electronics

MDPI

Article

An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality

Kranthi Kumar Singamaneni [1,†], Ali Nauman [2,†], Sapna Juneja [3], Gaurav Dhiman [4,5,6,7], Wattana Viriyasitavat [8], Yasir Hamid [9,*] and Joseph Henry Anajemba [9,*]

1 Department of Computer Science and Engineering, School of Technology, GITAM Deemed to be University, Visakhapatnam 530045, India
2 Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Korea
3 Department of CS, KIET Group of Institutions, Delhi NCR, Ghaziabad 201206, India
4 Department of Electrical and Computer Engineering, Lebanese American University, Beirut 1102 2801, Lebanon
5 University Centre for Research and Development, Department of Computer Science and Engineering, Chandigarh University, Gharuan, Mohali 140413, India
6 Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India
7 Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, CP, Mexico
8 Business Information Technology Division, Department of Statistics, Faculty of Commerce and Accountancy, Chulalongkorn University, Bangkok 10330, Thailand
9 Information Security and Engineering Technology, Abu Dhabi Polytechnic, Abu Dhabi 111499, United Arab Emirates
* Correspondence: yasir.hamid@adpoly.ac.ae (Y.H.); joseph.anajemba@adpoly.ac.ae (J.H.A.)
† These authors contributed equally to this work.

Citation: Singamaneni, K.K.; Nauman, A.; Juneja, S.; Dhiman, G.; Viriyasitavat, W.; Hamid, Y.; Anajemba, J.H. An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality. *Electronics* **2022**, *11*, 3510. https://doi.org/10.3390/electronics11213510

Academic Editors: Celestine Iwendi and Thippa Reddy Gadekallu

Received: 26 September 2022
Accepted: 21 October 2022
Published: 28 October 2022

Abstract: Cloud computational service is one of the renowned services utilized by employees, employers, and organizations collaboratively. It is accountable for data management and processing through virtual machines and is independent of end users' system configurations. The usage of cloud systems is very simple and easy to organize. They can easily be integrated into various storages of the cloud and incorporated into almost all available software tools such as Hadoop, Informatica, DataStage, and OBIEE for the purpose of Extraction-Transform-Load (ETL), data processing, data reporting, and other related computations. Because of this low-cost-based cloud computational service model, cloud users can utilize the software and services, the implementation environment, storage, and other on-demand resources with a pay-per-use model. Cloud contributors across this world move all these cloud-based apps, software, and large volumes of data in the form of files and databases into enormous data centers. However, the main challenge is that cloud users cannot have direct control over the data stored at these data centers. They do not even know the integrity, confidentiality, level of security, and privacy of their sensitive data. This exceptional cloud property creates several different security disputes and challenges. To address these security challenges, we propose a novel Quantum Hash-centric Cipher Policy-Attribute-based Encipherment (QH-CPABE) framework to improve the security and privacy of the cloud user's sensitive data. In our proposed model, we used both structured and unstructured big cloud clinical data as input so that the simulated experimental results conclude that the proposal has precise, resulting in approximately 92% correctness of bit hash change and approximately 96% correctness of chaotic dynamic key production, enciphered and deciphered time as compared with conventional standards from the literature.

Keywords: cloud model; QH-CPABE; privacy; security

1. Introduction

Cloud Computing offers many types of facilities, among them Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), providing enormous malleability for cloud consumers. Because of the exponential growth of the decentralized reckoning and WWW cyberspace structures, there is a substantial prerequisite for cloud consumers' personal and confidential data management and disseminating facilities provided via cloud-based environments. The third-party service-based dealer must use a trustworthy and consistent control supervision approach to improve the privacy and security aspects for cloud consumers. Specifically, such scenarios as the big data of cloud consumers stored over the cloud-based environment cultivates, then it leads user sensitive data such as consumers' pecuniary info, biometric info, and public media info to be tremendously exposed over cyberspace and simply retrieved by intruders and attackers via some malicious third-party applications and [1].

The Identity-based Encipherment (IBE) and Attribute-based Encipherment (ABE) methodologies are established for the maintenance of consumers' privacy by concealing a portion of consumers' sensitive data. The enhanced editions of conventional IBE and ABE enciphered approaches comprise a look-up approach for enciphered consumer text [2–5]. Therefore, the same technique can be employed in security maintenance apps over the domains such as banking, biomedical, and government warehouses to achieve a similar standard of integrity, privacy, and implementation alongside alternative traditional approaches are extra expensive w.r.t computational, storage costs, and network transmission expenditures. Most of the conventional Ciphered text Policy-ABE techniques failed to fulfill the requirements of ascendable diversified multimedia storing and distribution [6]. To address the abovementioned problems HQCP-ABE (Hybrid Quantum-based CP-ABE) technique is coined that is capable of handling large scales of diversified data with secure distribution over the cloud and cyberspace.

- Large volumes of cloud consumers' text messages are enciphered with the help of the encipherment method then produce the consumers' ciphered text.
- A key-policy-based tree is built, and the multimedia data are enciphered via the available keys by thinking cloud consumers' admittance freedoms.
- Consequently, the cloud consumer has essential attributes that fit with cloud consumers' access-policy rights, and the decipherment algorithm is implemented.

In the case of cell phones, the trouble occurs due to inadequate availability of resources. This problem may be addressed with the subcontracting procedure of computational procedures to cloud servers. Because of this approach, we can improve the efficacy, security, privacy, and confidentiality of the cloud consumers' sensitive info [7–9].

The primary objective of the distribution of keys among multiple cloud consumers is to restrict the sharing of private and secret info primarily to concur on a chaotic, arbitrary key, which persists secret after an antagonist overhears their transmission. In traditional cryptographical and info methods, it is taken for granted that sensitive transmission may be constantly observed passively by intruders and cyber criminals, such that the cyber attackers and hackers guess their whole end-to-end transmission info such as type of data, source IP, destination IP, open ports available, possibility of data injections, etc., without knowledge and intelligence of the intended sender and receiver. But in the case of communication using elementary quantum systems, it is impossible to track the state of info during transmission of data because that intruder can't predict the state of photon during transmission. When sensitive consumers info is enciphered over the fundamental quantum classifications such as the solitary photon, it may be conceivable to yield a communication link whose transmission [10] may not in code be consistently observed or altered by an intruder unaware of confident info cast-off in establishing the communication. The intruder does not even get a portion of information about such communication without troubling it in a chaotic and unmanageable manner, possibly to be discovered by the links' intended cloud consumers [11]. The important quantum acreage concerned, a demonstration of

Heisenberg's uncertainty law, is the presence of a combination of principles that are antagonistic in the perception that determining one acreage essentially arbitrarily changes the values of the others. For instance, determining an individual photon's co-linear SOP randomizes its globular polarity [12–14], and vice versa. In more general, any set of SOPs will be described as a base if they relate to a consistently discernible policy of a single photon, and two basements will be treated to be congruent [15,16]. If quantum physical properties proclinate, that determination of one acreage entirely randomizes the others. The elementary quantum key distribution (QKD) standard starts with a cloud consumer A transmits a randomized flow of the four canonic types of differentiated photons to another cloud consumer B. B then selects arbitrarily and individually for each photon (and separately of the preferences made by A, of course, since these preferences are unfamiliar to him at this instance) whether to determine the photon's rectilinear or circular SOP's. B then reveals openly which type of measurement he selected but not the output value of the measurement, and A reveals to B openly whether he did the exact measurement (i.e., horizontal, vertical, or left/right orthogonal). A and B then approve openly throwing away all cubit postures for which B executed the incorrect calculation. Likewise, they decide to remove cubit spots where B's polarizers are unsuccessful in identifying the photon at all—a general occurrence with present polarizers at ophthalmic wavelengths. The polarization angles of the rest of the cubits are translated as bit 0 for horizontal or left-orthogonal and bit 1 for vertical and right-orthogonal. The resultant binary array of bits could be distributed private info among A and B, supplied that there is no snooping on the quantum link. The outcome of the above-mentioned stages is described as quantum communication (or occasionally the intense cubit transmission to accentuate, which was acquired soon after this procedure).

The rest of the paper is organized as follows: In Section 2, a review of the related literature works is presented. In Section 3, quantum and related cryptographic models and issues are discussed, research methodology is discussed in Section 4, Section 5 presents the results and analysis, and finally, the paper concludes in Section 6.

2. Related Work

2.1. Conventional Hashing Standards on Cloud Environment

Ref. [9] proposed a Compound-Agency ABE scheme which enables any user to act as authorization. There is no need for mutual communication instead of creating a primary group of generally associated metrics. Any user may directly behave like an ABE authority by constructing a public key and distributing private keys to several people that signify their characteristics. Any person may encipher text in the form of any Boolean procedure on user attributes released by any selected group of agencies. Ultimately the proposed structure need not involve any third-party agency. Ref. [10] presented an IBE unrecognizability standard on connectionless kinds of data. They offered a partial secret prerogative management method and called it anonym control to accomplish info and individual confidentiality over whole admittance approval methods. It regulates all prerogative functions over the connectionless kind of data.

Ref. [16] examined the disadvantages of conventional hash-based techniques, which require a huge volume of resources. To address this drawback, authors combined the Distinct Chaotic based Mapped Network (DCMN) with Cyclic-DM, functional employs numeral disciplines as an alternative to applying decimal positions. Researchers implemented their proposal with better efficacy and conflict endurance than the existing standards. The authors also simulated an improved sort of randomized hash standard, which is applied over the parallel randomized neural networks. Their suggested purpose is conflict endurance and yields good results, which are demonstrated through the simulated outcomes. The authors also acknowledged a novel kind of threat and named that as quasi-conflict threat. Consequently, additional advanced research is needed to avert this threat.

Ref. [17] employed an elliptical curve cryptographic approach (ECC) and chaotic scheme to design a novel digital sign process. The authors combined simplex hash tech-

nique, a two-dimensional pro-chaotic map with asymmetric cryptographic standards to outline their innovative methodology. Their method inhibits redundant sign key attacks. Thus, the anticipated process is consistent, reliable, and easy to apply in real-time situations. In forthcoming works, they enhance the same approach over other standards such as Message Digest (MD), Secure Hash Algorithm (SHA) [18], Hash-based Message Authentication Code (HMAC) [19], whirlpool, and so on. Researchers investigated that several research works have been conducted in this field focused on computational functionality and novel apps. Researchers also examined several former existing standards analyzing store space patterns over the cloud, which headed to a variety of cloud space allocation and sensitive data distribution challenges that even address a few alternative existing challenges such as consumer text encipherment, cloud edge preservation, and statistical evidence. The whole of these processes is monitored and handled by the vision administration system. A few additional pros of this approach include object confidentiality, info accessibility, secure users' sensitive info distribution, etc. Every consumer has their personal view and has a protected limit.

Discretionary Access Control (DAC) [20] and Mandatory Access Control (MAC) [21] approaches are combined along with their authoritative characteristics and mix-up of the above-mentioned models and designed a new model called Role-based admittance controller (RBAC) [22]. Corresponding to the fundamental idea of asymmetric encipherment, the mutual procedure of enciphering and deciphering are begun with the source call for the public key from Key Dissemination Controller (KDC). The Public Key Infrastructure (PKI) [23] validates the public by logging and transferring it to the destination. The source needs the public key for enciphering the source text effectively. The enciphered text is transferred from source to destination over the cloud network, which is not secure. At the destination end, they require the associated private key for successful decipherment of the source text. This technique has a few cons, such as that the source requires interaction with PKI-admin to further interact with the designation. Most of these methods comprise four end-to-end stages: the initialization stage, key generation stage, encipherment, and decipherment stages.

Ref. [24] Identity-based Encryption Models and Issues in [1], the authors have proposed a new kind of crypto-graphical system that supports every set of clients to transmit their information safely and to authenticate every pair of client's signs with no need for swapping their public/private keys, no need of maintaining key almanacs, and no need of requiring the facilities of an intermediate party. The researchers of [25] presented a competent IBE approach that is absolutely reliable with no integration of chaotic oracles. Additionally, they showed that the coined methods could be applied to develop a novel key signature procedure that is more secure upon the executable Diffie-Hellman notion. Boyen et al. used an IBE-based cryptographic structure that introduces entirely secret ciphered texts and classified key allocation upon the moderate Decision Linear complexity hypothesis over the bi-linear groups. They resolved two primary issues relating to secret IBE by providing privacy along with a comprehensive secret HIBE at all stages in the order. The authors in [26] proposed an ID-based cloud storage system where mutual requests after the intra-field and inter-field are deemed, and complicity incidents could be avoided. Additionally, the admittance approval could be decided by the intended user individually. Ref. [27] presented a scheme for understanding complicated admittance management on enciphered text; by applying this scheme, the enciphered text could remain classified even though the third-party server is not trustable; additionally, this method has more confidence over the complicity occurrences by using users' attributes as IDs, while the enciphered text decides an access policy intended for the specific user to decipher. Ref. [28] developed a novel cryptographic structure for well-refined distribution of enciphered text that user-ciphered text is classed with a group of characteristics and secret keys are related with admittance approval that decides which ciphered texts a specific consumer is capable of deciphering. The authors practically validate the pertinence of the proposed structure

for the distribution of users' sensitive data over the public cloud platforms with enhanced security and privacy towards users' sensitive data.

2.2. Drawbacks of Conventional Attribute Encipherment Approaches

Usually, the cloud servers have numerous commercial and business-oriented applications and user-specific data, which leads to the diminishing of original user rights over their information. Nonetheless, everyday agility and sensitivity are evolving. Recently, as cloud proficiency has risen, there is much less requirement for organizations to emphasize their technical and support facilities and resources. To improve the level of advancement, they emphasize their organizational guidelines and practices. Therefore, daily cloud environment practice and its apps are spreading exponentially [29]. Even consumers gain system memories, processors, bandwidth, and space through the net. Cloud platforms comprise several practices, such as maintenance-related design, virtual machine computation, WWW, etc. Cloud platforms and app-related techniques also have numerous security problems. Because of the demand for sufficient sources, cloud services are required by various companies and organizations. The primary objective of cloud service providers is to optimize resources [30]. Efficient resource sharing is one more vital characteristic of a cloud computational environment that supports efficient resource sharing for all cloud consumers dynamically. At the same time, the consumer finishes the utilization of a specific cloud resource and afterwards, the same resource is allocated to another consumer as per their service requirement. Because of all these advantages of cloud computing, many companies and consumers are migrating from conventional technologies to cloud technology. The security of cloud computing platforms would comprise various technologies, IT checks, and methods to protect users' sensitive info, services, and resources. Security of the cloud has been a primary concern since it is extremely vulnerable to attacks. Consequently, the cloud needs a few additional security checks and preliminaries [31]. The existing basic design of security is superseded as consumers do not need to use their individual resources and infrastructure. Consumers typically miss their access control on their data via the subcontracting technique when the data is positioned upon a cloud server and provide full access control to unreliable cloud service providers. Though the cloud environments have a reliable and secure server, there are large volumes of internal and external threats and intruders that cause cloud environment susceptibilities that endanger the cloud consumer's data privacy, security, integrity, and data access control. Unreliable cloud service providers continuously suppress their structure's vulnerability to maintain their standing [32]. By eliminating a smaller amount of retrieved info, cloud platforms are every so often enhanced because many clients and corporations might use cloud services to preserve their sensitive data.

Ref. [33] launched a novel user-secure confidentiality-based method for cloud environments. Together privacy and security are counted as the primary objective to enhance the effectiveness of cloud platforms. At present, there are several service-based apps that could be strengthened by implementing the same over the cloud environments. There is no considerable volume of studies that have been conducted throughout the procedure of secrecy maintenance over wireless cloud platforms. This method is also called privacy-augmented safety framework (PASF). This approach requires advanced consumer admittance management to fulfill the disparity among intruders and hackers. Ref. [34] announced an improved hand-over validation method and key prior allocation over the cloud internetworks. The ticket-centered encipherment method is treated as a multifaceted method to offer privacy and integrity toward wireless cloud environments. This method allows secure transmission among iPad, desktops, laptops, mobiles, and several types of connectionless nodes. The primary objective of this method is to reduce the overall hand-off lag. Parallelly this method improved the conventional key prior-dissemination technique during the hand-off validation process. The authors applied a novel ABE-centered validation to encipher each specific key prior dissemination text. This comprehensive method of key prior-dissemination techniques require stable computational and transmission costs. Developing the key policy-

ABE process [35], Wang et al. introduced a novel technique that stimulates portable node platform info security and consumer access annulment. The authors blended lethargic re-encipherment and substitution-based re-encipherment concepts to attain consumer rights, privacy, consumer private key responsibility, and to decrease operating expenses. As this method stimulates well-organized admittance policies, the computational time needed is relatively large, which is a drawback of the presented approach. In the future, we will extend the same work to eradicate this drawback and reduce computational time. Ref. [36] designed a vibrant re-enciphered ciphered text-ABE model. The primary objective of this approach is to provide security and privacy to records and file distribution over wireless cloud environments. This method permits wireless facility providers to re-encipher and routes the distributed info to certain validated and intended users to disclose sensitive info load-up supervision and data access management. In a wireless-based cloud platform, by means of providing security about policy-based admittance management and actual user info, the planned system is appropriate for distributing users' sensitive data securely. They corroborated this method and developed that the novel method does not obstruct the safety of cipher text-ABE and observed incredible efficacy. The user characteristics (attributes) are allotted by means of several substances corresponding to their urgency. The importance of user attributes makes this method most appropriate and suitable to deploy over the wireless cloud platforms as compared to other existing methods. This method is nearer to the practical situation. This method requires a threshold admittance control structure. Ref. [37] combined the selected user attributes of ciphered text-ABE approach through homomorphic encipherment. The authors' approach permits clients to acquire the required info from records warehoused over the wireless cloud servers deprived of copying the ciphered content. Record and file distributed structures are the popular facilities offered through the ISPs. They formed a connectionless record structure and amalgamated it with ciphered text-ABE. With this method, authors established a safe and efficient record distribution structure (SRDS) that provides additional security and privacy. Ref. [38] examined and discovered the time-ingesting kind of individual threaded hash-based approach and offered a novel hash technique that encourages concurrency. The anticipated method needs less time since this method operates over multiple CPU units. The authors also acknowledge that their method offers the best privacy, security, fast, and efficacy. They found one drawback of ciphered text-ABE approach, i.e., the actual consumer has no clue regarding their earliest data. Therefore, the degree of well-organized admittance diminishes. Prior to the intended consumer exchanging info, it explores whole relationships among information admittance policy structures and consumers and their attributes. Beyond this technique, actual info in the form of the consumer's final data is attained. Consumer admittance is attained only where attributes admittance structure matched with the actual consumer's admittance structure. The authors presented a rationale for their proposal and examined the recommended proposal. They stated that they may conduct their future work over multiple users controlled by one-to-all networks. The searchable Encipher-based Admittance Control Alert Search (SE-ACAS) method is offered in [39] as admittance control fortification for the searchable encipherment approach by P. Sheng-lu et al. The primary goal of this approach is to enhance the admittance control over the user's info. This is a mixed procedure that involves together of searchable encipherment and admittance control methods. This technique accomplishes privacy and security after wireless cloud platforms and consumer perception. The projected idea constrains consumer info admittance for unapproved clients also. According to the properties of admittance control alert search, the crossbred method is further susceptible to illegal incidents. To address this con, the researchers included a reliable sieve to the consumer website. They amalgamated the notions of searchable symmetrical encipherment and key policy-based ABE methods. The proposed approach has a few pros, and they are multiuser admittance control, privacy, and maintenance of admittance control alert search properties. They assessed the operation of the methods as per the lookup and index strategies. The authors also confirmed that if the time spent for indexing grows automatically when the collection size rises. A novel and

revised form of ciphered text policy-based ABE method upon searchable scheme [40]. The researchers studied the decisional-based Diffie-Hellman (DBDH) and Discrete Logarithm (DL) assumptions to improve confidentiality for their proposed idea. Their method additionally maintains languid substitution-based re-encipherment. Multi-counted attributes facilitate to conceal consumers' text via the rule-based admittance policies, which again provides the elasticity of the proposal. In the future, the proposed work might comprise an unsigned multi-distributed authorization approach to enhance inventiveness. Likewise, the security, banality, efficacy, and implementation could be boosted by offering additional attempts. Ref. [41] projected a secret policy validated CP-ABE with a decipherment exploration process with a secret policy for providing privacy, and outsourced decipherment exploration may validate the exactness of the deciphered result features. Ref. [42] proposed a Multi-Authority Ciphertext Policy Attribute Based Encryption with Elliptic Curve Cryptography (MA-CPABE-ECC) for cloud data privacy because of its minimal key size, more security, and need less time for computation. In this work, the keys produced act as elliptical curve pairs of points; based on this, they performed encipherment which provides superior security.

3. Quantum and Related Cryptographic Models and Issues

ABE standard is one of the finest cost-effective methods to provide data privacy over the cloud environment with various user personal attributes and access rules. In this standard, each consumer has a number of certified attribute collections, access policies, and a private key. For the duration of a few centuries, numerous ABE standards have been proposed. Because the key size [43] and a group of consumer attributes need initialization at the setup phase, the volume of the user's data and associated group of attributes are quadratically restricted to security techniques. In a basic ABE standard, the access structures encipher secrecy essentials, secret keys, and ciphered text. Consumers can decipher their original text if and only if the associated attribute set must satisfy their admittance policies. Because of this model's flexible behavior, ciphered text policy-ABE operates as a basic module for several dependent standards. The drawback of key policy-ABE is that it has no control over their decipherment liberties which is resolved in ciphered text policy-ABE scheme. Apart from this, the proposed standards could not be applied to the large-scale organizational strategy. This drawback is because of the less tractability and lack of revocation. The entire procedure of decipherment needs a single group of attributes. Therefore, consumers are qualified to choose only one attribute or group of attributes after that major group. Hierarchy-based ABE standard was established with the help of the basic ABE model. This entire method was characterized in a hierarchical fashion. The initiation procedure for the key is taken out by a core controller, which works together with numerous field controllers—each domain admin works together with several end consumers. The stated standard has apps over the cloud environment along with substitutional-based re-encipherment. Asymmetric cryptographical methods [44] enable the property that anybody could encipher their data with the help of their public key, and that enciphered data should be deciphered successfully if and only if that intended user can have the private key of the associated pair of that public key Because of this individual pair of keys, this approach needs a large number of paired public and private keys when the number of users increases even though they have common data to share, which is the major drawback of this approach. The abovementioned drawback is easily addressed by ABE schemes which facilitate users to decipher emails if their decipher key satisfies the ciphered text admittance policy. Consumer's sensitive info could be protected from intruders and hackers. Ref. [45] proposed a framework in which consumer attribute-based properties are secured through a dynamic non-linear multinomial chaotic map task to initialize the key, encipherment, and decipherment. The authors used the combination of structured and unstructured large volumes of consumer medical data as inputs for consistent validation and encipherment. As related to the current approaches, this practical model findings determined that the acknowledged model is further accurate with respect

to the rate of change of bits, and time required for randomized key initiation, encryption, and decryption. [46] analyses the keys age utensil and encipherment and decipherment computations necessary over the cloud environmental circumstances, the authors projected a novel security method for a cloud environment that contemplates the quantum-key distribution (QKD) and incapacitates dissimilar safety and user privacy issues.

Conventionally Developed Chaotic Hash Map

The planned technique is a protracted hash-based chaotic map, reliant upon a set of chaotic maps along with a renewed hash key base. Here we gathered cloud consumer's info and passed that as input to calculate the value of the hash-based chaotic map [47,48].

- In the initial instruction, the consumer's data is converted to an array of bytes denoted as X [ ]. If the array does not contain the data in powers of two, then apply the padding method to represent the array data as powers of two.
- The transformed data is further alienated into B blocks of fixed or variable size in the 2nd instruction.
- If needed, apply padding again for a few of or all the B blocks to represent that block data in the form of powers of two in 3rd instruction.
- For each iteration, a new secret key is generated from the chaotic, random method CR fourth instruction. An expanded chaotic random method is utilized to enhance the randomization procedure to produce the session-wise hash key. To enhance the intricacy of the reliability and trust count, here used, a separate set of chaotic functions.
- With the help of the abovementioned instructions, we successfully produced the X[i] value in the fifth instruction.
- In sixth instruction, various substitutional and transformational procedures are applied to randomize the outcomes of instruction 5th along with row and column shifts.
- In the seventh instruction, we integrated the hash value Hv of each iteration.

4. The Projected Model

Security over the cloud [49] has turned into a complex and one of the important research fields with large volumes of sensitive consumer data and authenticated access structure design. To achieve more secure and reliable cloud services, we need to incorporate complex encipherment strategies; for this purpose, we used an enhanced Attribute Based Encipherment (ABE) [50] process along with a quantum key distribution model (QKD). The QKD is applied for the proposed CP-ABE model to provide additional security for the user's sensitive data over public networks. The QKD-based crypto-graphical approach is entirely based upon quantum physical and mechanical properties. The primary goal of QKD is to generate a secret key used for cloud consumers' info encryption without the help of a third-party service provider. Conventional ABE schemes are not reliable, not secure, and vulnerable to M-I-M Attacks (Man in the Middle Attacks) [41] over the transmittable sensitive info over the cloud and internet. When the size of the consumers' data grows, conventional ABE schemes go bad w.r.t various parameters, such as encipherment time, key generation time, and revocation facility, etc. To address the abovementioned key issues, we use up the message digest, integrity, and QKD approach, which proposes a new CP-ABE scheme presented over the cloud platform. Along with these, we take some vital parameters of chaotic methods comprising pseudo-random number production property and sensitivity property to the actual primary requirements. Using all these properties, we can produce more complex confusion and diffusion characteristics, which are crucial for the encipherment process. For consumer information confidentiality and validation task, hash-based chaotic methods are employed to enhance the consumer's info security and arbitration. Chaotic mappings are methods that are extremely sensitive to their initial requirements, which can develop highly variant outcomes. A small change in starting inputs towards chaotic methods can generate distinct outcomes.

Tri-linear Map: Tri-linear maps are a set of numerous arbitrary values that are linearly separate from each arbitrary value. Further accurately, a tri-linear map is a function

$$F_n: V_{S1} \times V_{S2} \times \ldots \ldots \times V_{SN} \to \omega \tag{1}$$

here $V_{S1}, V_{S2}, \ldots, V_{SN}$ and ωare vector spaces with the subsequent characteristic. For every j, if all the arbitrary values except V_{Sj} kept fixed, then F_n ($V_{S1}, V_{S2}, \ldots, V_{SN}$) acts as a tri-linear function of V_{Sj}. One arbitrary value of a tri-linear function is a linear function, and two arbitrary values is a bilinear function. More generally, a multi-linear map of three arbitrary values is called a tri-linear map. If the subdomain of a tri-linear function is the domain of scalars, it is called a tri-linear structure [48]. If all arbitrary values fit into the similar vector space, then we may assume they are symmetrical, anti-symmetrical, and chaotic tri-linear functions. The later match is if the inherent areas (spaces) have a distinguishing behavior after two; otherwise the previous two match.

Let Fn: $V_{S1} \times V_{S2} \times \ldots \ldots \times V_{SN} \to \omega$be a tri-linear functional map among finite-dimensional vector spaces, where V_{Sj} has dimension d_{nj}, and ωhas dimension d_n if we choose a basis $\{e_{j1}, e_{j2}, \ldots, e_{jdj}\}$ for each V_{Sj} and a basis $\{b_{j1}, b_{j2}, \ldots, b_{jdj}\}$ for ωwith the help of bold part of vector spaces, then we can define a collection of scalars $S^c{}_{i1,i2\ldots,in}$ by

$$F_n\,(e_{1j1}, e_{1j2}, \ldots, en_{jn}) = S^1{}_{i1,i2\ldots,in}\, b_{j1} + \ldots \ldots + S^d{}_{i1,i2\ldots,in}\, b_{jdj} \tag{2}$$

Then the scalars $\{S^c{}_{i1,i2\ldots,in} \mid 0 < i_j < d_{j-1,}\ 0 < c < d-1\}$ completely determine the tri-linear method F_n. In particular if

$$V_{Si} = \sum_{i=0}^{dj} v_{ij}\, e_{ij} \text{ for } 0 < j < n, \text{ then} \tag{3}$$

$$F_n\,(V_{S1}, V_{S2}, \ldots V_{SN}) = \sum_{i_1=0}^{d_1} \ldots \sum_{i_n=0}^{d_n} \sum_{c=1}^{d} S^c{}_{i_1\, i_2 \ldots in}\, Vs_{1j_1} \ldots\ Vs_{nj_n}{}^{b_c} \tag{4}$$

Admissible Trilinear Map: Let's take a tri-linear function

$$T_n:\ M^3 \times M^3 \times M^3 \to M \text{ where } V_j = M^3,\ d_j = 3,\ j = 1,\ 2,\ 3, \text{ and } = M,\ d = 1. \tag{5}$$

A basis for each Vj is

$$\begin{gathered}\left\{e_{j1}, \ldots, e_{jdj}\right\} = \{E_1, E_2, E_3\} = \\ \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}\end{gathered} \tag{6}$$

$$\text{Let } T_n\,(e_{1k}, e_{2j}, e_{3i}) = F_n\,(e_k, e_j, e_i) = S_{kji} \tag{7}$$

where k, j, i ∈ (1, 2, 3). In other words, the constant S_{kji} is a method value at one of the eight possible triples of basis vectors, each vector $v_k \in V_k = M^3$ can be expressed as a bilinear combination of the basis vectors.

$$\begin{gathered}v_k = \textstyle\sum_{k=1}^{3} v_{jk}\, e_{jk} = v_{j1} \times (e_{j1}, \ldots, e_{jdj}) + v_{j2} \times (e_{j1}, \ldots, e_{jdj}) + v_{j3} \times (e_{j1}, \ldots, e_{jdj}) \\ = v_{j1} \times (E_1, E_2, E_3) + v_{j2} \times (E_1, E_2, E_3) + v_{j3} \times (E_1, E_2, E_3) \\ = v_{j1} \times \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\} \\ + v_{j2} \times \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\} \\ + v_{j3} \times \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}\end{gathered} \tag{8}$$

The method value at an arbitrary collection of three vectors $vj \in M^3$ can be expressed as

$$T_n\,(v_1, v_2, v_3) = \textstyle\sum_{k=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} S_{kji}\, v_{1k} v_{2j}\, v_{3i} \tag{9}$$

The fundamental benefits of chaotic functions are confrontation to trifling alterations in the preliminary conditions and constraints, unified physiognomies, periodicity, indefinite,

consistent gesticulations with extensive stages of instant and replication of unique fashion. To achieve reliable info privacy and veracity, a piecewise linear map and three-dimensional chaotic maps are employed for the production of hash value and encipherment standards.

The two-dimensional CATCM and 3-D maps are defined as:

$$\begin{bmatrix} E_{\mathrm{i}}(k+1) \\ E_{\mathrm{j}}(k+1) \end{bmatrix} = T_n \begin{bmatrix} E_{\mathrm{i}}(k) \\ E_{\mathrm{j}}(\mathrm{k}) \end{bmatrix} (\bmod \mathrm{n}) = \begin{bmatrix} V_{i1} & V_{i2} \\ V_{j1} & V_{j2} \end{bmatrix} \begin{bmatrix} M_1(k) \\ M_2(k) \end{bmatrix} (\bmod \mathrm{n}) \tag{10}$$

$$\begin{bmatrix} E_{\mathrm{i}}(k+1) \\ E_{\mathrm{i}}(k+1) \end{bmatrix} = T_n \begin{bmatrix} 1 & e_{j1} \\ e_{j2} & 1+e_{j1}e_{j2} \end{bmatrix} \begin{bmatrix} M_1(k) \\ M_2(k) \end{bmatrix} (\bmod \mathrm{n}) \tag{11}$$

$$\begin{bmatrix} M_{\mathrm{i}}(c+1) \\ M_{\mathrm{j}}(c+1) \\ M_{\mathrm{k}}(c+1) \end{bmatrix} = T \begin{bmatrix} M_{\mathrm{i}}(c+1) \\ M_{\mathrm{j}}(c+1) \\ M_{\mathrm{k}}(c+1) \end{bmatrix} (\bmod \mathrm{n}) \tag{12}$$

$$T_n = T_{\mathrm{ij}} T_{\mathrm{ik}} T_{\mathrm{ji}} T_{\mathrm{jk}} T_{\mathrm{ki}} T_{\mathrm{kj}} \; \textit{is a } 3 \times 3 \textit{ matrices} \tag{13}$$

$$T_{\mathrm{ij}} = \begin{bmatrix} 1 & v_{ij} & 0 \\ 0 & 1+v_{ij}e_{ij} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad T_{\mathrm{ik}} = \begin{bmatrix} 1 & 0 & v_{ik} \\ 0 & 1 & 0 \\ e_{ik} & 0 & 1+v_{ik}e_{ik} \end{bmatrix} \tag{14}$$

$$T_{\mathrm{ji}} = \begin{bmatrix} 1 & 0 & 0 \\ v_{ij} & 1+v_{ij}e_{ij} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad T_{\mathrm{jk}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & v_{jk} \\ 0 & 1+v_{jk}e_{jk} & 1 \end{bmatrix} \tag{15}$$

$$T_{\mathrm{ki}} = \begin{bmatrix} 1 & 0 & e_{ik} \\ 0 & 1 & 0 \\ v_{ik} & 0 & 1+v_{ik}e_{ik} \end{bmatrix} T_{\mathrm{kj}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1+v_{ik}e_{ik} \\ 0 & v_{jk} & 1 \end{bmatrix} \tag{16}$$

In Figure 1, we used a novel Tinkerbelle map [46] which is a discrete-time chaotic randomized system given by

$$\mathrm{P_{i+1}} = \mathrm{P^2_i} - \mathrm{Q^2_i} + \mathrm{X_1 P_i} + \mathrm{Y_1 Q_i} \tag{17}$$

$$\mathrm{Q_{i+1}} = 2\mathrm{P_i Q_i} + \mathrm{X_2 P_i} + \mathrm{Y_2 Q_i} \tag{18}$$

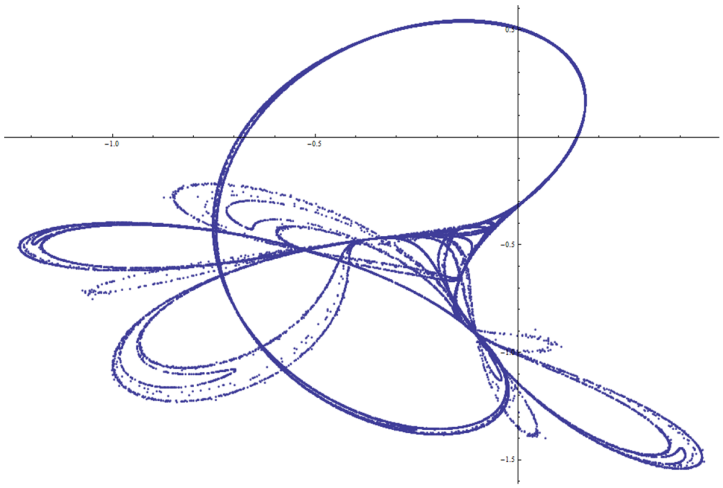

Figure 1. Tinkerbelle Chaotic randomization with $X_1 = 0.912$ $X_2 = -0.613$. $Y_1 = 2.01$ $Y_2 = -0.52$. Used starting values of $P_0 = -0.712$ and $Q_0 = -0.63$.

Some commonly used inputs of X_1 X_2 Y_1 and Y_2 are
$X_1 = 0.912$ $X_2 = -0.613$ $Y_1 = 2.01$ $Y_2 = -0.52$
$X_1 = 0.351$ $X_2 = 0.601$ $Y_1 = 2.13$ $Y_2 = 0.26$

The novel Tinkerbelle map can also be represented in the form of time bands, subsequently a definite count of recapitulations. Any point upon this map to the accurate will catch itself at its initial position. This map could produce a chaotic set of values, which is resolved steadily by the first set of values p, Q, and set of values X and Y. The askew Tinkerbelle map is cast-off to produce the extremely chaotic set of tenets for every repetitive procedure which is used in hash-based functions. To enhance the complexity of novel Tinkerbelle map we employed a novel slant bivouac map which is defined as follows:

$$f_{Ø}(b) = \begin{cases} \frac{b}{Ø}, & -0.7 < Ø < 1 \\ \frac{b-1}{Ø-1}, & Ø < b \leq 1 \end{cases} \tag{19}$$

The transposed method of the slant bivouac map is specified as

$$\mathrm{f}_{Ø}^{-1}(\mathrm{b}) = ØX \text{ or } \mathrm{f}_{Ø}^{-1}(\mathrm{b}) = 1 + (Ø - 1)(\mathrm{b} - 1) \tag{20}$$

In the non-linear vibrant scheme, commotion is an omnipresent portent. The Lyapunov characteristic exponent could be shown in many nonlinear maps and the statistical quantity of them may reproduce the gradation of energy of the contiguous focal point.

$$\text{Hybrid}^{-}\text{Chaotic “Lü” model} = \begin{cases} \mathrm{P_i} = \mathrm{E_j}(\mathrm{Q_i} - f_{Ø}(b)) \\ \mathrm{Q_i} = -\mathrm{P_i}\mathrm{f}_{Ø}^{-1}(\mathrm{b}) + T_n \\ \dot{\mathrm{P}}^{\mathrm{q}} + \mathrm{Q}^{\mathrm{p}} = \mathrm{P_i}\mathrm{Q_i} - \mathrm{bf}_{Ø}^{-1}(\mathrm{b}) \end{cases} \tag{21}$$

$$\text{Hybrid}^{-}\text{Chaotic “Chin” model} = \begin{cases} \mathrm{P_j} = F_n(\mathrm{Q_i} - \mathrm{P_i}) \\ \mathrm{Q_j} = -\mathrm{Q_i}\mathrm{V_k} + \mathrm{d_j}\mathrm{P_i} + \mathrm{c_i}\mathrm{Q_i} \\ \mathrm{R_j} = \mathrm{P_i}\mathrm{Q_i} - \mathrm{f}_{Ø}^{-1}(\mathrm{b})T_n \\ \dot{\mathrm{Q}}^{\mathrm{r}} + \mathrm{R}^{\mathrm{q}} = \mathrm{R_i} + f_{Ø}(b) \end{cases} \tag{22}$$

$$\text{Hybrid}^{-}\text{Chaotic “Roslier” model} = \begin{cases} \mathrm{P_k} = -\mathrm{Q_j} - \mathrm{R_j} \\ \mathrm{Q_k} = \mathrm{P_k} + \mathrm{d_j}\mathrm{Q}^{\mathrm{r}} + \mathrm{V_s} \\ \mathrm{R_k} = \mathrm{b} + \mathrm{P_j}\mathrm{R_j} \\ \dot{\mathrm{R}}^{\mathrm{p}} + \mathrm{P}^{\mathrm{r}} = -\mathrm{c_k}F_n + \mathrm{f}_{Ø}^{-1}(\mathrm{b})\ T_n \end{cases} \tag{23}$$

Hybrid-chaotic models with exponential Lyapunov exponent of usually produce many multifarious edifices and chaotic characteristics over the chaotic schemes with an exponential Lyapunov exponent. Though, firm hybrid-chaotic models can easily break with specific variable count's predictive tools since their gradation of energy is meeker and the degree of non-linear tensor productive variable count is deprived. Consequently, hybrid-chaotic models are necessary to enhance the security and integrity for the user's sensitive info, cloud frameworks, and apps with superior intricacy.

Proposed Hybrid QKD Standard for Big Cloud Data Security

The proposed hybrid QKD [51] standard with frenzied reliability needs two distinct transmission links: are the quantum link and a regular conventional link. At both edges of the source and the target employs a trilinear map-based Tinkerbelle chaotic randomization technique to produce session-wise secret keys along with a group of polarizers to capture the state of cubits. We combined both the Ciphered text Policy-based ABE standard and a trilinear-based hybrid QKD validation practice [52,53] cast-off in this proposal to produce a joint validated key without the involvement of a third party. The elementary configuration of the planned prototype is shown in Figure 2.

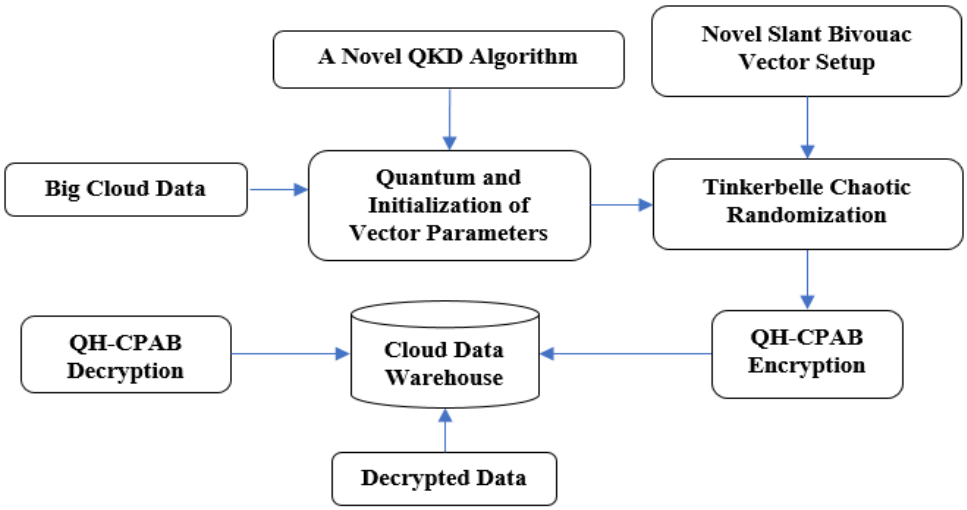

Figure 2. Proposed Model QHCP-ABE.

The fundamental step-by-step procedure of the planned key production based on the QKD procedure shown in Figure 3 is abridged beneath:

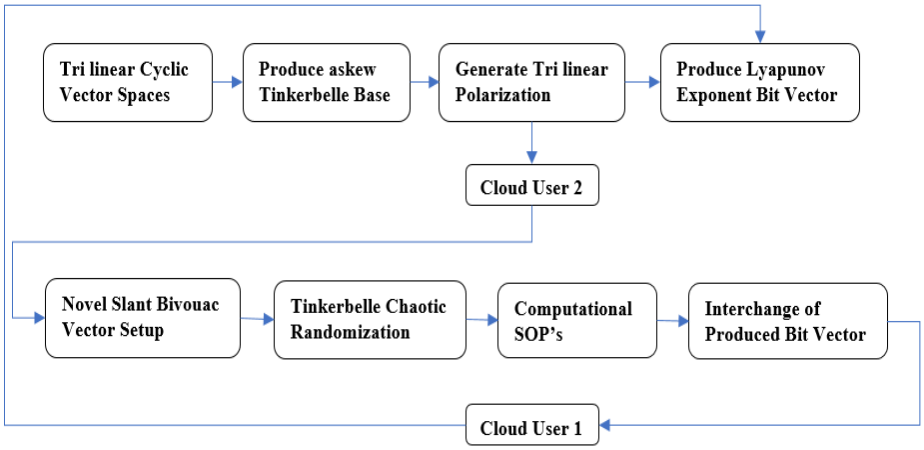

Figure 3. Proposed Polygon Polarization Based QHCP-ABE.

Step 1: Cloud Consumer 1 (CC1) selects a group of trilinear cyclic vector spaces with the help of a chaotic session-wise group key generator [54].

Step 2: CC1 produces a state of polarizations with the help of askew Tinkerbelle base info. Here, different trilinear-based SOPs are utilized to produce the initial trilinear vector spaces.

Step 3: CC1 directs the calculated state of polarized info to Cloud Consumer 2 (CC2).

Step 4: CC2 produces an arbitrary base with the help of the trilinear structure-based SOPs.

Step 5: CC2 computes the received polarized info with the help of the CC1 polarized info.

Step 6: CC3 produces the secret key and directs it back to CC1.

Step 7: At last, the mutually shared key is produced at both sides, and that final randomized key is used for the encipherment and decipherment process. This common key is cast off to produce chaos-based pseudo-randomization in the encipherment and decipherment stages over the big cloud data security [55].

The session-wise random secret key with the help of QKD is passed to the Hybrid Quantum-based Ciphered text Policy-based ABE standard of the official cloud clients. The Hybrid Quantum based Ciphered text Policy based ABE, along with Chaos-based

uprightness, comprises some essential procedures such as Key Production, Initialization, Encipherment, and Decipherment elaborated underneath.

A. Initialization Stage: In this stage, we produce pooled randomized quantum key (PRQK), main key (M_K), and attributes for public key (P_K). Let F be the trilinear cyclic group with an order of prime p which satisfies trilinear map and non-degeneracy property such that $Ø_1$ and $Ø_2 \in F_p$ so that the main key and public key are produced as

$$P_K = \{T\_Chaotic(HQKD(PRQK)), F_p(V_{sn}), k, x = k^{Ø}{}_2, y = k^{1/Ø}{}_1, T_n\ (e_{nk})\} \quad (24)$$

$$M_k = \{Ø_1, k^{Ø}{}_2, V_k\} \quad (25)$$

B. Enciphered Stage: The encipherment process practices the primary consumers' text (Ct) to produce the associated ciphered text. As part of the encipherment process, the Ct is enciphered with help of M_K and P_K and then design a bit vector. Opening with the root point of rp–integeral modulo Z*, this technique chooses an arbitrary value av and shows E(rp,0) = av.

It arrays E(Ct,0) = E(rpnode(rp_value, P_k)) for the rp_value midway plugs. If Ln is a group of leaf nodes in the tree hierarchy of admittance, then the ciphered text is generated on the base of the input tree admittance Ta as:

$$\begin{aligned} CipherText(Ct) = \{C^1 = M_K.\ E(T_n\ (e_{nk}))^{Ø}{}_2.{}^{rp}, F_p, C^n = Ct^{rp} \\ \forall\ rp \in R: C_n = k\ E^{(rpnode(rp\_value,\ Pk))}, \\ C^1{}_n = Lyapunove\ Exp(Ct)^{(rpnode(rp\_value,\ Pk))}\} \end{aligned} \quad (26)$$

C. Key Production Stage: In this stage, we gathered the set of big cloud data consumers' attributes (C_{attrib}) to produce the peculiar random key (P_{rK}). This stage needs a group of C_{attrib}, HQKD (P_{rK}) attributes for the initial inputs and produces a furtive key as the outcome. This process selects the randomized value called Slant Bivouac group of values Sb and rand for every user characteristic uc, which is elected as the shared key variable in $Z^*{}_p$.

$$P_{rK} = \{S_b = k^{(Ø2+rand)/Ø1}, S_b(i) = k^{rand*H(j).rand}{}_i, S_b(i) = k^{rand}{}_i\} \quad (27)$$

D. Decrypt Scheme: It receipts responses individual significant (S_k, group of attributes (C_{attrib})), ciphered text (Ct), access admittance edifice (Ta) combined, and Peculiar random key P_{rK}.

5. Experimental Results

The principal goal of the uprightness validation approach is to enhance the safety of the big cloud consumer's info. In the investigational findings, diversified kinds of multimedia data, such as a transcript, picture, audiovisual, json, msi, etc., are considered to calculate the hashed value with random hash proportions. Conventional enciphered models are sovereign with respect to uprightness validation because more memory is required for computation and time-band such as logistic logarithm, GPU-centric program design and huge volume-based revocation approaches. Many of the conventional hash-based models have fewer complex computations for consumers to generate their identifiable cryptographic credentials. The primary use of the randomization comportment over the hash-based approaches is to produce chaotic behavior and needing less time to produce complex identifiable cryptographic credentials with less size for the uprightness validation. It is not good practice to reveal the personal key. A portion of symmetrical encipherment methods such as global-key standards distribute their public key deprived of data integrity and confidentiality. Figure 4 illustrates the official cloud consumers have to choose the content for truthfulness validation.

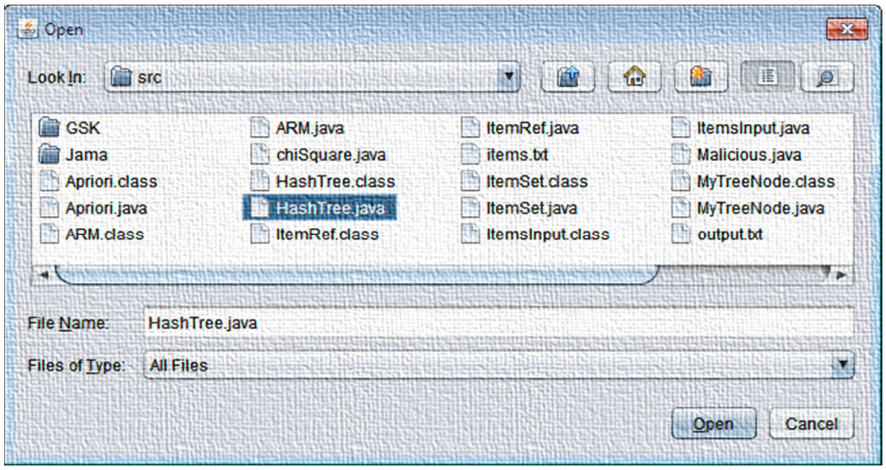

Figure 4. User selected file for reliability validation.

We used the AWS orders and S3 service to simulate and produce all the investigational findings. The cloud consumer conformations are 16 GB RAM, an Intel(R) CPU 3.5 GHz, and the Windows 10 or Ubuntu OS. For a successful operation of this proposed approach, we used some Java standard libraries, such as Java Quantum APIs, Java core layer low-level API, cloud base simulator, local host simulators, java.util.random, ACL, RBAC, and ABAC castoff as exterior libraries for progress.

The investigational findings in Table 1, CPABE, KPABE, and FHABE models are implemented over around 3000 KB of users' info volume with support of MD-5, SHA-256, and SHA-512, and the minimum computational periods are tabularized. Projected models are measured to be superior to the conventional models as it is perceived that the computational period is around 40% lesser as per the above-mentioned tabularized info.

Table 1. Analysis of different Hash-based Encryption Techniques.

	Info Size (KB)	Hash Period (m/s)	Enciphered Period (m/s)	Deciphered Period (m/s)
CPABE + MD-5	≅3000	4647	7690	5677
KPABE + SHA-256	≅3000	5484	5687	5125
FHABE + SHA-512	≅3000	6384	7599	7128
MUH-ABE	≅3000	2635	3868	3915
CIH-ABE	≅4000	2103	3917	3135
Hybrid QHCP-ABE	≅6000	1879	2789	2959

As per Table 2 results, it is evidently clear that planned Hybrid QCP-BE standard took a smaller amount of cloud info space even though the consumers' info volume is equivalent to the conventional standards of the size of 5000 KB. Therefore, we can conclude that even the size of the input info rises, our standard model devours a very small volume of cloud space as compared with conventional standards.

Table 3 signifies the relationship between the proposed model with conventional hash models and observed that the planned standard took very small execution time as related to the conventional standards.

Figure 5 exemplifies the comparative analysis of various Hash-based Encryption Techniques with the proposed one.

Table 2. Memory occupancy efficacy of proposed standard vs. conventional ABE standards.

Standard	Info Volume (KB)	Cloud Info Space (KB)
CPABE	5000	5287
KPABE	5000	5142
FHABE	5000	4278
MUHABE	5000	3729
Hybrid QCPABE	5000	2547

Table 3. Relative investigational findings of planned reliable hybrid quantum CPABE over the conventional enciphered standards w.r.t execution time as parameter.

CPABE (m/s)	KPABE (m/s)	DUPHA (m/s)	FHABE (m/s)	QKD/CPABE (m/s)	Proposed Standard (m/s)
845.54	761.66	571.51	629.56	356.55	294.34
837.35	752.73	622.39	786.37	338.34	302.13
972.33	884.30	545.47	719.98	329.21	295.54
859.44	734.54	432.23	727.27	359.29	275.64
836.59	708.12	411.32	892.09	345.95	302.34
830.65	700.13	623.12	786.62	329.63	244.63

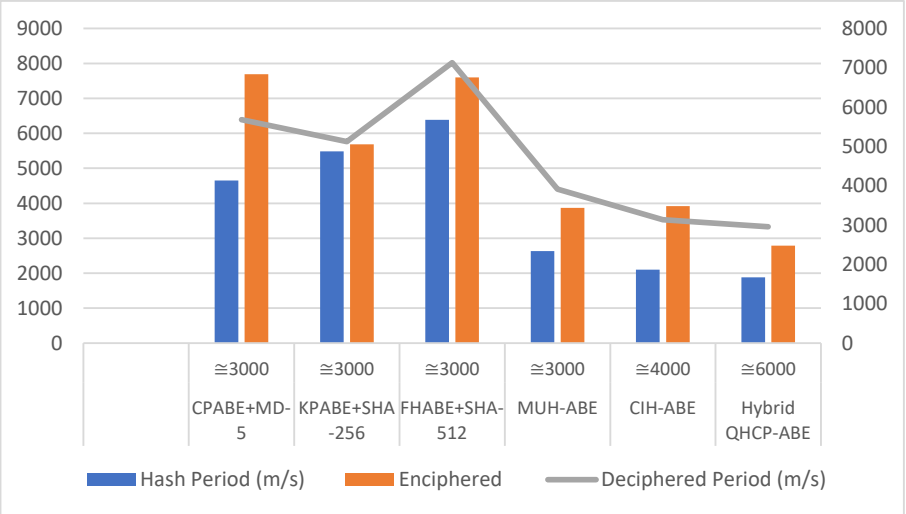

Figure 5. Relative investigational analysis of processing time band of planned standard over the conventional standards on dissimilar datasets.

Figure 6 exemplifies the comparative analysis of the memory occupancy efficacy of the proposed standard with respect to conventional ABE standards.

Figure 7 exemplifies the relationship between the proposed model with conventional hash models and observed that the planned standard took very small execution time as related to the conventional standards.

Figure 8 exemplifies the comparative analysis of the Hybrid QCPABE over the conventional models with dissimilar processing time (m/s). As displayed in Figure 5, it is observed that the presented standard took less processing time as linked to the conventional standards w.r.t diversified structured and unstructured data formats.

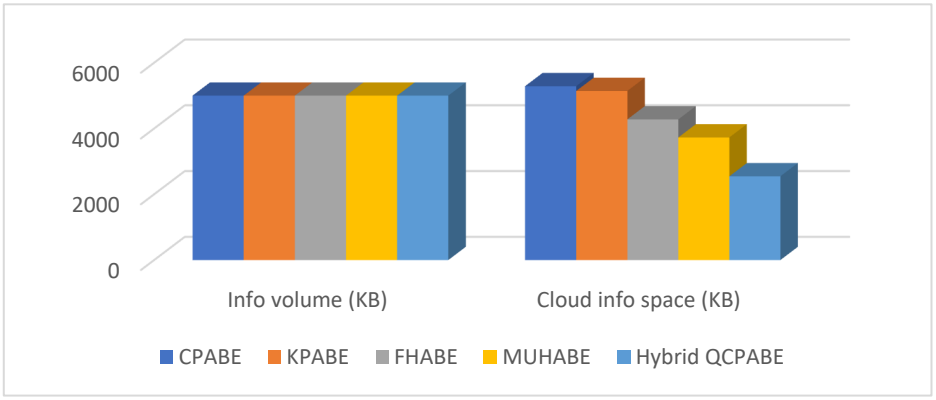

Figure 6. Relative investigational analysis of processing time band of planned standard over the conventional standards on dissimilar datasets.

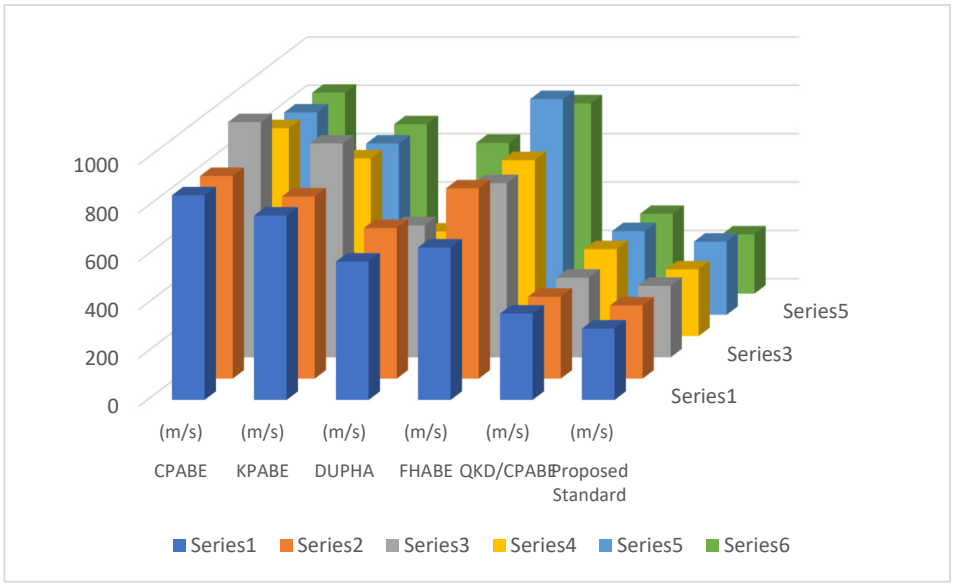

Figure 7. Relative investigational analysis of processing time band of planned standard over the conventional standards on dissimilar datasets.

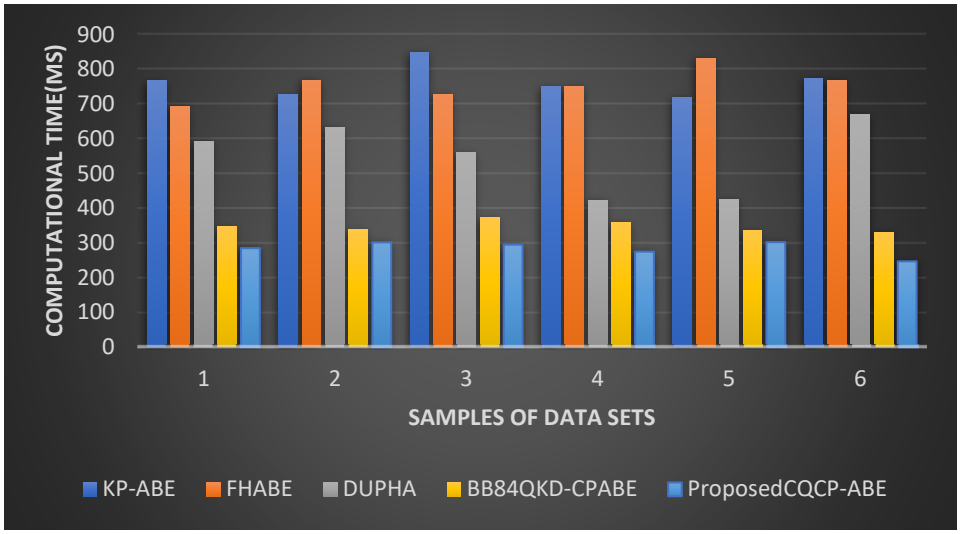

Figure 8. Relative investigational analysis of processing time band of planned standard over the conventional standards on with dissimilar datasets.

6. Conclusions and Future Scope

In the conventional ABE models, many of the models considered their input user attributes are text-based info and used fixed values for key production, consumer text encipherment and decipherment procedure. To address the existing problems, we proposed a new trilinear Tinkerbelle chaotic map-centric hash technique applied to enhance the cloud consumer security of the proposed hybrid quantum-based CPABE standard. In the planned standard, consumer's attributes are any type, and those are protected with the help of the trilinear Tinkerbelle chaotic function for key setup, cloud consumer text encipherment, and decipherment procedure. Investigational findings conclude that the projected model is working well to achieve big cloud consumers' sensitive data integrity and privacy with less enciphered, deciphered, and key production time as compared with the conventional ABE models. Our proposed model used both structured and unstructured big cloud clinical data as input so that the simulated experimental results conclude that the proposal has precise, resulting in approximately 92% correctness of bit hash change and approximately 96% correctness of chaotic dynamic key production, enciphered and deciphered time as compared with conventional standards from the literature. In the future, this research contribution may extended over decentralized blockchain apps, establish secure communication among IoT and IIoT devices along with client service level validation.

Author Contributions: Conceptualization, K.K.S.; methodology, K.K.S.; software, A.N. and S.J.; validation, K.K.S. and G.D.; formal analysis, K.K.S. and W.V.; investigation, K.K.S. and G.D.; resources, G.D.; data curation, K.K.S.; writing—original draft preparation, K.K.S.; writing—review and editing, G.D., Y.H. and J.H.A.; visualization, K.K.S., A.N. and S.J.; supervision, G.D., Y.H. and J.H.A.; project administration, Y.H. and J.H.A.; funding acquisition, Y.H. and J.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data will be available from first author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Qian, L.; Luo, Z.; Du, Y.; Guo, L. Cloud Computing: An Overview. In *Cloud Computing, Proceedings of the IEEE International Conference on Cloud Computing, Beijing, China, 1–4 December 2009*; Springer: Berlin/Heidelberg, Germany, 2009.
2. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, 9–11 April 1984*; Springer: Berlin/Heidelberg, Germany, 1984.
3. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO 2001, Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001*; Springer: Berlin/Heidelberg, Germany, 2001.
4. Amit, S.; Waters, B. Fuzzy Identity-Based Encryption. In *Advances in Cryptology—EUROCRYPT 2005, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005*; Springer: Berlin/Heidelberg, Germany, 2005.
5. Waters, B. Efficient Identity-Based Encryption without Random Oracles. In *Advances in Cryptology—EUROCRYPT 2005, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005*; Springer: Berlin/Heidelberg, Germany, 2005.
6. Xavier, B.; Waters, B. Anonymous Hierarchical Identity-Based Encryption (without Random Oracles). In *Advances in Cryptology—CRYPTO 2006, Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2006*; Springer: Berlin/Heidelberg, Germany, 2006.
7. Han, J.; Susilo, W.; Mu, Y. Identity-based data storage in cloud computing. *Future Gener. Comput. Syst.* **2013**, *29*, 673–681. [CrossRef]
8. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Berkeley, CA, USA, 20–23 May 2007.
9. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006.

10. Lewko, A.; Waters, B. Decentralizing attribute-based encryption. In *Advances in Cryptology—EUROCRYPT 2011, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 15–19 May 2011*; Springer: Berlin/Heidelberg, Germany, 2011.
11. Zhuang, Z.; Zhang, J.; Geng, W. Analysis and Optimization to an NFC Security Authentication Algorithm Based on Hash Functions. In Proceedings of the International Conference on Wireless Communication and Mesh Network, Wuhan, China, 13–14 December 2014; pp. 240–245.
12. Pei, S.L.; Ma, Z.L.; Li, Y.; Ma, Y.Z. AKA Security Algorithm Design Based on Chaotic Mapping. In Proceedings of the 2nd International Conference on Advanced Computer Control, Shenyang, China, 27–29 March 2010; Volume 5, pp. 451–453.
13. Wang, G.; Liu, Q.; Wu, J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In Proceedings of the ACM Conference—Computer and Communications Security (ACM CCS), Chicago, IL, USA, 4–8 October 2010; pp. 4–8.
14. Da Lio, B.; Bacco, D.; Ding, Y.; Cozzolino, D.; Dalgaard, K.; Rottwitt, K.; Oxenl, L.K. Two-Dimensional Quantum Key Distribution (QKD) Protocol for Increased Key Rate Fiber-Based Quantum Communications. In Proceedings of the 2017 European Conference on Optical Communication (ECOC), Gothenburg, Sweden, 17–21 September 2017; pp. 1–3.
15. Wadhwa, S.; Ahmad, M.; Vijay, H. Chaotic hash function based plain-image dependent block ciphering technique. In Proceedings of the 2016 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), Jaipur, India, 21–24 September 2016; pp. 633–637.
16. Xiao, D.; Liao, X.; Wang, Y. Parallel keyed hash function construction based on chaotic neural network. *Neurocomputing* **2009**, *72*, 2288–2296. [CrossRef]
17. Yang, X.; Layuan, L.; Chuanhui, C. Application research-based ant colony optimization for WMN. In Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, Wuhan, China, 22–24 September 2006; pp. 1–4.
18. Xiao, Y.; Zhao, Q.; Kaku, I.; Mladenovic, N. Variable neighbourhood simulated annealing algorithm for capacitated vehicle routing problems. *Eng. Optim.* **2014**, *46*, 562–579. [CrossRef]
19. Jung, T.; Li, X.; Wan, Z.; Wan, M. Privacy preserving cloud data access with multi-authorities. In Proceedings of the 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 6–8 December 2013; pp. 2625–2633.
20. Fei, P.; Shui-Sheng, Q. One-way hash functions based on iterated chaotic systems. In Proceedings of the 2007 International Conference on Communications, Circuits and Systems, Kokura, Japan, 11–13 July 2007; pp. 1070–1074.
21. Xiong, A.; Gan, Q.; He, X.; Zhao, Q. *An Integrity Based Encryption of CP-ABE Scheme in Cloud Storage*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 345–349.
22. Wang, Y.; Zhang, D.; Zhong, H. Multi-authority Based Weighted Attribute Encryption Scheme in Cloud Computing. In Proceedings of the 10th International Conference on Natural Computation, Xiamen, China, 19–21 August 2014; pp. 1033–1038.
23. Mo, T.L.; Lin, F. A dynamic re-encrypted ciphertext-policy attributed-based encryption scheme for cloud storage. In Proceedings of the 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, China, 8–10 November 2014; pp. 14–19.
24. Chandar, P.P.; Muthuraman, D.; Rathinraj, M. Hierarchical Attribute Based Proxy Re-Encryption Access Control in Cloud Computing. In Proceedings of the International Conference on Circuit, Power and Computing Technologies [ICCPCT], Nagercoil, India, 20–21 March 2014; pp. 1565–1570.
25. Kumar, R.; Mahajan, G. A novel framework for secure file transmission using modified AES and MD5 algorithms. *Int. J. Inf. Comput. Secur.* **2015**, *7*, 91–112. [CrossRef]
26. Singamaneni, K.K.; Ramana, K.; Dhiman, G.; Singh, S.; Yoon, B. A Novel Blockchain and Bi-Linear Polynomial-Based QCP-ABE Framework for Privacy and Security over the Complex Cloud Data. *Sensors* **2021**, *21*, 7300. [CrossRef]
27. Singamaneni, K.K.; Naidu, P. Secure key management in cloud environment using quantum cryptography. *Ing. Syst. D'inf.* **2018**, *23*, 213–222. [CrossRef]
28. Chase, M.; Chow, S.S.M. Improving Privacy and Security in Multiauthority Attribute-Based Encryption. In Proceedings of the 16th ACM Conference on Computer and Communications Security 2009, Chicago, IL, USA, 9–13 November 2009; pp. 121–130.
29. Gao, L.; Wang, X.; Zhang, W. Chaotic Hash Function Based on Tandem-DM Construction. In Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China, 16–18 November 2011; pp. 1745–1749.
30. Zavattoni, E.; Perez, L.D.; Mitsunari, S.; Sanchez-Ramirez, A.; Teruya, T.; Rodriguez-Henriquez, F. Software implementation of an attribute-based encryption scheme. *IEEE Trans. Comput.* **2015**, *64*, 1429–1441. [CrossRef]
31. Jayant, D.B.; Swapnaja, A.U.; Sulabha, S.A.; Dattatray, G.M. Analysis of dac mac rbac access control based models for security. *Int. J. Comput. Appl.* **2014**, *104*, 6–13.
32. Pirretti, M.; Traynor, P.; McDaniel, P.; Waters, B. Secure attribute-based systems. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VI, USA, 30 October–3 November 2006; ACM Press: New York, NY, USA, 2006; pp. 99–112.
33. Singamaneni, K.K.; Naidu, P.S.; Kumar, P.V.S. Efficient quantum cryptography technique for key distribution. *J. Eur. Syst. Autom.* **2018**, *51*, 283. [CrossRef]

34. Singamaneni, K.K.; Naidu, P.S. IBLIND Quantum Computing and HASBE for Secure Cloud Data Storage and Accessing. *Rev. D'Intell. Artif.* **2019**, *33*, 33–37. [CrossRef]
35. Singamaneni, K.K.; Juneja, A.; Abd-Elnaby, M.; Gulati, K.; Kotecha, K.; Kumar, A.S. An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security. *Secur. Commun. Netw.* **2022**, *2022*, 4206000. [CrossRef]
36. Singamaneni, K.K.; Dhiman, G.; Juneja, S.; Muhammad, G.; AlQahtani, S.A.; Zaki, J. A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks. *Sensors* **2022**, *22*, 6741. [CrossRef]
37. Singamaneni, K.K.; Naidu, P.S. An efficient quantum hash-based CP-ABE framework on cloud storage data. *Int. J. Adv. Intell. Paradig.* **2022**, *22*, 336–347. [CrossRef]
38. Singamaneni, K.K.; Naidu, P.S. An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security. *Int. J. Knowl. Based Intell. Eng. Syst.* **2020**, *24*, 145–156. [CrossRef]
39. Wang, T.; Yang, Q.; Shen, X.; Gadekallu, T.R.; Wang, W.; Dev, K. A privacy-enhanced retrieval technology for the cloud-assisted internet of things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4981–4989. [CrossRef]
40. Kumar, R.; Tripathi, R.; Marchang, N.; Srivastava, G.; Gadekallu, T.R.; Xiong, N.N. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *J. Parallel Distrib. Comput.* **2021**, *152*, 128–143. [CrossRef]
41. Reddy, G.T.; Sudheer, K.; Rajesh, K.; Lakshmanna, K. Employing data mining on highly secured private clouds for implementing a security-asa-service framework. *J. Theor. Appl. Inf. Technol.* **2014**, *59*, 317–326.
42. Nauman, A.; Jamshed, M.A.; Ali, R.; Cengiz, K.; Zulqarnain; Kim, S.W. Reinforcement learning-enabled Intelligent Device-to-Device (I-D2D) communication in Narrowband Internet of Things (NB-IoT). *Comput. Commun.* **2021**, *176*, 13–22. [CrossRef]
43. Zhao, Y.; Zhang, X.; Xie, X.; Ding, Y.; Kumar, S. A verifiable hidden policy CP-ABE with decryption testing scheme and its application in VANET. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3785. [CrossRef]
44. Sandhia, G.K.; Raja, S.K. Secure sharing of data in cloud using MA-CPABE with elliptic curve cryptography. *J. Ambient Intell. Humaniz. Comput.* **2022**, *13*, 3893–3902. [CrossRef]
45. D'Alconzo, G.; Gangemi, A. TRIFORS: LINKable Trilinear Forms Ring Signature. *Cryptol. Eprint Arch.* **2022**. Available online: ia.cr/2022/1170 (accessed on 24 September 2021).
46. Dhopavkar, T.A.; Nayak, S.K.; Roy, S. IETD: A novel image encryption technique using Tinkerbell map and Duffing map for IoT applications. *Multimed. Tools Appl.* **2022**. [CrossRef]
47. Uppal, M.; Gupta, D.; Juneja, S.; Dhiman, G.; Kautish, S. Cloud-based fault prediction using IoT in office automation for improvisation of health of employees. *J. Healthc. Eng.* **2021**, *2021*, 8106467. [CrossRef]
48. Juneja, S.; Jain, S.; Suneja, A.; Kaur, G.; Alharbi, Y.; Alferaidi, A.; Alharbi, A.; Viriyasitavat, W.; Dhaiman, G. Gender and age classification enabled blockschain security mechanism for assisting mobile application. *IETE J. Res.* **2021**. [CrossRef]
49. Dhiman, G.; Juneja, S.; Mohafez, H.; El-Bayoumy, I.; Sharma, L.K.; Hadizadeh, M.; Aminul Islam, M.; Viriyasitavat, W.; Khandaker, M.U. Federated learning approach to protect healthcare data over big data scenario. *Sustainability* **2022**, *14*, 2500. [CrossRef]
50. Dhiman, G.; Rashid, J.; Kim, J.; Juneja, S.; Viriyasitavat, W.; Gulati, K. Privacy for healthcare data using the byzantine consensus method. *IETE J. Res.* **2022**. [CrossRef]
51. Mittal, S.; Bansal, A.; Gupta, D.; Juneja, S.; Turabieh, H.; Elarabawy, M.M.; Sharma, A.; Bitsue, Z.K. Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health. *Comput. Intell. Neurosci.* **2022**, *2022*, 7016554. [CrossRef]
52. Gupta, N.; Gupta, K.; Gupta, D.; Juneja, S.; Turabieh, H.; Dhiman, G.; Kautish, S.; Viriyasitavat, W. Enhanced virtualization-based dynamic bin-packing optimized energy management solution for heterogeneous clouds. *Math. Probl. Eng.* **2022**, *2022*, 8734198. [CrossRef]
53. Sharma, S.; Gupta, K.; Gupta, D.; Juneja, S.; Turabieh, H.; Sharma, S. SWOT: A Hybrid Hardware-Based Approach for Robust Fault-Tolerant Framework in a Smart Day Care. *Secur. Commun. Netw.* **2022**, *2022*, 2939469. [CrossRef]
54. Juneja, S.; Juneja, A.; Bali, V.; Upadhyay, H. Cyber Security: An Approach to Secure IoT from Cyber Attacks Using Deep Learning. In *Industry 4.0, AI, and Data Science*; CRC Press: Boca Raton, FL, USA, 2021; pp. 135–146.
55. Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; Khan, A.I. Intrudtree: A machine learning based cyber security intrusion detection model. *Symmetry* **2020**, *12*, 754. [CrossRef]