sensors

Article

A Novel Blockchain and Bi-Linear Polynomial-Based QCP-ABE Framework for Privacy and Security over the Complex Cloud Data

Kranthi Kumar Singamaneni [1], Kadiyala Ramana [2], Gaurav Dhiman [3], Saurabh Singh [4,*] and Byungun Yoon [4]

[1] Department of Computer Science and Engineering, GITAM Institute of Technology, GITAM Deemed to be University, Visakhapatnam 530045, India; kkranthicse@gmail.com
[2] Department of Artificial Intelligence & Data Science, Annamacharya Institute of Technology and Sciences, Rajampet 516115, India; ramana.it01@gmail.com
[3] Department of Computer Science, Government Bikram College of Commerce, Patiala 147001, India; gdhiman0001@gmail.com
[4] Department of Industrial and System Engineering, Dongguk University, Seoul 04620, Korea; postman3@dongguk.edu
* Correspondence: saurabh89@dongguk.edu

Abstract: As a result of the limited resources available in IoT local devices, the large scale cloud consumer's data that are produced by IoT related machines are contracted out to the cloud. Cloud computing is unreliable, using it can compromise user privacy, and data may be leaked. Because cloud-data and grid infrastructure are both growing exponentially, there is an urgent need to explore computational sources and cloud large-data protection. Numerous cloud service categories are assimilated into numerous fields, such as defense systems and pharmaceutical databases, to compute information space and allocation of resources. Attribute Based Encryption (ABE) is a sophisticated approach which can permit employees to specify a higher level of security for data stored in cloud storage facilities. Numerous obsolete ABE techniques are practical when applied to small data sets to generate cryptograms with restricted computational properties; their properties are used to generate the key, encrypt it, and decrypt it. To address the current concerns, a dynamic non-linear polynomial chaotic quantum hash technique on top of secure block chain model can be used for enhancing cloud data security while maintaining user privacy. In the proposed method, customer attributes are guaranteed by using a dynamic non- polynomial chaotic map function for the key initialization, encryption, and decryption. In the proposed model, both organized and unorganized massive clinical data are considered to be inputs for reliable corroboration and encoding. Compared to existing models, the real-time simulation results demonstrate that the stated standard is more precise than 90% in terms of bit change and more precise than 95% in terms of dynamic key generation, encipherment, and decipherment time.

Keywords: cloud platform; ciphertext policy-based attribute-based encryption; blockchain; hashing; information security; non-polynomial chaotic mapping; quantum key distribution

check for updates

Citation: 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. https://doi.org/10.3390/s21217300

Academic Editors: Juan M. Corchado, Rajani Singh, Ashutosh Dhar Dwivedi and Mamoun Alazab

Received: 29 August 2021
Accepted: 27 October 2021
Published: 2 November 2021

1. Introduction

The various types of IoT applications include smart cities, smart health care, and smart transportation applications [1,2]. The critical entities in an IoT device include the device itself, a sensor, and an actuator. Sensor-equipped IoT devices collect data from their surroundings and transmit it via the Internet to a storage device. Analyses of the data are then conducted to determine the best course of action or share data with remote host machines.

The data are not stored locally because the local device has limited resources, such as insufficient memory for data storage and insufficient computation capacity for data analysis and action. This will result in the incorporation of cloud computing into the Internet of Things, with cloud computing providing services to IoT devices such as data storage and processing, as exemplified in Figure 1.

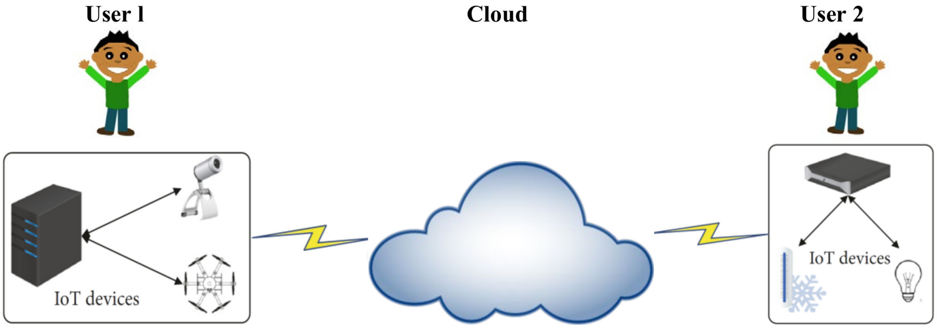

Figure 1. Cloud-Based IoT data sharing.

As depicted in Figure 1, User 1 collects different states of information from different locations via sensors and stores it in the cloud; these data can then be shared with remote host User 2 via IoT Device 2, which is part of a more cost-effective data-sharing method between communicating entities. However, the issue with this is that the cloud is untrustworthy, as there might be a chance of cloud consumer's sensitive data leakage. Numerous policies based on cryptographic tools are available to restrict user access and safeguard user privacy [3,4]; however, on rare occasions, an insider at the cloud end can delete these policies, thus jeopardizing the user's privacy.

To address this issue securely, cloud computing and blockchain technology are combined to store and share IoT data. Blockchain technology is a distributed ledger [5] with numerous applications, including IoT [6–9], e-currency [10,11], information loading [12,13], and data lineage [14].

We propose a fusion of blockchain and attribute-based cryptosystems [15,16] to address two critical cloud-related issues: preserving user privacy and sharing data in a manner that involves complete user control. This allows the data owner to choose whom to share their information without jeopardizing their data or privacy. This proposal includes the following:

- Data collected from IoT devices are converted to a ciphered text, then combined with an attribute encryption mechanism [17,18], which is then shared in small chunks. The key is then converted to ciphered text. Access policies are applied to the ciphered key using the QHCP-ABE framework for everything from determining who will become the temporary owner of the ciphered key to decrypting the cipher text.
- The smart contract provides scalability by storing access control policies in tables; users requesting to share data will interact with smart contracts via transactions.

Over the fast evolution and growth of the cloud centralized computing and WWW centric operational strategy, there are large volumes of user's information handling and distribution of resources over the cloud environments [6–9,13–16,19]. The external cloud resource manager wants to provide authorized access structure/policy and privacy towards the cloud users. Correspondingly, it is greatly recommended that the large sized apps are enabled one to one, one to multicast, and one to broadcast services to lessen the time and space required for users' data encipherment and decipherment as in traditional mathematical encryption techniques, since the cloud apps like Google drives and Dropbox, cloud structures like Amazon's EC2, and platforms like Amazons' Simple Storage Services (S3), Window's Azure have dissimilar structures and diverse facilities [20]. In these types of infrastructures and applications, when the cloud user's data increase more and more in large volumes day by day, extreme confidentiality is important to maintain those data alongside un-approved external apps, software, and manipulators, specifically in the case of public nets and medicinal accounts. Security along with privacy are the key issues in the cloud environment [2,21,22]. The existing old-fashioned cryptographic structure constructed over the public key infra-structure (PKI) may achieve users' info safety, privacy, and non-repudiation but it is associated with many problems, concerns, and restrictions. In the process of data encipherment, the external cloud authority wants to acquire the official persons' public keys, i.e., transfer the ciphered text to the users in one to one fashion that leads to bandwidth misutilization or wastage along with more computational time and network overhead. To address these key issues in place of traditional mathematical cryptographic models we replaced advanced Attribute Based Cryptographic schemes which encipher the cloud data only once w.r.t individual user which could be more beneficial to end users. In modern Attribute Based Encipherment (ABE), all users have their individual group of certified attribute subsets, rules/policies, and a secret key [3,4,21,22]. Numerous ABE structures are anticipated on different user's data but when the volume of user attributes and data increase those models fail to maintain proper access policies to access the user's confidential data. In the fundamental ABE process, secret and private keys along with ciphered text are also deciphered by using the access policies [3,4]. The end user can only decipher ciphered text contingent upon the corresponding user attribute set fulfilling the access control structure.

ABE is a public key cryptosystem which performs the decipherment of a ciphertext by any person and fulfils the designed access policy based on users' personal attributes. AB Encipherment scheme is part of the Identity Based Encipherment (IBE) base approach [3,4,21,22]. The idea of ABE is enhanced to integrate sophisticated and effective access control over the user's confidential data. Through implementing additional broad level access strategies, ABE structures attract the academic world as well as industrial users since these approaches allow the unauthorized users to gain admittance to legitimate users' personal information deprived of the central admittance regulate arrangement. Above and beyond subsidiary admittance rheostat claims, ABE also supports appliance additional academia and industry attention-grabbing claims like auditing log based encipherment and is directed towards multicast encipherment [4], unlike traditional mathematical encipherment models. In broad ABE cryptosystem two primary and significant schemes have been coined: Key Policy Attribute Based Encryption (KP-ABE) and Cipher text Policy Attribute Based Encryption (CP-ABE). In the past few years CPABE scheme has already been developed, and extensive research has been undertaken on that scheme and it has been instigated in many academic and industrial applications for users' cloud data security and privacy [2–4,21,22]. In this scheme the access policy is assimilated over the user's ciphered text, and a personal decipherment key is produced over the collection of users' subgroup attributes. Whatever the attribute held by specific users, only that attributes' combination should gratify the designed admittance rule/access policy, that a specific user only shall decipher the ciphered text which was enciphered under the designed rule/policy. Aimed at the design of the access structure/policy w.r.t CPABE models that specific access policy/structure should be well-known prior to the encipherment along with the user's subset of attributes based personal/secret keys. Conversely, KPABE [5,7,21] permits the users' block of data can be enciphered with the help of users' personal attributes which act as public-keys. In case of private/secret key generation this scheme uses a certain access policy/structure well-defined above the subset of user's personal attributes or characteristic based values like bio-metric values, passwords, pins, etc. (For a clear exemplification of the work flow see Figure 1). Due its dynamic and easy implementation, CPABE has been incorporated as a fundamental public key encipherment approach for all types of applications. On the other hand, KPABE has failed to access structure design on users' data, which is one of the major drawbacks of KPABE.

It is worth noticing the analysis of QKD practice in the noise-free channel as a part of base experiment level [17,23–25]. Furthermore, for the future reliable and confidential web communication by multiple cloud users, the practical experimental base model is mandatory. Furthermore, we tried the same approach in a noisy channel with the help of QKD model as shown in Figure 2. Due to this unrestricted privacy and confidentiality of quantum cryptographic approach, it is more apt for web applications and cloud computing as forever-growing defies problems which are inexorable in the upcoming period. QKD integrates the discrete session level dynamic secret key generation over numerous cloud users' over the one-to-one quantum link. QKD is effusively cast-off at abundant cloud consumers' secret generic procedures to achieve security and privacy [26–28]. QKD is derivative of quantum physical science aimed at generation of a secret key that leads to flawless persistence, in every single situation QKD cast-off over many different apps. Safety and privacy should be achieved through their elementary quantum physical particles called photons performance which are reliable, stable, and imperceptible. The prime advantage of integrating QKD with CPABE structure is that this unification provides the advanced confidentiality and privacy for the individual cloud users' private data.

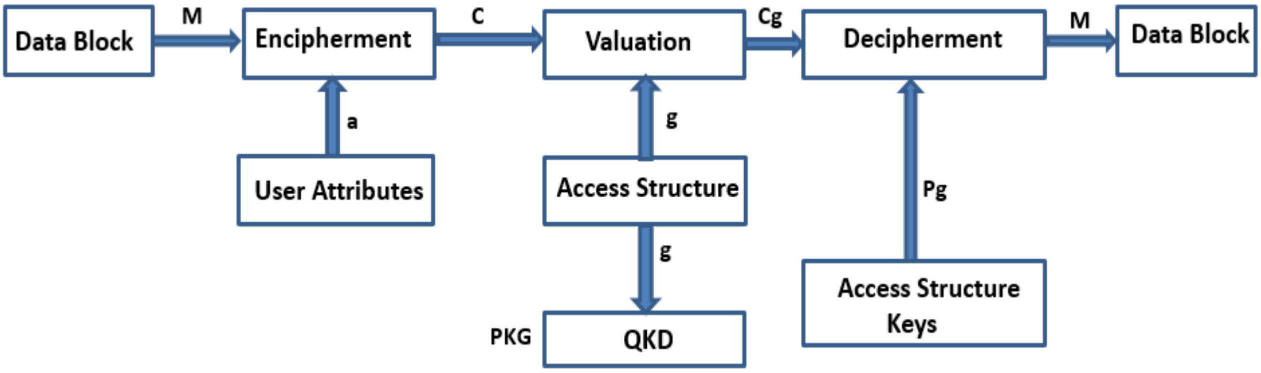

Figure 2. Exemplification of the QHCPABE scheme work flow.

The distinctive QKD approach is shown in Figure 3. Individual pairs of QKD are linked by a quantum channel. The quantum channel is linked to classical open network channel [29]. In this QKD approach, Sender (Alice) and Receiver (Bob) communicate their cubits via the secure quantum communication link and actual information is communicated with a classical cryptographic approach by means of open communication link [30]. To retrieve the cloud user data, block chain is also an effective technique [31–35]. Automated electrical user's personal clinical database is the present operational patient monitory facility contributing the main portion of preserving and monitoring the user's information, which was the key problem in w.r.t confidential patient's personal files breach [26]. To observe and access the sick person's personal data or clinical medical reports/records we use block chain related approaches with ledger feature. Block chain provides additional advantages like confidentiality, uprightness, and authentication along with privacy, ease of real time medical and clinical data accessing [18] and other user application oriented data, and administration [36–39]. Consequently, the key goal of the present contribution is to facilitate strict data privacy and security framework for cloud users' data by combining the block chain technique with quantum base ciphered text attribute encryption technique for additional security and to avoid man in the middle attacks [40–42]. Figure 4 shows how the model provides the security to cloud data.

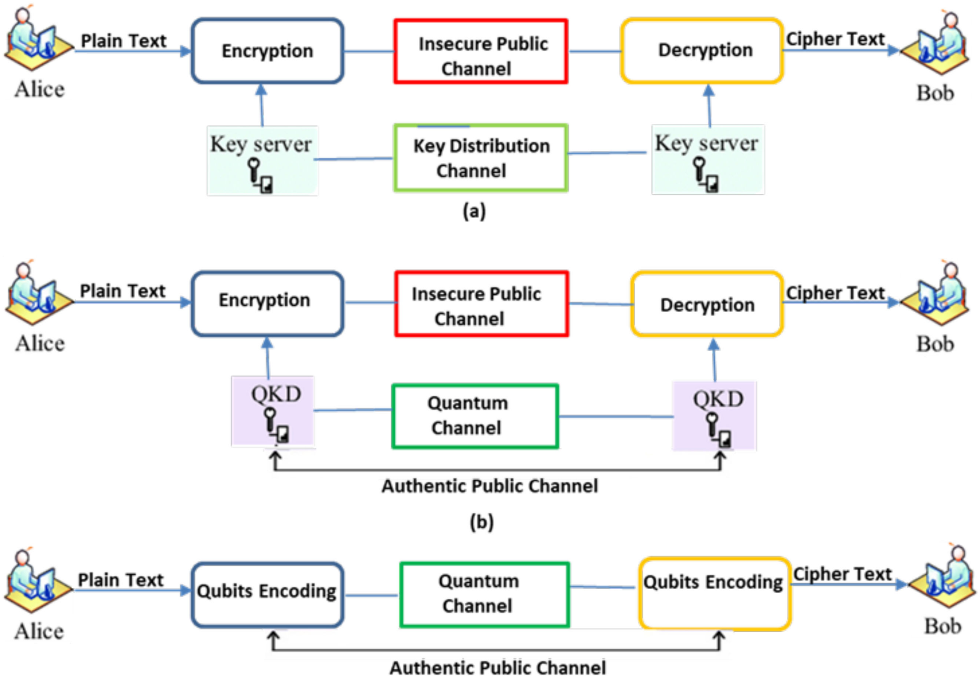

Figure 3. Traditional and Conventional QKD in Cryptographic Representation.

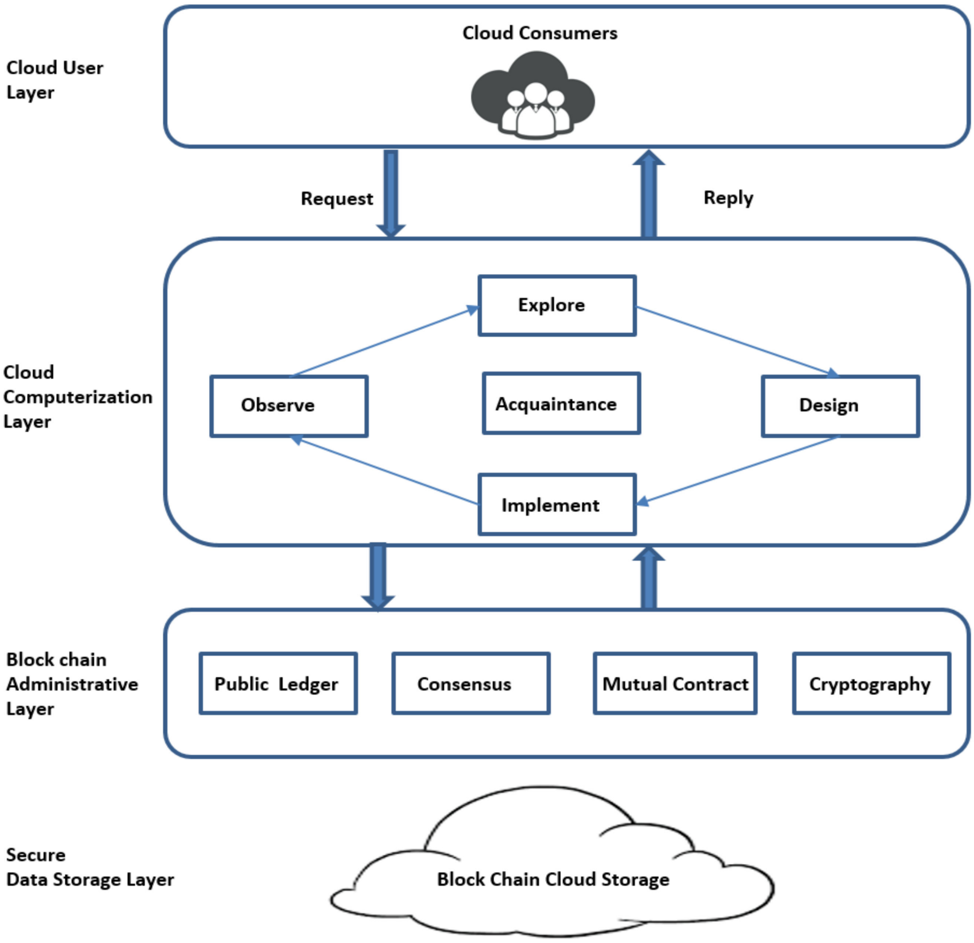

Figure 4. Secure Block chain QCPABE based Cloud Framework.

In this article, a Novel Block Chain Non-linear Polynomial Quantum Ciphered text Policy Attribute Base Encryption model is offered which can be implemented with the help of chaotic randomized non-linear polynomial curves for massive volumes of users confidential cloud data like patient medical records, bank transactions, etc. The planned system is well structured and it can handle large cloud data volumes and also produce an optimum resolution to obtain control over the framework through the different layers as shown in Figure 4.

The projected prototypical framework necessitates a reduced amount of computational time-band and smaller amount of network overhead to perform efficient user's confidential data encryption, decryption, and key production as compared to traditional models. Moreover, the outmoded representations are not successful in accessing structure rules/policies revocation and policy structures dynamic updating as per necessity. The projected design successfully implements the revocation process and dynamically updates access policy structures by way of less processing overhead parallel. This model comparatively needs lower processing time for block chain based cryptographic process, chaotic dynamic key production with the help of QKD approach, and the QCPABE set of rules. The considerable objects of the proposed model are mentioned here:

1. This one reassures large volumes of cloud consumer confidential data which may be structured and unstructured or both.
2. This one successfully moderates the cryptographic process and key generation time over the large volumes of personal cloud data.
3. This one successfully works on structured, semi structured, unstructured, and hybrid patient clinical records like doc, xls,.pdf, images, decom images, x-rays, etc. and diversified image representations.

2. Related Work

Chen, R. et al. [1] examined the personal information by using their biometric values and their confidential data preservation with the chaotic enciphering approaches. Overall the existing approaches are integrated with the traditional randomized enciphering process with the aid of Bernoulli's logistics basis. This research acknowledged plenty of workers' sensitive information privacy issues as well as previous issues with bio-metric users' information apps, and the authors of that study reconnoitered and inspected the previous recognized cryptographic varieties along with demerits of the approaches. Additionally, they mentioned the issues of biometric sensitive information. To overcome those existing problems a developed enciphering process is coined that can be combined with a three dimensional Bernoulli-Logistic family of curves approach. A thorough investigational assessment was accomplished, and the stemmed conclusions demonstrate that the described practice indicates more improved influence in the case of co-relation dissemination and histogram. That study additionally shows that the inefficacy and unreliability of the present approach are less than that integrated with Bernoulli-Logistic family of curves. The approach described above ensures extensive security and flawlessly retains the hiddenness of the encipherment. The outcomes of relative propagation of cloud consumer's information are more intermingled by dissemination and fabrication. The stochastic qualities of the histogram prove that the enciphering process is improved. Accordingly, it becomes more complicated to break down together the original user message system and the ciphered message system. Similarly, this methodology is very broadly applied in the electronic bio-metric users' information network [3,4,6]. During the period of PKE, two individual keys are used to encipher mentation and non-scrambling commotion. Both allocated keys are accessible and one more key is used for exclusive personal purpose. Operators in the public key are openly accessible, whereas the personal key is only accessible to the envisioned user. All users' plaintext is enciphered by the envisioned acceptors' publicly available key, and the procedure of decipher mentation is completed after the envisioned cloud consumer secret key. This method proposed a purpose to the enormous overheads associated with key administration/administrative; henceforth, it is cost ineffective for cloud computation. Policy based ABE [10,21,22] model addresses the base postulated issues. Moreover, the employers' characteristic based attribute sets should fulfil the challenging control structure polices, lone the worker only eligible for decipher mentation [7]. This contrived approach is exceptional to wide-open key crypto graphical techniques, stemming from its epicenter functioning rate all over the period compensated for in critical monitoring. In similar scenarios a certain clandestine key of a user is threatened, so only the information of that exact operator might be unscrambled by contemplation of user attributes. Homomorphic hash encipher mentation would be definite for the administration of cloud consumers information for their security and privacy [17]. This is assumed to be an acute practice in the cloud. This approach authenticates the cloud consumer's sensitive information privacy in determining the fortification problem of resource reservation over the cloud user whether he is an authenticated user or not. Users are expert at making use of resources offered by cloud continuously by the Internet. Thus, the system deploys the inclination cloud features. Abrading and termination pay might be contemplated as dual different practices can directly expand the cloud systems' user-friendliness and flexibility. In addition, some more block-chain and cloud related work can be read and referred to the references [20,31–39,43,44]. The CPABE practice leads to several key problems when installed at cloud consumer's information interchange policy construction. The secret keys of cloud users are created through the Key Production Center (KPC) though the Master Secret Key based attributes put off by cloud consumers. The suggested pseudo code needs fewer efforts to deposit public key certificates (PKCs) in contrast to whole conventional PKIs' [1,2]. The approach mentioned above fails to resolve key distribution issues by means of the KPCs which can decode every ciphered text chosen to all exclusive clients using the attributes of the keys' creation. The indicated issue impinges on users' information privacy limits of personal information allocating schemes. Another major disadvantage is revocation of key which is already considered as a known problem [8,9,15,16]. In the ABE-Technique, the main problem in the procedure of key revocation/cancelation is the revision of every new characteristic/attribute of both existing and new users. Each user's characteristic is used by more than the single client, and numerous clients might transmute the acquaintance-based attributes or otherwise alter specific secret keys. This practice of revocation is essential to preserving users' sensitive information security and users' information privacy. Every client from the cluster is influenced by one specific attribute or the other.

Traditonal Cryptographic Techniques Based on QKD

The main use of QKD is to generate a key with help of cubits which is used for the transmission of private data among sources and destination by using quantum signals without aware of what is the private key value. The QKD process is as shown in Figure 5. Here BB84 protocol for QKD is used, while smearing the crypto graphical approach to offer safety to cloud consumer's personal information exchange [29,30,44–48].

Tseng F.K. et al. [2] developed an improved biometric base arrangement to protect medicinal electronic health information over the cloud [3,10]. Implementing private electronic health checking applications has resolved many encounters in the healthcare domain, resulting in pointedly additional conjoint welfares for ill people and healthcare professionals. To achieve this goal, HMA techniques must continuously monitor a patient's history and condition. This is typically accomplished using sensor devices that collect information about sick people as well as diagnostic reports attached to the corpses of sick people. These are considered to be highly confidential and sensitive. As a result, cloud servers must maintain the privacy and security of stored personal and sensitive information about sick people. The purpose of this research paper is to design and advance a protective security structure specifically for cloud centric HMA patient files. This structure has the following advantages.

1. Thwarts unauthorized admittance access after unintended operators or invaders.

2. Whole patient related information is secured by means of the biometric validation scheme.

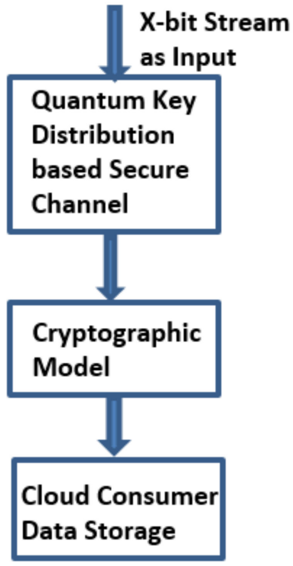
X-bit Stream as Input
Quantum Key Distribution based Secure Channel
Cryptographic Model
Cloud Consumer Data Storage

Figure 5. QKDs Cryptographic model.

Yang Y. et al. [21] offered an encipher mentation identifying technique to improve upon the biometric authentication process. The presented research paper designed a novel technique where biometric photographs are gathered with the help of the visual encipher mentation process. This type of techniques is characteristically positioned on the theoretical based assumptions of Compacted Sensing (CS) and Double Random Period Encipherment (DRPE). Furthermore, encoded detecting DRPE is also connected with the Digital Holographic method (DHM). Many studies are conducted at the valuation state. Enciphered bio-metric pictures are taken with the help of thump print pictures and thumb vein pictures. Repair might be accomplished exactly with the gathered encoded photographs' support.

Song X. et al. [22] presented a novel, refined biometric encipher mentation [3,4,11]. In The presented paper, authors castoff a slant authentication technique. The variant tokens are produced with the registration procedure that is typically reserved on biometric database. All the secure tokens are not completely equated along with all newly provided biometric tokens. Such things are considered to be an important facility towards biometric approaches. PIN/password authentication methods typically contain the symmetrical authentication technique. Suppose the required PIN/password may change by chance, apart from the initially selected one. In that case, the authentication action should fail [11]. Due to that, cloud consumers' trustworthiness should be unauthenticated. In the traditional mathematical research, the utilities in which i/p failed to generate o/p that means anywhere nearby the scope/scale for the given i/p is called chaotic. On behalf of this, Figure 6 shows the bilinear chaotic randomization [5,49].

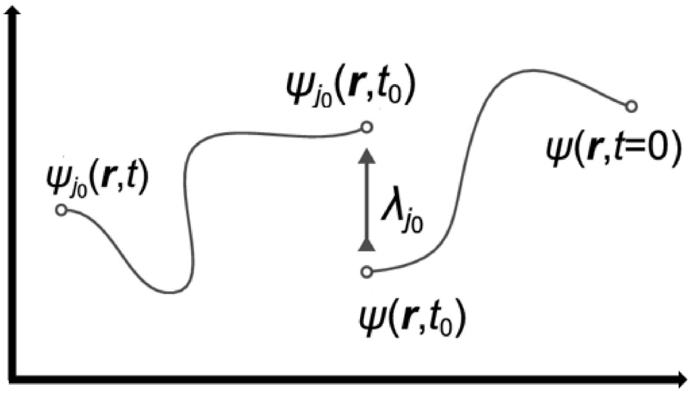
$\psi_{j_0}(\boldsymbol{r},t_0)$
$\psi_{j_0}(\boldsymbol{r},t)$
λ_{j_0}
$\psi(\boldsymbol{r},t=0)$
$\psi(\boldsymbol{r},t_0)$

Figure 6. Non-Linear Quantum Chaotic Randomization.

The quantum state as shown above signifies the part of computing the size of the key which breakdown into an arbitrarily/randomly designated function of this evident, ψj_0 and the extent outcome is a chaotic random position w.r.t Eigen-value λj0 (any prime number). The outcome is absolutely arbitrary/random and the consequence dimension devastated the previous state of Ψ(r, t) so this is considered the primary condition ψ (r, t = 0) at the time of initiation. None of this progression sequence evokes the past form/state and at every level it arises by way of totally arbitrarily designated function of the noticeable ψj_0(r, t0).

3. Proposed Model

Proposed block chain and bi-linear polynomial based QCP-ABE need communiqué passages like a quantum network communication link and a normal network communication link. The source user and destination user together need chaotic randomized producers after the bi-linear cyclical cluster and a pair of rudimentary and polarizing cubits [46–48]. We implemented this model on the basis of BB84 QKD to avoid the substantial Q link being confronted throughout communiqué from the M-I-M attacks. The rudimentary stages involved in the projected model are presented in Figure 7.

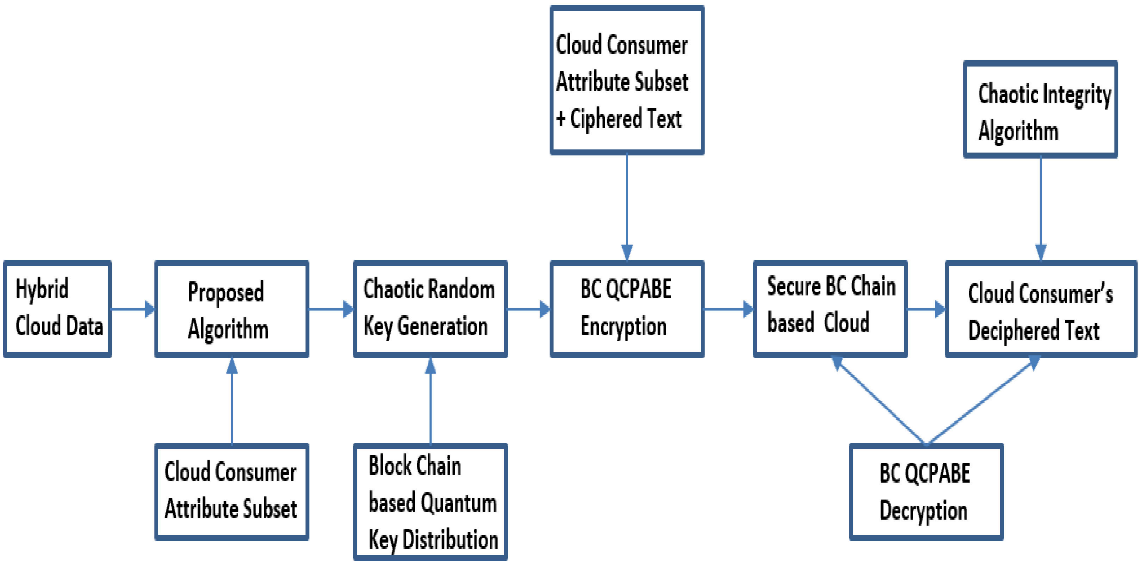
Cloud Consumer Attribute Subset + Ciphered Text
Chaotic Integrity Algorithm
Hybrid Cloud Data
Proposed Algorithm
Chaotic Random Key Generation
BC QCPABE Encryption
Secure BC Chain based Cloud
Cloud Consumer's Deciphered Text
Cloud Consumer Attribute Subset
Block Chain based Quantum Key Distribution
BC QCPABE Decryption

Figure 7. Block Diagram of the Proposed Model.

The offered prototypical framework has three methodologies: consumer integrity metric computation, QKRD, and encipher, decipher process of cloud users' private data. In the initial process the input accepts the cloud consumer attribute values to compute user integrity, and then each user's value can forward to the secure block chain based quantum key production after implement encipher and decipher algorithms. The next step consists in chaotic integrity metric based quantum key production process in cloud consumer attributes, control structures/policies, and individual session key generation based on CP-ABE [3,15,21,22,25]. The last step consists in the computed user integrity metrics and chaotic quantum key used in the first step of set-up, random key creation, and encipher, decipher processes. The quantum, public, private, and master keys are used on cloud consumer input attributes/characteristics. The ciphered text can only decipher by these attributes/characteristics, and the control structure policy accessed decision tree set in cloud consumer's ciphered message is represented in Figure 8.

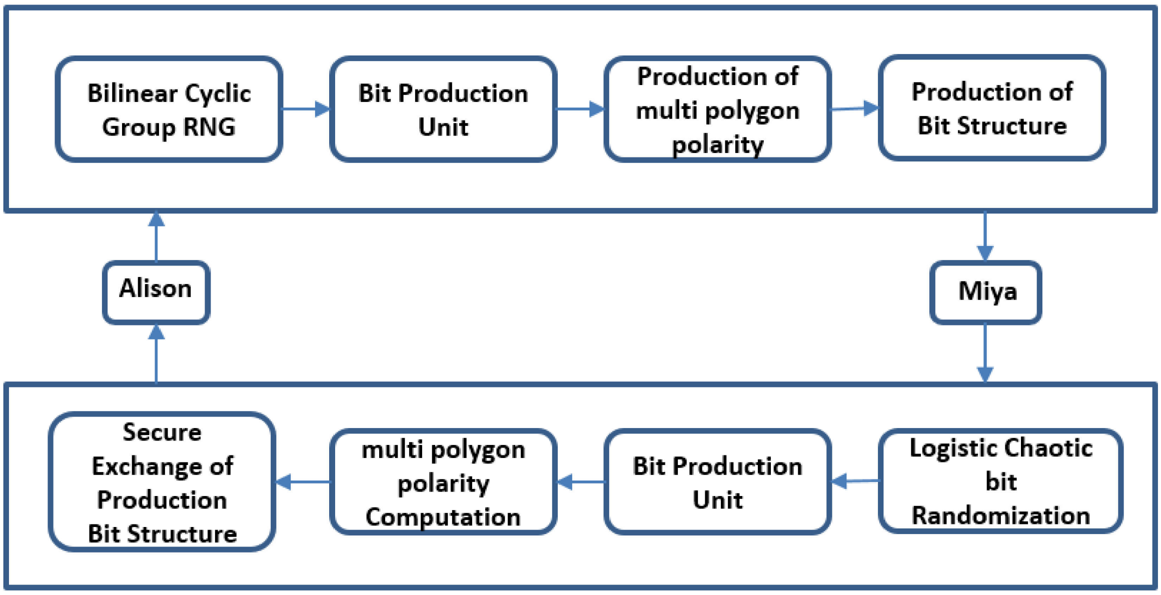
Bilinear Cyclic Group RNG
Bit Production Unit
Production of multi polygon polarity
Production of Bit Structure
Alison
Miya
Secure Exchange of Production Bit Structure
multi polygon polarity Computation
Bit Production Unit
Logistic Chaotic bit Randomization

Figure 8. Proposed polygon random polarization-based CBCQKD.

3.1. *Novel Blockchain and Bi-Lienear Polynomial Based Quantum Ciphered Policy Attribute-Based Encipherment Algorithm (NB-BPQCP-ABE)*

A bi-linear map is a function B:X $*$ $Y \rightarrow Z$: $\forall$ y $\in$ Y, the map B_y then x $\rightarrow$ B(x, y) is a bi-linear map from X to Z, and $\forall$ x $\in$ X, the map B_y: y $\rightarrow$ B(x, y) is a bilinear map from Y $\rightarrow$ Z. X, Y, Z are three vector spaces upon the same field F. The bilinear productive cyclical set with 'o' has a group order $Order(o) \leq Order(Z(o^2, *))$. Our novel projected pseudo code, a bi-linear chaotic arbitrary polynomial curve, is used for the enhancement of the privacy metrics/input for the session wise key making progress. The rudimentary iterative co-relation of bi-linear randomized polynomial value can be articulated by way of

$$Z_{n+1} = K\, Z_n\, (1 - Z_{n-3}) \tag{1}$$

where K is a constant and Z_0 is the initialization term is computed by the above relation

$$Z_0 = 1 \tag{2}$$

$$Z_1 = K\, Z\, (1 + K^3) \tag{3}$$

Finally, $\frac{dSz}{dn}$ indicates a set of bi-linear randomized graphs with exponent entitlements. Here K is a chaotic privacy check metric which can take from the range of Z(m, *) to Z(m^n, $*$). Using the above method can get the different set of bi-linear randomized polynomial graphs along with a wide range of co-factors through determining the recurrence equivalence.

Inputs: Start to prepare input cloud user attribute based parameters, message block size BLK_M, Over-all computational serial iterations CS_I, block-bytes, Cyclical confusion, diffusion set CD_S, cloud consumer private data load CP_L, first i/p info FI_I, TM_X and TM_K are transformation matrices.

Outputs: Authorized Integrated Biometric measurement AIB_M

Step 1: Declared and then initialized i/p cloud user attribute based parameters along with bi-linear cyclical hash vector. BCH_V [block-bytes/32] ← 0. Initially make bi-linear cyclical hash vector value as NULL.

Step 2: Choosing any randomized bi-linear polynomial graph value with private key $P_{(K)}$. It can enhance the overall privacy and security with chaotic arbitrary behavior which is based on logistic model of Bernoulli which leads to generation of strong chaotic randomized practical structure [16]. Logistic plotting is an orthodox frantic plotting exercise whatever the results generated through this model are extremely complicated with chaotic structure. The making of state run follows the below equation

$$r(b + 1) = \beta(Ci)\ (1 + x(Ci)) \tag{4}$$

Here, β deceits from 0 to 1 with randomized time band of bi-linear polynomial dynamic construction. The above-mentioned equation can produce a wide range of chaotic bi-linear cyclic sequence.

$$B(x) = r(k) \times b(x) \tag{5}$$

Here B(x) is a type of curve taken from the set of bi-linear polynomial curves and r(k) is a randomized factor taken from group Z.

Step 3: Calculate

$$\mu = \mathrm{LCM}(r_{e1} - 1, r_{e2} - 1) \text{ and } \text{Þ} = \mathrm{GCD}(r_{e1} + 1, r_{e2} + 1),\ n = r_{e1} \times r_{e2} \tag{6}$$

where r_{e1} and r_{e2} are the rudiments taken from bi-linear cyclical set Z(m, ∗).

Step 4: Opt an arbitrary value which act as co-prime to μ and Þ. Based on λ and Þ, calculate r_{p1} and r_{p2}

$$r_{p2} = \frac{\Omega}{(r_{p1} + 2)} \tag{7}$$

Step 5: Select any randomized inputs r_{v1} and r_{v2} which are taken from $Z(m^n, *)$

Step 6: Determine PM_{K1}, PM_{K2}, PM_{K3}, PM_{K4} as shown below:

$$PM_{K1} = 1 + r_{v3} \times (r_{p1} \times r_{p2}) \tag{8}$$

$$PM_{K2} = \mathrm{pow}\ (PM_{K1}, r_{v2}) \bmod (m^2) \tag{9}$$

$$PM_{K3} = S_{m1} \cdot \mathrm{pow}\ (PM_{k1}, {r_{v1}}^2) \bmod (m^2) \tag{10}$$

$$PM_{K4} = S_{m1} \cdot PM_{k3} \cdot q1 \cdot (r_{e1} \times r_{e2}) \bmod (m^2) \tag{11}$$

Step 7: Session key $SK_{P1} = \{PM_{K2}, PM_{K3}, PM_{K4}, S^{m1}, c_{g1} \cdot c_{g2}, B(m)\}$.

Step 8: Session key $SK_{P2} = \{m_1, r_{v1}, r_{v3}, \alpha, r(k)\}$

Step 9:

```
while (CP_L>Block_Bytes/32)
{
BLK_M ← First 32 bytes of sub block
for all parts of block BLK_M
{
for initial bit to CS_I
{
```

```
opt $SK_{P1}$, $SK_{P1}$ keys with $PM_{k1}$, $PM_{K2}$ as arbitrary transformation box.
        $PM_{k1} = (pow(PM_{k2}, T), PM_{k1})\ mod(min\{PM_{k1} \cdot randomvalues(\ )\})$
        $x1 = PM_{k1} \cdot T * PM_{k2} \cdot scale(1024)$
        $r_i = BLK\_M[j] + s[min(1, j-1)]$
        $r_{i+1} = min\{Rv1, Rv2\} \oplus r_i \oplus x_i$
}
$BLK\_M \leftarrow$ RIghtShift ($BLK\_M[j]$)
$BLK\_M[j] \leftarrow$ LeftForward ($BLK\_M[j]$, 10)
if(s+i<CS_I)
{
$BLK\_M[j] \leftarrow$ LeftReverse ($BLK\_M[j]$, 6)
$BLK\_M[j] \leftarrow$ RightShift ($BLK\_M[j]$, 12)
$BLK\_M[j] \leftarrow$ LeftShift ($BLK\_M[j]$, 6)
}
$C = c_0 + c_1 \ldots \ldots c_{n-r}$
}
```

3.2. *Bi-Linear Coupling*

Bi-linear coupling produces the multiplicative of any two pairs belonging to a polynomial cyclical set G. Once G is a state of identical elements what we selected from the pair the same pair produces a cyclic polynomial bi-linear relative set. Therefore, the bi-linear coupling gives a wide-range of randomized multiplicative pairs. Let G be a commutative cyclical group with transposed set t, and imagine that g_1, g_2, and g_3 are G-pairs [5]. The combination of each G-bi-linear map gbp: $g_1 \times g_2 \rightarrow g_3$; i.e., it must follow

$$\text{gbp}\ (c \cdot g_1, g_2) = \text{gbp}(g_1, G \cdot g_2) = G \cdot \text{cbp}(g_1, g_2)$$

$$\text{gbp}\ (g_{11} + g_{12}, g_2) = \text{gbp}\ (g_{11}, g_2) + \text{gbp}\ (g_{12}, g_2)$$

$$\text{gbp}\ (g_1, g_{21} + g_{22}) = \text{gbp}\ (g_1, g_{21}) + \text{gbp}\ (g_1, g_{22})$$

For all $g \in G$ and whole $g_1, g_{11}, g_{12} \in G$ parallel whole $g_2, g_{21}, g_{22} \in G_2$ which is an optimal pair of G-bilinear map. $G_1 \otimes_g G_2 \rightarrow G_3$ and $G_1 \otimes_G G_2$ indicates the multiplicative of G_1, G_2. A bilinear curve is also treated as a G-bilinear family of cures iffy and only if Ø: $G_3 \rightarrow$ HomoM (G_2 G_1); which exactly suits through the definition by representing as Ø (g_3) (g_2): = ê(g_3, g_2). A G-bilinear family of curves said to be finite and apt if and only if given randomized curve instance Ø is also an isomorph of all G-pairs. A G-bilinear combination of curves are said to be not a degenerative type if and only if ê(g_3, g_2) = null to all g_3 belongs to g_2 as same as null; similarly, ê is described as not degenerative if the pair (g_3, g_2) is also null for all g_2 belong to g_3 also said to be null. So, if all above mentioned constraints are satisfactory further the polynomial set of bi-linear curves can be valuated. This practice is efficiently combined with Bernoulli logistic map of family curves of the same type which provide more security in terms of chaotic randomization and enactment [17,23,24,49].

3.3. *Chaotic Key Making with BQKD*

Block chain based QKD uses numerous internetwork communication links, which are a combination of secure quantum link and a general user info link [19,24,36–39]. The source and destination together get a randomized pair of values on any place of G-bilinear cyclical group by adding cubits which are generated via different polarizers. The planned prototype combined an improved BB-84 authentication decorum which helps to create a randomized key which can access intended cloud users only but not even to cloud admin which avoids MIM bouts [49]. The session wise random key is generated with help of BQKD is supplied to licensed cloud users for the proposed model. The proposed model needs four basic methods, which are QKey_Pdn, I_Setup, CP-En_cipher, and CP-De_cipher.

3.4. *I_Set_Up Step*

Let G be the cyclic bi-linear pair of curves with co-prime order Co and originator O_k which must fulfill the G-bilinear principle and compliment degenerative principle so that Ø_1, Ø_2 belongs to G_{CO}. The public key and master key generated as shown below.

$$\begin{gathered}\text{Public-Key}(\text{Pb}_k) = \{\text{Offered\_BQKD(Quantum Key \& Consumer attributes)} \\ \text{where } (g_1 \epsilon\, G_1(CH_V[j]),\ g_{co}\ \epsilon\ G_2(CH_V[j] \text{ where } G_1, G_2 \text{ are Integrity metrics} \\ (CH_V, CH_V[j]\ \epsilon\ Z^2{}_r,\ O_k = \text{random}(g_1, g_{co})\}\end{gathered} \tag{12}$$

$$\begin{gathered}\text{Matser\_Key}(M_k) = (\mu\ \epsilon\ \text{Pb}_k(g_{co}),\ \text{Þ}\ \epsilon\ \text{BQKD(Private key}(CH_V\text{\_Att0}[1]\ \hat{}\ \\ CH_V\text{\_Att1}[2]\ \hat{}\ \ldots\ CH_V\text{\_Att}_{n-1}[n])),\ Z^{2*},\ \text{random}(\mu, \text{Þ})^{\text{Ø}}{}_2\}\end{gathered} \tag{13}$$

In this way we can generate Master key (M_k), BQKD private key (Prk), and public key factors (Pb_k).

3.5. *CP-Encipherment Structure*

The enciphered procedure gets the cloud consumers unique private info **Up** which as initial i/p through this we can make get final users ciphered text. Next we can encipher the cloud consumers unique private info **Up** which can be utilized to get control over the access policy **Ap**. Base from the starting point vertex **Sv**, our approach selects a randomized number **Rn** from mod (abs (random integers, Z^2) and institutes **q(Rk,0) = Rn** which understand that the middle level vertices, **Mv**, are arranged like (In,0) = Q (Sv(Rn,index_value)). Assume **Lv** to be the set of leaf vertices at the control access structure/policy; from this ciphered text can be generated over the existing access structure tree of policies **Ast** as shown below:

$$\begin{aligned}&\text{Ciphered Text(Ct)} = \{\text{Ct}^0 = \text{Pt. rand(R1,Rn)}^{\text{Ø}}{}_1{}^{\cdot rv},\ \text{Pt},\ \text{Ct}^1 = b^{rv}\ \forall\ \text{In}\ \epsilon \text{I\_N}: C_y \\ &= \text{R1}^{qkd(in,1)}, \\ &\ \text{Cy}^1{}_{in} = \text{CHv}(\text{A(In)}^{qkd(in,n)}\end{aligned} \tag{14}$$

Confirming overall homomorphism principles to mien original text message enciphering: Homomorphism based encipher, decipher uses $\Omega(r0)$, $\Omega(r1)$ as initial values.

$\Omega(r0)$ = CPEncD (j_1): = CPEncD(j_1) = (j_1 + $\gamma\mu * \text{Þ}$) mod Me $\Omega(r1)$ = CPEncD($j1$): = CPEncD($j2$) = (j_2 + $\mu * \text{Þ}$) mod Me whereas Me = $\alpha * \beta$; *CPEncD*(j_1 + j_2): = CPEnc($\Omega(r0)$) + CPEnc($\Omega(r1)$);

CPMEncD($j.j_2$): = CPMEncD($\Omega(r0)$).CPMEncD($\Omega(r1)$): = (j_1 + $\mu * \text{Þ}$) mod Me + (j_2 + $\mu * \text{Þ}$)mod Me.

3.6. *QK_Pdn Step*

The session wise key production process can generate Private key (P_{rk}) by using cloud consumers' set of personal parameters (S_{pp}). The QK_Pdn process ingests cloud consumers parameter set S_{pp} act as initial i/p for BQKD (Open key), and the formed o/p is the secret key. This process opts for a couple of arbitrary numbers, A1 and A2; for combination of each cloud consumer parameter set S_{pp}. These random values are part of selected co-factor of BQKD (shared key) which belongs to $Z^n{}_p$.

$$\text{Private\_key}(P_{rk}) = \{\text{Qk}(0) = kv^{(\text{Ø}1+A2)/\text{Ø}2},\ \text{QK}(f) = kv^{randf*Chv(f).A2}\ \} \tag{15}$$

3.7. *CPDecipherment Process*

In this process a private key P_{rk}, cloud consumers set personal parameters S_{pp}, ciphered text Ct along with access policy tree structure (Ast) and public-key (Pb_K) as i/p. The deciphering procedure is implemented iteratively. Verification of homomorphism property for user information decipherment is as follows: let be $P_{rk}.S_{pp}$(*CPEnc*(j_1 + j_2), *MCPEnc*($j_1.j_2$). S_{pp}($Ct(j)_1$, $K_{1,i}$). S_{pp}($TK_{1,j}$). S_{pp}($Ct(k)_3$,$K_{1,f}$) to get the created cloud consumer control structure.

$$\begin{aligned}&\mathrm{CPEnc}(j_1 + j_2) = \mathrm{CPEnc}\ (\Omega(r0) + \Omega(r1)) = \mathrm{CPEnc}(\Omega(r0)) + \mathrm{CPEnc}(\Omega(r0));\\ &: = (\Omega(r0) + \mu * \text{Þ})\mathrm{mod\ Me} + (\Omega(r1) + \mu * \text{Þ})\mathrm{mod\ Me}\end{aligned} \tag{16}$$

$$\begin{aligned}&\mathrm{CPEnc}(j_1.j_2) = \mathrm{CPEnc}(\Omega(r0) * \Omega(r1)=): = \mathrm{CPEnc}(\Omega(r0)).\mathrm{Enc}(\Omega(r1));\\ &: = (\Omega(r0) + \mu * \text{Þ})\mathrm{mod\ Me} + (\Omega(r1) + \mu * \text{Þ})\mathrm{mod\ Me}\end{aligned} \tag{17}$$

$$\begin{aligned}&\mathrm{CPDec}(EncD(j_1 + j_2)): = (\mathrm{CPEncD}(\Omega(r0) + \Omega(r1))\ \mathrm{mod}\ \beta\\ &: = ((\Omega(r0) + \mu * \text{Þ})\mathrm{mod\ Me} + (\Omega(r1) + \mu * \text{Þ})\mathrm{mod\ Me})\ \mathrm{mod}\ \beta: = j_1 + j_2\end{aligned} \tag{18}$$

$$\begin{aligned}&\mathrm{CPDec}(\mathrm{EncD}(j_1.j_2)): = (\mathrm{CPEncD}(\Omega(r0) * \Omega(r1)): =\\ &\mathrm{CPEncD}(\Omega(r0)).\mathrm{CPEnc}(\Omega(r1))\mathrm{mod}\beta\\ &: = ((\omega(i)_0 + \mu * \text{Þ})\mathrm{mod\ Me} + (\omega(i)_0{}' + \mu * \text{Þ})\mathrm{mod\ Me})\ \mathrm{mod}\ \beta: = i_1.i_2\end{aligned} \tag{19}$$

4. Experimental Results

The experimentations can be situated and executed over simple storage service (AWS-S3) with help after cloud consumer device details: processor i7 with speed of 2.30 GHz, 16 GB primary memory, 64-bit OS. This outline requires the usage of standard inbuilt packages and interfaces like EC2, Java, Net beans, and Eclipse.

Cloud Platform Base

AWS cloud services are utilized in the projected secure block chain based cloud environment to act out the projected model on users' confidential clinical and medical data. We used Amazon Elastic Compute Cloud and S3 buckets for generation of investigational outcomes to achieve effective public cloud security me integrating our proposed algorithms to the model. Elastic Compute Cloud offers upfront and tranquil cloud centric large scale calculations for all types of consumers. Elastic Compute Cloud cases are setup on Virtual Private Cloud. Using this cloud, consumers can do their trails in all possible cases with low cost for reliable services. For experimentation and analysis of Elastic Compute Cloud cases AWS, compromises an Internet based support, i.e., Cloud_Watch [2,6–9,13–16,19]. Cloud_Watch supervises resource reservation administration dynamically. Elastic Compute Cloud enables cloud consumers to opt for various functional objects, upgrade existing plans, 24/7 monitoring and management, along with emulation of executing capability in prior.

Figure 9 shows a comparison between the proposed model and the existing models with regard to changing the hash bit change. The tabletop showed the proposed method has a higher value than the standard models.

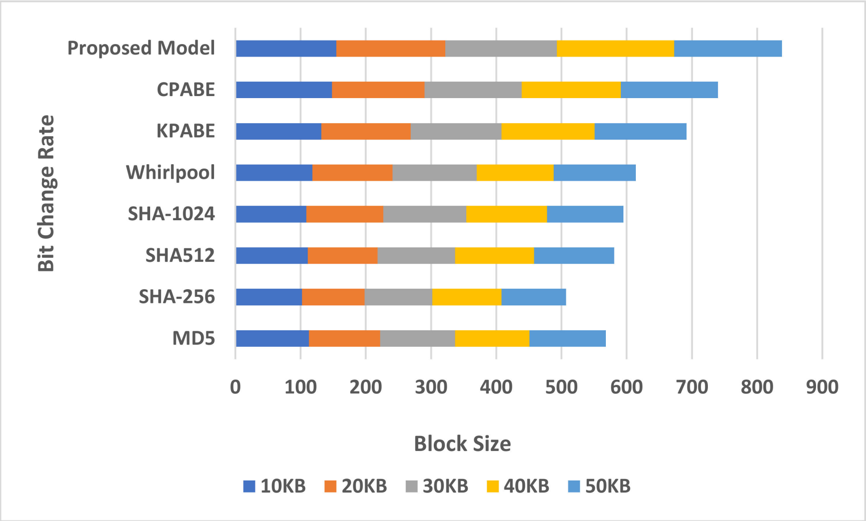

Figure 9. Computational time band for chaotic key production.

The projected method is compared with the past models; runtime calculations are illustrated in Figure 10. In the experimental trial, the average processing time is determined by varying the data sizes. The figure shows that the proposed models have good cloud safety computational efficiency.

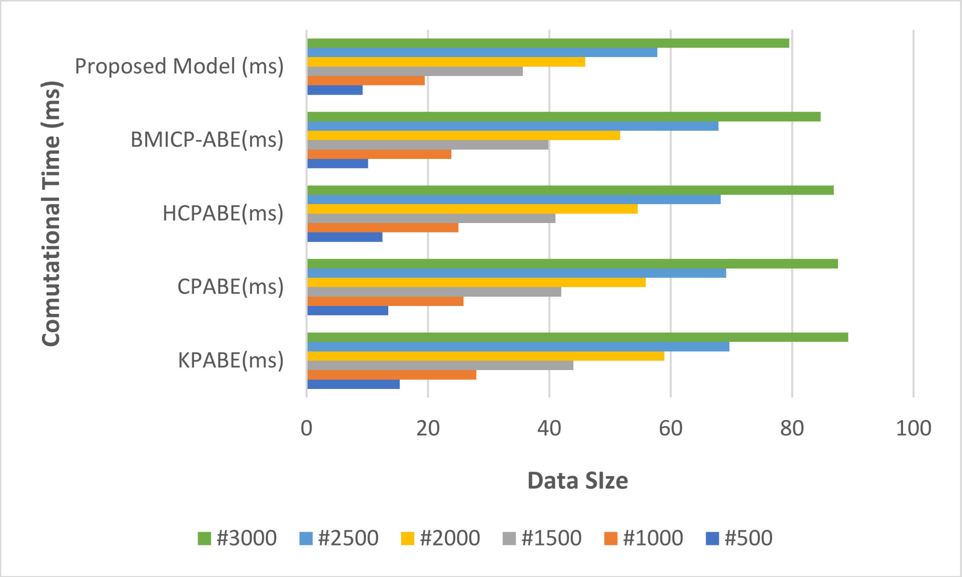

Figure 10. Comparative Analysis of Average Computational Time.

Figure 11 represents the computation time wanted on average for the projected technique with the past approaches with respect to the chaotic key construction process. In this projected technique, the chaotic dynamic key production system complete computation time is far lower than those of the available models.

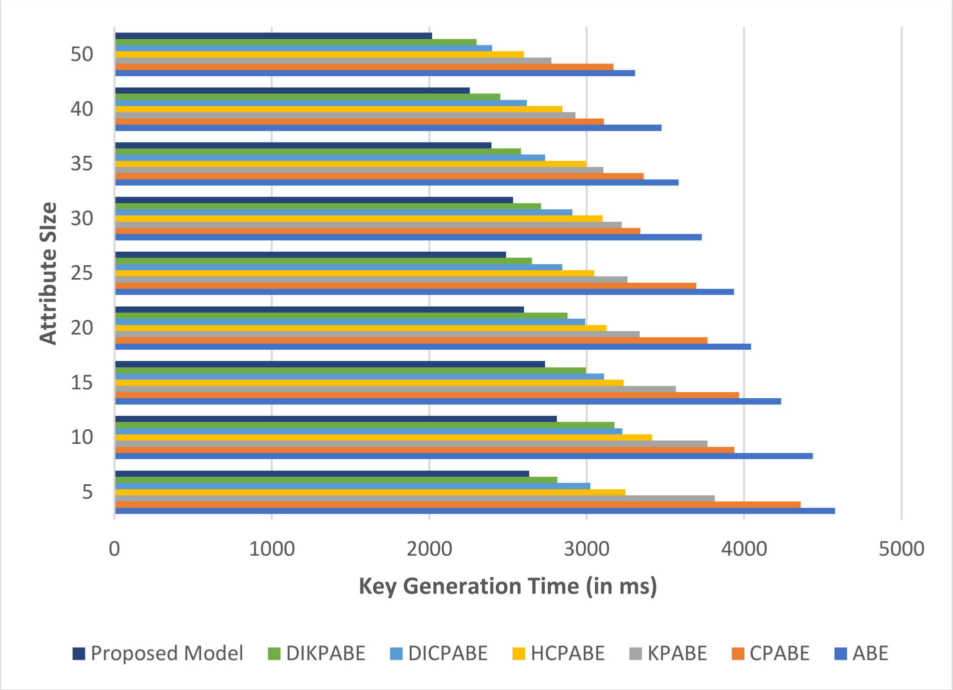

Figure 11. Comparative analysis of chaotic key creation time band and whole amount of cloud consumers' attributes.

Table 1 typifies the efficiency of the projected model with respect to past approaches validation process by means of bit change and dynamic randomized hash calculation. According to Table 2 above, the present dynamically randomized reliable approach is far better than the existing approaches for the production of chaotic hash values; ms stands for message size and kl signifies key length.

Table 1. Conventional Hash Technique-based proposed model efficacy.

Cloud Clinical Data-Set	MD5	QCP ABE	SHA-1024	Whirlpool	Proposed Model
Efficiency	O(msˆ2kl)	O(ms log(kl))	O(ms kl log(n))	O(ms log(ms kl))	O(ms log(kl/2))

Table 2. Summary of comparisons of state-of-the-art literature with proposed method.

Properties	MD5	SHA-256	Whirlpool	SHA-512	QCP ABE	SHA-1024	Proposed Model
Key length	Static	Static	Static	Static	variable	Static	Randomized
Dynamic key	Nope	Nope	Nope	Nope	Sure	Nope	Sure
Massive data	Nope	Nope	Nope	Nope	Sure	Nope	Sure
Transmission cost	More	More	More	More	Slightly Less	More	Very Less
Static key	Sure	Sure	Sure	Sure	Sure	Sure	Sure

Table 2 presents a proportional investigation of the acclaimed parameters with the traditional models. Table 2 shows the projected method has separate value added points like static key, a large volume of cloud consumers' personal information, and randomized chaotic session wise dynamic key creation process. The projected technique has one more asset: that it has extremely chaotic randomized flexible key sizes along with the fact that it takes far less communiqué network overhead compared to the related traditional methods.

5. Conclusions and Future Scope

The present approach provides a novel and enhanced bilinear QCPABE chaotic randomized key generation over the secure block chain cloud environment based user's sensitive data. The proposed approach uses a group of bilinear polynomial curves by means of extensively randomized complex chaotic utility. Conventional ABE approaches fail to handle the cloud consumer's large volumes of sensitive information and most existing methods are independent on integrity parameter due to lack of computational resources with less computational overhead. Our approach addresses all the traditional approaches issues and problems. Our proposed approach was implemented and successfully functional over the cloud consumers' large volume sets of sensitive data which are in the format of structured, semi structured, and non-structured. Our proposed approach can secure the cloud consumers' personal attributes by applying bilinear polynomial chaotic randomized map function designed for key setup, encipher, and decipher mention. The experimental replication results proved that our approach has the finest accuracy and rightness with respect to time required for dynamic key generation, encipher and decipherment process, and needed far less memory and computational overhead over the traditional approaches. Compared to existing models (CPABE, CQ-CPABE, KPABE, and QCP-ABE types), the real-time simulation results demonstrate that the stated standard is more precise than 90% in terms of bit change and more precise than 95% in terms of dynamic key generation, encipherment, and decipherment time. In the future this work may be protracted to advance the efficiency of the encryption and decryption process for the multi-document file formats using deep learning framework without loss of quality and resolution of the users various data representations over the cloud.

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

Funding: This work was supported in part by the National Research Foundation of Korea under Grant 2019R1A2C1085388, and in part by the Dongguk University Research Fund of 2020 under Grant S-2020-G0001-00050.

Data Availability Statement: Data are available on request due to restrictions, e.g., privacy or ethical reasons. The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy reasons.

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

References

1. Chen, R.; Mu, Y.; Yang, G.; Guo, F.; Wang, X. Dual-Server Public-Key Encipherment With Keyword Search for Secure Cloud Storage. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 789–798. [CrossRef]
2. Tseng, F.K.; Chen, R.J.; Lin, B.S.P. iPEKS: Fast and Secure Cloud Data Retrieval from the Public-Key Encipherment with Keyword Search. In Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 16–18 July 2013; pp. 452–458.
3. Nakouri, M.H.; Kim, T.H. A new biometric-based security framework for cloud storage. In Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 390–395.
4. Sabri, H.M.; Ghany, K.K.A.; Hefny, H.A.; Elkhameesy, N. Biometrics template security on cloud computing. In Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, India, 24–27 September 2014; pp. 672–676.
5. Gan, H.; Xiao, S.; Zhao, Y. A Novel Secure Data Transmission Scheme Using Chaotic Compressed Sensing. *IEEE Access* **2017**, *6*, 4587–4598. [CrossRef]
6. Shacham, H.; Waters, B. Compact Proofs of Retrievability. In Proceedings of the 14th International Conference Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), Melbourne, Australia, 7 December 2008; pp. 90–107.
7. Bowers, K.D.; Juels, A.; Oprea, A. Proofs of Retrievability: Theory and Implementation. In *Report 2008/175, Cryptology ePrint Archive*; ACM Digital Library: Bedford, MA, USA, 2008.
8. Naor, M.; Rothblum, G.N. The Complexity of Online Memory Checking. In Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05), Pittsburgh, PA, USA, 25 October 2005; pp. 573–584.
9. Chang, E.-C.; Xu, J. Remote Integrity Check with Dishonest Storage Server. In Proceedings of the 13th European Symp. Research in Computer Security (ESORICS '08), Málaga, Spain, 6–8 October 2008; pp. 223–237.
10. Tan, C.C.; Wang, H.; Zhong, S.; Li, Q. IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks. *IEEE Trans. Inf. Technol. Biomed.* **2009**, *13*, 926–932. [CrossRef] [PubMed]
11. Von Solms, S.H.; Tait, B.L. Solving the problem of replay in Biometrics- An electronic commerce Example. In Proceedings of the 5th IFIP Conference on Challenges of expanding internet: E-commerce, E-business, and E-government (I3E 2005), Poznan, Poland, 28–30 October 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 468–479.
12. Wang, Q.; Wang, C.; Li, J.; Ren, K.; Lou, W. Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing. In *European Symposium on Research in Computer Security, 14th European Symposium on Research in Computer Security, Saint-Malo, France, 21–23 September 2009*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 355–370.
13. Ateniese, G.; Burns, R.; Curtmola, R.; Herring, J.; Kissner, L.; Peterson, Z.; Song, D. Provable data possession at untrusted stores. In Proceedings of the 14th ACM Conference on Computer and Communications Security-CCS '07, New York, NY, USA, 31 October 2007; pp. 598–609.
14. Juels, A.; Kaliski, B.S., Jr. Proofs of Retrievability for Large FilesIn. In Proceedings of the 14th ACM Conference Computer and Communications Security (CCS'07), New York, NY, USA, 31 October 2007; pp. 584–597.
15. Shah, M.A.; Swaminathan, R.; Baker, M. Privacy-Preserving Audit and Extraction of Digital Contents. In *Report 2008/186, Cryptology ePrint Archive*; HP Labs Technical Report No. HPL-2008-32; Hewlett-Packard Development Company, L.P.: Palo Alto, CA, USA, 2008.
16. Oprea, A.; Reiter, M.K.; Yang, K. Space-Efficient Block Storage Integrity. In Proceedings of the 12th Ann. Network and Distributed System SecuritySymp. (NDSS '05), San Diego, CA, USA, February 2005.
17. Singamaneni, K.K.; Naidu, P.S. A Novel Integrity-Verification based Secured ABE model for cloud computing. *Int. J. Res.* **2018**, *5*, 372–378.

18. Subaja, C.M.; Sarathy, P.; Priyanka, C. An Efficient Data Security in Medical Report using Block Chain Technology. In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 4–6 April 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 0606–0610.
19. Schwarz, T.; Miller, E. Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage. In Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), Lisboa, Portugal, 4–7 July 2006; p. 12.
20. Mei, J.; Li, K.; Tong, Z.; Li, Q.; Li, K. Profit Maximization for Cloud Brokers in Cloud Computing. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 190–203. [CrossRef]
21. Yang, Y.; Chen, X.; Chen, H.; Du, X. Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encipherment in Cloud Computing. *IEEE Access* **2018**, *6*, 18009–18021. [CrossRef]
22. Song, X.; Wang, Y. Homomorphic cloud computing scheme based on hybrid homomorphic encipherment. In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 2450–2453.
23. Singamaneni, K.K.; Naidu, P.S. Secure key management in cloud environment using quantum cryptography. *Ingénierie Systèmes d Inf.* **2018**, *23*, 213–222. [CrossRef]
24. Singamaneni, K.; Naidu, P. IBLIND Quantum Computing and HASBE for Secure Cloud Data Storage and Accessing. *Rev. d'Intelligence Artif.* **2019**, *33*, 33–37. [CrossRef]
25. Singamaneni, K.K.; Naidu, P.S.; Kumar, P.V.S. Efficient quantum cryptography technique for key distribution. *J. Eur. Systèmes Autom.* **2018**, *51*, 283. [CrossRef]
26. Suseela, G.; Phamila, Y.A.V.; Niranjana, G.; Ramana, K.; Singh, S.; Yoon, B. Low Energy Interleaved Chaotic Secure Image Coding Scheme for Visual Sensor Networks Using Pascal's Triangle Transform. *IEEE Access* **2021**, *9*, 134576–134592. [CrossRef]
27. Natarajan, Y.; Kannan, S.; Dhiman, G. Task Scheduling in cloud using ACO. *Recent Adv. Comput. Sci. Commun.* **2020**, *13*, 1–6. [CrossRef]
28. Sowmiya, B.; Poovammal, E.; Ramana, K.; Singh, S.; Yoon, B. Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server. *IEEE Access* **2021**, *9*, 138245–138253. [CrossRef]
29. Chatterjee, I. Artificial Intelligence and Patentability: Review and Discussions. *Int. J. Mod. Res.* **2021**, *20*, 15–21.
30. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
31. Yan, Y.; Dai, Y.; Zhou, Z.; Jiang, W.; Guo, S. Edge Computing-Based Tasks Offloading and Block Caching for Mobile Blockchain. *Comput. Mater. Contin.* **2020**, *62*, 905–915. [CrossRef]
32. Song, R.; Song, Y.; Liu, Z.; Tan, M.; Zhou, K. GaiaWorld: A Novel Blockchain System Based on Competitive PoS Consensus Mechanism. *Comput. Mater. Contin.* **2019**, *60*, 973–987. [CrossRef]
33. Kumar, R.; Dhiman, G. A Comparative Study of Fuzzy Optimization through Fuzzy Number. *Int. J. Mod. Res.* **2021**, *20*, 1–4.
34. Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.; Nguyen, G.N.; Shankar, K. Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data. *Comput. Mater. Contin.* **2020**, *65*, 87–107. [CrossRef]
35. Li, T.; Ren, Y.; Xia, J. Blockchain Queuing Model with Non-preemptive Limited-priority. *Intell. Autom. Soft Comput.* **2020**, *26*, 1111–1122. [CrossRef]
36. Ra, G.-J.; Roh, C.-H.; Lee, I.-Y. A Key Recovery System Based on Password-protected Secret Sharing in a Permissioned Blockchain. *Comput. Mater. Contin.* **2020**, *65*, 153–170. [CrossRef]
37. Bordel, B.; Alcarria, R.; Martín, D.; Sánchez-Picot, Á. Trust provision in the internet of things using transversal blockchain networks. *Intell. Autom. Soft Comput.* **2019**, *25*, 155–170.
38. Wang, J.; Chen, W.; Wang, L.; Ren, Y.; Sherratt, R.S. Blockchain-Based Data Storage Mechanism for Industrial Internet of Things. *Intell. Autom. Soft Comput.* **2020**, *26*, 1157–1172. [CrossRef]
39. Chen, H.; Wan, W.; Xia, J.; Zhang, S.; Zhang, J.; Peng, X.; Fan, X. Task-Attribute-Based Access Control Scheme for IoT via Blockchain. *Comput. Mater. Contin.* **2020**, *65*, 2441–2453. [CrossRef]
40. Gomathi, S.; Soni, M.; Dhiman, G.; Govindaraj, R.; Kumar, P. *A Survey on Applications and Security Issues of Blockchain Technology in Business Sectors*; Elsevier: Amsterdam, The Netherlands, 2021.
41. Seraphim, B.I.; Poovammal, E.; Ramana, K.; Kryvinska, N.; Penchalaiah, N. A hybrid network intrusion detection using darwinian particle swarm optimization and stacked autoencoder hoeffding tree. *Math. Biosci. Eng.* **2021**, *18*, 8024–8044. [CrossRef]
42. Nair, R.; Gupta, S.; Soni, M.; Shukla, P.K.; Dhiman, G. *An Approach to Minimize the Energy Consumption during Blockchain Transaction*; Elsevier: Amsterdam, The Netherlands, 2020.
43. Liu, C.; Li, K.; Li, K.; Buyya, R. A New Service Mechanism for Profit Optimizations of a Cloud Provider and Its Users. *IEEE Trans. Serv. Comput.* **2021**, *9*, 14–26. [CrossRef]
44. Zhou, T.; Shen, J.; Li, X.; Wang, C.; Shen, J. Quantum Cryptography for the Future Internet and the Security Analysis. *Secur. Commun. Netw.* **2018**, *2018*, 8214619. [CrossRef]
45. Nicolas, G.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145.
46. Senkerik, R.; Pluhacek, M.; Zelinka, I.; Davendra, D.; Janostik, J. Preliminary Study on the Randomization and Sequencing for the Chaos Embedded Heuristic. In Proceedings of the Second International Afro-European Conference for Industrial Advancement AECIA 2015, Villejuif, France, 9–11 September 2015; Springer: Dordrecht, The Netherlands, 2016; pp. 591–601.

47. Vaishnav, P.; Sharma, S.; Sharma, P. Analytical Review Analysis for Screening COVID-19 Disease. *Int. J. Mod. Res.* **2021**, *1*, 22–29.
48. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.; Lvovsky, A.I.; Fedorov, A.K. Quantum-secured blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
49. Wang, Q.; Ren, K.; Lou, W.; Zhang, Y. Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance. In Proceedings of the IEEE INFOCOM, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 954–962.