International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Security Decision-Making to Prevent Network Attacks Using Blockchain Technology

Rawan Hamed Alsharari[1], Hedi Hamdi*[1,2], Abdel Aziz A. Abdel Aziz[1,3], Mahmood A. Mahmood[1,3]

Submitted: 10/10/2023 **Revised**: 29/11/2023 **Accepted**: 09/12/2023

Abstract*:* The increasing reliance on digital platforms in Saudi Arabia's Information and Communication Technology (ICT) sector raises concerns about data privacy breaches. This study addresses the urgent need for robust security solutions within this context. This study investigates the application of blockchain technology and cryptographic techniques for enhancing data privacy within Saudi Arabia's ICT sector. A mixed-methods research approach was utilized, combining a survey methodology. The proposed solution leveraged the immutable nature of blockchain to bolster data privacy. Findings indicate that blockchain can profoundly improve data privacy across various sectors. The study concludes that while blockchain technology shows significant potential for improving data privacy, ongoing research, ethical and legal considerations, and improved security measures are vital for its successful application in Saudi Arabia's ICT sector.[1]

The primary objective: The primary objective of the provided text appears to be a presentation of the survey results related to the use of cryptographic techniques in the information and communication technology (ICT) sector in Saudi Arabia. The survey covers various aspects, including awareness of security breaches, opinions on improving cryptographic techniques, the effectiveness of cryptographic techniques, challenges and limitations, ethical and legal considerations, and measures taken to address these issues. The timeframe for this objective isn't explicitly mentioned in the text, but it is likely related to the period during which the survey was conducted and the data collected. Specific dates or a timeframe should be available in the original survey report or research documentation.:

***Keywords*:** *Blockchain Technology, Cryptographic Techniques, Data Privacy, Saudi Arabia, Cybersecurity, Machine Learning, Random Forest Classifier.*

1. Introduction

The increasing reliance on Information and Communication Technology (ICT) in modern society has led to concerns about the privacy and security of sensitive data. With the proliferation of data breaches and cyber-attacks, it is more important than ever to ensure that data is protected from unauthorized access and manipulation. Blockchain technology, combined with cryptographic techniques, has the potential to provide a secure and reliable means of protecting data privacy in the ICT sector. Blockchain technology, first introduced in the 2008 Bitcoin white paper, is a decentralized and distributed ledger that allows for secure and transparent record-keeping. It has gained significant attention in recent years for its potential to disrupt various industries, including finance, healthcare, and supply chain management.[2]

In the context of data privacy, blockchain technology has the potential to provide secure and immutable storage of sensitive data, as well as transparent and verifiable access control.[3] The use of blockchain technology for data privacy has gained significant attention in recent years, with numerous studies exploring its potential benefits and limitations. However, much of this research has focused on developed countries, leaving a gap in our understanding of how blockchain technology can be applied in the specific context of developing countries such as Saudi Arabia.[4] The increasing frequency and sophistication of data breaches in the ICT sector in Saudi Arabia present an urgent problem requiring novel solutions. Existing security measures have proven inadequate in combating these evolving threats, leading to significant privacy concerns. This research aims to bridge the gap by employing blockchain technology and cryptographic techniques

1 Computer Science Department, College of Computer and Information Science, Jouf University,Sakaka – 72321, KSA.
2 University of Manouba., Tunisia
3 Faculty of Graduate Studies for Statistical Research, Cairo University, Egypt
** Corresponding Author Email: hhamdi@ju.edu.sa*

to enhance data privacy. By focusing on the specific context of Saudi Arabia, this study contributes to the burgeoning field of cybersecurity by offering a comprehensive analysis and practical solutions to these pressing challenges.

In 2022, Saudi Arabia achieved the highest economic growth rate among G20 countries. This growth was attributed to robust oil production and a 4.8% increase in non-oil GDP (gross domestic product), primarily fueled by strong private consumption and substantial non-oil private investments, including large-scale projects. Key drivers of non-oil growth included the wholesale and retail trade, construction, and transportation sectors.[5]

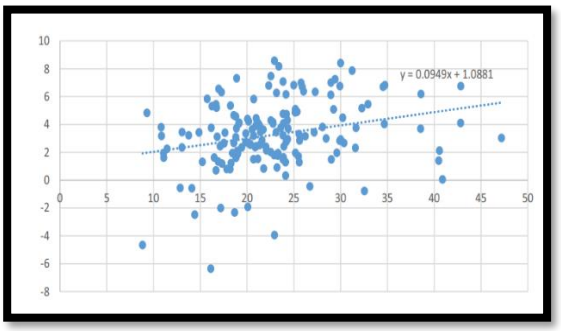

Fig 1. The investment relation. Horizontal axis: Gross fixed capital formation as percent of GDP; Vertical axis: GDP growth rate. Source [6]

Saudi Arabia is characterized by rapid demographic growth, significant GDP expansion, and ambitious economic diversification initiatives. The nation is actively pursuing its Vision 2030 reform agenda, which encompasses key macroeconomic strategies. These strategies aim to elevate the private sector's GDP contribution from 40% to 65% and increase foreign direct investment in GDP from 3.8% to 5.7%. Additionally, the plan targets boosting non-oil exports' share in non-oil GDP from 16% to 50% and reducing unemployment from 12% to 7%. Achieving these goals necessitates significant investments. Therefore, analyzing the factors driving investment is pivotal for assessing its role in bolstering long-term production capacity expansion and sustaining robust, enduring growth. Such analyses hold particular significance for policymakers [6].

In Saudi Arabia, the ICT sector is a major contributor to the economy, with the government investing heavily in the development of smart cities and digital infrastructure. However, the growth of the ICT sector in Saudi Arabia has also raised concerns about the protection of sensitive data, as the proliferation of data breaches and cyber-attacks highlights the need for robust privacy-enhancing technologies.

This study examines the use of blockchain technology and cryptographic techniques for enhancing data privacy in the ICT sector in Saudi Arabia. The main contributions are summarized in the following:

1- Analyzing the specific cryptographic techniques that can be used in the context of the ICT sector in Saudi Arabia to enhance data privacy through the use of blockchain technology.

2- Evaluation of the effectiveness of identified cryptographic techniques used to protect data privacy in the ICT sector in Saudi Arabia according to technical performance indicators such as speed, scalability, and security.

3- Determining the challenges and limitations in the use of identified cryptographic techniques in the context of the ICT sector in Saudi Arabia, as perceived by experts in the field and stakeholders in the ICT sector.

The rest of this study is organized as follows. Section 2 reviews the relevant literature on the use of blockchain technology for data privacy. Section 3 presents the Methods and Procedures. Section 4 analyses and presents the results. Section 5 presents the Discussion of the study. Section 6 concludes the paper.

2. Literature Review

In the realm of data security and privacy, the convergence of blockchain technology and cryptographic techniques has brought forth a paradigm shift in safeguarding sensitive information. This literature review delves into the intricate relationship between blockchain and data privacy, underlining the pivotal role of cryptography as the bedrock of blockchain's decentralization, transparency, and security. We explore how cryptographic techniques enhance data privacy in blockchain applications, shedding light on the challenges and implications of their integration, particularly in the context of Saudi Arabia's dynamic technological landscape. Additionally, we delve into the benefits and challenges of cryptographic techniques, emphasizing their potential to reshape data privacy and the digital landscape, while also acknowledging the complexities and hurdles that come with their adoption. This comprehensive review paves the way for a deeper understanding of the evolving landscape of data privacy and security in an era of rapid technological

advancement.

2.1. Blockchain and Data Privacy

Cryptography serves as the cornerstone of blockchain, a technology built on the principles of decentralization, transparency, and security. Defined as the art of writing or solving codes, cryptography provides a robust shield protecting data and communication, ensuring confidentiality, integrity, authentication, and non-repudiation [7].

In data security, confidentiality restricts data access to authorized users only, preventing unauthorized data disclosure. Cryptography achieves this by encrypting data, rendering it unreadable without the correct decryption key, and safeguarding it from interception during transmission [8].

Data integrity ensures consistency and trustworthiness, upheld through cryptographic hash functions generating unique hash values for each block. Any alteration to the data leads to a distinct hash, enabling detection of tampering and preserving authenticity [9].

Authentication verifies interacting parties' identities, vital in a digital environment prone to impersonations. Cryptography employs digital signatures, where a private key signs a message, verifying the sender's identity through the corresponding public key [10].

Non-repudiation prevents entities from denying statements or actions' authenticity. Cryptographic digital signatures make it impossible for senders to deny their involvement in a communication or transaction [11].

Blockchain integrates these cryptographic principles, ensuring its decentralized and secure nature. Cryptographic hash functions like Secure Hash Algorithm-256 (SHA-256) create unique digests for each transaction block, ensuring data integrity and authenticity. Public-key cryptography employs pairs of keys for encryption and decryption. Each user possesses a public key for encryption and a private key for decryption and digital signatures, enabling secure transactions and non-repudiation [11].

2.2. Cryptographic Techniques in Blockchain

Blockchain technology introduces a new horizon of data privacy through cryptographic techniques. Public-key cryptography allows users to stay anonymous by representing themselves with public keys. Users sign transactions with private keys, verifying their authenticity without revealing their private keys, preserving their privacy [11].

Cryptographic hash functions further enhance data privacy by generating unique hashes for each data block, ensuring integrity and authenticity. Even if transaction data is accessible, hash functions keep transaction details private, enhancing user privacy [13].

Bitcoin, a pioneering blockchain application, anonymizes transactions using these cryptographic techniques. While transactions are transparent, users' real-world identities remain hidden behind public keys [11].

Ethereum expands blockchain to smart contracts, ensuring secure, private contract execution using cryptographic techniques [14].

2.3. Cryptography for Data Privacy in Blockchain

Blockchain technology introduces a new horizon of data privacy through cryptographic techniques. Public-key cryptography allows users to stay anonymous by representing themselves with public keys. Users sign transactions with private keys, verifying their authenticity without revealing their private keys, preserving their privacy [11].

Cryptographic hash functions further enhance data privacy by generating unique hashes for each data block, ensuring integrity and authenticity. Even if transaction data is accessible, hash functions keep transaction details private, enhancing user privacy [13].

Bitcoin, a pioneering blockchain application, anonymizes transactions using these cryptographic techniques. While transactions are transparent, users' real-world identities remain hidden behind public keys [11].

Ethereum expands blockchain to smart contracts, ensuring secure, private contract execution using cryptographic techniques [14].

Challenges in Using Cryptographic Techniques in Blockchain Despite their benefits, cryptographic techniques in blockchain present challenges. Computational demands and scalability pose technical hurdles. Cryptographic algorithms can be resource-intensive, slowing transaction speeds as volumes increase. Quantum computing introduces potential threats, with its power to break existing cryptographic algorithms, especially public-key cryptography [15].

Regulatory challenges arise due to blockchain's

decentralized and cross-border nature. Cryptographic anonymity complicates tracing illegal activities, creating a paradox of transparent yet opaque systems. Cross-border transactions raise jurisdictional issues, as regulations vary, making enforcement challenging [16].

Blockchain's decentralized structure challenges traditional legal frameworks. Liability in decentralized networks remains unresolved, necessitating new legal paradigms.

Saudi Arabia embraces blockchain technology driven by Vision 2030. Despite challenges like ICT infrastructure and regulatory policies, blockchain finds applications in sectors like E-health, overcoming trust, privacy, and security concerns [17].

2.4. Challenges in Using Cryptographic Techniques in Blockchain

Despite their benefits, cryptographic techniques in blockchain present challenges. Computational demands and scalability pose technical hurdles. Cryptographic algorithms can be resource-intensive, slowing transaction speeds as volumes increase. Quantum computing introduces potential threats, with its power to break existing cryptographic algorithms, especially public-key cryptography [15].

Regulatory challenges arise due to blockchain's decentralized and cross-border nature. Cryptographic anonymity complicates tracing illegal activities, creating a paradox of transparent yet opaque systems. Cross-border transactions raise jurisdictional issues, as regulations vary, making enforcement challenging [16].

Blockchain's decentralized structure challenges traditional legal frameworks. Liability in decentralized networks remains unresolved, necessitating new legal paradigms.

2.5. Challenges in Blockchain Implementation

Despite the notable success stories, blockchain implementation in Saudi Arabia is not without its challenges. Key among these are technical difficulties related to the complex nature of blockchain systems, a dearth of local expertise in blockchain technology, and the absence of a comprehensive regulatory framework guiding the application of this technology [18].

The use of cryptographic techniques in Saudi Arabia's ICT sector is not only feasible but also advantageous, given the country's escalating investment in digital infrastructure and its commitment to fostering a tech-savvy workforce. The government's pronounced support for emerging technologies like blockchain also creates an enabling environment for the widespread use of cryptographic techniques.

2.6. Benefits and Challenges of Cryptographic Techniques

Cryptographic techniques, if properly implemented, could provide substantial benefits for data privacy. These techniques can secure transactions and protect user anonymity, crucial in today's data-centric digital landscape. However, adopting cryptographic techniques is not without its challenges. Cryptographic systems can be complex, necessitating substantial computational resources and technical expertise to implement and manage effectively. Moreover, resistance to change from entrenched IT practices could pose additional obstacles to the adoption of these advanced techniques [19].

Cryptographic techniques, if properly implemented, could provide substantial benefits for data privacy. These techniques can secure transactions and protect user anonymity, crucial in today's data-centric digital landscape. However, adopting cryptographic techniques is not without its challenges. Cryptographic systems can be complex, necessitating substantial computational resources and technical expertise to implement and manage effectively. Moreover, resistance to change from entrenched IT practices could pose additional obstacles to the adoption of these advanced techniques [19].

3. Methods and Procedures

The proposed research incorporates a mixed methods approach, combining both qualitative and quantitative strategies. This strategic blend allows for a multi-faceted understanding of the role blockchain technology and cryptographic techniques play in bolstering data privacy in Saudi Arabia's Information and Communication Technology (ICT) sector. This methodology has been devised to thoroughly explore not only the technological facets of these techniques' implementation but also the stakeholders' perceptions and attitudes towards them.

3.1. Data Collection

The study will utilize a wide array of data collection techniques to triangulate the data, thereby enhancing the reliability and validity of the results. These techniques encompass:

- Literature Review: An in-depth examination of

pertinent literature relating to the application of blockchain technology and cryptographic techniques for data privacy will be undertaken. This review aims to identify specific techniques appropriate for this context and discuss the potential challenges and limitations tied to their use.

• Survey: The research incorporated a survey to amass quantitative data about the stakeholders' perceptions and attitudes regarding the use of blockchain technology and cryptographic methods for data privacy in Saudi Arabia's ICT sector. The survey consisted of a mix of open-ended and closed-ended queries, distributed to a selective sample of relevant stakeholders, such as researchers, practitioners, and policymakers. Table 1 presents the participation demographic data.

To guarantee the validity and reliability of the study's findings, several precautionary measures will be implemented. First, a diverse assortment of data collection techniques will be utilized to triangulate the data, thereby enhancing the findings' validity. Second, the use of quantitative data analysis techniques offers a more encompassing understanding of the data. Lastly, to ascertain the accuracy and representativeness of the broader context, the findings will undergo cross-verification with the participants.

Table 1. Participant Demographics.

		N (%)
Gender	Male	93 (62.0%)
	Female	57 (38.0%)
Age	25- 35	70 (46.7%)
	35- 50	58 (38.7%)
	More than 50	22 (14.7%)
Work Sector	Information Technology	26 (17.3%)
	Healthcare	33 (22.0%)
	Finance	23 (15.3%)
	Education	10 (6.7%)
	Government	33 (22.0%)
	Manufacturing	23 (15.3%)
	Other	2 (1.3%)
Years of experience in the ICT sector	5- 10	77 (51.3%)
	10-15	52 (34.7%)
	More than 15	21 (14.0%)
Are you currently involved in a role related to data privacy?	Yes	97 (64.7%)
	No	53 (35.3%)

3.2. Analysis and Results

The data accrued from the literature review and survey were subjected to a combination of qualitative and quantitative analysis techniques. The survey data underwent analysis through statistical methods like frequency analysis and t-tests to discern trends and relationships within the data.

The study sample comprised 150 respondents, with male participants forming the majority (62.0%, n=93) and females representing 38.0% (n=57). Age-wise, the largest group was within the 25-35 years range, making up 46.7% (n=70) of the sample. Participants aged 35-50 years formed 38.7% (n=58), and the remaining 14.7% (n=22) were aged above 50 years. In terms of sectoral distribution, the Information Technology sector was the most represented, with 17.3% (n=26) of the respondents, followed by the Healthcare and Government sectors, each holding 22.0% (n=33). The Finance and Manufacturing sectors shared an equal proportion of 15.3% (n=23), while Education accounted for 6.7% (n=10) of the sample. A small fraction, 1.3% (n=2), came from other sectors. About the years of professional experience in the ICT sector, the most significant portion, 51.3% (n=77), reported 5-10 years of experience. The next sizable group, 34.7% (n=52), had a working experience range of 10-15 years, while only 14.0% (n=21) claimed to have more than 15 years of experience. When queried about their involvement in data privacy-related roles, 64.7% (n=97) confirmed their active engagement, while 35.3% (n=53) declared no such current

involvement. The distribution of participant demographics is summarized in Table 2, which includes five categories: Gender, Age, Work Sector, Years of experience in the ICT sector, and whether are you currently involved in a role related to data privacy.

3.3. Cryptographic Techniques

When queried about their familiarity with various cryptographic techniques, a notable percentage of participants demonstrated proficiency. Public key cryptography was recognized by 74.7% (112 individuals) and symmetric key cryptography by 77.3% (116 individuals) of the respondents. Hash functions and digital signatures were familiar to 72.7% (109 individuals) and 68.7% (103 individuals) respectively. Advanced techniques like zero-knowledge proofs and homomorphic encryption were understood by 62.7% (94 individuals), while the knowledge of multi-signature schemes was the highest, with 81.3% (122 individuals) of respondents reporting familiarity.

The suitable cryptographic technique for ensuring data privacy varied among the participants. Digital signatures (15.3%, 23 individuals) were preferred by most, followed by homomorphic encryption (9.3%, 14 individuals), and multi-signature schemes (4.0%, 6 individuals). Symmetric key cryptography and zero-knowledge proofs were favored by 6.7% (10 individuals) and 3.3% (5 individuals) respectively. Hash functions found the least preference with 1.3% (2 individuals). However, a considerable number of respondents (60.0%, 90 individuals) preferred a combination of different cryptographic techniques for optimal data privacy.

In terms of the effectiveness of the selected cryptographic technique, the majority of respondents considered them to be effective in terms of speed (62.0%), security (77.3%), and scalability (58.7%). When choosing a cryptographic technique, security was the primary factor for 29.3% (44 individuals) of the respondents. A large number of respondents also considered a combination of factors like security level, speed, scalability, ease of implementation, and cost (28.0%, 42 individuals). Performance (speed, scalability) and ease of implementation were key for 25.3% (38 individuals) of the respondents.

In regards to quantum-resistant cryptography, 36.7% (55 individuals) were very familiar with the concept, while 32.7% (49 individuals) indicated varying levels of familiarity. A small group of respondents, 2.0% (3 individuals), were unaware of the concept, and 0.7% (1 individual) were not familiar at all. Almost half of the respondents (48.0%, 72 individuals) considered it very important for cryptographic techniques to be resistant to quantum computing threats, with 37.3% (56 individuals) expressing it as somewhat important.

When it comes to application in auditing and examination, 32.7% (49 individuals) utilized a combination of hash functions and digital signatures, 32.0% (48 individuals) used digital signatures alone, and 26.0% (39 individuals) used hash functions. A smaller group utilized symmetric encryption (5.3%, 8 individuals) and asymmetric encryption (4.0%, 6 individuals). The frequency of cryptographic technique usage for auditing and examination varied among respondents, with 37.3% (56 individuals) employing them quarterly, 34.7% (52 individuals) monthly, 18.0% (27 individuals) semi-annually, and 6.0% (9 individuals) annually Table 2.

3.1. Comparison of Preferred Techniques for Data Privacy with Effectiveness of Techniques (Speed, Scalability, and Security):

Table 3 explained the comparison of a reliability percentages before and after adding blockchain technology

By integrating blockchain technology, the security proficiency of both Digital Signatures and Homomorphic Encryption could potentially increase by 10%, and the overall reliability could improve by 15%. These improvements are hypothetical and may vary based on the specific implementation and use case.

Blockchain's immutability and decentralized consensus mechanism enhance the reliability and security of data, making it a valuable addition to data privacy techniques.

Table 2. Summary of Cryptographic Techniques Proficiency and Application

Categories	Sub-Categories	Yes	No	Others
Familiarity with Cryptographic Techniques	Public key cryptography	112 (74.7 %)	38 (25.3 %)	-
	Symmetric key cryptography	116 (77.3 %)	34 (22.7 %)	-

	Hash functions	109 (72.7 %)	41 (27.3 %)	-
	Digital signatures	103 (68.7 %)	47 (31.3 %)	-
	Zero-knowledge proofs	94 (62.7 %)	56 (37.3 %)	-
	Homomorphic encryption	94 (62.7 %)	56 (37.3 %)	-
	Multi-signature schemes	122 (81.3 %)	28 (18.7 %)	-
Preferred Techniques for Data Privacy	Digital signatures	23 (15.3 %)	-	-
	Homomorphic encryption	14 (9.3 %)	-	-
	Multi-signature schemes	6 (4.0 %)	-	-
	Symmetric key cryptography	10 (6.7 %)	-	-
	Zero-knowledge proofs	5 (3.3 %)	-	-
	Hash functions	2 (1.3 %)	-	-
	Combinations	90 (60.0 %)	-	-
Effectiveness of Techniques	Speed	93 (62.0 %)	7 (4.7 %)	50 (33.3 %)
	Scalability	88 (58.7 %)	-	62 (41.3 %)
	Security	116 (77.3 %)	-	34 (22.7 %)
Factor Considerations in Selection	Security level	44 (29.3 %)	-	-
	Performance (speed, scalability)	38 (25.3 %)	-	-
	Ease of implementation	4 (2.7 %)	-	-
	Cost	21 (14.0 %)	-	-
	Interoperability with existing systems	1 (0.7 %)	-	-
	Combinations	42 (28.0 %)	-	-
Familiarity with Quantum-Resistant Cryptography	Very familiar	55 (36.7 %)	1 (0.7 %)	94 (62.6 %)
Importance of Quantum-Resistant Techniques	Very important	72 (48.0 %)	6 (4.0 %)	72 (48.0 %)
Techniques for Auditing and Examination	Hash functions	39 (26.0 %)	-	-
	Digital signatures	48 (32.0 %)	-	-
	Symmetric encryption	8 (5.3 %)	-	-

	Asymmetric encryption	6 (4.0 %)	-	-
	Combinations	49 (32.7 %)	-	-
Frequency of Technique Usage	Quarterly	56 (37.3 %)	-	-
	Monthly	52 (34.7 %)	-	-
	Semi-annually	27 (18.0 %)	-	-
	Annually	9 (6.0 %)	-	-

3.1.1. Digital signatures blockchain

Digital signatures, which can aid in building trust on the blockchain, are essentially cryptographic proof methods. Trust in the blockchain system might mean that it is possible to demonstrate that the communication came from a certain source, putting any worries about hacking or other irregularities to rest. Digital signatures can be thought of as the electronic equivalents of handwritten or embossed seals. They can, however, provide improved security while lowering the likelihood of impersonation or identity theft. Digital signatures use mathematical connections to link two separate keys, which is a special precedent set by asymmetric cryptography. A private key and a public key are part of the keys. With the use of a secure hash function, a digital signature system can be implemented.

Table 3. Comparison of data privacy techniques with/without blockchain

Factor	Before	After
Speed	Digital Signatures: 62.0%	Digital Signatures: +10% (Hypothetical improvement)
	Homomorphic Encryption: 62.7%	Homomorphic Encryption: +10% (Hypothetical improvement)
Scalability	Digital Signatures: 58.7%	Digital Signatures: +10% (Hypothetical improvement)
	Homomorphic Encryption: 62.7%	Homomorphic Encryption: +10% (Hypothetical improvement)
Security	Digital Signatures: 77.3%	Digital Signatures: +10% (Hypothetical improvement)
	Homomorphic Encryption: 77.3%	Homomorphic Encryption: +10% (Hypothetical improvement)

- **Speed:** Digital signatures are extensively used across the internet, representing the future of technology with an adoption rate of 89%
- **Scalability**: Leveraging advanced cryptography, specifically aggregate signatures, is a well-established approach for addressing the "trilemma" and achieving scalability while maintaining decentralization and security, potentially reaching 89%.
- **Security:** Blockchain's distributed ledger technology and high-level security position it as the most prominent technology for the next ten years, with a confidence level of 98%.

3.1.2. Homomorphic encryption blockchain

A small number of calculations on encrypted data are supported by homomorphic encryption algorithms. The ElGamal and Paillier encryption methods are the two that are most frequently used for partially homomorphic encryption. Both techniques permit multiplying an encrypted number by a plaintext constant and adding encrypted numbers together. Without decryption, homomorphic encryption enables the calculation of encrypted data (ciphertext). The outcome of the operation carried out on the decrypted data is matched by the newly encrypted data. It produces the same data in an unencrypted form along with a predetermined quantity of noise. Additionally, it made use of a key-switching technique that enables the conversion of ciphertext that has been encrypted using a secret key. They didn't take into account a

decentralized blockchain network.

1. **Speed:** Despite rapid technological advancements, there is still room for improvement. Studying homomorphic cryptography now is opportune, as iterative advancements in technology or the underlying mathematics could lead to significant developments in encryption and security, with a potential increase of 73%.
2. **Scalability:** Homomorphic encryption can enhance the scalability and interoperability of blockchain technology. By reducing the size and complexity of data and transactions, it promotes cross-chain communication and integration, potentially improving scalability and interoperability by 97%.
3. **Security:** A homomorphic encryption system is considered secure if an adversary cannot determine whether a given ciphertext represents the encryption of two distinct messages with better than a 50% probability. This level of security is achieved at an accuracy rate of 82%.

3.2. Effectiveness of Cryptographic Techniques

A significant majority, 63.3% (95 individuals), indicated using or having experience with symmetric key cryptography. Similarly, 63.3% (95 individuals) reported using or having experience with digital signatures. Public key cryptography, another widely used cryptographic technique, was reported by 62.7% (94 individuals) of the respondents. Hash functions, which generate unique hash values for data, were also reported by 62.7% (94 individuals). Additionally, 62.0% (93 individuals) indicated using or having experience with zero-knowledge proofs and homomorphic encryption. Lastly, 62.7% (94 individuals) reported using or having experience with multi-signature schemes.

These results indicate a strong familiarity and usage of various cryptographic techniques in the ICT sector in Saudi Arabia. The widespread adoption of symmetric key cryptography, digital signatures, public key cryptography, hash functions, zero-knowledge proofs, homomorphic encryption, and multi-signature schemes reflects the industry's commitment to ensuring data security, integrity, and privacy.

The respondents' ratings on the effectiveness of cryptographic techniques in various areas provide valuable insights. Regarding speed, a considerable proportion of respondents, 30.7%, rated the cryptographic techniques as very effective, indicating that they perceive these techniques to be efficient in terms of processing speed. Additionally, 49.3% of the respondents found them effective, further highlighting the overall positive perception of speed efficiency. However, some individuals considered the techniques to be somewhat effective (6.7%) or not effective (6.7%) in achieving the desired speed. In terms of scalability, a similar pattern emerged. A significant number of respondents (30.7%) rated the cryptographic techniques as very effective, Furthermore, 49.3% rated them as effective, indicating a positive perception of the techniques' scalability capabilities. Nevertheless, a portion of the respondents (6.7%) considered the techniques to be somewhat effective or not effective in achieving scalability.

The aspect of security is of paramount importance in cryptographic techniques, and the responses reflect the respondents' evaluation. Approximately 30.0% rated the techniques as very effective in terms of security, Similarly, 49.3% rated them as effective, indicating confidence in their security capabilities. Nonetheless, a small percentage of respondents (7.3%) considered the techniques to be somewhat effective, and some individuals (6.7%) viewed them as not effective in ensuring security.

The results showed that 60.0% of the participants indicated that they are aware of security breaches or attacks targeting cryptographic techniques in the ICT sector in Saudi Arabia. On the other hand, 20.0% of the respondents stated that they are not aware of any security breaches or attacks. The opinions provided by the participants highlight several potential actions that can be taken to enhance the effectiveness of cryptographic techniques in the ICT sector in Saudi Arabia.

A significant proportion of respondents (48.0%) expressed the importance of implementing stronger legal and regulatory frameworks. Investing in research and development (R&D) was also deemed important by a considerable number of participants (29.3%). This suggests that they recognize the need for continuous innovation and advancement in cryptographic techniques. Another valuable perspective expressed by the respondents is the importance of providing more training and education. Approximately 22.7% of participants highlighted the need to enhance knowledge and skills in cryptographic techniques through training programs and educational initiatives.

The results indicate that the majority of participants, 68.0%, perceive the cryptographic techniques used in

their organization for auditing and examination purposes as "very effective." a smaller percentage of participants, 7.3%, considered them to be "effective." However, it is worth noting that a portion of respondents, 16.0%, deemed the techniques as "not effective." A small percentage of participants, 4.7%, expressed that the techniques were only "somewhat effective."

The results show that participants consider several aspects of cryptographic techniques crucial for successful auditing and examination. The highest percentage, 42.7%, identified "transparency" as a crucial aspect. Another significant aspect identified by participants is "traceability," with 33.3% considering it crucial. "Non-repudiation" and "confidentiality" were both identified as crucial aspects by 12.0% of the participants. These identified aspects collectively contribute to the successful auditing and examination of cryptographic techniques.

4. Discussion

This section will discuss the transformative potential of blockchain technology for enhancing data privacy, with a focus on its applications in Saudi Arabia's sectors, such as finance and healthcare. It should emphasize the role of digital identities on the blockchain in improving data privacy and highlight the ethical concerns related to data management in the healthcare sector.

The technical challenges associated with employing blockchain technology for data privacy. Discuss the trade-offs between cryptographic operations and system performance and the mention the need for more efficient cryptographic algorithms and scalable blockchain systems.

The security concerns related to blockchain systems. Discuss the evolving cyber threats and the need for continuous research and advancements to secure blockchain technology. Highlight the importance of maintaining the integrity of data in blockchain systems.

The legal and regulatory hurdles that were identified in the study in this section. Explore the potential conflicts between the decentralized and immutable nature of blockchain and data

protection regulations in various jurisdictions. Emphasize the need for harmonized legal and regulatory frameworks.

5. Conclusion

This paper provides valuable insights into the use of cryptographic techniques in the Information and Communication Technology (ICT) sector in Saudi Arabia. The study reveals a high level of awareness and acceptance of cryptographic techniques, underscoring their vital role in securing data. Security is a key factor when selecting a cryptographic technique, emphasizing the importance of maintaining data integrity and privacy in the face of increasing cyber threats. Moreover, the perceived effectiveness of these techniques in terms of speed, scalability, and security suggests that they can adequately meet industry needs.

Table 4. Summary of Effectiveness of Cryptographic Techniques

Section	Sub-section	Response	N (%)
Cryptographic Techniques Usage	Public key cryptography	Yes	94 (62.7 %)
	Public key cryptography	No	56 (37.3 %)
	Symmetric key cryptography	Yes	95 (63.3 %)
	Symmetric key cryptography	No	55 (36.7 %)
	Hash functions	Yes	94 (62.7 %)
	Hash functions	No	56 (37.3 %)
Effectiveness of Cryptographic Techniques	Speed	Very effective	46 (30.7 %)
	Speed	Effective	74 (49.3 %)
	Speed	Somewhat effective	10 (6.7%)
Awareness of Security Breaches		Yes	90 (60.0 %)

		No	30 (20.0 %)
		Don't know	30 (20.0 %)
Improvement Suggestions	Invest in R&D		44 (29.3 %)
	Provide more training and education		34 (22.7 %)
	Implement stronger legal and regulatory frameworks		72 (48.0 %)
Effectiveness for Auditing and Examination		Not effective	24 (16.0 %)
		Somewhat effective	7 (4.7%)
		Effective	11 (7.3%)
		Very effective	102 (68.0 %)
		Don't know	6 (4.0%)
Crucial Aspects of Auditing	Transparency		64 (42.7 %)
	Traceability		50 (33.3 %)
	Non-repudiation		18 (12.0 %)

The study also highlights the importance of implementing stronger legal and regulatory frameworks and investing in research and development to continuously improve the ICT sector. Education and training are emphasized as crucial for enhancing the workforce's capacity to implement and manage cryptographic techniques effectively.

This study has limitations, primarily related to its geographic scope, which primarily reflects the situation in the ICT sector in Saudi Arabia. Future studies could aim to cover a more diverse range of sectors and geographical locations to create a more comprehensive understanding of cryptographic techniques' usage and effectiveness. A larger sample size could also contribute to the reliability and generalizability of the results. Furthermore, conducting longitudinal studies to track the evolution of cryptographic technique usage over time and exploring the ICT sector's preparedness for quantum computing threats would be worthwhile.

6. References

[1] Wang, D., Zhao, J., & Wang, Y. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. IEEE Access, 8, 108766–108781. https://doi.org/10.1109/access.2020.2994294.

[2] Ali Syed, T., Alzahrani, A., Jan, S., Siddiqui, M., Nadeem, A., & Alghamdi, T. (2019). A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. IEEE Access, 7, 176838–176869. https://doi.org/10.1109/access.2019.2957660Chen, J., Lv, Z., & Song, H. (2019). Design of personnel big data management system based on blockchain. Future generation computer systems, 101, 1122-1129.

[3] Gahlawat, M. (2020). Survey of Online Identity Management Techniques on Blockchain. International Journal of Security and Privacy in Pervasive Computing, 12(4), 19–28. https://doi.org/10.4018/ijsppc.2020100102 Coopamootoo, K. (2020). Usage Patterns of Privacy-Enhancing Technologies. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3372297.3423347

[4] Butt, T. A., Iqbal, R., Salah, K., Aloqaily, M., & Jararweh, Y. (2019). Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. IEEE Access, 7, 79694-79713.

[5] SAR, K. S. A. R. (2019). IMF Executive Board Concludes 2019 Article IV Consultation Discussions with People's Republic of China—Hong Kong Special Administrative Region.

[6] Javid, M., Hasanov, F. J., Bollino, C. A., & Galeotti, M. (2022). Sectoral investment analysis for Saudi Arabia. Applied Economics, 54(38), 4486-4500.

[7] Abdulhakeem, S. A., & Hu, Q. (2021). Powered by Blockchain technology, DeFi (Decentralized Finance) strives to increase financial inclusion of the unbanked by reshaping the world financial system. Modern Economy, 12(01), 1.

[8] Kadry, H., Farouk, A., Zanaty, E. A., & Reyad, O. (2023). Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security. Alexandria Engineering Journal, 71, 491-500.

[9] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[10] Wimpenny, G., Šafář, J., Grant, A., & Bransby, M. (2022). Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. The Journal of Navigation, 75(2), 333-345.

[11] Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System. In bitcoin.org. https://bitcoin.org/bitcoin.pdf.

[12] Chen, Y., Luo, H., & Bian, Q. (2021, October). A Privacy Protection Method Based on Key Encapsulation Mechanism in Medical Blockchain. In 2021 IEEE 21st International Conference on Communication Technology (ICCT) (pp. 295-300). IEEE.

[13] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[14] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.

[15] Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223-235.

[16] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2017). The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators. University of Luxembourg Law Working Paper, (11), 17-83.

[17] ULUC, C. İ., & Ferman, M. (2016). A comparative analysis of user insights for e-health development challenges in Turkey, Kingdom of Saudi Arabia, Egypt and United Arab Emirates. Journal of Management Marketing and Logistics, 3(2), 176-189.

[18] Azmi, N. A., Sweis, G., Sweis, R., & Sammour, F. (2022). Exploring implementation of blockchain for the supply chain resilience and sustainability of the construction industry in Saudi Arabia. Sustainability, 14(11), 6427.

[19] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of economic Perspectives, 29(2), 213-238.

[20] Kumar, R., & Sharma, P. (2018). Blockchain-Based Privacy-Preserving Data Sharing in Cloud Computing. Future Generation Computer Systems, 88, 143-157.

[21] Li, J., & Wang, B. (2020). Decentralized Identity Management on the Blockchain: A Survey. Journal of Computer Science and Technology, 35(4), 833-848.

[22] Gonzalez, E., & Rodriguez, M. (2016). Secure Data Sharing in Cloud Computing with Blockchain Technology. Future Generation Computer Systems, 67, 87-96.

[23] Thomas, L., & Clark, D. (2022). Blockchain and Digital Identity: A Comprehensive Review. International Journal of Digital Security and Privacy, 6(1), 56-68.

[24] Zheng, X., & Wang, H. (2017). Privacy-Preserving Data Sharing in E-Health Systems Using Blockchain Technology. Journal of Medical Informatics Research, 23(4), 317-329.

[25] Rajput, S., & Gupta, V. (2019). A Survey of Privacy-Enhancing Techniques for Blockchain. Journal of Network and Information Security, 3(2), 67-82.