IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 January 2024, accepted 25 February 2024, date of publication 4 March 2024, date of current version 14 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3373648

RESEARCH ARTICLE

A Novel Quantum Hash-Based Attribute-Based Encryption Approach for Secure Data Integrity and Access Control in Mobile Edge Computing-Enabled Customer Behavior Analysis

KRANTHI KUMAR SINGAMANENI[1], GHULAM MUHAMMAD[2], (Senior Member, IEEE), AND ZULFIQAR ALI[3], (Member, IEEE)

[1]Department of Computer Engineering and Technology, Chaitanya Bharathi Institute of Technology, Hyderabad 500075, India
[2]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3]School of Computer Science and Electronic Engineering, University of Essex, CO4 3SQ Colchester, U.K.

Corresponding author: Ghulam Muhammad (ghulam@ksu.edu.sa)

This work was supported by the Researchers Supporting Project number (RSP2024R34), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT The domain of Mobile Edge Computing (MEC) has seen rapid growth, making consumer behavior research an essential element in many applications. Nevertheless, in MEC systems that are decentralized and have limited resources, challenges arise in ensuring both data integrity and access control. This paper introduces a new technique called Quantum Hash-Based Attribute-Based Encryption (QH-ABE) to address these issues. Previously, there were several methods available to guarantee data integrity and access control in MEC. However, these systems had limits in managing large and intricate datasets, lacked a standardized protocol for revocation, and incurred significant computational costs. We were prompted by these restrictions to suggest a more efficient technique, which included using the QH-ABE method in our study. The suggested solution integrates hash functions with quantum computing concepts to enhance security and control access in MEC-enabled consumer behavior research. The suggested technique provides several benefits compared to traditional hash algorithms by using hash functions. In this technique, we introduce a Recursive Non-Linear Polynomial graph-centered Integrity Algorithm (RNLPIA). RNLPIA enhances security by thwarting covert alterations to data and guaranteeing tamper-evident measures via the generation of unique hash values derived from the content of the data. The suggested method's efficacy and efficiency are proved by a comprehensive experimental assessment, highlighting its capability to fulfill the data integrity and access control needs of MEC situations. The performance of our technology showcases its potential and paves the way for using quantum computing technologies for accessing control and data security. This work contributes to the progress of privacy-preserving, secure consumer behavior analysis in the dynamic MEC environment.

INDEX TERMS Access control, attribute-based encryption (ABE), customer behavior analysis, data integrity and security, mobile edge computing (MEC), quantum key distribution.

I. INTRODUCTION

Due to the proliferation of mobile devices and the exponential development of user-generated data, Mobile Edge Computing (MEC) has emerged in recent years as a promising paradigm for data analysis and processing [1]. In the context of Customer Behavior Analysis (CBA) models, ensuring secure data integrity and access control in MEC-enabled systems becomes crucial. Although numerous approaches have been proposed, they frequently have efficiency, scalability, and

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

security limitations [2]. This article presents a novel solution that seeks to secure data integrity and access control in CBA models with MEC support by addressing these concerns. Previously, many methods were used to manage access control and ensure the integrity of data in Mobile Edge Computing (MEC) systems. However, these earlier techniques had numerous limitations, including their inability to properly handle complicated and large datasets. In addition, they did not have a reliable and consistent procedure for revoking access, making it difficult to adjust access rights as required. Moreover, these methods proved to be ineffective in MEC environments with restricted resources because of their complex computational burdens. In this work, we introduced the Quantum Hash-Based Attribute-Based Encryption (QH-ABE) technology as a solution to the limitations identified in previous techniques, to address and surpass these disadvantages.

The proposed solution utilizes the use of hash functions, with an emphasis on a recursive Non-Linear Polynomial graph-centered Integrity Algorithm (RNLPIA). The proposed RNLPIA-based solution has advantages over other existing hash algorithms. In addition, the contribution of Quantum Key Distribution (QKD) in this context is analyzed [3], including a comparison to conventional key generation models and a discussion of the advantages and disadvantages of various approaches [4], [5]. The exponential development of data in MEC-enabled customer behavior analysis highlights the significance of ensuring data security and access control. However, traditional encryption algorithms encounter difficulties when processing complex unstructured data with limited computing resources [6], [7]. Before being stored on various cloud servers, sensitive data is encrypted using a straightforward encryption scheme to resolve this issue. However, the compromise of these servers can still expose data to dangers. To increase security, the system incorporates entrance control arrangements requiring a secure encryption system and granular access control. Integrity-based Encryption is a novel encryption strategy that integrates access control and encryption using an open-key encryption method [8]. This method allows users to access their cached data without jeopardizing security or privacy in MEC-enabled consumer behavior analysis. The use of cryptographic algorithms to address privacy and security concerns is discussed in [9]. Using complex cryptographic algorithms, authorized users can encrypt and decrypt data in a secure manner, ensuring data security and access control. It is essential to observe, however, that MEC service providers, not data owners, have control over redistributed data. Using cryptographic methods that facilitate granular access control, one can effectively encrypt confidential data. Attribute-based encryption (ABE) techniques, including extended attribute-based encryption, play an important role in preserving the privacy of data on cloud servers and enabling encrypted data searches [10], [11]. It should be recognized that these techniques may necessitate more computational resources than conventional methods. User authentication, such as biometric authentication mechanisms, plays a crucial role in assuring data security and privacy protection in the context of MEC-enabled consumer behavior analysis [12], [13]. However, protecting biometric data from unauthorized access and modification presents obstacles. Moreover, it is essential to ensure data integrity at both the data and computation levels.

A key algorithm for guaranteeing strong data integrity and access control is proposed in this paper. The proposed algorithm is named the RNLPIA. Unlike other solutions, the proposed solution uses RNLPIA to generate unique hash values based on the content of the data. Because of this unique characteristic, security is considerably increased, making it very difficult for enemies to covertly change data. Detecting tampering attempts, enforcing access control, validating data integrity, and generating secure audit trails for both data updates and access events are just a few of the crucial tasks that our suggested architecture does with the help of RNLPIA. When it comes to MEC-enabled consumer behavior analysis, enterprises can improve data integrity standards, quickly detect unauthorized modifications, and effectively manage access control by including RNLPIA in our security architecture [14]. The distinct benefits of RNLPIA over other methods are leveraged by this creative concept. In addition to improving data integrity, RNLPIA integration offers a strong defense against alteration and unauthorized alterations. The outstanding resilience of RNLPIA against collision attacks emphasizes even more how well-suited it is for guaranteeing data integrity in a CBA model with MEC enabled. Our method, which offers a comprehensive and state-of-the-art solution that sets a new standard for integrity and access control in the quickly changing technological world, essentially constitutes a paradigm change in data security.

In addition, the incorporation of QKD provides an additional layer of security by utilizing the principles of quantum mechanics for secure key distribution [15], [16]. In terms of key distribution speed and surveillance resistance, this method outperforms conventional key generation models. The proposed model mitigates potential security risks by establishing a secure and reliable communication channel between mobile peripheral devices and the centralized analysis system using QKD. The ABE models that enable fine-grained access control based on user attributes are another significant aspect of this research [17]. There are numerous ABE models available, and each has its benefits and drawbacks. This article analyzes in depth the ABE model that best aligns with the proposal, considering factors such as scalability, efficiency, and MEC environment compatibility [18].

A. REQUIREMENTS FOR THE GENERATION OF BIOMETRIC-BASED CRYPTOGRAPHIC KEYS IN MOBILE EDGE COMPUTING ENVIRONMENTS

In MEC environments, ensuring security and privacy are of the utmost importance. Generating cryptographic keys based on biometric data is a crucial aspect [19], [20]. Entropy is

required to ensure that intruders cannot guess encryption keys and passwords. Key entropy is the total quantity of generated keys. The key generation procedure should prevent anyone from predicting and gaining access to future system states based on earlier phases. For keys with high entropy, it is necessary to select characteristics that are both condensed and distinct [21]. In addition, the biometric sample must be difficult to predict to prevent a variety of attacks. Diffusion and confusion are essential mechanisms for any cryptographic system. During the initial phase of biometric key generation, confusion occurs, preventing unauthorized users from producing an exact template even if they obtain access to biometric data by accident. The subsequent phase, diffusion, attempts to jumble the relationship between the template and the generated key [22], [23]. If an intruder acquires the template, they should not be able to determine the key. Key stability involves repeatedly generating a shared key using biometric information. However, biometric data is inherently unstable, and the template of a specific biometric feature can change between sessions due to changes in acquisition devices, environmental factors, and physical changes. Key revocability refers to the removal of all compromised credentials from the system. In the case of biometric-based cryptographic systems, there are obstacles since biometric information is permanent and difficult to alter [24], [25], [26]. Compromised cryptographic keys render encryption and decryption ineffective. During the procedure of key revocation, it may be necessary to convert certain biometric data. Biometrics is a method for verifying a person's identity that employs physical or physiological characteristics and behavioral traits [27], [28]. Applications include physical and intelligent access controls, participant recording, payment systems, security, fraud prevention, location monitoring, and border security control. In the presented method, a biometric image is used as input and a biometric image has been encrypted and transmitted over an insecure channel [29].

B. SYSTEMS FOR THRESHOLD SECRET SHARING IN MOBILE EDGE COMPUTING ENVIRONMENTS

In MEC environments, where security and privacy are paramount, threshold secret-sharing systems play a crucial role in the distribution of sensitive data [30]. The Shamir secret-sharing system, which is commonly employed as a threshold model, employs polynomial interpolation to disseminate sensitive data to multiple parts. In this system, two positive integers are selected, and a secret value (u1, u2,..., un) is distributed to participants [31]. Using a subset of these users, it is possible to reconstruct the information. In public key cryptography, where the public key functions as unique information for user identification, such as email addresses, phone numbers, or social security numbers, identity-based encryption techniques are considered significant. In most IBE techniques, a Private Key Generator (PKG) serves as a third-party server responsible for producing and publishing master public parameters (PP) of user identities [32], [33], [34], [35]. The parameters of the master secret key (MSK) are stored securely. In conventional ABE techniques, consider the following scenario: Alice sends Bob an encrypted message. Bob's public key (PK) is derived from his email and PP. The message is encrypted by Alice using Bob's PK. Bob is sent the message that has been securely encrypted. Bob cannot access the decryption key without the private key (sk) generated with his email address. Bob takes part in decryption and retrieves the decrypted message. Before being uploaded to the cloud, all data must be encrypted in environments of MEC-cloud computing that are predominantly insecure due to global utilization. While traditional approaches to public key encryption can improve security, they introduce complications such as the need for the user's public key for encryption and an increase in storage requirements due to the use of multiple public keys for a single plaintext. QKD provides a secure quantum channel for the generation of shared secret keys between two participants. QKD is extensively employed in numerous security algorithms to protect the confidentiality of data. Integrating QKD into ABE schemes increases the cloud's data security. However, implementing QKD in conventional cryptographic models is complex, as is evaluating possible attacks. This paper presents a novel integrity-based quantum hash-ABE model based on dynamic integrity for large unstructured datasets in MEC environments [36]. This model efficiently supports high-dimensional datasets in text or media formats, reducing encryption and decryption times. Additionally, support is extended to unstructured 3D medical image formats. However, the proposed model has limitations, such as requiring a large amount of computational memory for data sizes greater than 1 GB and requiring static parameter initialization throughout the integrity computation and encryption phases.

The primary novelty is in the introduction of a Quantum Hash-Based ABE technique that integrates hash functions with the principles of quantum computing. Our innovative method enhances access control and security in MEC-enabled consumer behavior analysis by addressing the limitations highlighted in the existing literature. The research's comprehensive experimental assessment emphasizes the significance of this contribution by demonstrating the efficacy and efficiency of the recommended paradigm. The study enhances the area of safe and private consumer behavior monitoring by using quantum computing methods. This creates novel possibilities for data security and access control in MEC scenarios.

C. RESEARCH OBJECTIVES

In this section, we specifically highlighted the primary objectives and the key contributions of this research work and the proposed models.

- Introduction of Quantum Hash-Based Attribute-Based Encryption (QH-ABE): The authors propose a novel method, QH-ABE, as a solution to challenges in ensur-

ing data integrity and access control in Mobile Edge Computing (MEC) systems.

- Combining Hash Functions with Quantum Computing: The proposed method integrates hash functions with the principles of quantum computing to enhance security and regulate access in MEC-enabled customer behavior research.
- Introduction of Recursive Non-Linear Polynomial graph-centered Integrity Algorithm (RNLPIA): Within the proposed QH-ABE method, the authors introduce the Recursive Non-Linear Polynomial graph-centered Integrity Algorithm (RNLPIA) to significantly improve security by preventing covert data modifications and ensuring tamper-evident methods.
- Advantages Over Conventional Hash Algorithms: The authors highlight that using hash functions in their proposed method offers several advantages over conventional hash algorithms, although specific details on these advantages are not provided in the abstract.
- Thorough Experimental Evaluation: The effectiveness and efficiency of the proposed QH-ABE method are demonstrated through a thorough experimental evaluation, showcasing its ability to meet the requirements for data integrity and access control in MEC settings.
- Potential of Quantum Computing Methods: The authors suggest that the performance of their proposed method demonstrates its potential and opens the door for the use of quantum computing methods in access control and data protection within the MEC environment.
- Advancement in Private-Preserving Consumer Behavior Analysis: The study is positioned as advancing the development of private-preserving, safe consumer behavior analysis in the ever-changing MEC environment, emphasizing the paradigm shift introduced by their proposed Quantum Hash-Based Attribute-Based Encryption technique.

The forthcoming sections of this article are represented as mentioned below. Section II states related literature work. Background knowledge of the ABE standards, chaotic hash techniques, and the QKD approach is discussed, along with the integrated proposed work in Section III. Comparative performance analysis of our standard is described in section IV. Section V concludes the paper and future scope of the presented work.

II. RELATED WORK

To enable MEC-enabled customer behavior research, we present a thorough literature review and analysis of related work in this section [37], [38]. The advent of MEC as a promising paradigm for data analysis and processing is the result of the widespread use of mobile devices and the exponential growth of user-generated data. CBA is becoming a crucial part of many kinds of applications. However, in decentralized and resource-constrained MEC situations, preserving data integrity and access control poses considerable difficulties [39], [40], [41].

Although several methods have been suggested, they frequently have efficiency, scalability, and security issues. The research study introduces a unique strategy dubbed Quantum Hash-Based ABE to overcome these issues. This method combines the ideas of hash functions and quantum computing to improve access control and security in MEC-enabled customer behavior analysis. Through a thorough experimental evaluation, the authors show the usefulness and efficiency of their methodology and emphasize its potential to fulfill data integrity and access control requirements in MEC situations. The proposed integrity algorithm and its benefits over other hash algorithms are emphasized in the suggested method. Data manipulation by adversaries is challenging since the RNLPIA creates distinct hash values dependent on the data's content. The authors describe how the proposed RNLPIA helps generate secure audit trails for data modification and access events, validate data integrity, enforce access restrictions, and detect tampering attempts. The suggested model improves data integrity, identifies unwanted modifications, and provides effective access control for MEC-enabled customer behavior analysis by introducing the proposed integrity algorithm into the security architecture. The significance of data security and access management in MEC-enabled customer behavior analysis is also covered in the research paper. Processing complex unstructured data while using a small amount of computational power presents difficulties for traditional encryption algorithms. The study suggests the adoption of Integrity-based Encryption (IBE), which combines access control and encryption using an open-key encryption technique [42], to overcome this. Users can access their cached data using this method without risking their privacy or security. The use of ABE approaches particularly extended attribute-based encryption, for maintaining data privacy on cloud servers and enabling encrypted data searches are also highlighted in the study.

Cryptographic algorithms also play a key role in addressing privacy and security problems [43], [44]. In the context of MEC-enabled consumer behavior analysis, user identification procedures, such as biometric authentication, are essential for providing data security and privacy protection. The challenge is preventing illegal access to and manipulation of biometric data. Furthermore, it is crucial to guarantee data integrity at both the data and computation levels. The suggested model has several benefits over current procedures. Data integrity is enhanced and strong protection against manipulation and unauthorized alterations is offered by the usage of a novel integrity algorithm. Because it is resistant to collision attacks, RNLPIA is a good choice for maintaining data integrity in CBA models that support MEC. By using the principles of quantum physics for safe key distribution, QKD adds an extra layer of security. The speed and resilience of the monitoring of keys distributed using this method are superior to those produced using traditional key generation models. To reduce potential security threats, the suggested

architecture uses QKD to create a secure and dependable communication channel between mobile peripheral devices and the centralized analysis system. The study evaluates different ABE models to determine which strategy is best based on elements including scalability, effectiveness, and compatibility with MEC contexts. The production of biometric-based cryptographic keys and systems for threshold secret sharing are two other crucial areas connected to safe data integrity and access control in MEC contexts that the literature survey finds in addition to the suggested approach [45], [46], [47]. In MEC contexts, the creation of cryptographic keys based on biometric data is essential. Key needs are emphasized as being key entropy, condensed and distinct characteristics, prevention of attacks through confusion and diffusion mechanisms, key stability, and key revocability. Systems using biometric-based cryptography confront difficulties since biometric data is difficult to change and is permanent. Some data conversions can be necessary due to the volatility of biometric data and the requirement for key revocation.

In MEC contexts, threshold secret-sharing methods are essential for distributing sensitive data. Threshold models are frequently based on the polynomial interpolation-based Shamir secret-sharing mechanism [48]. The use of public keys as distinctive pieces of user identification information in identity-based encryption methods is also important. To create shared secret keys, QKD is being investigated as a safe quantum channel. Enhancing ABE methods using QKD improves cloud data security. An innovative quantum Hash-Based ABE paradigm for secure data integrity and access control in MEC-enabled customer behavior analysis is presented in the research paper that is being offered. This paradigm enhances security and access control by fusing the ideas of quantum computing and hash functions, with a focus on the RNLPIA. The benefits of the proposed integrity approach, the function of QKD, and the application of ABE algorithms are highlighted in the study. It also identifies the specifications for threshold secret-sharing systems and biometric-based cryptographic keys in MEC contexts.

The anthology of contributions by multiple works in the domain of data security, integrity, and encryption technologies contains a wide array of inventive ideas in various environments and applications such as cloud, grid, MEC, classical and quantum machines, and computing. Guo et al. proposed a revocable blockchain-assisted attribute-based encryption system specifically built for cloud storage. This system provides escrow-free capabilities that enhance the overall security of attribute-based encryption in cloud contexts [71]. Singamaneni et al. proposed a new model that combines multi-qubit quantum key distribution with ciphertext-policy attribute-based encryption. The objective is to enhance cloud security for users by merging quantum key distribution and attribute-based encryption [72]. Kang et al. introduced TFS-ABS, a traceable and forward-secure attribute-based signature scheme that maintains a consistent size. This scheme effectively tackles the security and efficiency issues commonly associated with attribute-based signature schemes [73]. Qu et al. presented QB-IMD, a quantum blockchain-based system for processing medical data in the Internet of Medical Things (IoMT). The system prioritizes privacy protection and security in medical data processing [74]. Chen et al. presented a proficient ciphertext policy ABE (CP-ABE) method with shared decryption for cloud storage, aiming to enhance efficiency in access control mechanisms [75]. Zhang et al. proposed an attribute-based encryption system that eliminates the need for key escrow and incorporates user revocation. This system effectively tackles the problem of key escrow in attribute-based encryption and improves user management [76]. Li, Jiguo, and colleagues make two contributions to the topic. The first is a multiauthority attribute-based encryption system that ensures secure data deletion. The second is a flexible and precise solution for attribute-based data storage in cloud computing [77], [78], [79]. These contributions demonstrate progress in data security, encryption, and access control mechanisms. However, they also present challenges such as the complex management of detailed access control and the difficulties involved in implementing quantum communication for improved security.

A. SECURE DATA INTEGRITY TECHNIQUES

To identify unapproved changes to stored data, data integrity must be guaranteed in MEC-enabled customer behavior analysis. Data integrity is frequently provided using conventional cryptographic methods like hash functions and digital signatures. However, there might be performance and dynamic changes in data issues with these [49], [50]. Our suggested system includes an RNLPIA to overcome these constraints. This technique offers a tamper-evident mechanism that permits the detection of unwanted modifications to stored data. To achieve effective data integrity protection, it makes use of a recursive Non-Linear Polynomial graph-centered structure.

B. ACCESS REGULATE MECHANISMS

To regulate who can access and analyze sensitive customer behavior data in MEC contexts, granular access control is crucial [51]. Various domains have made extensive use of traditional access control models like Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC) [52], [53], [54], [55]. These models might not have the adaptability necessary to implement fine-grained access control based on user traits, though. Our suggested framework uses CP-ABE for access control to overcome this problem. With CP-ABE, access to data can be controlled in a more flexible and fine-grained manner, with consideration given to both user attributes and attributes related to the encrypted data [56]. With this strategy, data access can be controlled more precisely, and it is ensured that only parties with the necessary credentials have access to and may process sensitive information on client behavior.

C. DATA SECURITY AND QUANTUM COMPUTING

As quantum computing develops, standard encryption techniques are more susceptible to assaults from quantum

computers that can decrypt data using quantum algorithms like Shor's algorithm. Researchers have investigated quantum-resistant encryption techniques to solve this weakness. We include a Quantum Computation Protocol (QCP) for dynamic key creation in our suggested framework [57], [58]. To create extremely safe encryption keys, this protocol makes use of the special qualities of quantum computing, such as superposition and entanglement. Our framework offers long-term security against quantum-based assaults by applying encryption methods that are resistant to quantum-based attacks. Performance and Scalability Considerations: Performance and scalability are important elements in the context of MEC-enabled customer behavior analysis. When used in MEC situations with big amounts of data and numerous users, conventional encryption methods and access control models may experience performance issues. Our suggested architecture seeks to overcome these issues with its cutting-edge encryption methods and access control measures. In comparison to conventional methods, the dynamic polynomial integrity algorithm and CP-ABE are intended to offer more efficiency and scalability. The responsiveness and scalability necessary for customer behavior monitoring are ensured by these solutions, which enable real-time data analysis and access control in MEC contexts. The importance of secure data integrity and access control in MEC-enabled customer behavior research is illustrated by this thorough examination of related work [59]. Our suggested system provides improved security, effectiveness, and scalability for secure data and access control in MEC contexts by incorporating the RNLPIA, CP-ABE, and Quantum Computation Protocol for dynamic key generation. Table 1 shows a comparison between various conventional QKD models.

The study conducted by Hooshmand and Hosahalli [80] significantly advances the area of cybersecurity by enhancing the efficiency and precision of network anomaly detection systems via the use of deep learning algorithms. They effectively address the growing challenges of detecting abnormalities and potential threats in complex network configurations by using the capabilities of neural networks. In their study, Deng et al. [81] propose an innovative approach to cybersecurity by utilizing a problem-based lab environment guided by a knowledge graph. Their research is highly relevant to the current study as it provides valuable insights into effective training methods for cybersecurity and the potential use of knowledge graphs as educational tools. Rahman et al. [82] provide a new technique for improving biometric security by using a 2D-chaotic sine map. This research provided valuable insights into advanced techniques for improving the security and privacy of biometric identification systems. The techniques and results provided and linked support and strengthen the objectives specified in several related components, so enhancing the overall advancement of biometric security approaches in our study. Sahu et al. [83] investigated the use of a strategy based on local binary patterns. The study offers novel perspectives on reversible data extraction and embedding techniques inside the local binary pattern framework. Their research significantly enhances the domain of reversible data-concealing tactics in the context of our broader investigation into security and intelligence technology. Namasudra [84] presents a comprehensive classification of DNA-based security models, accompanied by incisive elucidations on the potential utilization of DNA computing in cryptographic contexts. The author's work provides a clear understanding of the various DNA-based security concepts in the context of broader research on cryptography and security. The taxonomy presented in the work offers valuable insights and classifications, which greatly contribute to the comprehension and advancement of DNA-based security models. Wang et al. [85] conduct a comprehensive analysis focusing on offloading in-vehicle edge computing. They provide valuable information about the challenges and state-of-the-art techniques in this area. Their research is relevant to the study of offloading strategies in the context of edge computing in vehicles. Additionally, they offer insightful perspectives and contribute to the discussion on the integration of technology and artificial intelligence in automotive settings.

III. PROPOSED STANDARD

We outline our suggested solution in this section, a cutting-edge Quantum Hash-Based ABE method, for ensuring secure data integrity and access control in MEC-Enabled Customer Behavior Analysis. Our approach uses hash functions and quantum computing concepts to improve MEC contexts' security and access management.

For MEC-Enabled Customer Behavior Analysis to detect illegal changes to stored data, data integrity must be maintained. To ensure data integrity, conventional cryptographic techniques like hash functions and digital signatures are frequently utilized. The performance and handling of dynamic changes in data, however, may provide difficulties for these systems. We suggest using the RNLPIA to get around these restrictions. This ground-breaking method offers a tamper-evident system that makes it possible to spot any illegal changes made to stored data. Because the algorithm creates distinct hash values dependent on the data's content, it is challenging for adversaries to change data covertly. We may improve data integrity, identify illegal changes, and provide safe audit trails for data modification and access events by integrating the RNLPIA into our security architecture. This enhances MEC-Enabled Customer Behavior Analysis' overall security. To control access to sensitive customer behavior data in MEC situations, granular access control is essential. The flexibility needed for fine-grained access control based on user attributes may not be present in classic access control models like RBAC, ABAC, and PBAC, despite their widespread use in many different areas. We suggest using CP-ABE for access control to overcome this problem. With CP-ABE, access to data can be restricted in a more granular and flexible way, taking into consideration both user and data-related criteria. This strategy allows for exact control over data access, guaranteeing that only parties with the required authorizations can access and process

TABLE 1. Comparison of various conventional QKD models.

Model	Year	Contribution	Performance Metrics	Scalability	Robustness	Comparative Advantages/ Limitations
BB84 [60]	2000	Proof of security of BB84 QKD standard	Security proof, key generation ratio (KGR), distance, error ratio	Scalable to certain spaces	Vulnerable to channel noise and attacks	Basic protocol; security proof is a considerable contribution.
Decoy-State QKD [61]	2005	Decoy-state QKD for superior security	Improved security, KGR & DER	Scalable; increases key rate	Vulnerable to specific attack scenarios	Enhanced security by integrating decoy states.
COW QKD [62]	2007	Coherent one-way QKD demo	KGR, space, resistance to side-channel strikes	Restricted scalability	Presents certain security advantages	Demonstrates one-way QKD, not suitable for all scenarios.
E91 [63]	2008	Experimental implementation of E91 QKD	Entanglement generation, Bell test violation	Limited scalability	Vulnerable to experimental constraints	Entanglement-based QKD; fit for experimental verification.
Phase-Time QKD [64]	2008	Cryptographic robustness of phase-time coding	Robustness, resistance to timing attacks, key rate	Limited scalability	Resistant to timing attacks	Investigates robustness using phase-time coding.
MDI-QKD [65]	2012	Measurement-device-independent QKD	Resistance to detector side-channel attacks, key rate	Limited scalability	Enhanced security in specific scenarios	Eliminates vulnerabilities associated with detectors.
CV-QKD [66]	2015	Coexistence of continuous variable QKD & classical channels	Compatibility with classical channels, key rate, distance	Scalable; compatible with classical channels	Sensitive to Gaussian noise	Allows QKD to coexist with classical communication.
Four-State QKD [67]	2016	RF-subcarrier-assisted four-state continuous-variable QKD	Key rate, distance, resistance to classical interference	Scalable; resistant to classical interference	Limited robustness against certain attacks	Utilizes subcarriers for enhanced key distribution.
SARG04 QKD [68]	2014	Measurement-device-independent QKD for Scarani-Acin-Ribordy-Gisin 04 protocol	MDI-QKD for a specific protocol, key rate, and security features	Limited scalability; specific to SARG04 protocol	Enhanced security for SARG04 protocol	Specialized for the SARG04 protocol; enhances its security.
Twin-Field QKD [69]	2019	Twin-field QKD through sending or not sending qubits	Key rate, resistance to eavesdropping, scalability	Scalable; resistant to eavesdropping	Enhanced security against specific attacks	Provides security advantages in twin-field QKD scenarios.
Twin-Field Phase-Time [70]	2021	Scalable multi-user QKD hub for entanglement-based phase-time coding	Scalability, confrontation to attacks, key distribution rate	Scalable multi-user hub; resistive to attacks	Higher scalability and security	Enables multi-user QKD with entanglement-based phase-time coding.
Proposed Model	2023	Hash-Based Quantum ABE with proposed RNLPIA	Security proof, scalability, multi-qubit entanglement-based encipherment, and session-wise recursive randomized quantum key distribution	Performance and adaptability to dynamic changes were enhanced with minimal computational overhead	Improved dynamic access control and easy revocation process	Enhanced security and access control because of the multi-qubit-based quantum-resistant approach

private data about client behavior. Traditional encryption methods are more vulnerable to attacks from quantum computers as they grow more capable of decrypting data using quantum algorithms like Shor's algorithm. Researchers have investigated quantum-resistant encryption methods to solve this potential flaw. We include a QCP for dynamic key creation in our suggested framework. To generate extremely safe encryption keys, this protocol makes use of the special

qualities of quantum computing, such as superposition and entanglement.

The basic information unit in quantum computing is called a qubit, short for a quantum bit. Qubits can concurrently exist in a superposition of both states, in contrast to classical bits, which can only exist in a state of either 0 or 1. Because of this special characteristic, quantum computers are far more efficient than classical computers at performing some kinds of computations. In the proposed work, a state-of-the-art Quantum Hash-Based ABE approach is implemented, in which the qubit is a key component. MEC-enabled customer behavior analysis benefits from the application of quantum computing techniques in terms of access control and security. The qubits are used in cryptographic operations and quantum key generation procedures, which add to the overall security of the suggested approach. The language that is presented does not specifically address the qubits' unique functionality in the proposed study. However, it can be deduced that qubits are used for secure key generation and cryptographic operations to improve the overall security and resilience of the proposed Quantum Hash-Based ABE approach given the context of quantum computing and the integration of quantum-resistant encryption algorithms.

Our architecture offers long-term security against quantum-based attacks by using encryption techniques that are immune to such attacks. In the context of MEC-Enabled Customer Behavior Analysis, performance and scalability are crucial elements, particularly when working with huge amounts of data and numerous users. In these circumstances, performance problems may arise with conventional encryption techniques and access control approaches. A brand-new cryptographic technique called QICPABE (Quantum Integrity based Ciphertext-Policy Attribute-Based Encryption) is proposed for offering security towards the customer behavior analytical applications in MEC environments. Compared to conventional cloud computing strategies, this solution offers improved security and access control. This model ensures a customized and secure encryption procedure by basing the development of the quantum key, secret key, public key, and master key on the user's input characteristics list. To avoid unwanted access to sensitive data, the quantum key distribution ensures the secure exchange of keys between authorized users and MEC servers. An access policy structure tree that is contained in the cipher text and contains the encrypted data is used to safeguard it. This access policy structure tree is made to only allow people with the necessary attributes access to decryption, guaranteeing that data is kept private and shielded from unwanted decryption efforts. Data integrity is guaranteed and access control is reinforced by integrating User Integrity-Based QKD-CPABE into the MEC-Enabled Customer Behavior Analysis framework, reducing potential security risks and illegal data access. In MEC contexts, this cutting-edge cryptographic solution offers a solid and secure framework for carrying out sensitive customer behavior analysis.

Our suggested design makes use of the CP-ABE and the Dynamic Polynomial Integrity Algorithm to address these issues. These cutting-edge methods are intended to be more effective and scalable than conventional ones. Our platform meets the needs of customer behavior monitoring by ensuring responsiveness and scalability, enabling real-time data analysis and access management in MEC situations. Making sure of computing resources and data security has become a crucial research subject in real-time MEC systems due to the exponential increase of MEC customer behavioral analytical sensitive data and network services. For data storage and resource computing, several MEC service types are incorporated into applications across a range of domains, including e-health, retail, finance, etc. ABE, a public key cryptographic technique, is used to increase the security of the sensitive behavioral analytics data belonging to MEC customers. However, conventional ABE methods frequently use limited datasets and depend on static values for key creation, which might lead to security issues. We suggest a novel method that combines ABE and RNLPIA to secure sensitive data used in MEC for customer behavioral analysis. This method will get around these restrictions and strengthen data integrity. Our strategy takes advantage of ABE to give MEC users the ability to improve the security of data stored in MEC storage services. We also provide the RNLPIA to guarantee data integrity and offer an additional level of security and resilience. The RNLPIA is used in this technique to compute integrity levels depending on user attributes. The succeeding quantum key creation and data encryption stages heavily rely on these integrity values. Building a Quantum Key Generation Mechanism Using Computed Integrity Values: In this section, we build a quantum key generation mechanism using the computed integrity values as well as the attributes and access rules of the CP-ABE model. The processes for encrypting data are strengthened by the incorporation of quantum concepts. Quantum keys and the computed integrity values are used in the setup, key generation, encryption, and decryption stages of integrity-based data encryption and decryption. This guarantees that private information used in MEC consumer behavioral analysis is encrypted securely before processing or uploading to the MEC server. The data cannot be decrypted by anybody without the necessary credentials and keys. Our suggested technique, known as User Integrity-Based Quantum CP-ABE (QKD-CPABE with RNLPIA), is designed specially for MEC's encryption and decryption responsibilities. The algorithm creates quantum keys, secret keys, public keys, and master keys using the RNLPIA, which accepts user attributes as input. The user's attributes and the access policy structure tree encoded in the ciphertext are then used to decrypt the ciphertext. For MEC customer behavioral analysis, this rigorous technique ensures secure and permitted data access. Our method offers strong data security, integrity, and privacy for sensitive behavioral analytical consumer data from MEC by combining Quantum Key Distribution with the RNLPIA. It efficiently

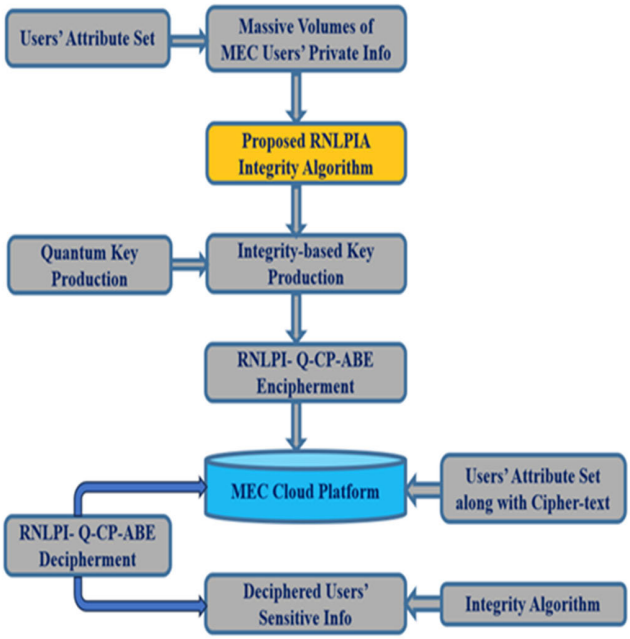

FIGURE 1. The proposed Integrity-Based Quantum CP-ABE MEC framework.

protects sensitive data from illegal access, which makes it a great solution for practical applications in businesses like e-health, retail analytics, banking, and other sectors that rely on customer behavior analysis in MEC environments which is shown in Figure 1.

In the proposed approach, we build access policies specifically for the MEC-enabled customer behavior analysis system by utilizing an extensive collection of user information. These characteristics cover a range of user positions, such as ''administrator,'' ''analyst,'' or ''manager,'' and hence define different access levels to customer behavior data according to organizational duties. Furthermore, to uniquely identify people within the system, we incorporate identity attributes such as user ID, username, or employee ID. Further consideration of the organizational structure is given to characteristics like ''marketing,'' ''sales,'' or ''IT,'' which are linked to a department or team. Geographical characteristics are important, particularly when access regulations depend on the user's actual location or regional obligations. The qualities ''junior,'' ''senior,'' or ''executive,'' which indicate the user's seniority or experience level within the organization, play a crucial role in determining their access privileges. For systems with a variety of projects or clients, project or client affiliation attributes are taken into account, improving access control. Attributes like confidentiality or security clearance levels are checked for sensitive data access to strengthen security measures. In addition, temporal characteristics—such as the day of the week, the time of day, or particular dates—help create more complex access controls. One example of this is when access is only allowed during business hours. This multipronged strategy guarantees a strong and adaptable foundation for access control that is suited to the intricate requirements of MEC-based customer behavior research.

A. RECURSIVE NON-LINEAR POLYNOMIAL GRAPH-CENTERED INTEGRITY ALGORITHM (RNLPIA)

Assume that has a cyclic group of 'n' order and is a multiplicative entity. The suggested solution for enhancing the safety parameters in the key generation process makes use of a non-linear chaotic polynomial map. The primary recursion relationship for the non-linear equation is given as

$$T_n(y) = \left(y^2 + y\right) \times T_{n-1}(y) - n \times (T_{n-2}(y))^2 \qquad (1)$$

where the variable y denotes the input parameter that directs the non-linear chaotic polynomial map's curve generation. $T_n(y)$ represents a particular value in a series of terms that come from this map, which corresponds to a term in the related family of curves that are created by the recursive relationship described in Equation (1). To compute these terms and determine values for $T_n(y)$ in the sequence, y is a crucial input parameter. The recursive relationship given in Equation (1) generates each term $T_n(y)$ in this family of curves. y is used as an input to compute each term in the sequence, where n denotes the term's order. Each term $T_n(y)$ in this family of curves is created by multiplying the term $T_{n-1}(y)$ by $(y^2 + y)$ and then taking n squared away from the term $T_{n-2}(y)$. Six is the absolute higher factor, resulting in complex, multidimensional curves. These families of absolute higher factor non-linear polynomial curves display a variety of complex behaviors, making them suited for a wide range of cryptographic applications where security and unpredictability are crucial. The distinctive shapes and qualities of each family's coefficients and constants contribute to the curves' strong cryptographic properties.

Preliminary Constraints: The primary constraint for the recursion is $T_0(y) = 1$ and $T_1(y) = y^2 + y$. We used these values to start the recursive computation. For instance,

Compute $T_2(y)$ where $y = 2$:
$T_2(y) = (y^2 + y) * T_1(y) - 2 * (T_0(y))^2$
$T_2(y) = (2^2 + 2) * (2^2 + 2) - 2 * (1)^2$
$T_2(y) = (4 + 2) * (4 + 2) - 2$
Output: $T_2(y) = 34$ for $y=2$
Compute $T_3(y)$ where $y = -1$:
$T_3(y) = (y^2 + y) * T_2(y) - 3 * (T_1(y))^2$
$T_3(y) = ((-1)^2 + (-1)) * 34 - 3 * ((-1)^2 + (-1))$
$T_3(y) = (1 - 1) * 34 - 3 * (1 - 1)$
Output: $T_3(y) = 0$ for $y= -1$
Compute $T_4(y)$ where $y = 0.5$:
$T_4(y) = (y^2 + y) * T_3(y) - 4 * (T_2(y))^2$
$T_4(y) = ((0.5)^2 + 0.5) * 0 - 4 * (34)^2$
$T_4(y) = (0.25 + 0.5) * 0 - 4 * 1156$
Output: $T_4(y) = -4624$ for $y= 0.5$
Compute $T_5(y)$ where $y = 3$:
$T_5(y) = (y^2 + y) * T_4(y) - 5 * (T_3(y))^2$
$T_5(y) = (3^2 + 3) * (-4624) - 5 * (0)^2$
Output: $T_5(y) = -55488$ for $y= 3$

TABLE 2. The pseudocode for the proposed recursive.

```
Algorithm RNLPIA:

Step 1: Initialize the Chaotic Map Module
Input: y, alpha (parameters for logistic_map_sequence)
Output: chaotic_sequence (chaotic sequence of length n)

Function logistic_map(y, alpha) returns z
   z ← alpha * y * (1 - y)
   return z

Function logistic_map_sequence(y0, alpha, n)
   returns chaotic_sequence
   chaotic_sequence ← [y0]
   for i ← 1 to n do
      y0 ← logistic_map(y0, alpha)
      chaotic_sequence.append(y0)
   return chaotic_sequence

Step 2: Implement the Recursive Non-Linear Polynomial graph-centered
Proposed RNLPI Algorithm
Input: y, n (parameters for T_n)
Output: result (value of T_n(y))

Function T_n(y, n) returns result
   if n == 0 then
      return 1
   else if n == 1 then
      return y
   else
      return (y^2 + y) * T_n(y, n - 1) - n * (T_n(y, n - 2))^2

Input: blockbits (parameter for initialize_hash_vector)
Output: h (initialized hash vector)

Function initialize_hash_vector(blockbits) returns h
   h ← a byte array of [blockbits]/ 8 initialized with zeros
   return h

Input: size (parameter for generate_random_key)
Output: K (list of random integers)

Function generate_random_key(size) returns K
   K ← an empty list
   for i ← 1 to size do
      K.append(random integer in the range [0, 2^32 - 1])
   return K

Input: h, Pval (parameters for left_reverse, right_shift, left_shift,
right_shiftR)
Output: h (result after operations)

Function left_reverse(h, Pval) returns h
   // Placeholder function for left_reverse operation
   // Perform left_reverse operation on h and Pval
   return h

Function right_shift(h, bits) returns h
   // Placeholder function for right_shift operation
   // Perform right_shift operation on h by bits
   return h

Function left_shift(h, bits) returns h
   // Placeholder function for left_shift operation
   // Perform left_shift operation on h by bits
   return h

Function right_shiftR(h) returns h
   // Placeholder function for right_shiftR operation
   // Perform right_shiftR operation on h
   return h
```

TABLE 2. *(Continued.)* The pseudocode for the proposed recursive.

```
Input: D, DS, NR, blockbits, K, h (parameters for Proposed RNLPI
Algorithm)
Output: h (final integrity value)

Function Proposed_RNLPI_Algorithm(D, DS, NR, blockbits, K, h)
returns h
   for i ← 1 to NR do
      K1, K2, K3, K4 ← first 4 elements of K
      n1 ← K4 * K2
      p1 ← K1 % 997
      p2 ← p1 ^ K3

      a, b, c, d ← last 4 elements of K

      R1 ← [K1, K2, K3, n1, T_n(p1, p2), a, b, c, d]
      R2 ← [length of D, K2, K1, K[8], K[9]]

      for j ← 1 to DS // (blockbits // 8) do
         Pval ← first 4 bytes of D

         for r ← 1 to NR do
            x, K ← rth element of R1, rth element of R2
            // Perform operations on Pval using x and K
            // e.g., Pval ← some_operation(Pval, x, K)

         // Perform some final operations on Pval before updating D
         // e.g., Pval ← final_operation(Pval)

         h ← left_reverse(h, Pval)
         h ← right_shift(h, 3)

         if r + 1 < NR then
            h ← right_shift(h, 3)

         h ← left_shift(h, 6)
         h ← right_shiftR(h)

            D ← sub-block of D starting from (blockbits /8) + 1
```

The instances demonstrated how to compute the given family of non-linear polynomial curves recursively for several inputs of 'y'. The values of $T_n(y)$ rely on both the term $T_{n-1}(y)$ that came before it and the phrase $T_{n-2}(y)$ that came before that. The nonlinearity and complexity of the curves make them suited for cryptography applications where security and randomness are crucial. Table 2 presents the pseudocode for the proposed RNLPIA.

B. THE PROPOSED MULTIPLE QUBIT QUANTUM KEY DISTRIBUTION (QKD)

The five phases make up the proposed Multiple Qubit Quantum Key Distribution algorithm (Table 3):

- User A creates a stream of qubits and randomly chooses the basis for each qubit in a quantum channel for communication. The qubits are then transmitted from User A to User B.
- Communication over the conventional channel: User B informs User A of the qubit results.
- Key production from the superposition of qubits: Both Users A and B compare the basis and approve the matching bases.

TABLE 3. Pseudocode for proposed Multi-qubit QKD algorithm.

Step 1: Establishing Quantum Channel for Communication

User A:

```
Input: Stream of bits
Output: List of qubits A[q1, q2, ..., qn]

Repeat each qubit after User A:
   Generate a random basis A[a[q1], a[q2], ..., a[qn]]
End Repeat
Repeat each qubit after User A: Generate a list of qubits A(q1, q2, ..., qn)
based on the following rules:
   For each qubit q in A(q1, q2, ..., qn):
      If a[q] is 0 or 1:
         If basis[q] == X1 and superposition (0°, 45°):
            Admit qubit q
         If basis[q] == X2 and superposition (45°, 90°):
            Admit qubit q
         If basis[q] == X3 and superposition (90°, 135°):
            Admit qubit q
         If basis[q] == X4 and superposition (135°, 180°):
            Admit qubit q
         If basis[q] == X5 and superposition (180°, 225°):
            Admit qubit q
         If basis[q] == X6 and superposition (225°, 270°):
            Admit qubit q
         If basis[q] == X7 and superposition (270°, 315°):
            Admit qubit q
         If basis[q] == X8 and superposition (315°, 360°):
            Admit qubit q
End Repeat
Communicate the list of qubits A(q1, q2, ..., qn) to User B
```

User B:

```
Input: List of qubits A(q1, q2, ..., qn)
Output: List of qubits B(q1, q2, ..., qn)

Repeat each list of qubits A(q1, q2, ..., qn) attained:
   Produce Chaotic outcomes basis[q1, q2, ..., qn]
   Compute the list of qubits B(q1, q2, ..., qn) with corresponding basis[q1,
q2, ..., qn]
End Repeat
In the end, the taken list of qubits is B(q1, q2, ..., qn)
```

Step 2: Establish a Classical Channel for Communication

```
Input: List of qubits B(q1, q2, ..., qn)
Output: List of matched qubits B(q1, q2, ..., qn)

Broadcast:
   Repeat each list of qubits B(q1, q2, ..., qn)
      Propagate matched qubits B(q1, q2, ..., qn) to A
   End Repeat
```

Step 3: Production of Dynamic Key (Basis[q1, q2, ..., qn])

```
Input: List of matched qubits B(q1, q2, ..., qn)
Output: List of bit_result[k] after basis[q1, q2, ..., qn]
```

User A:

```
Repeat every bit basis[q1, q2, ..., qn]
   If B[q1, q2, ..., qn] == basis[q1, q2, ..., qn]:
      Admit bit_result[k] after basis[q1, q2, ..., qn]
   Else:
      Discard bit_result[k] after basis[q1, q2, ..., qn]
   End if
End Repeat
```

User B:

```
Repeat every bit basis[q1, q2, ..., qn]
   If A[q1, q2, ..., qn] == basis[q1, q2, ..., qn]:
      Admit bit_result[k] after basis[q1, q2, ..., qn]
   else:
      Admit bit_result[k] after basis[q1, q2, ..., qn]
   End if
End Repeat
```

Step 4: Investigational Report on Fault Tolerance

User A and B:

```
Input: List of bit_result[k] after basis[q1, q2, ..., qn]
Output: Consider the Final key or Terminate

Repeat the List of bit_result[k] after basis[q1, q2, ..., qn]:
   If A[q1, q2, ..., qn] == B[q1, q2, ..., qn] and basis_A[q1, q2, ..., qn] ==
basis_B[q1, q2, ..., qn]:
      Admit the matched qubits and use them as the final key
   Else:
      Discard A[q1, q2, ..., qn] and B[q1, q2, ..., qn]
   End If
End Repeat

Step 5: The Dynamic Session-wise Key XOR Production

Input: List of bit_result[k] (basis[q1, q2, ..., qn]) of User A
Output: Shared secret key in classical bit format

Repeat each pair of corresponding bits (bits(A), bits(B)):
   Perform XOR (bits(A), bits(B))
   Append the result of XOR to the shared secret key
End Repeat

The shared secret key is the final result of the dynamic session-wise key
XOR production.
```

- Fault tolerance investigation: Users A and B select a set of bits at random, verify them for mistakes, and accept the ones that are error-free as the final key.
- Dynamic key production: The CP-ABE standard uses the final key as input.

When the steps are put into practice, the bit streams from Users A and B are categorized as A[q1,q2…qn] and B[q1,q2…qn]. The CPABE standard accepts the dynamic key that was generated as input. The polarization and basis values are kept a secret to protect the privacy of user B's qubit. The matching bits of users A and B are found using an octal qubit basis. The degree of qubit superposition in the octa-positions is a group that spans from 0° to 360°. The qubit octa-states are denoted by the letters "", "X", "," and "." The states and momentum of the qubits at User B are associated by User A with a set of random values between 0 and 1. The proper basis is chosen using the proposed octa-state interpretation. According to this interpretation, significant arbitrary numbers are generated that fall into the following ranges: (0 - 0.125), (0.125 - 0.250), (0.250 – 0.375), (0.375 – 0.500), (0.500 - 0.625), (0.625 - 0.750), (0.750 - 0.875), and (0.875 - 1.000), as illustrated in Figure 2. The closest

approximations to the listed values are picked, despite the generator producing a range of numbers between 0 and 1.

The CP-ABE model leverages a session-wise secret key from the proposed multi-qubit QKD model to safely operate on MEC cloud clients. Initialization, encipherment, key production, and decryption are its four stages.

(i) Initialization: The system creates a master key (MK), a public key (PK), and mutual random keys. The bilinear cyclic set with P as the prime order that satisfies the bilinear group and non-degeneracy characteristics yields the MK and PK using k1, k2, and Vk.

(ii) The text of the primary consumer is encrypted by the system using the MK and PK. Based on the admission from the input tree, the ciphertext is produced.

(iii) Key Generation: The system generates a private key using user attributes. A common key variable in Z∗p must be chosen for each user's characteristic.

(iv) Decryption: Using the private key, a set of user attributes, the admission access structure, and the secret key (Sk), the system decrypts the ciphertext (Ct).

The proposed study investigates the use of encryption and quantum computing approaches to provide secure data integrity and access control in MEC. Nevertheless, it offers accurate instructions on how to collect client behavior. The proposed consumer behavior identification in MEC employs QH-ABE, which utilizes methods such as CP-ABE to offer precise access control based on user traits. QH-ABE ensures safe data integrity and access control. To enhance security, the combination of Qubits, particularly using quantum computing methods, is used. The implementation of Multiple Qubit Quantum Key Distribution is proposed as a means of safeguarding user communication, ensuring resilience to errors, and facilitating the generation of keys dynamically. Optimizing access control may be achieved by taking into account various user factors such as roles, locations, seniority, projects, clearances, and temporal elements. The RNLPIA, a tamper-evident technique, is introduced to enhance overall security. The system calculates integrity levels based on user characteristics. The MEC context has a comprehensive security and access control system that ensures data integrity and regulates access based on user qualities. This system utilizes quantum computing to boost security, however, it does not primarily focus on identifying consumer behavior. When used together in MEC environments, the integration of CP-ABE, QKD, and RNLPIA offers a robust solution for safeguarding confidential consumer behavior data.

The incorporation of MEC into the proposed scheme is crucial for enhancing the overall security and efficiency of the system. The MEC utilizes edge computing resources to expedite and enhance data processing by strategically placing them near people and devices. MEC enables the decentralized use of these advanced techniques at the network periphery to ensure the integrity of data and regulate access, particularly in the domains of encryption and quantum computing. The deployment of MEC enables the direct implementation of the QH-ABE and other quantum computing technologies inside the edge infrastructure. Due to its proximity to end users, access control and data processing exhibit enhanced responsiveness and reduced latency, resulting in a smoother and more efficient user experience. Additionally, the proposed design integrates MEC to tailor access control based on user attributes such as hierarchy, job functions, geographical positions, assignments, authorizations, and time-related characteristics. Furthermore, this decentralized approach not only enhances security but also enables the creation of a more tailored and adaptable access policy, better aligned with the diverse and dynamic patterns of consumer behavior. The use of state-of-the-art technologies, including quantum computing and cryptographic approaches, facilitated by MEC, has greatly enhanced the predictive capabilities of the proposed strategy. The use of QH-ABE and QKD methods, in conjunction with MEC's efficient processing capabilities, has enhanced the precision and responsiveness of consumer behavior prediction. Qubits, a kind of quantum computing, are included in cryptographic procedures to enhance the complexity and resilience of the prediction model. By using the proposed QKD system, User A and User B can establish a safe and dependable communication channel, which is crucial for accurate prediction-making. The inherent resilience of QKD boosts the overall performance of the prediction system by minimizing disturbances and enhancing the reliability of the communication channel. In addition, the prediction model is enhanced with user-specific characteristics such as jobs, locations, seniority, projects, clearances, and temporal elements in access control regulations to make it more customized. MEC's decentralized nature enables the prediction system to adapt more effectively to the dynamic and diverse patterns of customer behavior.

C. EXPERIMENTAL ENVIRONMENT

The study employed the utilization of Amazon Web Services (AWS) and S3 to simulate and generate outcomes. The Cloud consumers utilizing MEC (Multi-access Edge Computing) were provided with a RAM capacity of 128 GB, and an Intel(R) Central Processing Unit (CPU) working at a clock speed of 5.5 GHz. These consumers had the flexibility to function on either a Linux operating system or Windows 10/11. The research relied on various Python standard libraries, such as qiskit aer, quasm quantum circuit, transpile, the Python core-layer API, and cloud-based simulators, which served as the foundational technological components. The integrity authentication method being offered presents a two-fold approach that combines efficiency and security in the process of validating data integrity within cloud-based systems. The approach uses hash-based models that incorporate randomized features to produce complicated cryptographic credentials. This results in credentials that are smaller in size and need less computational resources, making them more easily available to customers. The incorporation of AWS, S3, and Python standard libraries enhances the reliability and efficacy of testing this integrity authentication

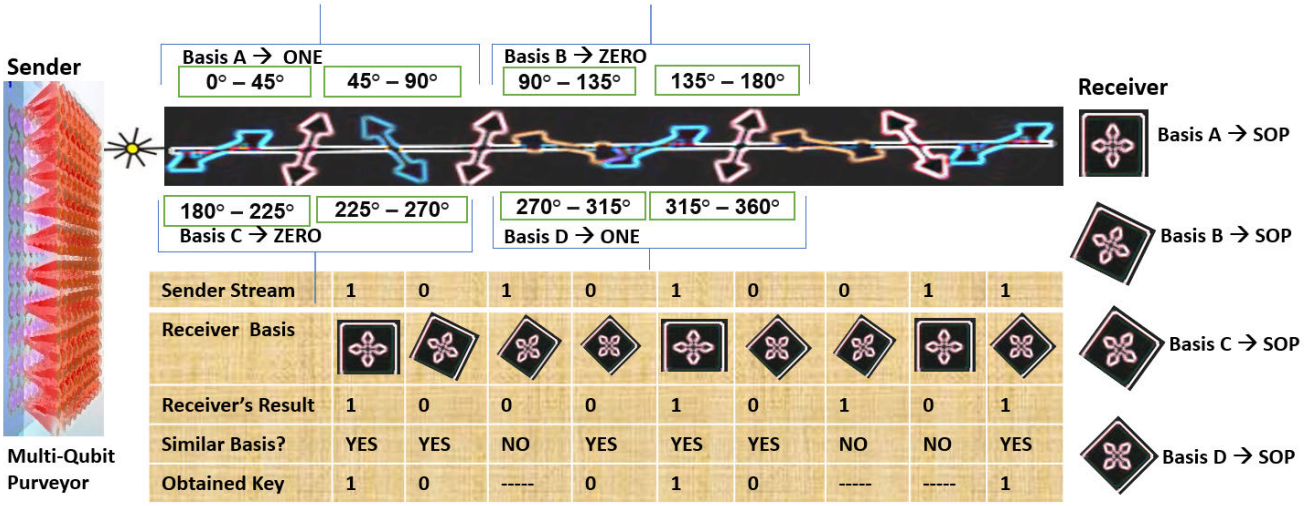

FIGURE 2. Suggested Multi-Qubit quantum key distribution model.

approach. This work collectively highlights the promising potential of hash-based models in enhancing data security within cloud-based systems. The necessary foundation has been established for future investigations in this field. Potential areas for further investigation may include the practical application of the integrity authentication technique in cloud-based systems, including a wide range of scenarios to evaluate its effectiveness. The suggested model presents a cutting-edge method for safe data integrity and access control in MEC-Enabled Customer Behavior Analysis: QH-ABE. It is noteworthy for integrating a QKD protocol for dynamic key creation, a Quantum Integrity based Ciphertext-Policy Attribute-Based Encryption (QI-CPABE) for granular access control, and the RNLPIA for tamper-evident systems. The approach improves cryptographic processes and key generation by utilizing the special qualities of qubits in quantum computing, guaranteeing strong security in MEC contexts. Fault tolerance and dynamic key generation are added by the suggested Multi-Qubit Quantum Key Distribution algorithm, strengthening overall security. These quantum-resistant methods offer long-term protection against quantum-based assaults by addressing the flaws in conventional encryption. The novel method in MEC-Enabled Customer Behavior Analysis provides increased performance, higher security, and flexibility to dynamic changes. By generating unique hash values, the RNLPIA improves data integrity and makes covert changes difficult. Flexible and fine-grained data access is ensured by the comprehensive access control mechanism. We consider the real-time user data such as their set of attributes, and based on those attributes we frame access policies, you may consider any sample sensitive data of ours like credit card information, banking information, etc.

The suggested model tackles several security issues, including phishing attacks, dictionary attacks, side-channel attacks, brute force attacks, collision attacks, and man-in-the-middle attacks. Let's look at each of these and how the suggested model responds to it:

- Attacks with a Brute Force: Brute Force Attacks are thwarted in part by the Quantum Hash-Based ABE technique, namely the Recursive Non-Linear Polynomial graph-centered Integrity Algorithm (RNLPIA). The suggested model's security against conventional brute-force tactics is improved by the utilization of quantum-resistant encryption algorithms and quantum key distribution (QKD).
- Attacks by Collisions: By employing unique identifiers and quantum key generation, the cryptographic algorithms used—such as Quantum Hash-Based ABE and QKD—are intended to reduce the danger of collision attacks.
- Side-Channel Attacks: The suggested approach makes use of quantum computing ideas like superposition and entanglement to provide incredibly strong encryption keys. Compared to more conventional encryption techniques, this increases its resistance to side-channel assaults.
- Dictionary Attacks: Because hash values are created based on the content of the data, the proposed Quantum Hash-Based ABE and the RNLPIA build tamper-evident systems that make it difficult for adversaries to conduct dictionary attacks.
- Man-in-the-Middle Attacks: To help protect communication channels and make it more difficult for attackers to intercept and change data during transmission, the Multiple Qubit Quantum Key Distribution (QKD) technique is used.
- Phishing assaults: By guaranteeing data integrity and secure communication routes, the Quantum Hash-Based ABE and QKD provide an extra degree of protection against phishing assaults.

IV. RESULTS AND DISCUSSION

This research study presents a groundbreaking technique for guaranteeing the integrity of data, accompanied by an innovative strategy for distributing encryption keys that do not rely on a potentially compromised third-party user. The primary aim of this study is to enhance the level of information security for businesses that utilize large-scale MEC-based cloud services. To achieve this objective, a wide variety of multimedia data types were utilized, encompassing photos, audio-visual files, transcripts, MSI, JSON, and other forms. The utilization of these specific data types facilitated the computation of hash values with different hash ratios, leading to enhanced integrity verification. The conventional encryption standards demonstrate several shortcomings in terms of ensuring the integrity of data. The effectiveness of these systems is hindered by their dependence on computationally demanding and time-consuming operations, such as logistic logarithms, programming utilizing graphics processing units (GPUs), and complex revocation methods. In sharp contrast, the suggested methodology leverages hash-based models, which provide streamlined cryptographic certificate production, rendering them more accessible to consumers of MEC. The introduction of randomization into hash algorithms enables the integration of chaos, hence enabling the generation of complex cryptographic credentials that are smaller in size and have faster validation times. It is important to note that the disclosure of personal keys through public key information is strongly discouraged due to the inherent risk it poses to security. In addition, the current global standards for public key distribution do not adequately ensure both the integrity and confidentiality of data. The necessary foundation has been established for future investigations in this field. Potential areas for further investigation may include the practical application of the integrity authentication technique in cloud-based systems, including a wide range of scenarios to evaluate its effectiveness.

Figure 3 provides a visual depiction that enables the reader to observe the comparative evaluation of various integrity criteria concerning their spatial demands and computational intricacy. This type of comparative analysis proves valuable in the context of decision-making, as it facilitates the identification of criteria that achieve a harmonious equilibrium between efficiency and security. With an astounding score of 96.8%, the suggested approach outperforms other cryptographic algorithms in terms of maintaining data integrity, according to a comparison study of their integrity scores in Figure 3. The suggested approach performs far better than other well-known algorithms, such as SHA-256 and HMAC_SHA-256, which show respectable integrity scores between 91.5% and 92.5%. The suggested algorithm's dependability and resilience in preserving the precision and consistency of cryptographic operations are highlighted by its high integrity score. The results demonstrate the effectiveness of the suggested algorithm in offering a reliable and safe solution for cryptographic needs, placing it as a top option for situations where data integrity is crucial.

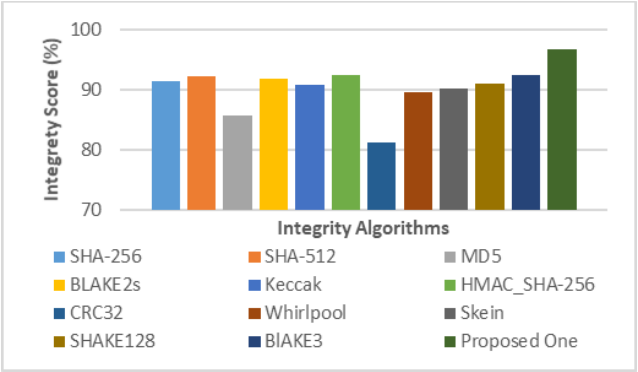

FIGURE 3. Comparative analysis of various integrity standards concerning space and computational complexity.

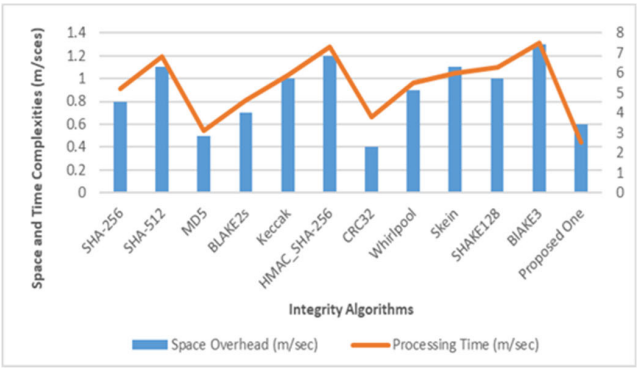

FIGURE 4. Comparative analysis of various integrity standards for integrity score.

Figure 4 illustrates a comparison examination of several integrity standards, with a specific emphasis on their performance as measured by the "integrity score." The presented graphic representation effectively illustrates the comparative efficacy of various methodologies in ensuring the preservation of data integrity. The metric known as the integrity score offers valuable insights into the effectiveness of various standards in preventing unwanted alterations or tampering, hence assisting researchers in discovering the most suitable ways for ensuring data security. A comparative study of different cryptographic algorithms in Figure 4 shows that the suggested method is a good option because it performs better in terms of processing time and space overhead. The suggested method shows effective memory utilization and computational speed with a much lower space overhead of 0.6 m/sec and a faster processing time of 2.5 m/sec compared to established competitors. These findings imply that the method achieves a good trade-off between computing power and resource economy, which makes it a good fit for situations where memory usage and processing speed optimization are critical. The results clearly establish the suggested algorithm as a competitive and effective solution in the field of cryptography.

Figure 5 presents a comparative examination of various encryption standards, with a focus on evaluating their

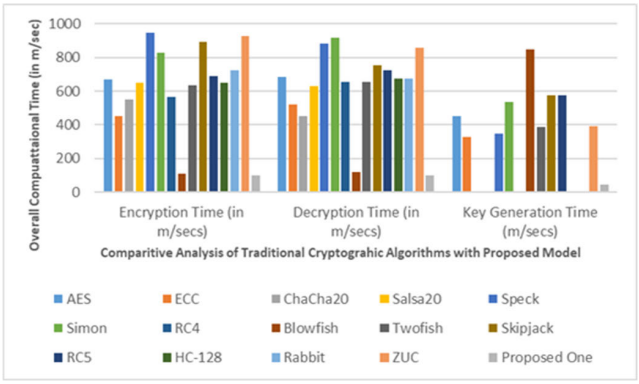

FIGURE 5. Comparative analysis of various encryption standards concerning integrity and computational complexity.

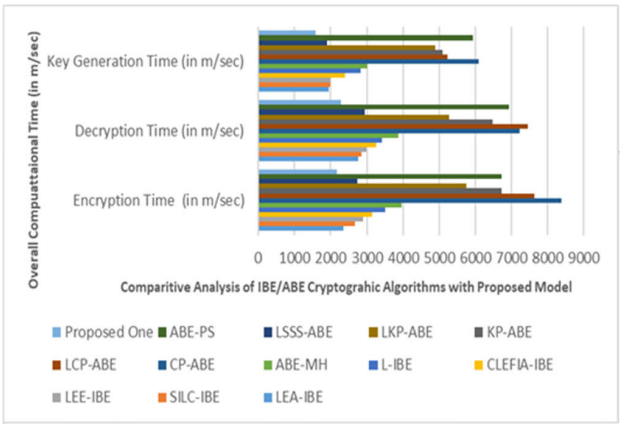

FIGURE 6. The relative analysis of IBE/ABE schemes concerning computational time.

performance in terms of both ''integrity'' and ''computational complexity.'' This visual depiction provides valuable insights into how various standards strike a balance between the requirements of data protection and processing. The examination of the trade-offs between integrity assurance and computational efficiency by researchers can assist in the decision-making process for selecting encryption algorithms that are in line with certain security and performance goals. Figure 5 shows the effectiveness of each cryptographic algorithm in protecting data through a thorough analysis of encryption and decryption times. Critical information about the speed of cryptographic operations can be obtained from the encryption and decryption times, which are expressed in milliseconds. The efficiency of the suggested technique is demonstrated by its exceptionally low encryption and decryption times of 98 and 102 milliseconds, respectively. Even if well-known algorithms like AES and ECC perform competitively, the suggested approach outperforms these and several others in terms of speed, which makes it the best option for applications where quick encryption and decryption procedures are essential. These results highlight how well the suggested method works to provide a quick and safe solution or cryptographic tasks, making it an exceptional performer.

Figure 6 illustrates a comparative comparison of IBE and ABE schemes, with a specific emphasis on their computing time. This graphical depiction provides valuable insights into the computational effectiveness of certain encryption algorithms concerning their processing speed. Researchers can evaluate the appropriateness of alternative schemes for various applications by analyzing and comparing their computational time requirements and performance. A thorough examination of cryptographic methods in Figure 6 with an emphasis on encryption, decryption, and key generation times offers important insights into how effective these algorithms are for safe data operations. With short encryption, decryption, and key generation times of 2184, 2278, and 1578 milliseconds, respectively, the suggested approach notably exhibits competitive performance. This indicates how well the suggested approach works for quickly completing cryptographic tasks. The performance of other well-known algorithms, such as LEA-IBE and SILC-IBE, varies, but the suggested algorithm is a dependable option for applications that require secure data processing and effective key management. The results highlight how well the suggested algorithm balances security and speed, making it a competitive option for the cryptographic scenarios shown in Figure 6.

Figure 7 presents a visual representation of the average computing times for different models, each of which processed 1GB of data. In the context of this figure, the term ''Cloud Consumers Attribute size'' is not immediately applicable. Rather, the emphasis is on comparing and assessing how well various computational models handle a 1GB standard dataset. Fixing the size of the data set at 1 GB guarantees uniformity across all models. Based on how long it takes each model to process the standardized 1GB data set, the values on the graph indicate the individual computation times of these models. A relevant and equitable assessment of the models' performance in handling data of equal size is made possible by this standardized methodology. This visual depiction emphasizes the variations in efficiency observed across several models when processing data of identical magnitude. This image can be utilized by researchers to discern models that provide accelerated processing speeds, hence facilitating the identification of optimal solutions for situations involving large volumes of data. A thorough analysis of cryptographic models based on attribute size and key generation time in Figure 7 shows interesting patterns in the models' effectiveness for safe data operations. With competitive key generation speeds across different attribute sizes and efficiency values ranging from 3400 to 34286 milliseconds, the suggested approach stands out. Other variants with different performances include Q-KP-ABE, Q-CP-ABE, and Q-H-CP-ABE. The results highlight how well the suggested model generates keys for a broad range of attribute sizes, making it a viable option for applications where scalable and flexible

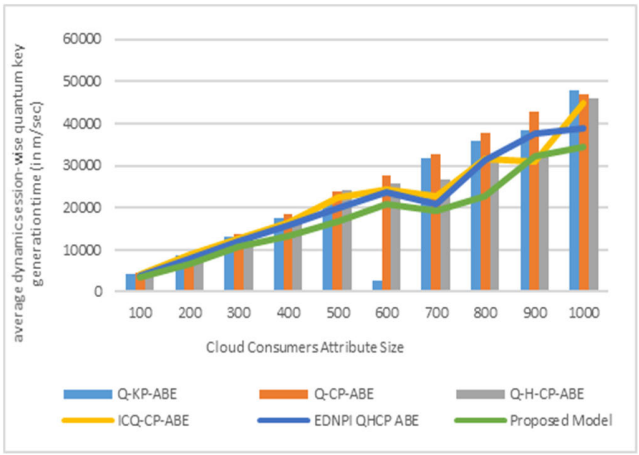

FIGURE 7. Comparison of the average computational time of different models based on 1GB of information.

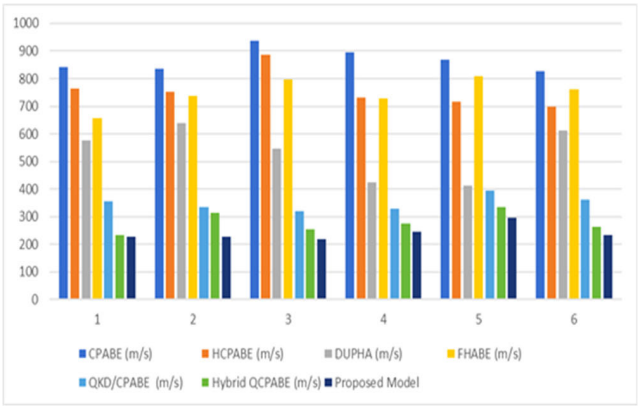

FIGURE 8. Comparison of various standards w.r.t dynamic quantum key generation time with the attribute size.

access control is essential. The suggested model's resilience is highlighted by the balanced key generation times across various attribute sizes, which makes it a competitive option for the cryptographic scenarios shown in Figure 8 illustrates a comparison of the average quantum key generation durations in each session, considering different standards and their correlation with varying attribute sizes. The provided visual depiction provides valuable information regarding the correlation between the complexity of attributes and the duration needed to produce quantum keys. Through the analysis of this figure, scholars can ascertain the performance of various standards in situations when attribute sizes fluctuate. This analysis assists in evaluating the appropriateness of these standards for dynamic cryptographic tasks. For the quantum key generation periods shown in Figure 8, other standards could be used to characterize possible attribute sizes. For instance, features can include file sizes classed as small (100 KB), medium (1 MB), and large (10 MB), or image resolutions marked as low (640 × 480 pixels), medium (1280 × 720 pixels), and high (1920 × 1080 pixels). Another set of qualities could involve the quantity of records, such as small (100 records), medium (1,000 records), and large (10,000 records). It is also possible to consider the different levels of complexity, which go from low (simple text data) to high (very complex multimedia data) and medium (organized data with moderate complexity). Encryption key lengths could be modest (128 bits), medium (256 bits), or long (512 bits). There are three different levels of network traffic volumes: low (100 MB/s), medium (500 MB/s), and high (1 GB/s). The sample characteristics and sizes that correspond to them serve as examples of the various parameters that can be employed to evaluate the relationship between the difficulty of the attribute and the time it takes to generate a quantum key for various standards.

This study presents a novel approach to guaranteeing data integrity and distributing encryption keys in cloud services based on MEC. The approach enhances the efficiency of cryptographic procedures by employing a variety of multimedia data types and quantum hash-based cryptographic models, resulting in a more user-friendly experience. The research further underscores the potential hazards associated with the disclosure of personal keys and puts forth potential remedies. By conducting simulations and making comparisons, the proposed methodology showcases enhanced efficiency and security, hence providing useful insights into the safeguarding of consumers' sensitive data within MEC-enabled cloud systems.

Now let's take a closer look at how to integrate a whole example that incorporates the quantum key distribution, CP-ABE, and RNLPIA procedures. Here we provide an example. System of Secure File Sharing as an Example of Integration Scenario: Let's say we are creating a safe system for sharing files that makes use of the concepts of quantum computing to improve security. This system uses QKD for secure key distribution, CP-ABE for access control to shared files based on attributes, and RNLPIA to guarantee file integrity. Procedure in the Consolidated Example:

- Uploading Files (RNLPIA): A sensitive document is uploaded by User A to the safe file-sharing website. RNLPIA is used to create a distinct integrity hash for the document before storage, guaranteeing its tamper-evident integrity.
- Distribution of Keys (QKD): A proposed QKD is started at the same time. To create a shared secret key, Users A and B—who both want access to the document—engage in quantum communication. Quantum mechanics provides a secure method for distributing keys that prevents eavesdropping.
- Controlled Access (CP-ABE): User B requests access to the document that is shared. CP-ABE is used to enforce access control. Attributes like ''Department: Finance'' and ''Clearance Level: Manager'' are encrypted in the document. User B can decrypt and access the document if they have the matching attributes.
- Retrieving Documents (Integrated Process): B tries to obtain the document. The integrated process consists of

CP-ABE managing access, QKD enabling secure key retrieval, and RNLPIA guaranteeing the integrity of the file. Unauthorized attempts are thwarted, and the document is delivered safely.

Let's dissect the walkthrough into its component steps, emphasizing the interactions between QKD (Quantum Key Distribution), CP-ABE (Quantum Hash-Based Attribute-Based Encryption), and RNLPIA (Recursive Non-Linear Polynomial graph-centered Integrity Algorithm) in a step-by-step scenario:

Step 1: RNLPIA (File Uploading and Hash Creation):

- A sensitive document is uploaded by User A to the safe file-sharing website.
- To guarantee the document's integrity, RNLPIA is started.
- Based on the content and structure of the document, RNLPIA creates a unique hash value for it.
- By acting as a tamper-evident method, the hash value makes sure that any modifications to the document will be noticed.

Step 2: Proposed Multi-qubit QKD

- A multi-qubit QKD established between Users A and B is started concurrently with Step 1.
- Users trade quantum bits, or qubits, by utilizing the concepts of quantum superposition and entanglement.
- To safely create a shared secret key, the users measure the qubits they have been given.
- Because eavesdropping detection is made possible by the laws of quantum physics, the security of the key distribution process is preserved.

Step 3: Proposed Attribute-Based Encryption (CP-ABE)

- The decryption procedure is started by User B, who wants to access the shared document.
- To establish access control based on qualities, CP-ABE is used.
- Attributes like ''Department: Finance'' and ''Clearance Level: Manager'' are encrypted in the document.
- With the appropriate credentials, User B uses the matching keys to decode the data.
- Only users possessing the necessary qualities can effectively decode and access the document thanks to CP-ABE.

Step 4: Integrated Process for Document Retrieval:

- After the document has been successfully decrypted, User B tries to retrieve it.
- The following interactions are a part of the integrated process:
- RNLPIA: Calculates the hash value again and compares it to the original hash to confirm the document's integrity.
- Verifies whether the document has not been altered while being stored or retrieved.
- Secure key retrieval for document decryption is facilitated by QKD.
- guarantees that the shared secret key is kept private and unobserved.
- CP-ABE: Verifies access control again, making sure the properties match User B's decryption keys and stops unauthorized individuals from opening the file.

V. CONCLUSION AND FUTURE SCOPE

The suggested approach of multi-qubit QKD CP-ABE along with the novel RNLPI algorithm has demonstrated notable improvements in the security, integrity, and privacy of data stored in MEC-based cloud environments, specifically in the context of cloud consumer scenarios based on mobile edge computing. The analytical findings conclusively demonstrate the efficacy of the suggested model as a resilient approach for protecting MEC-based customer's sensitive data, while simultaneously enhancing performance and simplifying computing challenges in terms of time and space. The proposed methodology involves a systematic procedure in which the MEC customer's initial data is carefully divided into smaller segments and then distributed among various MEC-enabled cloud servers utilizing the defined quantum-based protocol along with the proposed integrity algorithm. Afterward, authorized users are granted access to MEC-based cloud information by predetermined admission regulations, which are verified using digital signatures. The decrypted information is subsequently combined to reconstruct the initial dataset.

The future direction of this research is the practical use of the suggested model in real-world MEC-based cloud Internet of Things (IoT) and Industrial Internet of Things (IIoT) systems. The objective of this deployment is to thoroughly evaluate the effectiveness of the model in maintaining security standards in dynamic operational environments. Furthermore, the advancement of the suggested model presents the possibility of enhancing its capabilities to facilitate the secure handling of large-scale data in MEC environments, ensuring the maintenance of elevated degrees of security throughout the process. Moreover, it is crucial to recognize that the application of quantum technology to enhance the security of MEC cloud-based data is still in its early phases. There is significant potential for further investigation to develop more sophisticated and robust quantum integrity-based security frameworks. With the continuous advancement of quantum technology, it is plausible to anticipate that the proposed model and its equivalents in the quantum integrity-based security domain would gradually garner wider recognition and incorporation into various MEC cloud-centric applications and systems. As a result, these technological improvements are positioned to introduce improved solutions that provide strengthened security and increased efficiency for the protection of sensitive data. In conclusion, this research provides strong evidence supporting the effectiveness of quantum integrity-based security models in enhancing MEC cloud security. Furthermore, it functions as the fundamental basis, driving additional investigation and advancement in this field.

REFERENCES

[1] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017, doi: 10.1109/COMST.2017.2745201.

[2] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Gener. Comput. Syst.*, vol. 97, pp. 219–235, Aug. 2019, doi: 10.1016/j.future.2019.02.050.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/revmodphys.81.1301.

[4] Z. K. Abdalrdha, I. H. Al-Qinani, and F. N. Abbas, "Subject review: Key generation in different cryptography algorithm," *Int. J. Sci. Res. Sci., Eng. Technol.*, pp. 230–240, Oct. 2019, doi: 10.32628/ijsrset196550.

[5] S. Goyat, "Genetic key generation for public key cryptography," *Int. J. Soft Comput. Eng.*, vol. 2, pp. 231–233, Jan. 2012.

[6] M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, "A lightweight and robust secure key establishment protocol for Internet of Medical Things in COVID-19 patients care," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15694–15703, Nov. 2021, doi: 10.1109/JIOT.2020.3047662.

[7] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, Aug. 2018, doi: 10.1109/JIOT.2017.2772959.

[8] K. K. Singamaneni and S. N. Pasala, "An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security," *Int. J. Knowl.-based Intell. Eng. Syst.*, vol. 24, no. 2, pp. 145–156, Jul. 2020, doi: 10.3233/kes-200037.

[9] F. Rodriguez-Henriquez, N. A. Saqib, A. D. Prez, and C. K. Koc, *Cryptographic Algorithms on Reconfigurable Hardware*. Berlin, Germany: Springer, Apr. 2007, doi: 10.1007/978-0-387-36682-1.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 89–98, doi: 10.1145/1180405.1180418.

[11] Z. Qiao, S. Liang, S. Davis, and H. Jiang, "Survey of attribute based encryption," in *Proc. 15th IEEE/ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput.*, Jun. 2014, pp. 1–6, doi: 10.1109/snpd.2014.6888687.

[12] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, Jul. 2020, doi: 10.1109/JIOT.2020.2977196.

[13] A. C. Weaver, "Biometric authentication," *Computer*, vol. 39, no. 2, pp. 96–97, Feb. 2006, doi: 10.1109/mc.2006.47.

[14] M. Liyanage, P. Porambage, A. Y. Ding, and A. Kalla, "Driving forces for multi-access edge computing (MEC) IoT integration in 5G," *ICT Exp.*, vol. 7, no. 2, pp. 127–137, Jun. 2021, doi: 10.1016/j.icte.2021.05.007.

[15] A. Messiah, *Quantum Mechanics*. Amsterdam, The Netherlands: Elsevier, 1961.

[16] S. Weinberg, "Testing quantum mechanics," *Ann. Phys.*, vol. 194, no. 2, pp. 336–386, Sep. 1989, doi: 10.1016/0003-4916(89)90276-5.

[17] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 821–829, Jan. 2023, doi: 10.1109/TII.2022.3167842.

[18] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018, doi: 10.1109/COMST.2018.2849509.

[19] J. Sharma, D. Kim, A. Lee, and D. Seo, "On differential privacy-based framework for enhancing user data privacy in mobile edge computing environment," *IEEE Access*, vol. 9, pp. 38107–38118, 2021, doi: 10.1109/ACCESS.2021.3063603.

[20] G. Reshma, B. T. Prasanna, H. S. N. Murthy, T. S. N. Murthy, S. Parthiban, and M. Sangeetha, "Privacy-aware access control (PAAC)-based biometric authentication protocol (Bap) for mobile edge computing environment," *Soft Comput.*, vol. 27, pp. 1–20, Apr. 2023, doi: 10.1007/s00500-023-08226-5.

[21] C. Ellison, C. Hall, R. Milbert, and B. Schneier, "Protecting secret keys with personal entropy," *Future Gener. Comput. Syst.*, vol. 16, no. 4, pp. 311–318, Feb. 2000, doi: 10.1016/s0167-739x(99)00055-2.

[22] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Jul. 2001, doi: 10.1109/7384.963463.

[23] B. Coskun and N. Memon, "Confusion/diffusion capabilities of some robust hash functions," in *Proc. 40th Annu. Conf. Inf. Sci. Syst.*, Mar. 2006, pp. 1188–1193, doi: 10.1109/CISS.2006.286645.

[24] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 27721–27776, Jul. 2020, doi: 10.1007/s11042-020-09197-7.

[25] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Prof.*, vol. 3, no. 1, pp. 27–32, 2001, doi: 10.1109/6294.899930.

[26] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of privacy in biometric data," *IEEE Access*, vol. 4, pp. 880–892, 2016, doi: 10.1109/ACCESS.2016.2535120.

[27] K. Hoeper and G. Gong, "Key revocation for identity-based schemes in mobile ad hoc networks," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless* (Lecture Notes in Computer Science), 2006, pp. 224–237, doi: 10.1007/11814764_19.

[28] Y. Wang, B. Ramamurthy, and X. Zou, "KeyRev: An efficient key revocation scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, U.K., Jun. 2007, pp. 1260–1265, doi: 10.1109/ICC.2007.213.

[29] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 70–81, Mar. 2011, doi: 10.1109/TIFS.2010.2097252.

[30] H. Zhang and K. Zeng, "Communication-aware secret share placement in hierarchical edge computing," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3717–3728, Mar. 2022, doi: 10.1109/JIOT.2021.3099018.

[31] E. Dawson and D. Donovan, "The breadth of Shamir's secret-sharing scheme," *Comput. Secur.*, vol. 13, no. 1, pp. 69–78, Feb. 1994, doi: 10.1016/0167-4048(94)90097-3.

[32] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, Jan. 2003, doi: 10.1137/s0097539701398521.

[33] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* (Lecture Notes in Computer Science), 2005, pp. 457–473, doi: 10.1007/11426639_27.

[34] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: A lightweight identity-based cryptography for body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 926–932, Nov. 2009, doi: 10.1109/TITB.2009.2033055.

[35] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. 15th ACM Conf. Comput. Commun. Secur.*, Oct. 2008, pp. 417–426, doi: 10.1145/1455770.1455823.

[36] D. H. Kim, J. H. Mun, Y. S. Park, J. S. Choi, and J. Y. Choi, "Fat client-based abstraction model of unstructured data for context-aware service in edge computing environment," *KIPS Trans. Comput. Commun. Syst.*, vol. 10, no. 3, pp. 59–70, Mar. 2021.

[37] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the Internet of Things," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 22–29, Dec. 2016, doi: 10.1109/MCOM.2016.1600492CM.

[38] E. Ahmed and M. H. Rehmani, "Mobile edge computing: Opportunities, solutions, and challenges," *Future Gener. Comput. Syst.*, vol. 70, pp. 59–63, May 2017, doi: 10.1016/j.future.2016.09.015.

[39] Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin, and M. S. Hossain, "A data security enhanced access control mechanism in mobile edge computing," *IEEE Access*, vol. 8, pp. 136119–136130, 2020, doi: 10.1109/ACCESS.2020.3011477.

[40] B. Li, Q. He, F. Chen, H. Dai, H. Jin, Y. Xiang, and Y. Yang, "Cooperative assurance of cache data integrity for mobile edge computing," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4648–4662, 2021, doi: 10.1109/TIFS.2021.3111747.

[41] W. Tong, B. Jiang, F. Xu, Q. Li, and S. Zhong, "Privacy-preserving data integrity verification in mobile edge computing," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Dallas, TX, USA, Jul. 2019, pp. 1007–1018, doi: 10.1109/ICDCS.2019.00104.

[42] P. Chaudhary, R. Gupta, A. Singh, and P. Majumder, "Analysis and comparison of various fully homomorphic encryption techniques," in *Proc. Int. Conf. Comput., Power Commun. Technol. (GUCON)*, New Delhi, India, Sep. 2019, pp. 58–62.

[43] Z. Qu, Y. Tang, G. Muhammad, and P. Tiwari, "Privacy protection in intelligent vehicle networking: A novel federated learning algorithm based on information fusion," *Inf. Fusion*, vol. 98, Oct. 2023, Art. no. 101824, doi: 10.1016/j.inffus.2023.101824.

[44] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020, doi: 10.1109/TII.2019.2938001.
[45] B. Chen and V. Chandran, "Biometric based cryptographic key generation from faces," in *Proc. 9th Biennial Conf. Austral. Pattern Recognit. Soc. Digit. Image Comput. Techn. Appl. (DICTA)*, Dec. 2007, pp. 394–401, doi: 10.1109/DICTA.2007.4426824.
[46] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris," in *Proc. Biometrics Symp.*, Tampa, FL, USA, Sep. 2008, pp. 59–64, doi: 10.1109/BSYM.2008.4655523.
[47] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Multi-biometrics based cryptographic key regeneration scheme," in *Proc. IEEE 3rd Int. Conf. Biometrics, Theory, Appl., Syst.*, Washington, DC, USA, Sep. 2009, pp. 1–7, doi: 10.1109/BTAS.2009.5339034.
[48] R. Schlegel, S. Kumar, E. Rosnes, and A. Graell i Amat, "Privacy-preserving coded mobile edge computing for low-latency distributed inference," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 3, pp. 788–799, Mar. 2022, doi: 10.1109/JSAC.2022.3142295.
[49] M. S. Giri, B. Gaur, and D. Tomar, "A survey on data integrity techniques in cloud computing," *Int. J. Comput. Appl.*, vol. 122, no. 2, pp. 27–32, Jul. 2015.
[50] W. Tong, W. Chen, B. Jiang, F. Xu, Q. Li, and S. Zhong, "Privacy-preserving data integrity verification for secure mobile edge storage," *IEEE Trans. Mobile Comput.*, vol. 22, no. 9, pp. 5463–5478, Sep. 2022, doi: 10.1109/TMC.2022.3174867.
[51] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018, doi: 10.1016/j.future.2016.11.009.
[52] R. S. Sandhu, "Role-based access control," *Adv. Comput.*, vol. 46, pp. 237–286, Jan. 1998, doi: 10.1016/S0065-2458(08)60206-5.
[53] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, Feb. 2015, doi: 10.1109/MC.2015.33.
[54] S. Hachem, A. Toninelli, A. Pathak, and V. Issarny, "Policy-based access control in mobile social ecosystems," in *Proc. IEEE Int. Symp. Policies for Distrib. Syst. Netw.*, Pisa, Italy, Jun. 2011, pp. 57–64, doi: 10.1109/POLICY.2011.50.
[55] P. Reddivari, T. Finin, and A. Joshi, "Policy-based access control for an RDF store," in *Proc. Workshop Semantic Web Collaborative Knowl. Acquisition*, Jan. 2007, pp. 1–10.
[56] G. Abirami and R. Venkataraman, "Performance analysis of ABAC and ABAC with trust (ABAC-T) in fine grained access control model," in *Proc. 11th Int. Conf. Adv. Comput. (ICoAC)*, Chennai, India, Dec. 2019, pp. 372–375, doi: 10.1109/ICoAC48765.2019.246870.
[57] N. Sharma and R. Ketti Ramachandran, "The emerging trends of quantum computing towards data security and key management," *Arch. Comput. Methods Eng.*, vol. 28, no. 7, pp. 5021–5034, Apr. 2021, doi: 10.1007/s11831-021-09578-7.
[58] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, "Quantum computing on encrypted data," *Nature Commun.*, vol. 5, no. 1, p. 3074, Jan. 2014, doi: 10.1038/ncomms4074.
[59] C. Cicconetti, M. Conti, and A. Passarella, "QKD-secure ETSI MEC," in *Proc. IEEE 15th Workshop Low Temp. Electron. (WOLTE)*, Matera, Italy, Jun. 2022, pp. 1–4, doi: 10.1109/WOLTE55422.2022.9882872.
[60] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000, doi: 10.1103/physrevlett.85.441.
[61] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230504, doi: 10.1103/physrevlett.94.230504.
[62] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden, "Coherent one-way quantum key distribution," *Proc. SPIE*, vol. 6583, pp. 194–197, May 2007, doi: 10.1117/12.722952.
[63] A. Ling, M. Peloso, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Experimental E91 quantum key distribution," in *Proc. SPIE, Adv. Opt. Concepts Quantum Comput., Memory, Commun.*, San Jose, CA, USA, vol. 6903, Feb. 2008, Art. no. 69030U, doi: 10.1117/12.778556.
[64] S. N. Molotkov, "Cryptographic robustness of a quantum cryptography system using phase-time coding," *J. Experim. Theor. Phys.*, vol. 106, no. 1, pp. 1–16, Jan. 2008, doi: 10.1134/s1063776108010019.
[65] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503, doi: 10.1103/physrevlett.108.130503.
[66] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New J. Phys.*, vol. 17, no. 4, Apr. 2015, Art. no. 043027, doi: 10.1088/1367-2630/17/4/043027.
[67] Z. Qu, I. B. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection," *Opt. Lett.*, vol. 41, no. 23, p. 5507, Nov. 2016, doi: 10.1364/ol.41.005507.
[68] A. Mizutani, K. Tamaki, R. Ikuta, T. Yamamoto, and N. Imoto, "Measurement-device-independent quantum key distribution for Scarani–Acin–Ribordy–Gisin 04 protocol," *Sci. Rep.*, vol. 4, no. 1, p. 5236, Jun. 2014, doi: 10.1038/srep05236.
[69] O. Amer, V. Garg, and W. O. Krawec, "A standardized design for sifting in quantum key distribution software," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Rio de Janeiro, Brazil, Dec. 2022, pp. 808–813, doi: 10.1109/GCWkshps56602.2022.10008730.
[70] L. Bialowons, E. Fitzke, M. Tippmann, O. Nikiforov, and T. Walther, "A scalable multi-user QKD hub for entanglement-based phase-time coding," in *Proc. Quantum Inf. Meas.*, Jan. 2021, pp. 1–4, doi: 10.1364/qim.2021.m2c.4.
[71] Y. Guo, Z. Lu, H. Ge, and J. Li, "Revocable blockchain-aided attribute-based encryption with escrow-free in cloud storage," *IEEE Trans. Comput.*, vol. 72, no. 7, pp. 1901–1912, Jul. 2023, doi: 10.1109/TC.2023.3234210.
[72] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers," *IEEE Trans. Consum. Electron.*, early access, Nov. 9, 2024, doi: 10.1109/TCE.2023.3331306.
[73] Z. Kang, J. Li, J. Shen, J. Han, Y. Zuo, and Y. Zhang, "TFS-ABS: Traceable and forward-secure attribute-based signature scheme with constant-size," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 9, pp. 9514–9530, Sep. 2023, doi: 10.1109/TKDE.2023.3241198.
[74] Z. Qu, Y. Meng, B. Liu, G. Muhammad, and P. Tiwari, "QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 40–49, Jan. 2024, doi: 10.1109/JIOT.2023.3285388.
[75] N. Chen, J. Li, Y. Zhang, and Y. Guo, "Efficient CP-ABE scheme with shared decryption in cloud storage," *IEEE Trans. Comput.*, vol. 71, no. 1, pp. 175–184, Jan. 2022, doi: 10.1109/TC.2020.3043950.
[76] R. Zhang, J. Li, Y. Lu, J. Han, and Y. Zhang, "Key escrow-free attribute based encryption with user revocation," *Inf. Sci.*, vol. 600, pp. 59–72, Jul. 2022, doi: 10.1016/j.ins.2022.03.081.
[77] J. Li, R. Zhang, Y. Lu, J. Han, Y. Zhang, W. Zhang, and X. Dong, "Multiauthority attribute-based encryption for assuring data deletion," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2029–2038, Jun. 2023, doi: 10.1109/JSYST.2022.3208149.
[78] Y. Meng, Z. Qu, G. Muhammad, and P. Tiwari, "Secure and efficient data transmission based on quantum dialogue with hyperentangled states in cloud office," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100911, doi: 10.1016/j.iot.2023.100911.
[79] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 785–796, Sep. 2017, doi: 10.1109/TSC.2016.2520932.
[80] M. K. Hooshmand and D. Hosahalli, "Network anomaly detection using deep learning techniques," *CAAI Trans. Intell. Technol.*, vol. 7, no. 2, pp. 228–243, Jan. 2022, doi: 10.1049/cit2.12078.
[81] Y. Deng, Z. Zeng, K. Jha, and D. Huang, "Problem-based cybersecurity lab with knowledge graph as guidance," *J. Artif. Intell. Technol.*, vol. 2, pp. 55–61, Feb. 2022, doi: 10.37965/jait.2022.0066.
[82] M. Rahman, A. Murmu, P. Kumar, N. R. Moparthi, and S. Namasudra, "A novel compression-based 2D-chaotic sine map for enhancing privacy and security of biometric identification systems," *J. Inf. Secur. Appl.*, vol. 80, Feb. 2024, Art. no. 103677, doi: 10.1016/j.jisa.2023.103677.
[83] M. Sahu, N. Padhy, S. S. Gantayat, and A. K. Sahu, "Local binary pattern-based reversible data hiding," *CAAI Trans. Intell. Technol.*, vol. 7, no. 4, pp. 695–709, Aug. 2022, doi: 10.1049/cit2.12130.
[84] S. Namasudra, *Taxonomy of DNA-Based Security Models*. Boca Raton, FL, USA: CRC Press, 2018.
[85] M. Wang, H. Yi, F. Jiang, L. Lin, and M. Gao, "Review on offloading of vehicle edge computing," *J. Artific. Intell. Technol.*, vol. 2, pp. 132–143, Aug. 2022.

KRANTHI KUMAR SINGAMANENI received the Ph.D. degree in applied cryptography and cloud security from GITAM Deemed to be University, Visakhapatnam, Andhra Pradesh, India, in 2020, the M.Tech. degree in information technology from JNTU Kakinada, Andhra Pradesh, in 2015, and the M.Tech. degree in computer science from Acharya Nagarjuna University, Guntur, Andhra Pradesh, in 2010.

He is currently with the Department of Computer Engineering and Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, India. He has about 16 years of experience in teaching, industrial, and research areas of computer science and a Data Specialist with IBM. His industrial experience includes data warehousing and big data analytics tools. His research interests include applied cryptography, networks, and cloud security.

Dr. Singamaneni has 25 research articles in reputed journals indexed by SCI, WOS, SCOPUS, and UGC and eight patents that address solutions for real-time problems in engineering speak volumes about his penchant for research. He is a member of ISTE, CSI, IFERP, and IAENG.

GHULAM MUHAMMAD (Senior Member, IEEE) received the B.S. degree in computer science and engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 1997, and the M.S. degree in knowledge-based information engineering and the Ph.D. degree in electrical and computer engineering from Toyohashi University and Technology, Toyohashi, Japan, in 2003 and 2006, respectively.

He is currently a Professor with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He holds three U.S. patents. He has authored or coauthored more than 300 publications, including IEEE/ACM/Springer/Elsevier journals and flagship conference papers. His research interests include AI, machine learning, image and speech processing, and smart healthcare.

Prof. Muhammad was a recipient of the Japan Society for Promotion and Science Fellowship from the Ministry of Education, Culture, Sports, Science and Technology, Japan.

ZULFIQAR ALI (Member, IEEE) received the M.Sc. and M.S. degrees in computer science from the University of Engineering and Technology Lahore, Pakistan, in 2007 and 2010, respectively, and the Ph.D. degree in electrical and electronic engineering from the University of Technology Petronas, Malaysia, in 2017.

He was a Researcher with the Department of Computer Engineering, King Saud University, from 2010 to 2018, and a Research Fellow with the BT Ireland Innovation Center, Ulster University, from 2018 to 2020. He is currently a Lecturer with the School of Computer Science and Electrical Engineering, University of Essex, Colchester, U.K. His current research interests include explainable AI, digital speech and image processing, privacy and security in healthcare using watermarking, and audio forgery detection.

Dr. Ali is a fellow of the Higher Education Academy, Advance HE, U.K. He has served in technical program committees for the IEEE Smart World Congress and IEEE ACAI. He is also serving as an Associate Editor for the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS.