenient than universal agreement, since it allows some items to have lower I-CVI values. A value of ≥ 0.90 is typically considered excellent overall content validity [42]. S-CVI/UA (Universal Agreement method), the proportion of items that achieved universal agreement among experts (i.e., *all* experts rated them as 3 or 4 = relevant) for the main factors evaluated in this research.

$$S - CVI/UA = \frac{Number\ of\ items\ with\ I-CVI = 1.00}{Total\ number\ of items} \quad (3)$$

Universal Agreement is much stricter than S-CVI/Ave. If even one expert rates an item as not relevant, it won't count toward universal agreement. Often produces lower values, especially when panel sizes are larger. Recommended cutoff = ≥ 0.80 because it is harder to achieve [42].

TABLE III. THE NUMBER OF EXPERTS AND THEIR INFLUENCE ON THE ACCEPTABLE CUT-OFF SCORE OF CVI.

No of experts	Acceptable CVI Values	Recommendations
2	At least 0.8	Davis (1992)
3 to 5	Should be 1	Polit & Beck (2006) Polit et. Al (2007)
At least 6	At least 0.83	Polit & Beck (2006) Polit et. Al (2007)
6-8	At least 0.83	Lynn (1986)
At least 9	At least 0.78	Lynn (1986)

Note : The definition and formula were based on the recommendation by Lynn (1986), Davis (1992), Polit & Beck (2006) and Poliy et al. (2007), as cited in [42].

Table III shows the content validity reference for the acceptable cut-off score. The correlation between the number of experts on a review panel affects the acceptable cutoff values for Content Validity Index (CVI). The reference is also shown in the table, where it refers to Davis (1992), Polit & Beck (2006), Polit et al. (2007) and Lynn (1986), as cited in [42].

In this research, we are engaging with six experts. The work we are referring to (Polit & Beck, 2006; Polit et al., 2007) and Lynn (1986), as cited in [42]. Both references agree that for at least six experts, the CVI must be equal to or higher than 0.83. The threshold to get more than 0.83 or 83% agreement is that there must be at least 5 out of 6 experts who must agree on the sub-factors. With 6 experts, some disagreement is tolerable because the chance of random agreement is much lower.

G. Ethical Considerations

For ethical consent, all the experts' participation was voluntary. Anonymity and confidentiality were maintained throughout the process. Revision and approval of the study protocols have been provided by the university, and a pilot test was conducted before it was answered by the experts.

IV. Findings and Analysis

A. Overview of Experts

The expert panel evaluated a total of 9 security factors with 54 sub-factors for data sharing security-related items across nine main factor dimensions: confidentiality, integrity, availability, decentralised, immutability, transparency, auditability, interoperability and governance. Each expert shares their review for each factor and subfactor. Then, for relevance and clarity, each item was rated using a 4-point Likert scale by the experts.

B. Demographics of Experts

The demographic profile of the respondents was gathered using five questions, and the analysis is presented in Table I. Of the experts interviewed, 83.3% were from the public sector, with 33.3% representing State Government, 33.3% from Public Universities, 16.6% from Federal Government, and the remaining 16.6% from industry. All experts are from an IT Technical background and are involved in government IT and Information security projects. 50% of the experts have more than 15 years of experience, and another 50% have 10 to 15 years of experience in IT and security. All of the expert responses have 2000 to 15,000 transactions per day involving data sharing in the government information system. 66.7% of the expert are using blockchain in their environment. They used a private and consortium blockchain platform running Ethereum in a private cloud environment. The concern of using blockchain in the e-government system is security, authenticity, integrity, tamper-proof records, public verifiability, compliance, and fault tolerance.

C. Thematic Analysis Coding Result on Expert Review Interview

The theme of audibility emerged as a significant dimension underpinning system traceability and auditability. Experts 1 and 4 uniformly affirmed that "allowing traceability" and "tracking transactions" help identify the keyword for the code. These findings underline the crucial function of traceability mechanisms in data sharing auditability. It is also shown and recognised that data trackable or normally defined as audit also enables thorough post-event auditability, thereby enhancing data sharing security needs. In Fig. 4, experts noted that it "ensures that all transactions can be traced back to their origin," which is the keyword of "essential for auditability and security," and emphasised how "data are tracked and can be audited." These remarks suggest that audibility not only supports technical oversight but also provides evidentiary value. Consequently, systems designed with robust traceability features are better equipped to manage demands, ensure fairness, and uphold stakeholder confidence in data sharing.

Confidentiality was identified as a theme, bridging the codes of secure access, data privacy, trust, confidentiality, privacy, authenticity, authentication, authorisation and sovereignty. Experts highlighted that "verifying authenticity is important to ensure data validity and access control" and that "Transparent data ensures that shared information is authentic and free from manipulation" has the key findings of authenticity with secure access control as the code used for this result. The experts also highlighted "Data openness helps build trust between parties sharing data" and "architecture and cryptographic safeguards ensure data confidentiality", for trust and confidentiality. The keyword of privacy is critically important, and the proper authentication keyword is highlighted by the expert for privacy and authentication. While for authorisation, the expert stated "consensus mechanism will authorise which node will write or read data", which can be coded for authorisation in confidentiality themes.

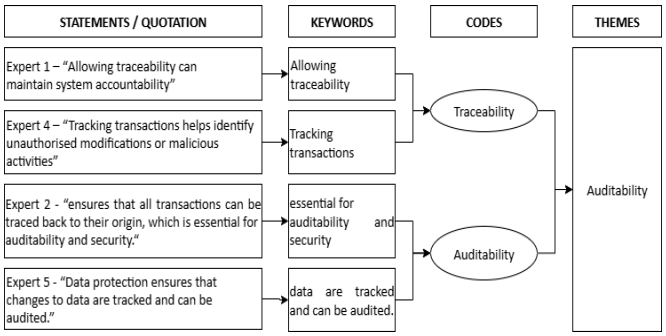

Fig. 4. Thematic analysis result for auditability.

Integrity emerged as a comprehensive theme incorporating reliability, validity, credibility, accountancy, accuracy and verifiability. Experts consistently remarked that digital public services must be "secure, accountable, transparent, and reliable," while emphasising the importance of "ensuring data validity and data integrity". These insights suggest that integrity is the backbone of trustworthy systems, covering technical correctness and ethical stewardship. In public sector applications, data integrity is essential to uphold service productivity.

Moreover, ensuring integrity is closely linked to building trust and institutional legitimacy. Experts conveyed that improving data integrity is vital "to build trust and credibility" and "enforce accountability". They also highlighted accurate data input and verifiability as prerequisites for maintaining stakeholder confidence. This reflects a recognition that integrity encompasses both accuracy and the perception of fairness. Consequently, designing systems that ensure and demonstrate integrity is essential for public accountability and trust.

The availability of data consistently emerged as a foundational requirement for effective digital systems. Experts emphasized that "making data consistently available is… a cornerstone for data sharing", and that stakeholders must be "able to control data access in and out". These findings highlight the importance of both technical accessibility in ensuring functional utility. In environments where timely information is critical—such as governmental decision-making systems—any interruption in availability could severely undermine operational effectiveness, as shown in Fig. 5.

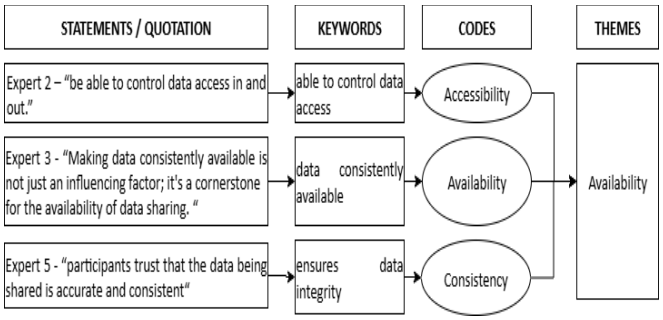

Fig. 5. Thematic analysis result for availability.

In addition, one expert remarked that "participants trust that the data being shared is accurate and consistent", illustrating how availability underpins both confidence in e-government systems and their actual performance. This implies that design strategies aimed at ensuring continuous access must also safeguard data integrity. Ensuring consistent availability thus fosters not only immediate usability but also long-term trust and system credibility.

The analysis also revealed decentralisation as a theme in the blockchain-based data sharing security factors. Expert 3 emphasised that blockchain "unlocks the full potential… to deliver credible, real-time, and decentralised data sharing across industries", highlighting the importance of decentralised infrastructure for enhancing transparency and credibility. Similarly, Expert 6 noted that "fault tolerance and decentralised enable recovery and readiness data", indicating that decentralisation also contributes to system robustness and continuity. These statements were coded under "Decentralise" and contributed to the overarching theme of Decentralise, which encompasses both technical and operational benefits of decentralised systems. Additional insights from Expert 3 regarding "distributed ledger architecture" and from Expert 5 referencing data being "securely stored in a separate location" were coded as "Distributed", reinforcing the decentralised theme. Collectively, the data suggest that experts view decentralisation not only as a structural feature of blockchain but also as a critical enabler of data security, trust, and recovery in digital systems.

The theme of immutability strongly reflects the necessity for data permanence and trustworthiness. Experts stated that systems "increase data immutability and integrity in data sharing," and underscored that "data has not been altered since it was recorded". These remarks reinforce the foundational role of immutability in preventing data tampering and ensuring historical fidelity. Particularly in contexts where auditability and legal reliability are paramount, immutability provides a cornerstone for data assurance. Additionally, immutability contributes significantly to stakeholder confidence in digital systems. One expert described how shared data remains "accurate, tamper-proof, and verifiable", and others emphasised that increased immutability enhances security. This indicates that immutability is not merely a technical attribute but a trust-building mechanism. Robust systems that guarantee unchangeable data records foster accountability and reduce risks of dispute. By anchoring data sharing in irreversible records, immutability ensures that systems remain reliable and transparent over time.

The theme of interoperability underscores the necessity for seamless collaboration and integration among systems, stakeholders, and technologies. It is widely acknowledged that achieving effective interoperability hinges not only on technical compatibility but also on cooperative alignment. Experts emphasised that "harmonising processes among systems develops protocol standardisation, which is one of the key interoperability security factors", and that "collaboration fosters mutual understanding and cooperation, which are essential for successful data sharing". These statements highlight the critical importance of cooperation in overcoming fragmented digital ecosystems. By drawing on these expert insights, it becomes clear that interoperability is best achieved when technical solutions are complemented by institutional coordination and mutual trust.

Furthermore, interoperability is presented not merely as a technological challenge but as a governance and coordination concern. Experts observed that "data integration provides meaning" and that interoperability "enables effective interoperability" when paired with trust and collaboration. These observations suggest that interoperability facilitates both system-level efficiency and stakeholder confidence. When systems are interoperable, they reduce redundancy, improve data accuracy, and accelerate decision-making processes—benefits that are particularly vital in complex environments such as government agencies. In light of this, effective interoperability must be carefully aligned with governance frameworks, standardisation efforts, and stakeholder collaboration to support robust digital transformation.

Transparency emerged as a foundational theme, closely associated with trust and accountability in digital governance. In Fig. 6, experts repeatedly emphasised the need for transparency, asserting that it is "essential for ensuring that digital public services are secure, accountable, transparent, and reliable", and that "seamless data sharing enforces protocol-level transparency". These assertions demonstrate that transparent processes are indispensable for institutional integrity and public trust. Moreover, the phrase "ensuring transparency and accountability in data-sharing practices" captures the broader expectation that transparency enhances not only visibility but also procedural fairness and legitimacy in public services.

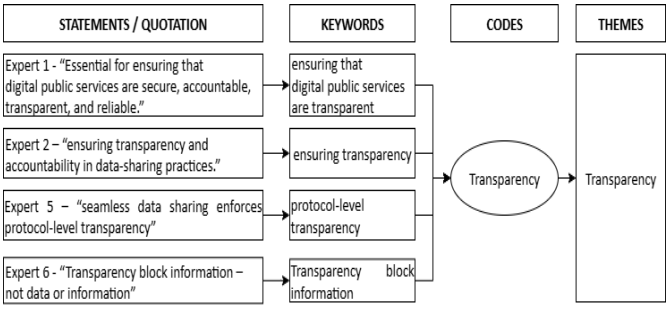

Fig. 6. Thematic analysis result for transparency.

Beyond enhancing public confidence, transparency is pivotal in preventing misuse and improving oversight. The remark that "transparency block information—not data or information" provides a nuanced understanding that transparency in data sharing should be structured: it should be

purposeful and controlled rather than indiscriminate. In other words, transparency involves enabling authorised access and traceability rather than full exposure. In government contexts, this structured transparency ensures that systems remain secure while still being open to necessary scrutiny. Thus, transparency supports democratic principles, fostering fairness, accountability, and informed participation in the digital era.

Governance surfaced as a comprehensive theme encompassing policy, regulation, standardisation, and control. Experts cautioned that "without effective data security, e-government governance becomes vulnerable, non-compliant, and unsustainable", and emphasised how "trusted data helps organisations comply with industry regulations and standards". These assertions emphasise that governance frameworks provide the underpinning for data stewardship and legitimacy in data sharing systems. The capacity for systems to meet legal and ethical standards is contingent upon governance structures that enforce accountability and continuity.

In parallel, governance involves harmonisation and administrative clarity across organisational boundaries. One expert noted that "well-defined policies protect sensitive government information from unauthorised access or misuse", while another remarked that "harmonised processes help different administrative zones operate under a common standard". These insights suggest that governance extends beyond regulatory compliance to include operational coherence. Effective data sharing security governance, therefore, requires both policy articulation and cross-institutional coordination to support integrated, secure, and sustainable e-government ecosystems.

In Fig. 7, the thematic analysis maptree shows the themes of factors and codes for subfactors that have been extracted from the interview transcript. The confidentiality theme has shown the most quoted code, with trust recording the highest quote of 74. The accuracy code recorded 34 quotes, followed by integrity 32 quotes and reliability 31 quotes under the integrity themes. The immutability themes recorded 27 quotes for each immutability and temper-proof. The transparency themes recorded 27 quotes, while the auditability themes recorded 16 quotes for traceability and 15 quotes for auditability. The availability themes and quotes recorded 21 transcripts. The governance themes recorded 13 quotes for standardisation and 9 for regulation quotes. The decentralised themes and quotes recorded 12, followed by the distributed code for two quotes.

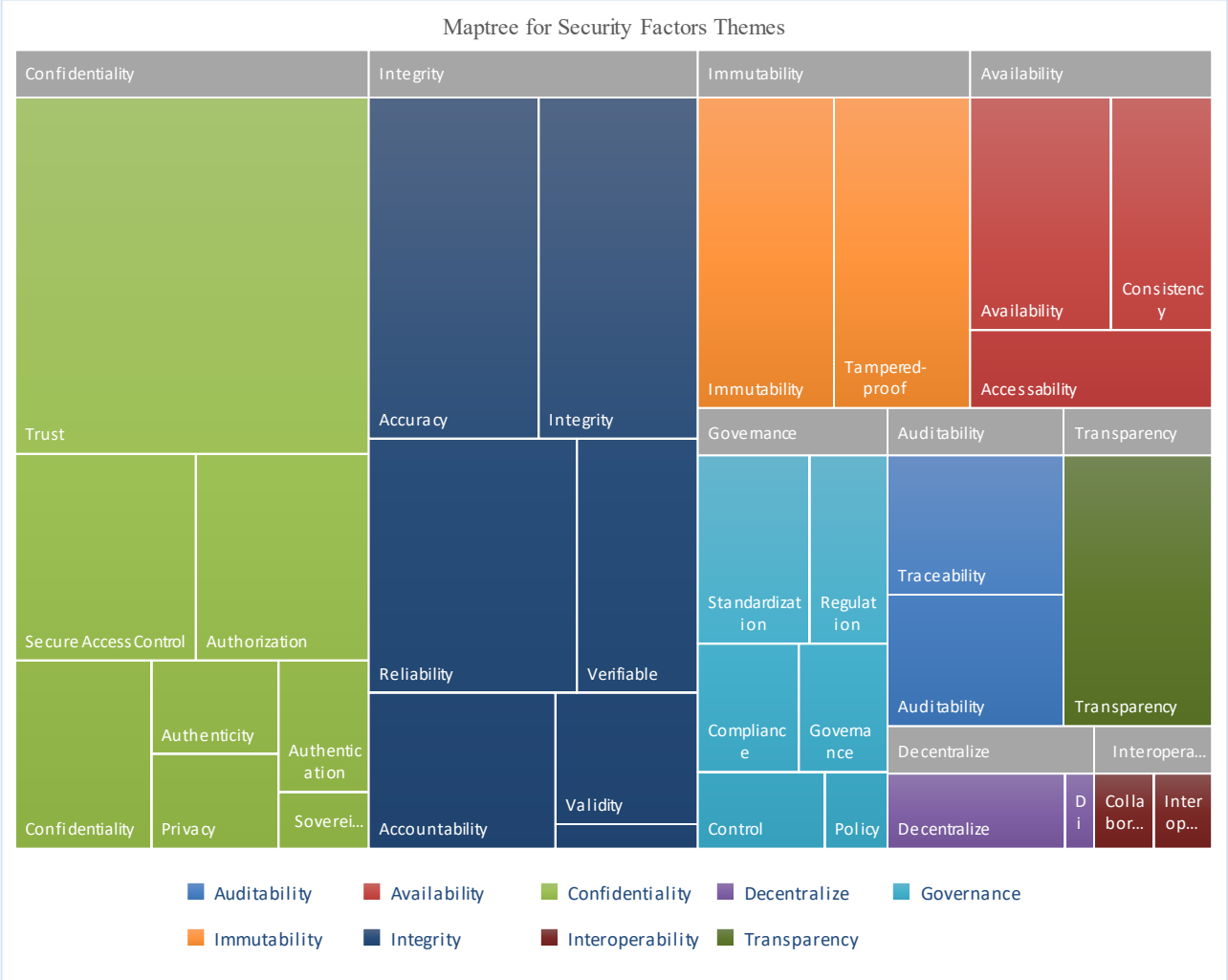

Fig. 7. Maptree thematic analysis.

D. Content Validity Results

The results of the content validity for the security factors are referred to Table II: The definition and formula were based on the recommendation by Lynn (1986), Davis (1992), Polit & Beck (2006) and Poliy et al. (2007), as cited in [42].

The confidentiality sub-factor in Table IV demonstrates generally high content validity with slight variation across sub-factors. Most items, including Trust between Parties, Privacy, Data Confidentiality, Data Ownership, Authentication, Authorisation, Secure Access Control, and Identity Security, achieved I-CVI values of 1.00, reflecting unanimous agreement on their relevance. However, the sub-factor Data Sovereignty received a slightly lower I-CVI of 0.83, indicating partial expert divergence.

TABLE IV. I-CVI RESULT FOR CONFIDENTIALITY

Factors	Sub-Factor	I-CVI	Accept /Reject
Confidentiality	i. Trust between parties	1.00	Accept
	ii. Privacy	1.00	Accept
	iii. Data Confidentiality	1.00	Accept
	iv. Data Ownership	1.00	Accept
	v. Authentication	1.00	Accept
	vi. Authorisation	1.00	Accept
	vii. Secure access control	1.00	Accept
	viii. Identity security	1.00	Accept
	ix. Data sovereignty	0.83	Accept

TABLE V. I-CVI RESULT FOR AVAILABILITY

Factors	Sub-Factor	I-CVI	Accept / Reject
Availability	i. Information-Sharing Across Organisations	1.00	Accept
	ii. Data Consistently Available	1.00	Accept
	iii. Data Usability	1.00	Accept

The findings presented provide compelling evidence of strong content validity for the availability sub-factor in Table V. All three sub-factors, Information-Sharing Across Organisations, Data Consistently Available, and Data Usability, achieved an I-CVI score of 1.00, which indicates unanimous expert agreement regarding their relevance to the construct under investigation. In addition, the scale-level indices further reinforce this conclusion. Consequently, the factor of availability, supported by its sub-dimensions, can be considered to exhibit excellent content validity.

The integrity sub-factors in Table VI demonstrate very high levels of content validity across a comprehensive set of sub-factors. Items including Ensuring Data Integrity, Protecting Data Integrity, Using Single Source of Truth, Trustworthiness of Data, Verifying Authenticity, Accuracy of Data, Use of Validation, Reducing Fraud, Trust of Data Integrity, Accountability of Data, Authenticity of Source, and Reliability of Data Sources/Used all scored I-CVI values of 1.00. The item Specificity of Data scored slightly lower at 0.83, suggesting modest divergence among experts.

TABLE VI. I-CVI RESULT FOR INTEGRITY

Factors	Sub-Factor	I-CVI	Accept / Reject
Integrity	i. Ensuring Data Integrity	1.00	Accept
	ii. Protecting Data Integrity	1.00	Accept
	iii. Using Single Source of Truth	1.00	Accept
	iv. Trustworthiness of Data	1.00	Accept
	v. Verifying Authenticity	1.00	Accept
	vi. Accuracy of Data	1.00	Accept
	vii. Specificity of Data	0.83	Accept
	viii. Use of Validation	1.00	Accept
	ix. Reducing Fraud	1.00	Accept
	x. Trust of Data Integrity	1.00	Accept
	xi. Accountability of Data	1.00	Accept
	xii. Authenticity of source	1.00	Accept
	xiii. Reliability of data Sources	1.00	Accept
	xiv. Reliability of Data Used	1.00	Accept

The decentralisation factor in Table VII exhibits excellent content validity with unanimous expert agreement across all sub-factors. Items such as Distributed Data Recovery, Decentralising Property Rights, and Large-Scale Data Security Management each achieved I-CVI scores of 1.00, confirming their full relevance. With no sub-factor requiring revision, this construct stands as one of the strongest validated domains in the study, reinforcing its importance in addressing issues in data sharing security.

TABLE VII. I-CVI RESULT FOR DECENTRALISATION

Factors	Sub-Factor	I-CVI	Accept
Decentralisation	i. Distributed Data Recovery	1.00	Accept
	ii. Decentralising Property Rights	1.00	Accept
	iii. Large-Scale Data Security Management	1.00	Accept

The immutability sub-factors in Table VIII show strong but slightly less consistent content validity compared with other factors. Sub-factors such as Reducing the Need for Trusted Third Parties, Data Protection Security, Tamper-Proof Record, Resistance to Attacks, and Non-Temperable Properties achieved I-CVI scores of 1.00, signifying agreement of expert endorsement. However, Isolating Data and Blocking Data Properties received slightly lower I-CVI values of 0.83, reflecting minor divergence.

Transparency and its sub-factors result in Table IX, shows a strong but not unanimous validity across its sub-factors. Items including Need for Greater Transparency, Seamless Data Sharing, Secure Transaction Visibility, and Allowing Traceability achieved I-CVI values of 1.00, reflecting complete expert agreement. The item Openness of Data scored slightly lower at 0.83, suggesting minor divergence in views.

TABLE VIII. I-CVI RESULT FOR IMMUTABILITY

Factors	Sub-Factor	I-CVI	Accept / Reject
Immutability	i. Reducing the Need for Trusted Third Parties	1.00	Accept
	ii. Data Protection Security	1.00	Accept
	iii. Tamper-Proof of Record	1.00	Accept
	iv. Resistance to Attacks	1.00	Accept
	v. Isolating Data	0.83	Accept
	vi. Blocking Data Properties	0.83	Accept
	vii. Non-Temperable	1.00	Accept

TABLE IX. I-CVI RESULT FOR TRANSPARENCY

Factors	Sub-Factor	I-CVI	Accept / Reject
Transparency	i. Need for Greater Transparency	1.00	Accept
	ii. Seamless Data Sharing	1.00	Accept
	iii. Secure Transactions Visibility	1.00	Accept
	iv. Allowing Traceability	1.00	Accept
	v. Openness of Data	0.83	Accept

TABLE X. I- CVI RESULT FOR INTEROPERABILITY

Factors	Sub-Factor	I-CVI	Accept / Reject
Interoperability	i. Data Integration between parties	1.00	Accept
	ii. Harmonizing Processes	1.00	Accept
	iii. Standardization Integration of system	1.00	Accept
	iv. Collaboration of parties	1.00	Accept

Interoperability sub factors shows in Table X demonstrates a solid content validity across its four sub-factors. Items Data Integration between Parties, Harmonising Processes, Standardisation of System Integration, and Collaboration of Parties each obtained I-CVI scores of 1.00, indicating all expert agreement.

The auditability sub factors construct in Table XI shows robust content validity, as reflected in unanimous expert agreement across all sub-factors. The items "Ability to Track Transactions", "Ability to Retain Transactions", and "Allowing Transaction Traceability", each received an I-CVI score of 1.00, which signifies complete endorsement of their relevance.

TABLE XI. I-CVI RESULT FOR AUDITABILITY

Factors	Sub-Factor	I-CVI	Accept / Reject
Auditability	i. Ability to Track Transactions	1.00	Accept
	ii. Ability to Retain Transactions aligning	1.00	Accept
	iii. Allowing Transaction Traceability	1.00	Accept

Governance sub-factors in Table XII also shows perfect content validity across all of its 6 evaluated sub-factors. The items Data Sharing Governance, Data Sharing Policy, Uniformity in Protocols, Security Controls, Regulatory Compliance, and Legal Data Security Applicability all received I-CVI scores of 1.00, demonstrating full agreement on their relevance.

TABLE XII. I-CVI RESULT FOR GOVERNANCE

Factors	Sub-Factor	I-CVI	Accept / Reject
Governance	i. Data sharing governance	1.00	Accept
	ii. Data sharing Policy	1.00	Accept
	iii. Uniformity in protocols	1.00	Accept
	iv. Security controls	1.00	Accept
	v. Regulatory Compliance	1.00	Accept
	vi. Legal Data Security Applicability	1.00	Accept

The findings provide strong evidence that governance is a critical and clearly defined construct within blockchain-based e-government security frameworks.

Table XIII shows the scale level of Content Validity of the main factors and the experts' agreement across all sub-factors in the main factors and the Universal Agreement Result for the main Factors. The result for The S-CVI/UA of confidentiality is 0.89, showing that most, but not all, items achieved universal agreement, but were acceptable based on a minimum score of 0.80. Despite this, the results confirm that confidentiality is broadly supported as a critical security dimension. The findings suggest that while the majority of sub-factors are conceptually robust, specific elements like data sovereignty may require refinement to ensure greater consensus. Nevertheless, the integrity factor achieved an S-CVI/Ave of 0.99 and an S-CVI/UA of 0.93, both exceeding recommended thresholds of 0.80. These results confirm that integrity is a well-validated and indispensable dimension in blockchain-based secure data sharing, encompassing accuracy, reliability, and authenticity of data.

TABLE XIII. S-CVI/UA AND S-CVI/AVE RESULT FOR 9 MAIN FACTORS

Factors	S-CVI/UA	Accept / Reject	S-CVI/Ave	Accept / Reject
Confidentiality	0.89	Accept	0.98	Accept
Integrity	0.93	Accept	0.99	Accept
Availability	1.00	Accept	1.00	Accept
Decentralisation	1.00	Accept	1.00	Accept
Immutability	0.71	Reject	0.95	Accept
Transparency	0.80	Accept	0.97	Accept
Interoperability	1.00	Accept	1.00	Accept
Auditability	1.00	Accept	1.00	Accept
Governance	1.00	Accept	1.00	Accept

Both the S-CVI/Ave (1.00) and the S-CVI/UA (1.00) for availability demonstrate complete alignment across the expert panel, thereby confirming that the availability construct is robustly represented within the measurement framework. The results are consistent with methodological expectations that

universal agreement across multiple experts provides a strong basis for accepting items without revision. At the aggregated level, the decentralised factor validity for both the S-CVI/Ave (1.00) and S-CVI/UA (1.00) indicates complete consistency among the experts. These results suggest that decentralisation is conceptually well-defined and universally recognised by experts as a core attribute of blockchain-driven e-government data sharing.

The overall S-CVI/Ave for Immutability is 0.95, indicating a strong average agreement, yet the S-CVI/UA of 0.71 reveals that the factors did not reach universal consensus, as the minimum score should achieve 0.80. At the scale level, the transparency factor attained an S-CVI/Ave of 0.97, which is well above the recommended threshold, but the S-CVI/UA of 0.80 indicates that universal agreement was achieved at par. At the scale level, the S-CVI/Ave (1.00) and S-CVI/UA (1.00) confirm the consensus across the experts, validating the construct of the interoperability factor as conceptually coherent and practically relevant. The overall S-CVI/Ave (1.00) and S-CVI/UA (1.00) in auditability factors demonstrate perfect consensus at the scale level, indicating that every expert perceived these dimensions as essential elements of auditability. This unanimity is further validated by an S-CVI/Ave of 1.00 and an S-CVI/UA of 1.00, both of which confirm the consensus across the expert panel for the governance factor.

V. Discussion

A. Theoretical Implications

The combined findings from the thematic analysis and content validity assessment offer a meaningful theoretical contribution to the understanding of secure data sharing in the public sector. By synthesising expert insights, the study advances existing knowledge on blockchain-enabled data-sharing systems, uncovering recurring patterns, experiential perspectives, and thematic constructs that inform the validation of security frameworks. The integration of thematic analysis with an empirically driven content validation approach enhances both conceptual coherence and methodological rigour, thereby providing a solid foundation for future theoretical development and scholarly discourse in the field of blockchain-based data sharing.

Consistent with existing literature, the findings of the themes from grounded theory reinforce that trust remains the most prominent concern in blockchain-based data sharing for e-governance. In addition, the study affirms experts' acceptance of key factors such as immutability, interoperability, and governance, all of which are integrated within a cohesive structure. The interconnected nature of these themes strengthens and refines existing theories on blockchain-based data-sharing security. Notably, the identification of accountability and governance as central constructs further enriches theoretical discourse on the application of decentralisation technologies in public administration. In summary, the research addresses a critical gap by offering a theoretically grounded and practice-informed framework for understanding secure data sharing in blockchain-enabled e-government systems.

Complementing these thematic insights, the Content Validity Index (CVI) findings contribute significantly to the refinement and validation of the core constructs underpinning secure data sharing via blockchain in e-government. The confirmation of factors such as confidentiality, integrity, availability, decentralisation, immutability, auditability, interoperability, transparency, and governance adds empirical depth to the theoretical base. As emphasised in the instrument development literature, content validation is essential to ensure that abstract constructs are operationalized with precision and consistency. By incorporating both I-CVI and S-CVI measures, this study enhances methodological rigour and demonstrates how triangulated expert consensus can bridge previously identified methodological gaps. Moreover, the findings reveal nuanced theoretical distinctions, such as the weaker consensus observed in the sub-factors of immutability and transparency which highlight the need for continued theoretical refinement and contextual adaptation of emerging security constructs.

Ultimately, the validated prominence of these security factors reflects a strong expert consensus on the essential requirements for secure data sharing in blockchain-enabled e-government applications. These validated constructs serve as concrete theoretical foundations for understanding and designing secure data-sharing mechanisms in public-sector blockchain systems. By employing both thematic analysis and content validity techniques, this research bridges a notable methodological gap in the literature, offering a robust and rigorous basis for advancing theoretical development in the domain of public sector blockchain security.

B. Practical Implications

Building on prior insights, the integration of thematic analysis and content validity assessment offers an enhanced practical contribution to the implementation of secure data sharing in the public sector. This study advances applied knowledge by preparing the approach from the real-world experiences and expert evaluations of blockchain deployment within public governance contexts. By combining qualitative thematic insights with empirically validated security constructs, the research provides a more robust foundation for guiding the design, development, and operationalization of blockchain-enabled data-sharing solutions.

From a practical perspective, the thematic findings offer actionable insights for policymakers, system architects, and public administrators engaged in data sharing security for digital transformation initiatives. The identification of key themes, confidentiality, integrity, availability, decentralisation, immutability, auditability, interoperability, transparency, and governance provides a framework for designing secure, citizen-centric data sharing systems. Specifically, the findings suggest that the incorporation of decentralisation and auditability mechanisms can significantly enhance data security and institutional trust. This implies that decision-makers should prioritise technologies that support tamper-proof records, controlled access, and transparent data flows. In addition, the emphasis on governance, interoperability, and regulatory compliance underscores the importance of aligning digital systems with legal and administrative policy frameworks. These insights are significantly relevant for e-government platforms where data sovereignty and trust are paramount. Furthermore, the thematic framework can be used as a diagnostic tool for

evaluating the readiness and resilience of secure data-sharing e-government systems.

The validated framework using content validity provides stakeholders and practitioners with a reliable foundation for secure data sharing for e-government systems implementation. The confirmation of strong content validity across most security factors means that decision-makers can draw on a structured set of indicators to guide system architecture, regulatory compliance, and policy development. As has been argued in applied research, the translation of validated constructs into practice enhances the credibility and sustainability of interventions. By identifying universally accepted elements such as data confidentiality, auditability, and interoperability, the study offers practitioners actionable criteria for designing systems that inspire security and trust. At the same time, the partial divergence observed in immutability and transparency highlights areas requiring refinement before operational deployment, ensuring that practical applications remain adaptive and responsive to contextual challenges. Ultimately, the findings strengthen the link between theoretical constructs and real-world design, supporting the creation of blockchain-enabled governance infrastructures that are both secure and citizen-centric.

The validated security factors provide a reliable checklist for designing and evaluating blockchain-based data sharing systems for implementation in the public sector. Emphasising factors like governance and confidentiality can enhance compliance and trust, especially in multi-agency or cross-agency data sharing. The validated item can be directly included in the current blockchain roadmap or data sharing policy to ensure the objective and target for a trusted, secure e-government service can be upheld. For instance, their relevance must be translated effectively to non-technical stakeholders. Thus, the study provides a practical roadmap for implementing secure data-sharing e-government systems in public sector environments.

The BSDSF integrates both traditional information security principles (Confidentiality, Integrity, Availability) and blockchain-specific properties (Decentralisation, Immutability, Transparency, Auditability, Interoperability, Governance). The unique blockchain security properties, particularly immutability, decentralised trust, built-in auditability, and consensus-based integrity, extend beyond the capabilities of traditional distributed databases. These properties make blockchain particularly suitable for secure, multi-agency data sharing in e-government environments, where trust, accountability, and regulatory compliance are critical.

C. Limitations and Future Research

Although the expert panel included a diverse range of perspectives, the relatively small number of experts from the public sector may limit the generalizability of the findings to broader e-government contexts. Moreover, the study primarily assessed the perceived relevance and conceptual clarity of the security factors, rather than evaluating their practical effectiveness in real-world implementations. As such, the operational impact of each factor within live or simulated e-government environments remains unexplored. To strengthen the practical applicability of these findings, future research should consider field-based validation, pilot implementations, or simulation-driven testing to assess how these security constructs perform under actual system conditions. The approaches would provide deeper insight into the usability and contextual applicability of the proposed framework with a suitable, validated, reliable instrument, thereby advancing both theoretical understanding and implementation readiness.

VI. Conclusion

This study set out to conduct methodological triangulation using thematic analysis for qualitative data and Content Validity Index to empirically validate the key security factors that underpin data sharing in blockchain-based e-government applications. Through an open-ended questionnaire interview and a structured content validity approach involving expert evaluation, the research identified a set of high-priority factors: confidentiality, integrity, availability, decentralisation, interoperability, transparency, auditability, and governance that are both relevant and clearly understood across experts. The immutability factors have been accepted as one of the security factors because they have been accepted as important security factors by the expert review interview in thematic analysis.

TABLE XIV. Factors Status

Factors	S-CVI/UA	S-CVI/Ave	Status
Confidentiality	0.89	0.98	Accepted
Integrity	0.93	0.99	Accepted
Availability	1.00	1.00	Strongest Consensus
Decentralisation	1.00	1.00	Strongest Consensus
Immutability	0.71	0.95	Reject / Refine
Transparency	0.80	0.97	Accepted
Interoperability	1.00	1.00	Strongest Consensus
Auditability	1.00	1.00	Strongest Consensus
Governance	1.00	1.00	Strongest Consensus

The key contributions of this study are the integration of traditional information security principles with blockchain-specific security attributes. The BSDSF extends the traditional Confidentiality, Integrity and Availability (CIA) model by incorporating blockchain-specific factors, including decentralisation, transparency, interoperability, auditability, and governance. Based on Table XIV, five factors that is Availability, Decentralisation, Interoperability, Auditability and Governance have the strongest consensus. The Confidentiality, integrity, and transparency are accepted, while the immutability needs to be refined. Interestingly, while immutability is a core blockchain feature, it failed the Universal Agreement (UA) threshold ($S-CVI/UA < 0.80$). This suggests experts have diverging views on how "permanent" data should be in a government context, possibly due to "right to be forgotten" regulations or data correction needs.

The thematic analysis revealed that Trust was the most frequently quoted code (74 quotes), highlighting that technology alone is insufficient without institutional and interpersonal trust. The research also provides evidence-based framework development through multi-method validation. The blockchain

frameworks are proposed, derived from a multi-method research design involving:

- Systematic Literature Review (SLR) to identify security factors.
- Thematic analysis to synthesise conceptual constructs.
- Expert validation using Content Validity Index (CVI).

The framework offers a holistic perspective that bridges the gap between information security theory and distributed ledger technology.

By applying the Item Content Validity Index (I-CVI) and Scale Content Validity Index (S-CVI) methodology, the study enhances the methodological rigour of information systems research and provides a replicable framework for future validation efforts. In summary, this study not only refines the conceptual landscape of blockchain security in e-government but also lays the groundwork for more secure, transparent, and citizen-centric digital governance. Based on the above approach, we can conclude that the thematic analysis with content validity index of I-CVI, S-CVI/Ave, and S-CVI/UA has met a satisfactory level of content validity.

REFERENCES

[1] Z. Shan, X. Chen, Y. Zhang, Y. He, and D. Wang, "Exploration and Practice of Constructing Trusted Public IT Systems Using Blockchain-Based Service Network," Tsinghua Sci. Technol., vol. 30, no. 1, pp. 124–134, Sep. 2024, doi: 10.26599/tst.2023.9010159.

[2] G. Niu, "Evaluation of Blockchain-Based Tracking and Tracing System With Uncertain Information: A Multi-Criteria Decision-Making Approach," IEEE Access, vol. 13, pp. 40795–40812, 2025, doi: 10.1109/ACCESS.2025.3546275.

[3] S. Prabowo et al., "Privacy-Preserving Tools and Technologies: Government Adoption and Challenges," 2025, Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ACCESS.2025.3540878.

[4] X. Zhang, T. Chen, Y. Feng, and Y. Yu, "A Data Sharing Scheme Based on Blockchain System and Attribute-Based Encryption," in ACM International Conference Proceeding Series, Association for Computing Machinery, Mar. 2021, pp. 195–202. doi: 10.1145/3460537.3460559.

[5] S. F. Wamba, S. L. Wamba-Taguimdje, Q. Lu, and M. M. Queiroz, "How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector," Gov. Inf. Q., vol. 41, no. 1, Mar. 2024, doi: 10.1016/j.giq.2024.101912.

[6] B. Rukanova et al., "Realizing value from voluntary business-government information sharing through blockchain-enabled infrastructures: The case of importing tires to the Netherlands using TradeLens," in ACM International Conference Proceeding Series, Association for Computing Machinery, Jun. 2021, pp. 505–514. doi: 10.1145/3463677.3463704.

[7] MyCERT, "MyCERT _ Advisories - Cyber Incident Quarterly Summary Report - Q1 2025," 2025, Accessed: Jul. 04, 2025. [Online]. Available: https://www.mycert.org.my/portal/advisory?id=SR-030.062025

[8] O. Konashevych, "Cross-blockchain protocol for public registries," International Journal of Web Information Systems, vol. 16, no. 5, pp. 571–610, Nov. 2020, doi: 10.1108/IJWIS-07-2020-0045.

[9] A. Z. A. Aljarwan and M. A. Bin Ngadi, "Review of Certificateless Authentication Scheme for Vehicular Ad Hoc Networks," IEEE Access, vol. 13, pp. 100074–100094, 2025, doi: 10.1109/ACCESS.2025.3576926.

[10] N. Ilyana Ismarau Tajuddin et al., "Content Validity Assessment Using Aiken's V: Knowledge Integration Model for Blockchain in Higher Learning Institutions," 2025. [Online]. Available: www.ijacsa.thesai.org

[11] F. Yahya, "A Security Framework to Protect Data in Cloud Storage [Doctoral Dissertation, University of Southampton]," UNIVERSITY OF SOUTHAMPTON, 2017. Accessed: Feb. 01, 2021. [Online]. Available: https://eprints.soton.ac.uk/415861/

[12] Y. Cao, "Research on the Application of Blockchain Technology in the Security Protection of Sensitive Data in Information Systems," Journal of Mobile Multimedia, vol. 14, no. 1, pp. 205–228, 2025, doi: 10.13052/jcsm2245-1439.1419.

[13] S. Capraz and A. Ozsoy, "A Secure Medical Data Sharing Framework for Fight Against Pandemics Like Covid-19 by Using Public Blockchain," IEEE Access, vol. 12, pp. 93593–93605, 2024, doi: 10.1109/ACCESS.2024.3423714.

[14] A. Azmi, F. Yahya, E. G. Moung, H. Sallehudin, R. G. Utomo, and N. A. Azman, "Blockchain-based Data Sharing Framework for Malaysia Government Aid Management System," in 2023 International Conference on Digital Applications, Transformation and Economy, ICDATE 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICDATE58146.2023.10248471.

[15] J. Clavin et al., "Blockchains for Government: Use Cases and Challenges," Digit. Gov.: Res. Pract., vol. 1, no. 3, Nov. 2020, doi: 10.1145/3427097.

[16] I. Lykidis, G. Drosatos, and K. Rantos, "The use of blockchain technology in e-government services," Dec. 01, 2021, MDPI. doi: 10.3390/computers10120168.

[17] S. Sriram, P. R. Tharaniesh, P. Saraf, N. Vijayaraj, and T. Murugan, "Enhancing Digital Identity and Access Control in Event Management Systems Using Sui Blockchain," IEEE Access, vol. 13, pp. 24295–24308, 2025, doi: 10.1109/ACCESS.2025.3539107.

[18] C. B. Basha et al., "Fostering Effective Cyber Threat Intelligence Sharing: Overcoming Challenges and Implementing Best Practices," in International Conference for Technological Engineering and its Applications in Sustainable Development, ICTEASD 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 177–182. doi: 10.1109/ICTEASD57136.2023.10585133.

[19] F. Mureddu, J. Schmeling, and E. Kanellou, "Research challenges for the use of big data in policy-making," Nov. 23, 2020, Emerald Group Holdings Ltd. doi: 10.1108/TG-08-2019-0082.

[20] C. S. Sung and J. Y. Park, "Understanding of blockchain-based identity management system adoption in the public sector," Journal of Enterprise Information Management, vol. 34, no. 5, pp. 1481–1505, Nov. 2021, doi: 10.1108/JEIM-12-2020-0532.

[21] L. D. Nguyen, J. Hoang, Q. Wang, Q. Lu, S. Xu, and S. Chen, "BDSP: A Fair Blockchain-enabled Framework for Privacy-Enhanced Enterprise Data Sharing," in 2023 IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICBC56567.2023.10174943.

[22] A. Bounceur, A. S. Berkani, H. Moumen, and S. Benharzallah, "The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms," IEEE Access, vol. 13, pp. 81769–81793, 2025, doi: 10.1109/ACCESS.2025.3567341.

[23] OWASP, "OWASP data security top 10," 2023. Accessed: Mar. 18, 2026. [Online]. Available: https://github.com/OWASP/www-project-data-security-top-10/blob/main/tab_Top-10.md

[24] J. Dai, J. Yang, Y. Wang, and Y. Xu, "Blockchain-Enabled Cyber-Resilience Enhancement Framework of Microgrid Distributed Secondary Control Against False Data Injection Attacks," IEEE Trans. Smart Grid, vol. 15, no. 2, pp. 2226–2236, Mar. 2024, doi: 10.1109/TSG.2023.3328383.

[25] A. Rashid, A. Masood, and A. ur R. Khan, "RC-AAM: blockchain-enabled decentralized role-centric authentication and access management for distributed organizations," Cluster Comput., vol. 24, no. 4, pp. 3551–3571, Dec. 2021, doi: 10.1007/s10586-021-03352-x.

[26] V. Reniers et al., "Authenticated and auditable data sharing via smart contract," in Proceedings of the ACM Symposium on Applied Computing, Association for Computing Machinery, Mar. 2020, pp. 324–331. doi: 10.1145/3341105.3373957.

[27] L. Al-Abbasi and W. El-Medany, "Blockchain Security Architecture: A Review on Technology Platform, Security Strength and Weakness," 2019.

[28] S. Kumarswamy and P. Athikatte Sampigerayappa, "Securing patient data and access control in electronic health records with Ethereum blockchain," Bulletin of Electrical Engineering and Informatics, vol. 14, no. 4, pp. 3037–3051, Aug. 2025, doi: 10.11591/eei.v14i4.9524.

[29] A. Azmi, F. Yahya, N. A. Azman, and H. Jalil, "Secure Data Sharing Using Blockchain Technology: A Systematic Literature Review," 2025. [Online]. Available: www.ijacsa.thesai.org

[30] K. Proudfoot, "Inductive/Deductive Hybrid Thematic Analysis in Mixed Methods Research," J. Mix. Methods Res., vol. 17, no. 3, pp. 308–326, Jul. 2023, doi: 10.1177/15586898221126816.

[31] M. N. Mohd Noor et al., "Developing a framework for medical student feedback literacy using a triangulated thematic analysis," Ann. Med., vol. 57, no. 1, 2025, doi: 10.1080/07853890.2025.2520395.

[32] B. Nowrouzi-Kia et al., "Functional work disability from the perspectives of persons with systemic lupus erythematosus: a qualitative thematic analysis," Arthritis Res. Ther., vol. 27, no. 1, Dec. 2025, doi: 10.1186/s13075-025-03572-1.

[33] K. F. Oguntegbe, N. Di Paola, and R. Vona, "Behavioural antecedents to blockchain implementation in agrifood supply chain management: A thematic analysis," Technol. Soc., vol. 68, Feb. 2022, doi: 10.1016/j.techsoc.2022.101927.

[34] M. H. Rahman, W. Yeoh, and S. Pal, "Exploring factors influencing blockchain adoption's effectiveness in organizations for generating business value: a systematic literature review and thematic analysis," Enterp. Inf. Syst., vol. 18, no. 8, 2024, doi: 10.1080/17517575.2024.2379830.

[35] S. Handage and M. Chander, "Development of An Instrument for Measuring the Student Learning Outcomes: A Content Validation Process," Indian Journal of Extension Education, vol. 57, no. 03, pp. 01–07, 2021, doi: 10.48165/ijee.2021.57302.

[36] J. M. Morse, "Approaches to qualitative-quantitative methodological triangulation," Nurs. Res., vol. 40, no. 2, pp. 120–123, 1991, doi: 10.1097/00006199-199103000-00014.

[37] J. Rattray and M. C. Jones, "Essential elements of questionnaire design and development," Feb. 2007. doi: 10.1111/j.1365-2702.2006.01573.x.

[38] N. Golafshani, "Understanding Reliability and Validity in Qualitative Research," 2003. [Online]. Available: http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

[39] M. Naeem, W. Ozuem, K. Howell, and S. Ranfagni, "A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research," Int. J. Qual. Methods, vol. 22, Jan. 2023, doi: 10.1177/16094069231205789.

[40] K. Fuchs, "A Systematic Guide for Conducting Thematic Analysis in Qualitative Tourism Research," Journal of Environmental Management and Tourism, vol. XIV, no. 5(69), 2023, doi: 10.14505/jemt.

[41] V. Braun and V. Clarke, "Using thematic analysis in psychology," Qual. Res. Psychol., vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.

[42] M. S. B. Yusoff, "ABC of Content Validation and Content Validity Index Calculation," Education in Medicine Journal, vol. 11, no. 2, pp. 49–54, Jun. 2019, doi: 10.21315/eimj2019.11.2.6.