Hindawi
Security and Communication Networks
Volume 2023, Article ID 9810502, 1 page
https://doi.org/10.1155/2023/9810502

Retraction

Retracted: An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

Copyright © 2023 Security and Communication Networks. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] K. K. Singamaneni, A. Juneja, M. Abd-Elnaby, K. Gulati, K. Kotecha, and A. P. S. Kumar, "An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security," *Security and Communication Networks*, vol. 2022, Article ID 4206000, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4206000, 13 pages
https://doi.org/10.1155/2022/4206000

WILEY | Hindawi

RETRACTED

Research Article

An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security

Kranthi Kumar Singamaneni,[1] **Abhinav Juneja**,[2] **Mohammed Abd-Elnaby**,[3] **Kamal Gulati**,[4] **Ketan Kotecha**,[5] **and A. P. Senthil Kumar**[6]

[1]*Department of Computer Science and Engineering, GITAM Deemed to be University, Visakhapatnam 530045, Andhra Pradesh, India*
[2]*KIET Group of Institutions, Delhi NCR, Ghaziabad, India*
[3]*Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[4]*Amity University, Noida, India*
[5]*Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International University, Pune, India*
[6]*School of Social Work, Jigjiga University, Somali Regional State, Ethiopia, Ethiopia*

Correspondence should be addressed to A. P. Senthil Kumar; senthilapsk@gmail.com

Received 28 March 2022; Revised 27 April 2022; Accepted 5 May 2022; Published 10 August 2022

Academic Editor: Mukesh Soni

Copyright © 2022 Kranthi Kumar Singamaneni et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Topics such as computational sources and cloud-based transmission and security of big data have turned out to be a major new domain of exploration due to the exponential evolution of cloud-based data and grid facilities. Various categories of cloud services have been utilized more and more widely across a variety of fields like military, army systems, medical databases, and more, in order to manage data storage and resource calculations. Attribute-based encipherment (ABE) is one of the more efficient algorithms that leads to better consignment and safety of information located within such cloud-based storage amenities. Many outmoded ABE practices are useful for smaller datasets to produce fixed-size cryptograms with restricted computational properties, in which their characteristics are measured as evidence and stagnant standards used to generate the key, encipherment, and decipherment means alike. To surmount the existing problems with such limited methods, in this work, a dynamic nonlinear poly randomized quantum hash system is applied to enhance the safety of cloud-based information. In the proposed work, users' attributes are guaranteed with the help of a dynamic nonlinear poly randomized equation to initialize the chaotic key, encipherment, and decipherment. In this standard, structured and unstructured big data from clinical datasets are utilized as inputs. Real-time simulated outcomes demonstrate that the stated standard has superior exactness, achieving over 90% accuracy with respect to bit change and over 95% accuracy with respect to dynamic key generation, encipherment time, and decipherment time compared to existing models from the field and literature. Experimental results are demonstrated that the proposed cloud security standard has a good efficiency in terms of key generation, encoding, and decoding process than the conventional methods in a cloud computing environment.

1. Introduction

The major objective of cloud-grounded, attribute-based encipherment is to expand the efficacy of access measures over the relevant and dynamic range of potentials. With a final objective of sustaining the domains of cloud computing, numerous cloud consumers find it necessary to obtain all these abilities as well as patron server production [1]. User validation is a vital parameter for protecting and preserving the privacy and security of information. This method operates by authenticating whether or not the distinctive-based identity offered is valid for accessing the information. In general, four methods are often instigated to validate the verification

and authentication [2, 3] of each distinct and specific user, which are

(i) Credentials: passwords or PIN or key lock

(ii) Tokens or code words

(iii) Dynamic biometric in-person validation

(iv) Static biometric in-person validation

A massive volume of users' information is distributed in cyberspaces [4]. The users' information is predominantly private/personal hypersensitive info. Currently, the majority of the apps are implemented in cloud platforms due to the extensive progression of cloud processing. Thus, the volumes of such users' information are ever-increasing exponentially [5]. In case an unauthorized/intruder will get access to users' private info, then all the confidential/sensitive users' info will be conceded. Therefore, there is a constraint of a robust and efficient practice to safeguard the users' information. The improved biometric-centered encipherment ruses contemplate the user's biometric particulars as input to the encipherment procedure to engender a private key. Furthermore, consistent biometric particulars are needed in the direct of decipherment for the purpose of deciphering the ciphertext effectively. In the case of the two sides, the biometric trials do not match up, therefore, the validation procedure failed and the user was not possible to decipher the ciphertext. Using the users' biometric info as input to the proposed algorithm, we generate a hash value as output for integrity which will be used in the process of the dynamic random key generation [6–10], encipherment, and decipherment process. Utilizing users' biometric information as input to the proposed algorithm, in this work, we generate a hash value as output for integrity, which will be used in the process of dynamic random key generation, the encipherment process, and the decipherment process.

Many chaotic enciphered practices have been discussed in the existing literature as means of ensuring the privacy of users' information and validation progression [11]. In this procedure of chaotic encipherment, an elementary constraint of bivouac maps and charts is unified with a private key in directive to yield chaotic order with the assistance of frontward reiteration [12, 13]. The chaotic dynamic mapping procedure provides a realistic pseudoarbitrary sequence in the procedure of encipherment, wherein $z(a+1) = E\ (z(a), y)$. The hitherto enciphered ciphertext is symbolized using $z(a)$. Certain characteristics of chaotic mappings, such as classified dependency on primary state-run, haphazard comportment, and topologic transitiveness, are also common. However, none of the existing practices commonly implemented are completely reliable and secure, and even the most apparently secure practices tend to have a few drawbacks. Instead, nearly all existing methodologies accentuate the encipherment proficiency and concoction implementation alongside corelation evaluation. None of these attempts has been borne out of accentuating capriciousness and static analogous to the histogram and corelation dissemination. Some cases of lesser histograms and the correlation do work efficiently, though, concealing unciphered user information securely.

1.1. Threshold Private Distribution Practices. Adi Shamir's (1979) "secret sharing," also called SSS, is a set of private distribution practices created as a means of disseminating secrets, or private information, in n parts. With SSS, the refurbishment of information would be taken out and used up from a subset of n components. This practice typically behaves as a threshold paradigm utilizing nonpolynomial utterance. In this method, two dissimilar positive numbers are chosen, namely, c and d, whose relationship is as follows: $c \leq d$. Moreover, an alternative dispersal of a secret/private value e is made between persons ($p1$, $p2$, . . ., pn). In this context, a subclass of c persons is allowed to take part in the renewal course of that secret/private value e.

Another method, identity-based encipherment (IBE), is a substantive and often-used approach to public-key cryptographical (PKC) techniques. Here, the public/open-key tends to be an arbitrary word of exclusive information that is held accountable for users' IDs. Additional furthermost communal instances include e-mail addresses, mobile numbers, Aadhar numbers, and PAN details. In many versions of the identity-based encryption methods, Personal Key Generator (PKG) is used. This PKG is essentially a third-party user, and it tends to be utilized as a means of producing and distributing master public metrics (PMs) of persons' IDs. From this, master private/secret parameters (MSPs) are then kept in a sheltered place. Below is the operational phenomenon of most of the conventional IBE techniques.

Consider a situation wherein the source (here, user A) transmits enciphered text to a specific destination (here, user B).

(1) User A's e-mail ID and PMs are utilized to estimate user B's public key (PK).

(2) User A is accountable for performing the encipherment process/algorithm utilizing user B's PK. The protected enciphered text is formerly transmitted through user B.

(3) User B utilizes the PK (itself engendered with the help of their e-mail ID) to gain access to the deciphered key.

User B's information is considered in the procedure of decipherment, and if correct, it repossesses the deciphered text, later performing the decipherment code/algorithm.

Even such approaches are not perfectly secure, though. Thus, despite their many uses in key fields, cloud computing platforms and environments are also often uncertain and potentially insecure because their assets are located, or at least touch upon, locations around the globe. In addition, such systems require users' confidential information to be enciphered prior to uploading into a cloud-based environment [14, 15].

Numerous orthodox PKE methods are already employed in order to improve security and protect users' sensitive information. However, their increased elasticities have also led to the intensification of several existing concerns and issues, including the following:

RETRACTED

(1) To execute plain-text process encipherment, data proprietors require the public key (PK).

(2) The cloud storage overhead is exponentially enlarged, i.e., to each individual's plain-text need and as many PKs as dependent on the number of end-users.

Quantum key distribution/delivery (QKD) is comprised of the private/shared secret key production among two different users through a protected quantum channel/path. QKD is extensively castoff at numerous users' sensitive information-centric algorithms for information confidentiality. QKD draws from quantum physical science for key creation and this leads to a high resolution on every occasion QKD castoff is utilized for various applications. By their nature, safety evidence is logical, rational, and conceptual and comes with math-based requisites for safety precision. The move to QKD from outmoded crypto graphical practices is tough to manage, but it is also a grim assessment to consider the attacks and bouts of unauthorized access that are risked otherwise [16]. However, the most outstanding benefit of assimilating QKD to ABE structure is that this combination offers further safety to users' sensitive information over the cloud [17]. The distinctive QKDs are represented in Figure 1. Here, individual approved and/or authorized parities of QKD are associated with each other through the quantum standard channel, rather than related via traditional channels [18]. By using the QKD process, user A and user B distributed their qubits through the quanta channel/path and all text conversations via the standard path [19].

In the current paper, we get offered a novel enhanced and dynamic nonlinear polynomial integrity-based quantum HCP-ABE model for big structured and unstructured cloud datasets. Consequently, the proposed EDNPI QHCP-ABE methodology will be possible to offer an ideal resolution to gain access to the centralized scheme via the practice of initialization, circulation, reflection, access permissions, and privacy. Some of the existing models take more computational time and resources for users' massive volumes of info encipherment, decipherment, and key generation process as compared to our proposed model; even the traditional models are failed to revoke user attribute-based access policies and dynamic updating of access policy structures according to the requirement [17, 20]. The proposed model is capable of revocation and dynamically updating access policy structures with very little computational overhead and very less computational time for encipherment, decipherment, and random key generation using the quantum key distribution process and QHCP-ABE algorithm. The central gains and limits of the projected standard are addressed beneath.

The key objectives of the proposed model comprise the following:

(1) The proposition of an advanced hash approach for strong data/big data security.

(2) Effectively reducing the encoding and decoding runtime on big datasets.

(3) The processing of both structured and unstructured 3D medical image formats.

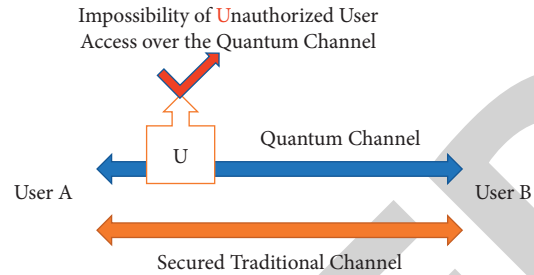


Figure 1: Classical QKD in the cryptographical model.

2. Related Works

Cloud computing delivers different services through the Internet to fulfill cloud users' requests. These services (storage space, processing power, and application software) are accessed dynamically on-demand. Companies can take advantage of cloud computing services without making a high investment. Indeed, rather than owning these services such as data repositories, organizations could control them from a third-party administrator. Hence, the important profit of a cloud computational environment is to avoid the complexity of implementing and maintaining the IT infrastructure required for the used services.

Chen et al. [1] did a detailed analysis of biometric users' sensitive info protection and chaotic encipherment practices. All these approaches are amalgamated with the conventional chaotic encipherment method with the help of Berboullis' mapping. In this study, they recognized numerous users' sensitive info security concerns and issues with biometric users' info apps. Those people explored and examined the earlier established cryptogram-centric methodologies and their downsides. Furthermore, they additionally cited the concerns of biometric user personal info app qualities. At this Juncture, an improved encipherment method is recommended which is integrated with a 3D Berboulli-Logistics map. Detailed and systematic tentative evaluation is completed, and the final outcomes determine that the opted attempt shows additional advanced stimulus in a case in point of relative diffusion. Separate after this ruse additionally confirms that the ASC and capriciousness of this methodology are more minimal as associated with the logistic mapping method. The overoffered method does not only ensure extensive security but also maintains the indistinctness of the encryption flawlessly. The results of correlation dissemination of enciphered users' info are further intermixed by diffusion and concoction. The stochastic traits of the histogram prove that the risen results of the encipherment procedure are better positioned. Consequently, it comes to be much more intricate to drop down the systems' plain and ciphertexts. Likewise, the highly broadly applied app of this methodology is an e-based biometric users' info grid [2, 3]. Throughout the time devoted to PKE, two idiosyncratic keys are employed for encipherment and unscrambling activity. Among two assigned keys, one of the keys is exclusive and the other one is accessible. Users' public key is disseminated publicly, and the secret key is just reachable to the intended collector.

RETRACTED

Every user's plain text is encoded with the intended acceptors' openly accessible key, and the technique of decipherment is finished with the intended users' secret key. This approach proposed a resolution to massive key supervision/administrative overheads; hereafter, it is not cost-effective and efficient adequate for cloud ailment.

Policy-centric ABE [21] practice resolves the underside stipulated concerns. Even if the users' attributes satisfy the competing access control plans, at this moment for decipherment only the user is allowed [22–24]. The CPABE contrive is exceptional among the public cryptographical techniques, in point of view of its center operating cost throughout the time paid for key management/administration. In such cases as when a certain secret key of a user is endangered, in that context, only info of that specific user may be unscrambled by pondering characteristics of the user. Hash-based homomorphic encipherment [4] administers enciphered user information on isolated cloud storage space that is prevented from deciphering it. This is often considered a critical methodology in cloud-based systems, structures, and research. Hash-based homomorphic encipherment validates the confidentiality of users' sensitive information in the directive of determining the protection back issue of storage space or administering users' confidential information by unauthorized parties [14, 15, 25–30]. With the affordances of WWW, cloud consumers are capable of utilizing cloud customer services just about every time and in any place. This 24/7 availability is only possible through the same characteristics that deliver constant readiness of cloud services. However, coarsening and severance could be also contemplated as doubled divergent methodologies that offer direct improvements to the accessibility of cloud systems. A ciphertext ABE (CP-ABE) methodology lends to numerous concerns/issues while instigated in the users' info distribution structure. Users' secret keys are produced through KGC while the MSK bout characteristics put off clients. The recommended algorithm/code requires a lessened quantity of attempts in the manner of depositing public-key certificates (PKCs) as contrasted to whole conventional PKI. The aforementioned approach flunks to solve the issue of key escrow KGCs which are able to decipher all ciphered text designated to each unique client by means of attributes keys' production. The stated problem infringes users' personal info confidentiality limitations in sensitive info distributing systems. One more significant drawback is that it is already well known as key revocation/annulment [5, 12, 13, 22].

2.1. Conventional QKDs Based on Crypto Graphical Techniques. The key objective of QKDs is to produce a key QK, which is utilized to transfer data among destination and source through links of quantum devoid of a secret key number [17, 19, 20]. The QKDs' procedure is demonstrated in Figure 2. In the figure, we used the BB84 protocol for QKD applying the cryptographical standard to provide security to users' private info storage.

Tseng et al. [31] established an enhanced biometric centered structure direct to defend medical e-health info in the cloud [2]. Enactment of secluded e-healthcare checking app has determined numerous challenges in the healthcare field and this significantly leads to more advantageous and mutual benefits to sick persons and healthcare specialists. In direct to accomplish this objective, HMA techniques need to observe a sick person's history and condition for the whole time.

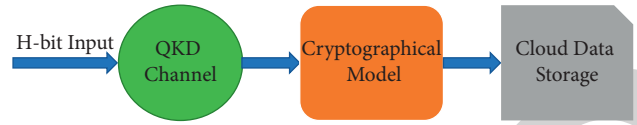


Figure 2: QKDs upon the cryptographical model.

Yang, et al. [21] presented an enciphered perceiving method to improvise the protection of the biometric validation approach. Here, the authors formed a novel method with help of biometric pictures collected by applying ocular encipherment methods. Various methods are already known as enciphered sensing methods. These methods are typically centered on the hypotheses of Dual Randomized Period Encipherment (DRPE) and Compacted Sensibility (CS). Also, enciphered DEPR is even harnessed with the assistance of the Digital Holo-graphic method (DHM). Numerous kinds of research studies are taken at the evaluation level. Enciphered biometric images are collected by using palmprint images and palm vein images. Refurbishment could be accomplished precisely with the assistance of the collected enciphered images.

Song and Wang et al. [4] offered a new-found and sophisticated biometric-centered encipherment method [2, 3]. In this proposal, they used a distorted validation procedure. The locus tokens are generated by the procedure of registration which is usually kept at biometric DBS. This protected token will not be utterly equaled alongside every recently supplied biometric indicator. It is a primary feature of biomatrix methods. IRIS and face-based centered validation techniques typically consist of a symmetrical validation procedure. If the needed password or PIN will somewhat vary apart from the initial collected one, then the validation activity will not succeed, and the truthfulness of the client is not authenticated. In a math-based study, randomized equations basically can give input from any place and it does produce various outputs which are not at all traceable back to detect what the possible outputs are. For instance, Figure 3 demonstrates the nonlinear chaotic interpretation.

3. Proposed Model

The cloud users' sensitive information, particularly in monitoring and maintenance, is a key issue and concern regarding massive volumes of both structured and unstructured big data often hosted in cloud-based systems [17, 20, 24, 32–36]. Likewise, many of the security measures currently utilized to protect that data cannot always do so adequately. Subsequently, the majority of third-party services currently offered still come with vulnerabilities that could leave users' sensitive private information open to theft

RETRACTED

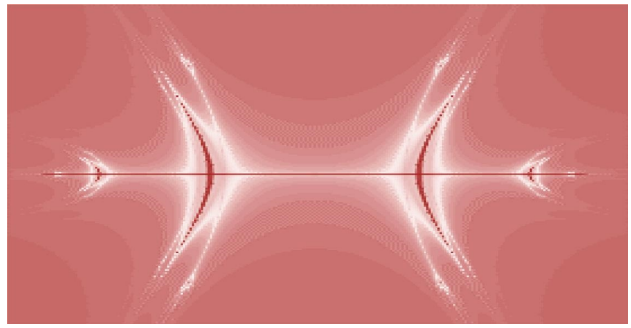


Figure 3: Chaotic randomization.

and unauthorized access or exposure [37–42]. Thus, in order to directly enhance the approaches to security and privacy concerns regarding users' personal information, this work presents an approach in which such information is enciphered through a novel enhanced and dynamic non-polynomial integrity centric quantum HCP-ABE prototype to store big cloud datasets prior to storage. This current projected model has tierce methods: user's integrity value calculation, quantum key production, and integrity-centered users' sensitive info encipherment and decipherment. The first method developed by taking inputs from cloud consumers combined with a set of attributes for digest calculation and availed fixed random digest values is applied for production of key and then at encipherment methods. The second procedure comprises the produced digest value for the production of a quantum key to the users' personal digest values based on their characteristics, access policies, and key production methods of the CPABE standard [17, 20]. Another possible method comprises the processed digest metrics and keys which are applied in the initial arrangement, production of key, encipherment, and decipherment stages. The outcome of this proposed approach is an Enhanced and Dynamic Nonlinear Polynomial Integrity-based Quantum Hash-Cipher Policy Attribute-Based Encipherment (EDNPIQHCP-ABE) algorithm, which can be made liable for top-tier encipherment and decipherment of users' sensitive information [43–45] across cloud-based servers and databases. In this model, the quantum, private, public, and master keys are centered on the user's personal input attributes or characteristics catalog [46–48]. The ciphertext is later deciphered with the help of the user's particular attributes, with control access gained policy through a formation tree entrenched in users' ciphertext, as represented in Figure 4.

In this work, a randomized security key is generated for the new data enciphering and deciphering process. Here, a novel chaotic-based dynamic key is initialized in each iteration for strong data security entitled Enhanced and Dynamic Nonlinear Polynomial Integrity-based Quantum Hash-Cipher Policy Attribute-Based Encipherment (EDNPIQ HCP-ABE).

Let $Z(m^2, *)$ is a multiplicative cyclic set with an order of 'm' such that $\text{Order}(m) \leq \text{Order}(Z(m^2, *))$. In our work, a nonlinear polynomial randomized equation is castoff to produce the key with enhanced security options. The elementary recursive relation for the nonlinear chaotic polynomial equivalence is represented as follows:

$$\begin{aligned} S_m &= Qky - S_{m-3}, \\ s_0 &= 1, \\ s_1 &= QK\left(1 + a^3\right). \end{aligned} \tag{1}$$

Definitively, dSm/dy signifies the nonlinear chaotic polynomial curves with exponential prerogatives wherever α is the arbitrative/randomized security constraint taken over from $Z(m^2, *)$. Through resolving the relapse equations, we can obtain the descendants of nonlinear polynomial chaotic equations followed by certain larger cofactors.

$1207959552y\wedge 29 - 1342177280y\wedge 27 - 830472192y\wedge 25 - 1870659584y\wedge 23 - 1014497280y\wedge 21 + 991952896y\wedge 19 + 964558848y\wedge 17 + 1175060480y\wedge 15 + 174272512y\wedge 13 - 1229955072y\wedge 11 + 155343449y\wedge 9 + 36067098y\wedge 7 + 208087657y\wedge 5 + 12653734y\wedge 3 + 873832y$ by the nonnegative factor of 17780647524

$1979711488y\wedge 29 + 578813952y\wedge 27 - 1029701632y\wedge 25 + 749731840y\wedge 23 + 871235584y\wedge 21 - 555614208y\wedge 19 - 1401847808y\wedge 17 - 774422528y\wedge 15 - 182041600y\wedge 13 + 1202926976y\wedge 11 + 965151200y\wedge 9 + 1092624y\wedge 7 + 206764y\wedge 5 + 783262y\wedge 3 + 206y$ by the nonnegative factor of 9657906

$-134255728y\wedge 23 - 733897504y\wedge 21 + 385875758y\wedge 19 + 2340472192y\wedge 17 + 7824629504y\wedge 15 + 878251136y\wedge 13 - 574588672y\wedge 11 + 724482800y\wedge 9 - 123107968y\wedge 7 - 685169920y\wedge 5 + 368980864y\wedge 3 + 21342y$ by the nonnegative factor of 1214440528

$268435256y\wedge 24 - 9646899320y\wedge 22 - 1507852478y\wedge 20 - 1792196384y\wedge 18 - 182694016y\wedge 16 + 95657184y\wedge 14 + 346522200y\wedge 12 + 818754732y\wedge 10 + 1242689120y\wedge 8 - 1220779936y\wedge 6 + 1062293360y\wedge 4 + 1155720y\wedge 2 + 210$ by the nonnegative factor of 3922114

$291727281y\wedge 29 - 627261231y\wedge 27 + 1073741824y\wedge 25 - 2147483648y\wedge 23 + 192937984y\wedge 21 + 2038431744y\wedge 19 + 946339840y\wedge 17 - 2002780160y\wedge 15 + 673841152y\wedge 13 + 1271791616y\wedge 11 - 331466752y\wedge 9 + 11834777\ 60y\wedge 7 + 2125078144y\wedge 5 + 42067584y\wedge 3 + 22472y$ by the nonnegative factor of 99057864

$-1073741824y\wedge 26 - 1342177280y\wedge 24 - 1342177280y\wedge 22 - 1092616192y\wedge 20 + 1160249344y\wedge 18 + 1465778176y\wedge 16 - 305397760y\wedge 14 + 1670414336y\wedge 12 + 1807517696y\wedge 10 + 684548608y\wedge 8 - 1988899328y\wedge 6 + 116777232\ y\wedge 4 +$

RETRACTED

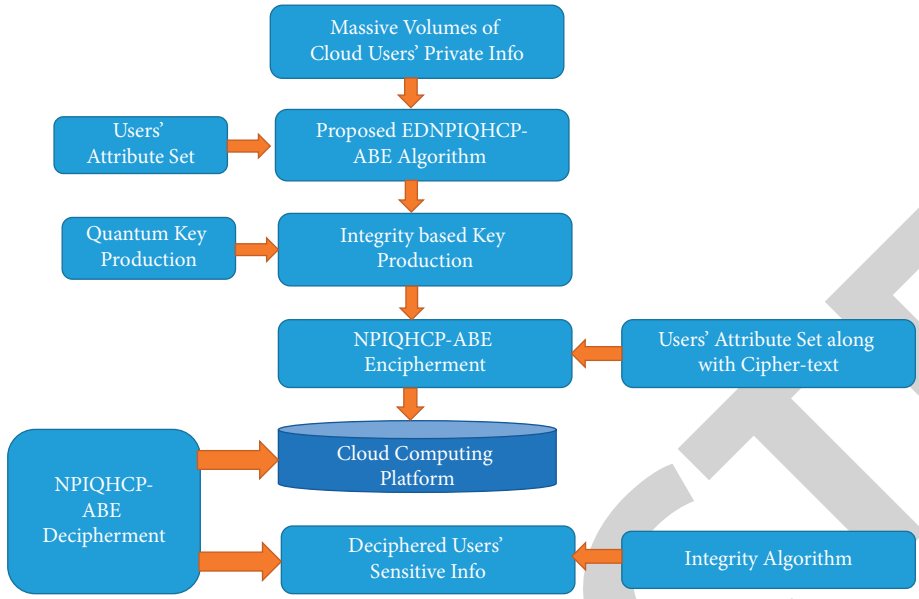


Figure 4: Proposed model block diagram.

1224936$y\wedge2$ + 214 by the nonnegative factor of 1178401066

$-1073741824y\wedge26-1879048192y\wedge24+1879048192y\wedge22-973078528y\wedge20+1317535744y\wedge18-1132331008y\wedge16-1912864768y\wedge14-1736417280y\wedge12-1969756160y\wedge10-2126109184y\wedge8$ − 512449024$y\wedge6$ + 128110752 $y\wedge4$ + 1294920$y\wedge2$ + 218 by the non − negative factor of 1304585562

295364613$y\wedge29$ + 753737249$\wedge27$ + 1073741824$y\wedge25$ − 2147483648$y\wedge23-1476395008y\wedge21-2013265920y\wedge19-873988096y\wedge17+2141192192y\wedge15+1522827264y\wedge13-643989504y\wedge11$ − 671623168$y\wedge9$ + 16017776 64$y\wedge7$ − 587544832$y\wedge5$ + 48787200$y\wedge3$ + 24200y by the non-negative factor of 1362704928

$-2147483648y\wedge26-1342177280y\wedge24-1207959552y\wedge22$ − 905969664$y\wedge20$ − 50331648$y\wedge18$ + 196476928$y\wedge16$ + 1350336512$y\wedge14+1163239424y\wedge12-870346752y\wedge10+404148736y\wedge8$ − 451731200$y\wedge6$ + 1403075520$y\wedge4$ + 1367520$y\wedge2$ + 222 by the nonnegative factor of 1499881762

$-1073741824y\wedge25-$ $-2147483648y\wedge23-1577058304y\wedge21-369098752y\wedge19-908066816y\wedge17+729808896y\wedge15+39321600y\wedge13+2026373120y\wedge11+1731749888y\wedge9-113717248y\wedge7+1978285184y\wedge5+64607360y\wedge3+27848y$ by the nonnegative factor of 1936249632

$-2147483648y\wedge26-268435456y\wedge24+939524096y\wedge22+973078528y\wedge20+218103808y\wedge18-229455360y\wedge16-1250656256y\wedge14-51470336y\wedge12+1250463744y\wedge10+1224784384y\wedge8-1123725056y\wedge6+1534160320y\wedge4+1442784y\wedge2$ + 226 by the nonnegative factor of 2116157726

$-1073741824y\wedge26+1342177280y\wedge24+805306368y\wedge22-704643072y\wedge20+295698432y\wedge18-307757056y\wedge16-785383424y\wedge14-1211670528y\wedge12-1616918528y\wedge10-$ 665903616$y\wedge8$ − 1794355712$y\wedge6$ + 1674863680$y\wedge4$ + 1520760$y\wedge2$ + 230 by the nonnegative factor of 951552102

295364613$y\wedge31$ + 753737249$\wedge29$ + 1073741824$y\wedge27$ − 2147483648$y\wedge25-1476395008y\wedge23-2013265920y\wedge19-873988096y\wedge17+2141192192y\wedge15+1522827264y\wedge13-643989504y\wedge11$ − 671623168$y\wedge9$ + 16017776 64$y\wedge7$ − 587544832$y\wedge5$ + 48787200$y\wedge3$ + 24200y by the non-negative factor of 2367205671

$3979711488y\wedge33+578813952y\wedge31-1029701632y\wedge27+749731840y\wedge23+871235584y\wedge21-555614208y\wedge19-1401847808y\wedge17-774422528y\wedge15-182041600y\wedge13+1202926976y\wedge11+965151200y\wedge9+1092624y\wedge7+206764y\wedge5+783262y\wedge3+206y$ by the nonnegative factor of 3456710297

Input: Beginning initialized parameters, block-size BLK_S, total count of rounds TC_R, block-bits, cyclic-hash vector CH_V, users' sensitive info-size USI_S, initial input info II_I, PM_X, and PM_K are permutation matrices

Output: Biometric centered integrity value BCI_V

Step 1: Declared and initialized input parameters and cyclic-hash vector. CH_V[block-bits/16]← 0

//declare and assign hash-based cyclic vector as NULL

Step 2: Opt for a specific single nonlinear equation followed by the private key $p(k)$ which is able to improve all over volatility nature and inert security; a novel randomized hash-based nonlinear polynomial randomized method is built. This is essentially an amalgamation of the logistic nature of Bernoulli along with a randomized functional system [6]. Logistic mapping is a conventional frenzied mapping practice that leads to the obtained outcomes much convoluted and randomized characteristic in nature

RETRACTED

from the interludes within the range [0, 1]. The production of state-run ensues as per the below-stated equation

$$s(m+1) = \beta H(Hi)(1 + y(Hi)).$$

Now, β ranges from 5 to 9.5, that is, [5, 9.5]. The mentioned equation is accountable for generating a quasi-randomized run cycle sequence by taking input as a randomized chaotic distinct-time non-linear polynomial active structure. Bernoulli's method could be well defined as a discrete stochastic time method.

$$Q(y) = S(k) * q(y).$$

Here, $Q(y)$ is one of the curves which is a part of a nonlinear polynomial curve set. $S(k)$ is the arbitrary cofactor which is available at the Z family group.

Step 3: Compute $\lambda = \mathrm{GCD}(R\_E1 - 1, R\_E2 - 1)$ and $n = R\_E1 * R\_E2$.

where R_E1 and R_E2 are brought from the Z family group.

Step 4: Choose a random digit that should be coprime to λ. Compute R_P1 and R_P2 with the help of λ

$$R\_P1 = \theta/(R\_p2 + n)$$

Step 5: Choose random values R_V1, R_V2, R_V3, R_V4 after $Z(m^2, *)$

Step 6: Calculate Pm_k1, Pm_k2, Pm_k3, Pm_k4 like

$$Pm\_k1 = 1 + R\_V4 * (R\_P1 * R\_P2),$$
$$Pm\_k2 = Pm\_k1^{R\_V3\wedge 2} \bmod (m2),$$
$$Pm\_k3 = sm1.Pm\_k2^{R\_V1\wedge 3} \bmod (m2),$$
$$Pm\_k4 = sm1.Pm\_k1q1.(R\_E1 * R\_E2) \bmod (m2).$$

Step 7: Round key permute $Rk\_p1 = \{Pm\_k2, Pm\_k3, Pm\_k4, M1, \mathrm{CG1.CG2}, Q(M)\}$.

Step 8: Round key permute $Rk\_p2 = \{M1, R\_V1, R\_V3, \alpha, S(k)\}$

Step 9: until (USI_S > BLK_Bits/16)

do

BSB ← First 128 bits of subblock

for every split block BSB Block

do

for ($C = 0$ to tc_r)

do

opt $rk1$ and $rk2$ keys like Pm_x and Pm_k as arbitrary permutation boxes.

$$Pm\_x1 = (Pm\_k^t.Pm\_x1) \bmod (\max\{Pm\_x1.\mathrm{eigenvalues}\})$$

$$y1 = Pm\_k.\mathrm{Kronproduct}(Pm\_x1).\mathrm{scale}(1024),$$

$$S_i = \mathrm{BSB}[i] + c[\max(0, i-1)],$$

$$S_i = \mathrm{Max}\{rk1, rk2\} \oplus S_i \oplus y_i.$$

done

BSB[i] ← Left_Shift (BSB[i])

BSB[i] ← Right_Reverse (BSB[i], 5)

if ($C + 1 <$ tc_r)

then

BSB[i] ← Right_Reverse (BSB[i], 3)

BSB[i] ← Left_Shift (BSB[i], 6)

BSB[i] ← Right_ShiftR (BSB[i], 3)

end if

done

$H = h_0 + h_1 \ldots\ldots h_{TC-R}$.

Done

3.1. C-Bilinear Pairing. C-bilinear pairing yields the production of two C-modules under the cyclic group C. Once C is a region and both element groups are identical, this yields a cyclic bilinear form. Consequently, C-bilinear pairings offer a broad view of internal multiplicative products.

Let C be a commutative cyclic group with inverse unit u, and assume that M_1, M_2, and M_3 are C-modules. A pairing is every C-bilinear map cbp: $M_1 \times M_2 \longrightarrow M_3$; i.e., it should obey the following:

$$\mathrm{cbp}(c.m_1, m_2) = \mathrm{cbp}(m_1, c.m_2) = c.\ \mathrm{cbp}(m_1, m_2)$$

$$\mathrm{cbp}(m_{11} + m_{12}, m_2) = \mathrm{cbp}(m_{11}, m_2) + \mathrm{cbp}(m_{12}, m_2)$$

$$\mathrm{cbp}(m_1, m_{21} + m_{22}) = \mathrm{cbp}(m_1, m_{21}) + \mathrm{cbp}(m_1, m_{22})$$

$\forall c \in C$ and all m_1, m_{11}, $m_{12} \in M_1$ all m_2, m_{21}, $m_{22} \in M_2 \equiv$ a paring is a C-bilinear map

$M_1 \otimes \mathrm{C}\ M_2 \longrightarrow M_3$ here $M_1 \otimes \mathrm{C}\ M_2$ signifies tensor product of M_1, M_2

A bilinear map is similarly considered a C-bilinear map if $\Phi: M_3 \longrightarrow \mathrm{Hom_C}(M_2 M_1)$; i.e., it fits the first definition via arranging $\Phi(m_3)(m_2) := e(m_3, m_2)$. A C-bilinear map-pair is termed perfect if the above chaotic type map Φ is an isomorphy of C-modules. A C-bilinear map-pair is termed nondegenerate; then, $e(m_3, m_2) = 0 \forall m_3 \in m_2 = 0$; likewise, e is described as nondegenerative if $(m_3, m_2) = 0 \forall m_2 \in m_3 = 0$.

3.2. Key Framing and Making with QKD. Intended quantum key distribution/dissemination (QKD) necessitates transmission network links like a quantum-based channel and a regular public data channel [10, 11]. The source and recipient together entail arbitrary originators from the C-bilinear cyclic group and a bunch of primitive and polarized qubits. In the proposed model, we incorporated enhanced BB84 validation protocol to counteract the quantum channel which is not confronted while transmission through the man in the middle (M-I-M) attacks [7]. The produced QKD public key is issued to certified clients for the EDNPIQ HCP-ABE standard. The EDNPIQ HCP-ABE system similarly requires four essential algorithms/procedures as Key_Gen, Set_up, En_cipher, and De_cipher all are portrayed underneath. In the QKD process, the key is generated at the source end in order to share the decryption secret key with the other end of the user.

3.2.1. Set_up Phase. For instance, G is the bilinear cyclic group where po is the prime order, and gk is the

RETRACTED

generator that should gratify bilinear cyclic property, confusion, and diffusion properties such as that Θ_1, $\Theta_2 \epsilon \mathrm{CG}_{po}$. The open-key and master-key could be produced with

$$\text{Public\_Key (Puk)} = \left\{ \begin{array}{l} \text{Proposed\_QHash (Quantum\_key|user\_attributes)}, (g0 \in CG1 (CH\_V[i]), \\ gpo \in CG2\left(\dfrac{CH\_V[i]}{CG1}, CG2 \in \text{Integrity\_values}(CH\_V[i], CH\_V \in Z2r, \right\}, \\ g0 = e(go, gpo) \end{array} \right.$$

$$\text{Public\_Key (Puk)} = \left\{ \begin{array}{l} \text{Proposed\_QHash (Quantum\_key|user\_attributes)}, (g0 \in CG1 (CH\_V[i]), \\ gpo \in CG2\left(\dfrac{CH\_V[i]}{CG1}, CG2 \in \text{Integrity\_values}(CH\_V[i], CH\_V \in Z2r, \right\}, \\ g0 = e(go, gpo) \end{array} \right. \quad (2)$$

$$\text{Matser\_Key (Mak)} = (\alpha \in Puk(gpo), \beta \in \text{QHash}(\text{private\_key}(CH\_V\text{Attr1}[0] \wedge CH\_V\text{Attr2}[1] \wedge \ldots CH\_V\text{Attr1}[n])), Z^2 r, e(\beta, \alpha)_1^{\theta}\}.$$

It produces the main key ($\mathrm{Ma_k}$) and QKD private key, and PU_{k1} and PU_{k2} are public-key parameters. In this work, the secret credentials are transferred to the other end of the user in a trusted encrypted channel with the shared key. Here, the large scale of information collected in the trusted third-party clouds is in encrypted form which can be accessed by the authorized user with the shared key.

3.2.2. Encipherment Phase. In this encipherment phase, we gave inputs as the users' plain text (PT) to produce the required ciphered text. The encipherment method enciphers the original plain text utilized to gain access to the tree-structure TS. Commencing from the head node, this method chooses an arbitrary number a_n from p–integer modulo Z^2 and establishes $q(\mathrm{RK}, 0) = \mathrm{r\_v}$. Meant for the intermediary nodes I_n, it aligns $q(i\_n, 0) = q(\text{parent\_node } (i\_n, \text{key}))$. Here, L_N is the bunch of nonroot odes in the control log on policy structure at the tree root level, and the ciphered text is produced centered on the offered control access policy tree-structure TS as

$$\text{Cipher\_Text (CT)} = \left\{ \begin{array}{l} \mathrm{CT}^1 = PT.e(k1, k1)^{\theta} 1^{r\_v}, PT, CT^2 = m^{r\_v}, \forall i\_n \in I\_N\colon Cx = k1^{q(i\_n,0)}, \\ \mathrm{CT}_{i\_n}^1 = CH\_V(A(I\_N))^{q(i\_n,0)} \end{array} \right. . \quad (3)$$

Verifying all homomorphic properties to do plain-text encipherment,

Homomorphic centered encipherment and decipherment utilize $\boldsymbol{\omega}(i)_0$, $\omega(i)_0'$ as inputs

Additive homomorphic encipherment: $\mathrm{AHEncD}(i_1 + i_2) = \mathrm{AHEncD}(i_1) + \mathrm{AHEncD}(i_2)$

Multiplicative homomorphic encipherment: $\mathrm{MHEncD}(i_1.i_2) = \mathrm{MHEnc}(i_1).\mathrm{MHEnc}(i_2)$

$\omega(i)_0 = \mathrm{AHEncD}(i_1) := \mathrm{AHEncD}(i_1) = (i_1 + \gamma * \beta) \mod m$ whereas $m = \alpha * \beta$

$\omega(i)_0' = \mathrm{AHEncD}(i) := \mathrm{AHEnc}(i_2) = (i_2 + \gamma * \beta) \mod m$ whereas $m = \alpha * \beta$

$\mathrm{AHEncD}(i_1 + i_2) := \mathrm{AHEnc}(\omega(i)_0) + \mathrm{AHEnc}(\omega(i)_0')$

$\mathrm{AHEncD}(i_1 + i_2) := (i_1 + \gamma * \beta) \mod m + (i_2 + \gamma * \beta) \mod m$

$\mathrm{MHEncD}(i_1.i_2) := \mathrm{MHEncD}(\omega(i)_0).\mathrm{MHEncD}(\omega(i)_0'): = (i + \gamma * \beta) \mod m + (i_2 + \gamma * \beta) \mod m$

3.2.3. Key_Gen Phase. The Key_Gen algorithm produces private_key (Pri_K) with user attribute set (U_A). The Key_Gen algorithm consumes users' attributes set U_A; input is QKD (shared_key) and produced output is private_key. This algorithm chooses a random number r_n and r and f to every user attribute $\mathrm{U\_}A_f$; also, these arbitrary numbers are chosen as the cofactor of QKD (shared_key) and stand at Z_p^2.

$$\text{Secret\_Key}(\mathrm{Se}_k) = \left\{ DT = k\_v^{(\theta 1 + \mathrm{rand}f)/\theta 2}, DT(f) = k\_v_f^{\mathrm{rand}f * CH\_V(f).\mathrm{rand}}, DT(f) = k\_v\,\mathrm{rand}_f \right\}. \quad (4)$$

RETRACTED

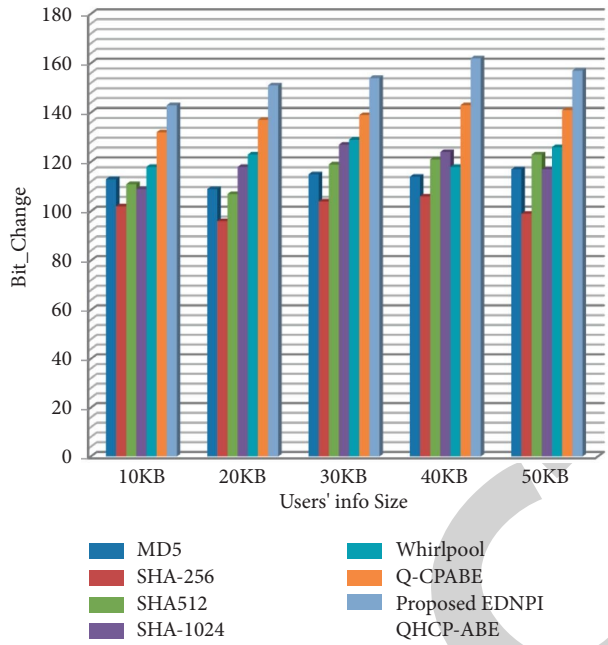


Figure 5: Computational evaluation of key production for the proposed EDNPI QHCP-ABE to the traditional models.

3.2.4. Decipherment Scheme. This phase receives *Prk* as a private key, *U_A* as a user attribute set, CT as ciphertext, *Ts* as a control access structure, and *PuK* as a public key for all inputs. The decipherment procedure is performed iteratively. A recursion-based process is performed based on three factors, i.e., ciphertext (CT), private key (*Prk*), users attribute set *U_a*, and the point node *I_n* of the *Ts*.

Verification of homomorphic property for user info decipherment is as follows.

Consider PT.e (AHEncD $(i_1 + i_2)$, MHEnc$(i_1.i_2)$).e(CT $(i)_1$, $K_{1,i}$).e(T $K_{1,j}$).e(CT $(k)_3$, $K_{1,f}$) to obtain constructed user access policy.

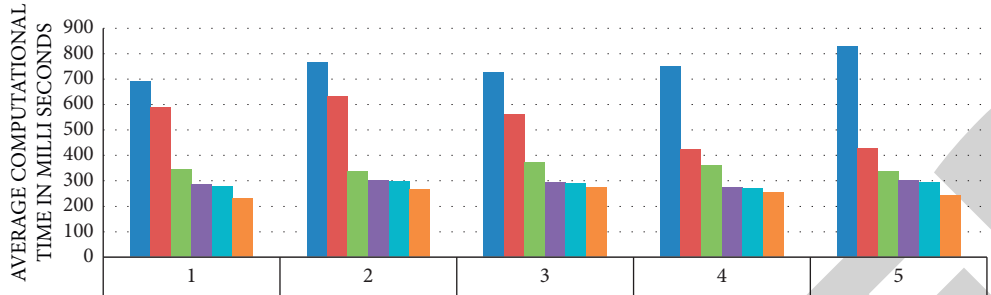
$$\begin{aligned}
AHEncD &= AHEnc\left(\omega(i)_o\right) + \left(\omega(i)_o'\right) \\
&= AHEnc\left(\omega(i)_o\right) + Enc\left(\omega(i)_o'\right) \\
&= \left(\omega(i)_o' + \gamma * \beta\right)\mathrm{mod}m + \left(\omega(i)_o' + \gamma * \beta\right)\mathrm{mod}m, \\
MHEnc\left(i_1.i_2\right) &= MHEnc\left(\omega(i)_o.\omega(i)_o'\right) \\
&= Enc\left(\omega(i)_o\right).Enc\left(\omega(i)_o'\right) \\
&= \left(\omega(i)_o + \gamma * \beta\right)\mathrm{mod}m + \left(\omega(i)_o + \gamma * \beta\right)\mathrm{mod}m, \\
AHDec\left(EncD\left(i_1 + i_2\right)\right) &= \left(AHEncD\left(\omega(i)_o\right) + \left(\omega(i)_o'\right)\right)\mathrm{mod}\alpha \\
&= \left(\left(\omega(i)_o + \gamma * \beta\right)\mathrm{mod}m + \left(\omega(i)_o' + \gamma * \beta\right)\mathrm{mod}m\right)\mathrm{mod}\alpha \\
&= i_1 + i_2, \\
MHDec\left(EncD\left(i_1.i_2\right)\right) &= \left(MHEncD\left(\omega(i)_o.\omega(i)_o'\right) = MHEncD\left(\omega(i)_o\right).MHEnc\left(\omega(i)_o'\right)\right)\mathrm{mod}\alpha \\
&= \left(\left(\omega(i)_o + \gamma * \beta\right)\mathrm{mod}m + \left(\omega(i)_o + \gamma * \beta\right)\mathrm{mod}m\right)\mathrm{mod}\alpha \\
&= i_1.i_2.
\end{aligned} \tag{5}$$

4. Experimental Results

Overall, the experimentations are performed over AWS SSS storage through every user's base arrangement as Intel(R) Core (TM) i7-3458M CPU@2.70 GHz, 16-GB RAM, 64-bit operating system. This framework necessitates third-party predefined system libraries Java SDK, Jama, Apache Commons, and Apache Math.

4.1. Cloud Platform Base. Our proposed cloud platform AWS cloud servers are utilized for results simulations of the proposed standard on biomedical user-sensitive private info

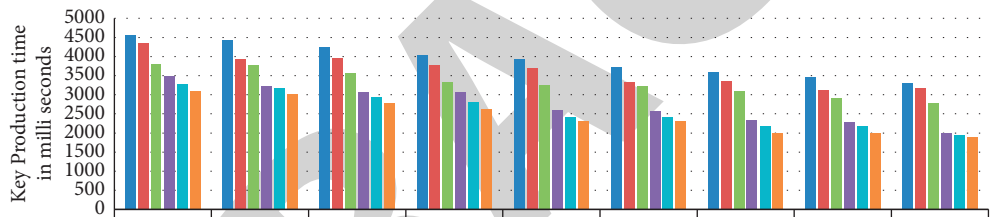
RETRACTED



	1	2	3	4	5
CPABE	692.356	768.307	727.958	751.237	829.709
FHABE	591.051	633.099	559.974	423.071	425.777
QKD CPABE	345.545	337.354	372.332	359.441	336.597
CQ CPABE	284.436	301.328	294.768	274.466	301.436
ICQ CPABE	278.568	297.354	291.536	271.633	295.642
EDNPI QHCP ABE	232.586	268.452	276.734	254.465	241.724

COMPARISION OF EXISTING ALGORITHMS WITH PROPOSED ALGORITHM

Figure 6: Relative evaluation of the planned prototype to traditional techniques with respect to mean computation time.



	5	10	15	20	25	30	35	40	50
ABE	4576.06	4435.54	4235.24	4043.24	3934.69	3731.25	3584.07	3475.93	3307.47
CPABE	4358.28	3937.9	3965.84	3767.17	3695.66	3339.3	3361.54	3108.91	3170.75
KPABE	3812.65	3766.17	3565.74	3336.36	3258.87	3222.08	3106.54	2927.51	2776.32
QKD CPABE	3494.69	3217.73	3081.91	3067.63	2588.67	2568.58	2352.2	2292.16	1997.24
ICQ CPABE	3265.23	3183.46	2946.36	2815.75	2428.57	2416.37	2185.75	2174.74	1935.19
EDNPI QHCP ABE	3102.32	3023.33	2775.89	2631.56	2313.81	2311.45	1990.85	1992.87	1895.9

Users' Attribute Size

Figure 7: Proportional analysis of suggested method with the existing methods with respect to chaotic centered dynamic key production time and total count of users' attributes.

security. In this cloud server, Amazon EC2 instances and Simple Storage Service (Amazon S3) are utilized to produce experimental results along with the sensitive info security making use of the integrity and encipherment algorithms. EC2 offers a flexible dynamic-sized calculation facility in the A cloud. EC2 provides simple and easy web-based scalar computation for inventors. An uncomplicated way to comprehend edge is available for the arrangement of kit control projected to the finest aspect along with no exertion countability. The overhead edge is capable of deliberation and omission of instances. EC2 instances are set up at Virtual Personal Cloud (VPC) by letting the clients do an experiment about which cases ought to be disclosed to WWW. The end goal is to pact together where in-bound and out-bound systems, privacy rallies, and system ACLs are implemented. Here, this model is applicable to image types in 2D or 3D format [10, 49, 50].

For testing and supervising EC2 instances, Amazon offers Cloud Watch [31] web assistance. Cloud Watch oversees dynamic resource management, demand layouts, and functional implementation. Elite registering provided by Amazon manages clients' complex computational burdens. With respect to Amazon EC2, cloud users are permitted to pick and choose a functioning structure, load existing standard apps, establish a system get hold of privileges, and emulate that case plus preprocessing power.

The suggested prototype is compared to traditional approaches with respect to the bit range of hash digest value and its arbitration, as shown in Figure 5. In our proposal, we

RETRACTED

Table 1: Relative analysis of the planned algorithm to the traditional techniques with respect to various computational properties.

Properties	Whirlpool	SHA-256	SHA-512	QCP-ABE	SHA-1024	MD5	Proposed EDNPI QHCP-ABE
Big data	NO	NO	NO	Yes	NO	NO	Yes
Dynamic key	NO	NO	NO	Yes	NO	NO	Yes
Transmission cost	High	High	High	Slightly low	High	High	Very low
Key size	Fixed	Fixed	Fixed	Variable	Fixed	Fixed	Highly randomized
Static key	Yes	High	Yes	Yes	Yes	Yes	Yes

Table 2: Efficacy Analysis among suggested standards to the conventional hash methods.

Cloud clinical dataset	MD5	SHA-1024	Whirlpool	QCP-ABE	Proposed EDNPI QHCP-ABE
Efficacy	O(bs2ks)	O(bskslog(n))	O(bslog(bsks))	O(bslog(ks))	O(bslog(ks/2))

have a higher bit change hash digest value than traditional models, as seen in the table.

Figure 6 depicts a resemblance of the coined proposal to traditional runtime computation techniques. Various data sizes were employed in the experiment to determine the average computational time. The suggested model for cloud security has great computational efficiency, as shown in Figure 7.

Figure 7 depicts the average computation time required for the proposed method versus the existing approaches for dynamic key creation. The overall computing time of the chaotic dynamic key production in the suggested method is substantially faster than the known models.

The relative evaluation of the planned large cloud info computational parameters to conventional approaches is shown in Table 1. The suggested nonlinear polynomial integrity technique has distinguishing aspects such as a constant/fixed key, a big volume of users' sensitive private data, and a chaotic dynamic key generation mechanism, as shown in the table. In addition, when compared to standard models, the suggested method uses highly randomized arbitrary/variable key sizes and has a very low communication/transmission overhead/cost.

Table 2 exemplifies the productivity of the proposed chaotic integrity corroboration method with conventional authentication procs with respect to sensitivity and chaotic hash calculation. From Table 2, one can notice that the current chaotic integrity method is much better than the conventional practices for random hash production. Hither, bs stands for bit-size, and ks signifies key size.

5. Conclusion and Future Scope

In the current paper, an Enhanced and Dynamic Nonlinear Polynomial Integrity-based Quantum Hash-Cipher Policy Attribute-Based Key Generation is proposed. Our method comprises a group of nonlinear chaotic curves produced with the convoluted randomized function. Conventional attribute-based encipherment methods tough to deal with massive volumes of users' sensitive info with the dynamic key production procedure. However, conventional attribute-based encipherment techniques are nondependent on integrity value because of insignificant computing resources. To overcome the existing challenges/issues, Enhanced and Dynamic Nonlinear Polynomial Integrity-based Quantum Hash-Cipher Policy Attribute-Based Encipherment was applied to users' sensitive massive volumes of structures and unstructured info. In the proposed method, clients' attributes are protected with nonlinear polynomial-based dynamic chaotic map function for key initialization/commencement, client's personal info enciphering, and deciphering procedure. Real-time experimental simulation results demonstrate and prove that the implemented model in this paper has the best precision and correctness with respect to users' private confidential info encipherment and decipherment time and calculated memory likened with prevailing attribute-based encipherment and decipherment methods. Practical experimental results demonstrated that the suggested method in this paper has a high-level computation rate, space-storage overhead/cost, and ensured key dissemination; i.e., the stated standard has superior preciseness of more than 90% with respect to bit change and more than 95% with respect to dynamic key generation, encipherment, and decipherment time as compared over the conventional CPABE, KPABE, CQ-CPABE, and QCP-ABE types. In future work, this work can be extended to improve the efficacy of the encipherment and decipherment process for the multidocument formats using a deep learning structure.

Data Availability

The data used to support the findings of the study can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest in the manuscript.

Acknowledgments

The authors would like to acknowledge the support received from Taif University Researchers Supporting Project Number TURSP-2020/147, Taif University, Taif, Saudi Arabia.

RETRACTED

References

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "Dual-server public-key encipherment with keyword search for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 789–798, 2016.

[2] M. H. Nakouri and T. H. Kim, "A new biometric-based security framework for cloud storage," in *Proceedings of the Thirteenth International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 390–395, Valencia, Spain, June 2017.

[3] H. M. Sabri, K. K. A. Ghany, H. A. Hefny, and N. Elkhameesy, "Biometrics template security on cloud computing," in *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 672–676, New Delhi, India, September 2014.

[4] X. Song and Y. Wang, "Homomorphic cloud computing scheme based on hybrid homomorphic encipherment," in *Proceedings of the Third IEEE International Conference on Computer and Communications (ICCC)*, pp. 2450–2453, Chengdu, China, June 2017.

[5] S. H. Von Solms and B. L. Tait, "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)*, pp. 468–479, Poznan, Poland, October 2005.

[6] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[7] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and secure sensor data storage with dynamic integrity assurance," in *Proceedings of the IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, pp. 954–962, Rio de Janeiro, Brazil, April 2009.

[8] G. Dhiman, S. Juneja, W. Viriyasitavat et al., "A novel machine-learning-based hybrid CNN model for tumor identification in medical image processing," *Sustainability*, vol. 14, no. 3, p. 1447, 2022.

[9] K. Singamaneni, P. S. Naidu, and V. S. K. Pasupuleti, "Efficient quantum cryptography technique for key distribution," *Journal Européen des Systèmes Automatisés*, vol. 51, no. 4-6, pp. 4–283, 2018.

[10] K. Kour, D. Gupta, K. Gupta et al., "Smart-hydroponic-based framework for saffron cultivation: a precision smart agriculture perspective," *Sustainability*, vol. 14, no. 3, p. 1120, 2022.

[11] M. A. Khan, D. E. Z. Baig, B. Ashraf, H. Ali, J. Rashid, and J. Kim, T. Schwarz and E. L. Miller, Dynamic modeling of a nonlinear two-wheeled robot using data-driven approach," *Processes*, vol. 10, no. 3, p. 524, 2022.

[12] J. S. Khan, W. Boulila, J. Ahmad et al., "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, Article ID 159732, 2020.

[13] H. Gan, S. Xiao, and Y. Zhao, "A novel secure data transmission scheme using chaotic compressed sensing," *IEEE Access*, vol. 6, pp. 4587–4598, 2018.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proceedings of the. 14th European Symp. Research in Computer Security (ESORICS '09)*, pp. 355–370, Berlin, Germany, June 2009.

[15] M. Uppal, D. Gupta, S. Juneja, G. Dhiman, and S. Kautish, "Cloud-based fault prediction using IoT in office automation for improvisation of health of employees," *Journal of Healthcare Engineering*, Hindawi Limited, vol. 2021, , Article ID 8106467, 2021.

[16] C. Patel, D. Joshi, N. Doshi, A. Veeramuthu, and R. Jhaveri, "An enhanced approach for three factor remote user authentication in multi - server environment," *Journal of Intelligent and Fuzzy Systems*, iOS Press, vol. 39, no. 6, pp. 8609–8620, 2020.

[17] H. Kaur, A. Rai, S. S. Bhatia, and G. Dhiman, "MOEPO: a novel Multi-objective Emperor Penguin Optimizer for global optimization: special application in ranking of cloud service providers," *Engineering Applications of Artificial Intelligence*, vol. 96, Article ID 104008, 2020.

[18] A. Qayyum, J. Ahmad, W. Boulila et al., "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, Article ID 140876, 2020.

[19] Y. Hajjaji, W. Boulila, I. Riadh Farah, I. Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: a systematic review," *Computer Science Review*, vol. 39, Article ID 100318, 2021.

[20] G. Dhiman, D. Oliva, A. Kaur et al., "BEPO: a novel binary emperor penguin optimizer for automatic feature selection," *Knowledge-Based Systems*, vol. 211, Article ID 106560, 2021.

[21] Y. Yang, X. Chen, H. Chen, and X. Du, "Improving privacy and security in decentralizing multi-authority attribute-based encipherment in cloud computing," *IEEE Access*, vol. 99, p. 1, 2011.

[22] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: a lightweight identity-based cryptography for body sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 926–932, 2009.

[23] S. Sharma, S. Gupta, D. Gupta et al., "Recognition of Gurmukhi Handwritten City Names Using Deep Learning and Cloud Computing," *Scientific Programming*, vol. 2022, Article ID 5945117, 16 pages, 2022.

[24] S. Juneja, S. Jain, A. Suneja et al., G. Dhiman, "Gender and age classification enabled blockschain security mechanism for assisting mobile application," *IETE Journal of Research*, pp. 1–13, 2021.

[25] M. Aksa, J. Rashid, M. Wasif Nisar, T. Mahmood, H. Y. Kwon, and A. Hussain, "BitmapAligner: bit-parallelism string matching with MapReduce and hadoop," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 3931–3946, 2021.

[26] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in *Proceedings of the 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08)*, pp. 90–107, 2008.

[27] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008.

[28] M. Naor and G. N. Rothblum, "The complexity of online memory checking," in *Proceedings of the. 46th Ann. IEEE Symp. Foundations of Computer Science (FOCS '05)*, pp. 573–584, New York, NY, U.S.A, January 2005.

[29] E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," *Computer Security - ESORICS 2008*, vol. 5283, pp. 223–237, 2008.

[30] K. K. Singamaneni and P. Naidu, "Secure key management in cloud environment using quantum cryptography," *Ingénierie des Systèmes d'Information*, vol. 23, pp. 213–222, 2018.

[31] F. K. Tseng, R. J. Chen, and B. S. P. Lin, "iPEKS: fast and secure cloud data retrieval from the public-key encipherment with keyword search," in *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and*

RETRACTED

Communications, pp. 452–458, Melbourne, VIC, Australia, July 2013.

[32] K. K. Singamaneni and S. N. Pasala, "An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security," *International Journal of Knowledge-Based and Intelligent Engineering Systems*, vol. 24, no. 2, pp. 145–156, 2020.

[33] J. Rashid, S. M. Adnan Shah, and A. Irtaza, "A novel fuzzy k-means latent semantic analysis (FKLSA) approach for topic modeling over medical and health text corpora," *Journal of Intelligent and Fuzzy Systems*, vol. 37, no. 5, pp. 6573–6588, 2019.

[34] G. Dhiman, S. Juneja, H. Mohafez et al., "Federated learning approach to protect healthcare data over big data scenario," *Sustainability*, vol. 14, no. 5, p. 2500, 2022.

[35] R. Kumar and G. Dhiman, "A comparative study of fuzzy optimization through fuzzy number," *International Journal of Modern Research*, vol. 1, no. 1, pp. 1–14, 2021.

[36] P. K. Vaishnav, S. Sharma, and P. Sharma, "Analytical review analysis for screening COVID-19 disease," *International Journal of Modern Research*, vol. 1, no. 1, pp. 22–29, 2021.

[37] K. K. Singamaneni and P. Naidu, "IBLIND quantum computing and HASBE for secure cloud data storage and accessing," *Revue d'Intelligence Artificielle*, vol. 33, no. 1, pp. 33–37, 2019.

[38] F. Masood, W. Boulila, J. Ahmad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "A novel privacy approach of digital aerial images based on Mersenne twister method with DNA genetic encoding and chaos," *Remote Sensing*, vol. 12, no. 11, p. 1893, 2020.

[39] C Rupa, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "A blockchain based cloud integrated IoT architecture using a hybrid design," in *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 550–559, Springer, Berlin, Germany, January 2020.

[40] S. Juneja, G. Dhiman, S. Kautish, W. Viriyasitavat, and K. Yadav, "A perspective roadmap for IoMT-based early detection and care of the neural disorder, dementia," *Journal of Healthcare Engineering*, Hindawi Limited, vol. 2021, , Article ID 6712424, 2021.

[41] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification," *Remote Sensing*, vol. 13, no. 11, p. 2221, 2021.

[42] G. T. Reddy, K. Sudheer, K. Rajesh, and K. Lakshmanna, "Employing data mining on highly secured private clouds for implementing a security-asa-service framework," *Journal of Theoretical and Applied Information Technology*, vol. 59, no. 2, pp. 317–326, 2014.

[43] I. Chatterjee, "Artificial intelligence and patentability: review and discussions," *International Journal of Modern Research*, vol. 1, no. 1, pp. 15–21, 2021.

[44] V. K. Gupta, S. K. Shukla, and R. S. Rawat, "Crime tracking system and people's safety in India using machine learning approaches," *International Journal of Modern Research*, vol. 2, no. 1, pp. 1–7, 2022.

[45] T. Sharma, R. Nair, and S. Gomathi, "Breast cancer image classification using transfer learning and convolutional neural network," *International Journal of Modern Research*, vol. 2, no. 1, pp. 8–16, 2022.

[46] S. K. Shukla, V. K. Gupta, K. Joshi, A. Gupta, and M. K. Singh, "Self-aware execution environment model (SAE2) for the performance improvement of multicore systems," *International Journal of Modern Research*, vol. 2, no. 1, pp. 17–27, 2022.

[47] A. Juels and B. S. Kaliski, "Pors: proofs of retrievability for large files," in *Proceedings of the. 14th ACM Conf. Computer and Comm. Security (CCS'07)*, pp. 584–597, New York, NY, U.S.A, October 2007.

[48] C. Shao, Y. Yang, S. Juneja, and G. T. Seetharam, "IoT data visualization for business intelligence in corporate finance." *Information Processing and Management*, vol. 59, no. 1, 2022.

[49] G. Dhiman, K. K. Singh, M. Soni et al., "MOSOA: a new multi-objective seagull optimization algorithm," *Expert Systems with Applications*, vol. 167, Article ID 114150, 2021.

[50] G. T. Reddy, M. P. K. Reddy, K. Lakshmanna et al., "Analysis of dimensionality reduction techniques on big data," *IEEE Access*, vol. 8, Article ID 54776, 2020.

RETRACTED