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

An Efficient Integrity Verification based Multi-User Cloud Access Control Framework using Block Chain Technology on EHR Database

Keesara Sravanthi[1,3], P Chandra Sekhar[2]

Submitted: 22/10/2023 **Revised**: 15/12/2023 **Accepted**: 25/12/2023

Abstract: Most of the traditional block chain based medical applications are insecure and difficult to provide strong data integrity with variable size due to large number of transactions and data storage type. Conventional healthcare software often faces security risks due to their reliance on fixed variables. On the other hand, cloud storage solutions designed for medical use provide improved data protection and computational security through the use of blockchain-based data structures and advanced memory management. The challenge of ensuring data security intensifies as media files grow larger on both public and private cloud services. This complexity is further amplified by the variety of file formats and the multi-dimensional nature of the data. To address these challenges, a novel mathematical chaotic function based multi-client encryption and decryption model is proposed in order to improve traditional block-chain frameworks on large cloud electronic health record(HER) datasets. In this work, a hybrid dynamic-sized hash verification and encryption framework in a cloud environment to provide data security for large medical databases. The approach enhances security in a real-time cloud computing environment. Experimental results indicate that it outperforms traditional blockchain frameworks for medical data types.

Keywords: *cloud computing, block chain, electronic medical records, encryption.*

1. Introduction

Cloud computing is a technology that provides a shared pool of computing resources, including storage services, computing power and applications, accessible to users over the internet[1]. In the healthcare industry, cloud computing offers several benefits, such as rapid access to healthcare information, apps, and solutions for patients, doctors, healthcare workers, and administrators[1].By using cloud computing, hospitals and emergency care providers can minimize the initial investment and eliminate the expenses of data centers, equipment, and IT, which allows healthcare organizations to focus their resources on providing high-quality patient care and improving outcomes. The lack of interoperability among clinical decision support systems across various agencies stems from the diverse data standards used by different medical organizations[2-4]. Additionally, only a few individuals are qualified to handle medical records securely and safely. Except for instances where patients request to send or view their own medical records, the transmission and exchange of medical data outside a medical institution are generally not authorized. These factors make it extremely challenging to exchange and share medical data, thereby reducing its utility. The current medical data management system, which is primarily designed for medical organizations, offers no guarantees of ongoing accuracy or reliability of patient data. Risks such as data loss or hacking are inevitable, and the centralized storage of patient information in medical institutions exposes it to various vulnerabilities, including intentional tampering and unauthorized access[5-6].

Blockchain technology is increasingly recognized as a promising solution to these security challenges. It offers a distributed, irreversible database that is also cost-effective. This technology, which underpins cryptocurrencies like Bitcoin, provides a decentralized and secure method of data storage that is nearly impervious to fraud. Its application extends beyond the financial sector and holds significant potential for healthcare systems[7]. For example, Ethereum's blockchain technology can reduce costs while ensuring the security and accessibility of Electronic Medical Records (EMRs). Unlike public blockchains, access to healthcare-related blockchain can be restricted to authorized organizations, allowing for inspection and block validation. Authorized users can view their health data at will by setting up personal anonymous accounts.The use of blockchain technology enhances data transparency, enabling patients to manage their own data more effectively. However, the full potential of blockchain for managing patient data and healthcare services has not yet been realized, according to experts[8]. This research proposal aims to advance the development of new algorithms and blockchain-based homomorphic encryption techniques to improve the speed and security of health record data access. This approach not only reduces administrative burdens but also maintains the confidentiality of sensitive data when distributing EMRs on an open platform. Blockchain technology is gaining traction for a broader range of healthcare applications. It offers a decentralized system for health data exchange, ensuring data accuracy. Among its benefits, blockchain can reduce the complexities and costs associated with data reconciliation and provide quick access to real-time health applications and

[1]*Research Scholar, Department of Computer Science and Engineering, GITAM, Vizag, AP, India.*
[2]*Associate Professor, Department of Computer Science and Engineering, GITAM, Vizag, AP, India.*
[3]*Assistant Professor, Department of Information Technology, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad,India.*

services.It is crucial for the healthcare system to maintain and share health records responsibly. A loss of data integrity could have disastrous consequences, including patient fatalities, if the system is compromised. Similarly, a lack of security could jeopardize the confidentiality of health data in health monitoring systems.

2. Related Works

Han et.al [9] prooposed a novel hashing technique specifically designed for path data, which is resistant to one-way collisions. In addition to this, they also offered potential upgrades for well-known algorithms such as MD4, MD5, and SHA. Their work serves as a comprehensive guide to improving existing cryptographic methods.The team delved into various strategies for optimizing cloud storage, revealing multiple challenges tied to data storage and sharing. Their research is a valuable contribution to understanding the complexities of cloud storage systems and offers solutions to some of the most issues in the block chain area[10-13].Their proposed system is multifaceted, covering aspects like boundary oversight, data verification, and encryption. These operations are coordinated by a centralized management system, which aims to provide a secure and efficient environment for data storage and sharing[14]. The system is designed to offer multiple advantages, including data privacy and secure data sharing. Furthermore, each sensor in the system has its own designated private boundary and viewing area, adding an extra layer of security.The authors introduced ACO-IBE, a comprehensive framework that includes four key algorithmic phases: configuration, key creation, authentication, and decryption. Despite having robust and secure servers, they noted that cloud vulnerabilities could still be exploited by both internal and external threats. This poses risks to data access, integrity, and confidentiality.To address these challenges, they developed a dual-layer encryption strategy[15]. The data owner applies the first layer for initial protection, while the server applies the second layer to adapt to any policy changes. This two-layer approach is both reliable and effective, especially when there are significant policy updates. The strategy also includes a method for formulating new policies that takes into account essential elements, ensures information privacy, and assesses the likelihood of collusion[16-18].The researchers also focused on the importance of resource allocation in cloud computing. They emphasized that the success of cloud services is highly dependent on the type and amount of resources allocated to each host application. When resource allocation issues arise, it's crucial to identify both the assigned assets and available resources to resolve the problem effectively.They introduced the CP-ABE model to tackle the issue of information shielding in restricted cloud networks[19-21]. This model focuses on encrypted text and is associated with access control strategies like secret keys. Given the security vulnerabilities inherent in transferring files online, a versatile decryption approach is essential. Users ought to have the latitude to select from a range of decryption methods that align with their specific requirements. Access to sensitive data is limited to individuals possessing the requisite decryption expertise. This is facilitated by an intricate attribute-based encryption framework that uses a tiered architecture to methodically oversee the decryption steps. The chief aim of this approach is to guarantee the secure transmission of files, all while preserving operational flexibility and efficiency.In the model outlined in this research, those who own the data take a hands-on role in its governance and oversight. This is especially advantageous in a cloud environment, as it fosters secure data sharing through the implementation of protective measures for both unencrypted text and access control data. Comprehensive tests validate the robustness of this method, which maintains the integrity of CP-ABE's security features. Prior to secure cloud sharing, each attribute undergoes an assessment and is allocated a particular significance. The effectiveness of this method is attributed to its unique capabilities, which surpass those of other cloud-based data sharing solutions in both efficiency and performance[22-24].With the rising demand for cloud-based file sharing solutions, a variety of systems have been introduced by multiple service providers. To meet this need, a novel cloud-based file system known as CP-ABE-WP was conceived and amalgamated with ABE, culminating in the creation of the Secure File Sharing System (SSFS). An exhaustive analysis of this system led to the development of an advanced hashing technique that delivers superior performance. By leveraging multi-threading, this cutting-edge technique has been fine-tuned for multi-core processors, achieving a notable reduction in processing time and an increase in security.Although the CP-ABE model is more adaptable than other attribute-based encryption techniques, it has its limitations, such as low efficiency rates and lack of flexibility. Further research is needed to address these issues and make the model more applicable to business systems.Finally, the team suggested that blockchain-based systems could offer a solution to many of these challenges. Blockchain technology eliminates the possibility of system failure and provides a transparent transaction history. This could be particularly useful for enhancing security in Internet of Things (IoT) transactions. The researchers also proposed other cryptographic schemes, such as a ring signature scheme and a dual RSA algorithm, to further enhance cloud data security. Their experiments showed that these methods were effective and did not compromise the security of existing systems, making them suitable for practical implementation.

3.Proposed Model

The section proposes a novel data security framework based on a role-based access control technique that assigns user access control rights and roles based on the organizational business function, with the role serving as the link between the user and the access permissions. The framework is designed for the cloud block chain mechanism.

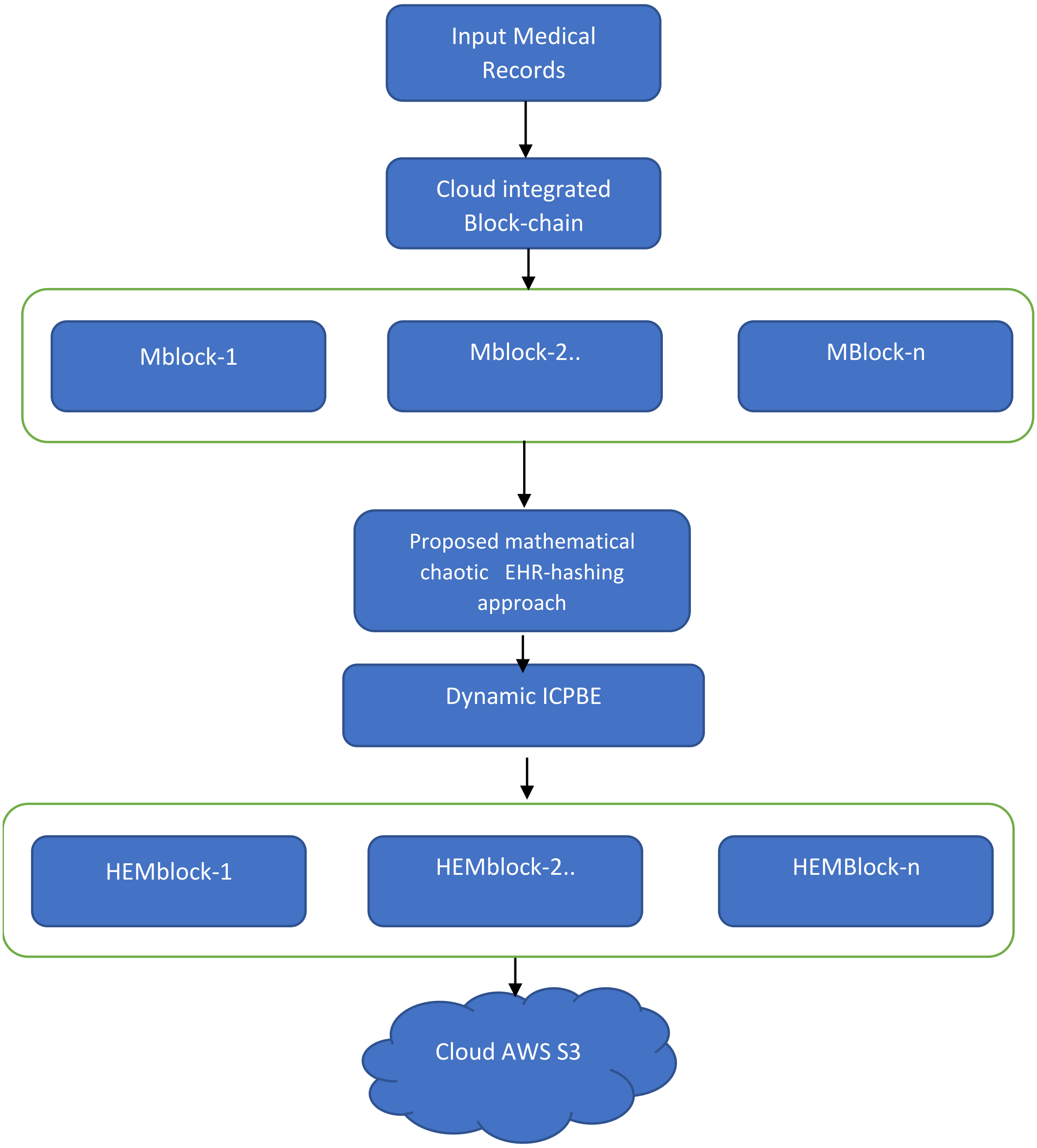

Figure 1: Proposed ICPABE model for cloud EHR databases.

In traditional cloud security models that use blockchain, standard integrity-checking algorithms like MD5, SHA, and Whirlpool are commonly employed to verify data integrity within the cloud. The suggested approach, however, leverages a unique, hybrid non-linear dynamic algorithm to enhance the variability of hash bits during blockchain construction. Medical data sets are processed in a way that each transaction is added to the blockchain to bolster its security. The hashing and encryption of these transactions are carried out through specialized security blocks, further strengthening the blockchain's security measures. This enhanced security is achieved by encoding both the current and previous block hash values, as shown in the figure 1. Decoding the encrypted text depends on meeting specific conditions that align with the access policy. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) can be seen as the counterpart to Key-Policy ABE (KP-ABE), and its flexibility is crucial in various systems. This allows users to choose either a single attribute or a combination of attributes from a given set. The Attribute-Based Encryption (ABE) model has been adapted to create a hierarchical encryption method, where the hierarchical structure serves as a holistic representation of the entire system.

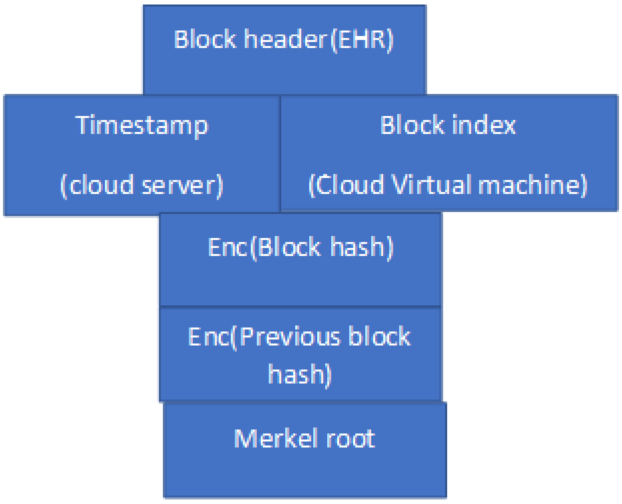

Figure 2: EHR Security Block

Blockchain technology serves as a decentralized, distributed ledger that captures and stores every transaction across a network of interconnected computers. This ledger is organized into a series of blocks, each holding multiple transactions. These blocks are sequentially linked via the cryptographic hash of the preceding block, forming a continuous chain. Each block features a block header, a compact section that holds essential metadata about the block. This metadata includes:

- The cryptographic hash of the previous block, ensuring the continuity of the chain.
- The Merkle Root, a condensed representation of all transactions within the block.
- A timestamp indicating when the block was created.
- A nonce, a numerical value used in the cryptographic mining process.
- The difficulty target, which sets the computational challenge for mining the block.
- The Merkle Root is generated through a Merkle Tree, a data structure that starts by hashing each transaction. Pairs of these hashes are then combined and hashed again. This process is repeated recursively until only a single hash remains, known as the Merkle Root as shown in figure 2. This unique hash serves as an efficient and secure way to verify the integrity of all transactions in the block.

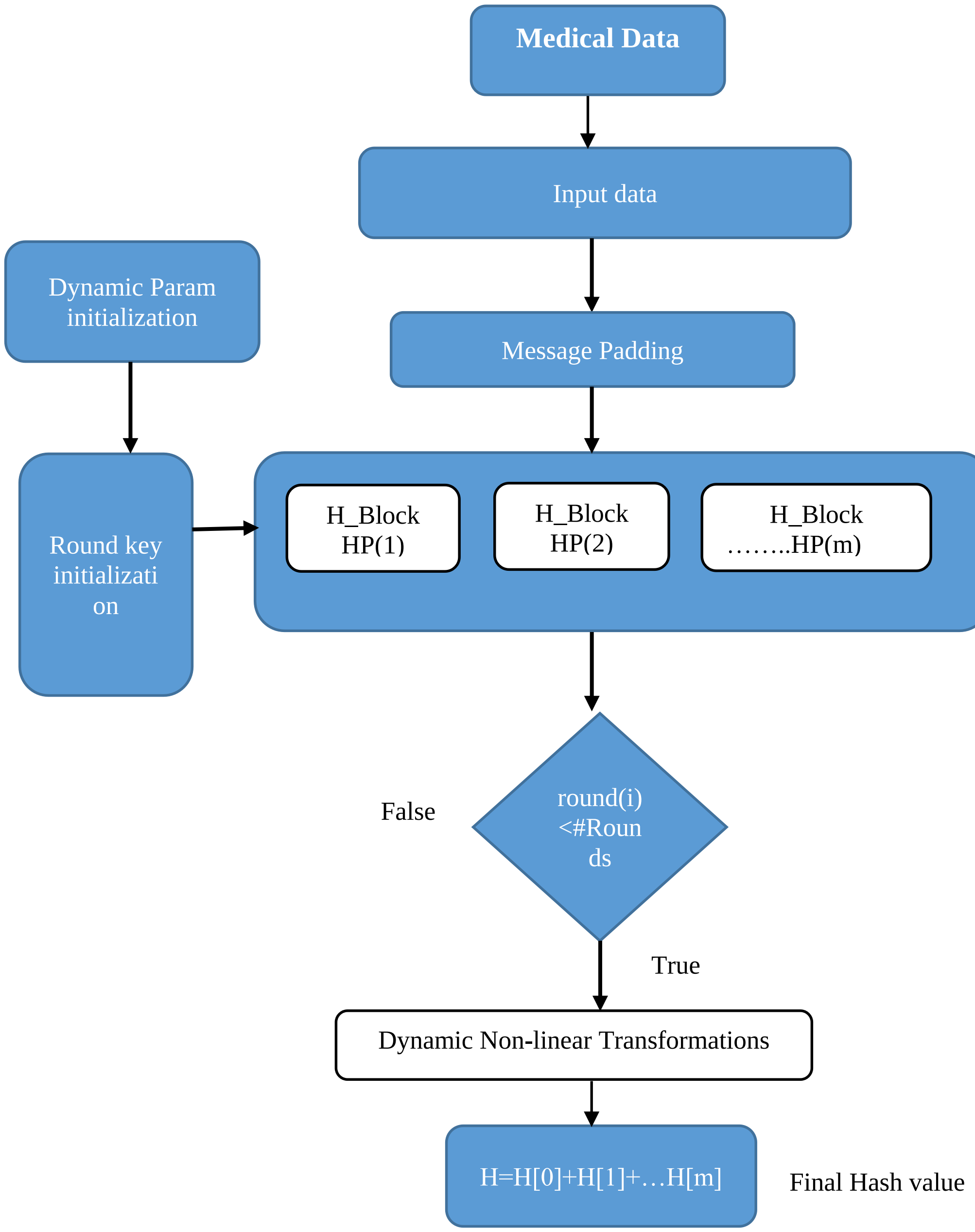

Figure 3: Proposed Dynamic Non-linear Polynomial transformation process

In this figure, a non-linear approach for integrity verification is formulated to calculate a distinct hash value essential for both the data encryption and decryption processes. This algorithm involves a series of non-linear mathematical transformations applied to the input data types to compute the hash value, as illustrated in Figure 3.

1. Initialize the cloud medical data and blockchain variables.
2. For each transaction in the cloud medical data, do the following:
3. Create a new block with a unique block ID and set the previous block ID to the hash value of the last block in the blockchain.
4. Set the block data to the current transaction data and the block timestamp to the current time.
5. Calculate the hash value of the block using a cryptographic hash function and store it in the block.
6. Add the block to the blockchain.
7. Partition the block data into k blocks of fixed size.
8. For each block in the k blocks, do the following:
9. Pad the block data if necessary to ensure that it has the fixed size.
10. Encrypt the block data using a symmetric encryption algorithm and a secret key.
11. Calculate the hash value of the encrypted block data using a cryptographic hash function and store it in the block.
12. Add the encrypted block data to the blockchain.
13. Repeat steps 2 to 4 for each transaction in the cloud medical data.
14. Securely backup the blockchain to prevent data loss or tampering.
15. **Process hash block**
16. For each input byte in SP[i]
17. Do

$$\text{Block Trans:=BT[]} = \left(\frac{[Q.SS(SK).|(SK)|]}{(\sum SK[i])}\right).\frac{e^{-|\sum SK-\mu|/rank(Q)}}{2.max\{eigens\}};$$

$$\mu = MeanBlock(SK[])$$

$$\dot{\eta} = det(\text{BT[]});$$

$$\lambda = maxrank(\text{BT[]});$$

$$gdf(\tau) = \frac{\lambda^{\alpha} x^{\alpha-1} e^{-\lambda\tau}}{\Gamma(\alpha)}, \quad for\, x, \alpha, \tau, x > 0$$

$$\phi 1 = SP[i];$$

$$\phi 2 = log\left(\frac{\lambda e^{-\lambda(\eta)}}{(1+e^{-\lambda})^2}\right).CauLB()$$

$$\phi 3 = max(gdf(\eta), gdf(\lambda))$$

$$H[i] = \phi 1 \hat{} \phi 2 \hat{} \phi 3$$

18. H=Hash[0]||Hash[1]…Hash[n].

Done.

Description : The process outlines a method for securely handling and storing medical data using blockchain technology. Initially, the system sets up the cloud-based medical data and blockchain variables. For each medical transaction or data entry, a new block is created in the blockchain. This block is given a unique ID and is linked to the previous block by its hash value. The block is then populated with the current medical transaction data and timestamped. After calculating a cryptographic hash for this block, it is added to the blockchain. The data within each block is then partitioned into smaller, fixed-size blocks. Each of these smaller blocks is padded to a fixed size if necessary and then encrypted using a symmetric encryption algorithm. A new cryptographic hash is calculated for this encrypted data, which is then also added to the blockchain. Advanced mathematical operations are performed for further data processing or enhanced security, although the specifics are complex. Finally, a hash value that represents the transformed data is calculated and stored. The entire procedure aims to provide a secure, efficient, and verifiable way to manage medical data.

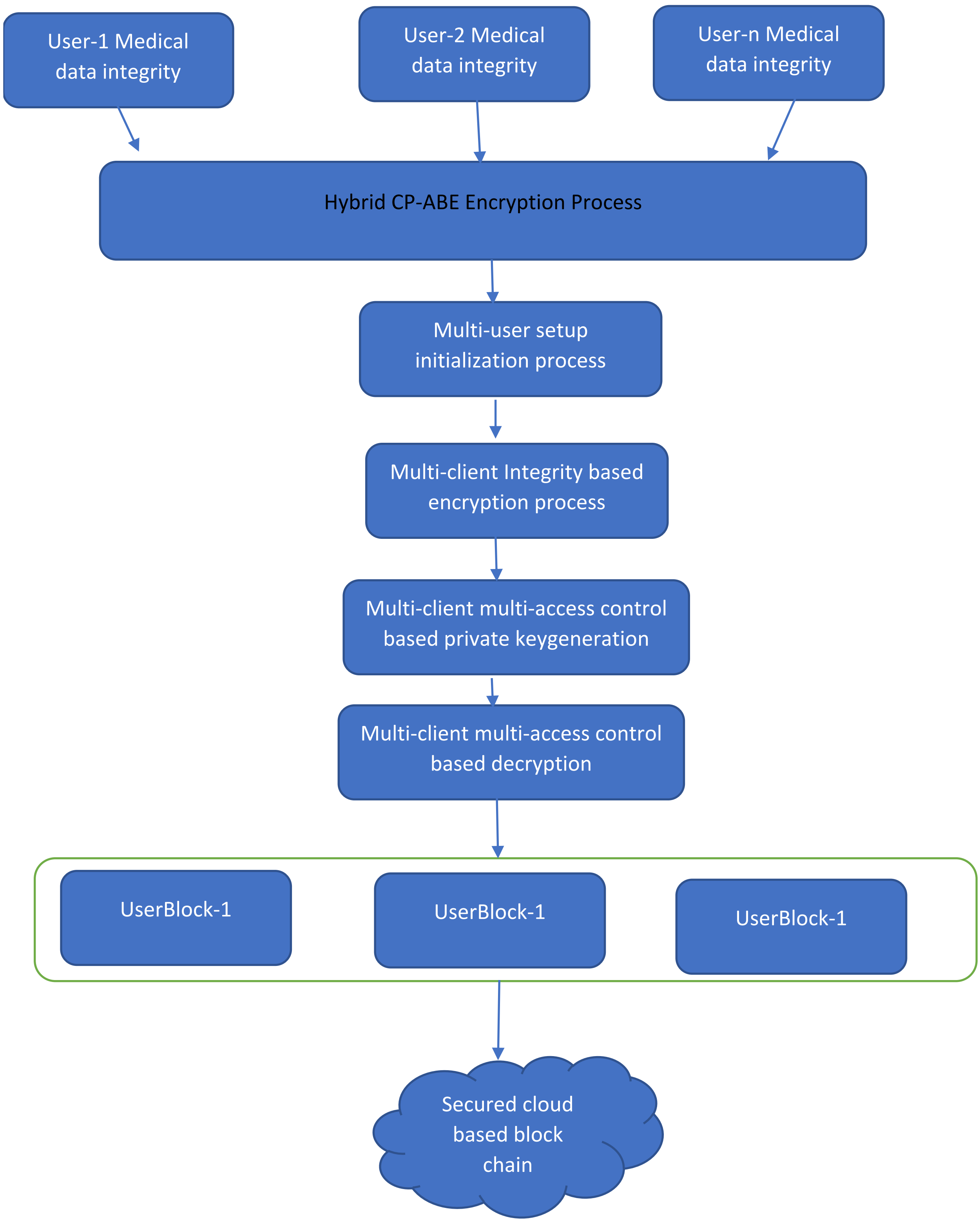

Figure 4: Dynamic integrity

This study presents a groundbreaking hybrid computational approach designed to strengthen cloud security by verifying the integrity of each user in a multi-cloud environment, with a particular focus on safeguarding healthcare data. As depicted in Figure 4, the framework utilizes a multi-user, non-linear encoding strategy that prioritizes data integrity. The model is structured into four distinct phases, each targeting the enhancement of data security through the use of blockchain encryption technologies. These phases include, multi-user access key initialization process, Multi-Access User EHR Data encryption phase, Multi-access secret key generation phase, Multi-Access user data decryption phase as shown in figure 4. Additionally, the model improves upon the conventional Ciphertext-Policy Attribute-Based Encryption (CP-ABE) by introducing a more sophisticated key generation and encoding process.

Phases:

A randomized hash key-based approach is employed in this step to construct the policies for the key generation process. the mathematical steps for the setup, key generation, encryption, and decryption of multi-client CP-ABE include:

Setup:

Select a security parameter and randomly generate a pairing-friendly elliptic curve group G.

Select a random generator g in G.

Select a random number x and compute g^x. This is the master public key (MPK).

Select a random number y and compute g^y. This is the master secret key (MSK).

Key Generation:

Select a set of attributes A for the user.

Select a random number z and compute g^z. This is the user's public key (UPK).

Compute (g^x)^z * (g^y)^(Hash(A)) as the user's secret key (USK).

Let H_Attlist is the 512 value of user's integrity(MD5).
G1, G2 are the cyclic groups .A set of random generators from cyclic groups are r, g_r, g_p, r_j.

Gaussian_distribution=GD(d)
SK.Dj = {g_r.mul(H_Attlist)*GD(d)};
$SK.Dj^*$ = PK.gp.powZn(r_j);
BlockSkey = {BC(g_r), SK.attr, Attlist, SK.Dj, $SK.Dj^*$, H_Attlist}

Encryption:

Select a set of attributes A required to decrypt the message.

Select a random number r and compute g^r. This is the encryption key.

Encrypt the message m with the encryption key and the set of attributes A. The ciphertext is represented as (g^r, m*(g^r)^(Hash(A))).

Decryption:

Compute (g^r)^(Hash(A)) with the user's secret key.

Divide the ciphertext by the computed value to obtain the original message.

Note: Hash(A) represents the hash value of the set of attributes A, and "^" represents exponentiation.

These steps provide a general overview of the mathematical operations involved in multi-client CP-ABE. The actual implementation and details may vary depending on the specific scheme used.

4. Experimental results

The study conducted experimental evaluations on a real-time cloud server with a Java environment. A blockchain architecture was deployed on an Amazon AWS server, specifically for handling medical data. To bolster security and data integrity, we incorporated third-party libraries such as Apache Math, JAMA, Java Pairing, and AWS JDK. The system's performance was evaluated based on several metrics, including changes in medical hash bits, the time required for encryption and decryption (measured in milliseconds), and the time taken for cloud-based encryption. The hash bit change metric specifically gauges the impact on integrity bits when there are alterations to the input data bits. The test results were generated by comparing the proposed encryption framework with traditional integrity algorithms.

Table 1: Secret key of proposed model

```
"ðû©_XM1¸¦µ«UOéÈüq
qW6òf'ò*S
€a9436f3c9eff7e0d8aab462822b50ed78f1619d8841
c3ea5060d0fcf2bc83c20c5cfd750e075118fccc1266
ae945b4917027280033233dba7bb13ebb948fd0a1E
€U$8BÖÌíâ
+Ì^ÓœÛ-ÂC!†)ëT‹Ð¢=Þ,Í*þ÷«¦°Â/1Út°â-á¢}dã/2ù
ÿ¡³>æM-
fx'P‵ DÂŽù$æ-′^Æ½ýQâµ•ñw¢>4Ÿv³œàÈßÂ‶Ž3Ü~&:÷+
è
ÝÞqwE   €cC\ÈR
pz_P•bï®ßµ-ù_†`zô-KÓÈŒ÷•¿YHþ«l3Ðo„"ýU
       ðå
‰h¦úLÿí``´àA¼Pì8ù²ák\»W°§®dàž+fú•˜‰ãý¹!S2ýRÌ
¤M¢ž   )ßRÅ{šî‡†Kù•                    åñ`•Ý¬vS
€83517460c323f8f0aa4c87897676909694dea0dad0c
a4a3fabb81dc1b362b16501b5757b8104970b667fea1
74f63a074dc9ee29a6409614e4bbfec1b9a04a994E
€U$8BÖÌíâ
+Ì^ÓœÛ-ÂC!†)ëT‹Ð¢=Þ,Í*þ÷«¦°Â/1Út°â-á¢}dã/2ù
```

ÿ¡³>æM–
fx'P' DÂŽù$æ-’^Æ½ýQâµ•ñw¢>4Ÿv³œàÈßÂ"Ž3Ü~&:÷+
è
ÝÞqwE € +ÏÉFDÁs®5;ö-Z™Ô¯ym"UÁ,®„•-
ó¾"St¤q€u•Ö--0Rw1ùfd}Ë~\%ýûÛ»_åšÃ•ó´ìtù-ðÂ
rÏ.Ž¶® ß*GTIã£hy-•Šñ
ãa £îÊú¯ªƒ³éÆ~M€yFõS
€1c63c887e42912342dca20eed9624531d7c1ad13fe7
90e57c377596ba2d7b2378797f589e93c109498e9dd0
8d48d52565310a5ca21ed4e3fe5843813c9c799e9E
€U$8BÖÌíâ
+Ì^ÓœÛ-ÂC!†)ëT‹Ð¢=Þ,Í*þ÷«¦°Â/1Út°â-á¢}dã/2ù
ÿ¡³>æM–
fx'P' DÂŽù$æ-’^Æ½ýQâµ•ñw¢>4Ÿv³œàÈßÂ"Ž3Ü~&:÷+
è
ÝÞqwE
€Ÿþ+¢ïtÍÅÞ¥-ŠÎPø´§Ö¥?m"G˜øf}nàYéSŽDÕ¶Døx-
#¶Ò`ž9:b0-B±Mõb›•SrÕk`[Î«6y,kÔÊÔ¸žA>•cùx25Š
"ÕÄÎ’²hÛ)\2O•ÓÂ•)í÷†ï„!£
'ÂŸŠÅÞ½
S
€d439c95ae403bc8ec9df01e50b2ad2bfb51c4b68409
8012193b32e31b286201fb60dcf2893ac67892b9173b
1520be747960fbd1e7481678a40a6c6b336cbb2acE
€U$8BÖÌíâ
+Ì^ÓœÛ-ÂC!†)ëT‹Ð¢=Þ,Í*þ÷«¦°Â/1Út°â-á¢}dã/2ù
ÿ¡³>æM–
fx'P' DÂŽù$æ-’^Æ½ýQâµ•ñw¢>4Ÿv³œàÈßÂ"Ž3Ü~&:÷+
è
ÝÞqwE €s¦¨ ´á)R¼…èËA(¿‡A
âS¹ÚRì¡h³Lšvr
Ü†{m}€%¥¢¦ŸÄø3'³-
1@°h¸ÒØà;®žÓ)Ã*ï•â¾¹@_•Ô÷»ŠÅXÃAÈnZfqd{öO†´¢²
MÖæf-my>?UÒ9Ž‡#10Ãò

Table 1 outlines the secret key value generated during the encryption process for the input data. This key is formulated using both the integrity and the attribute space.

Table 2: MasterKey generation in the encryption process

2)• ‹TU±×vADÁ¦'<Q• "$X+¤ ÑÞ• HÀ¥ÐÆ²0.1+ÐüÎ¶JÄÇm
PïÎ?9Î#?3Š#E €p(ðjiT8u±TBg+ÔA• P¼v{
çè«"• TLv• §?t–@fü8-úM;KÕ¬Ì°«õprpò]‹ÑÐž×^
6Ûeôç¹'tKz¹K¨•• 2(o„‹WÎž¨UrØNa®É+hkÊ",–
×©Ê±»Âq¼ç‰• ™¾Yí- JE €[û‰\ozç¢–
¦ìÎïÄ£¤ªX$Oö• 4G)z 6Œ8°B]æ°Ä ïÛ6òvÛ‡yÎâîÑ• ÁI+(
• Mï¹Ê±€ðUÚ0¦£%D,# Ú„©Ÿ:j¯¤• G~¡ÀbõDE‡ÔI4'þE
€-"µ÷þa±œˆ,Z4ªÿžÕ¹Œ@É6ž.ˆtôáj™{òBðdþ€|MŸàÎ=•sÿy_Åùèü
F:4Î7Û½}‰ýWŽ3bžªT)à=ìÄ®âmÌ)ÙŸO¸ƒÕA?• ¬Ý›0@Ex…h
Bœ„yb˜¸¦d é¶÷»òÙà¸°÷ =VE
€{5{q}t8»L7±g˜úr´`eÔÄ@ÀWZÉŒ,Í§-
„à\bÏ¹"ŽÂá±¯â€P™§AØz–ñ&I"• …H€
8ˆ-Ô2áÚ|
Ûdiå†ÜhªŸžÒßûz,Äï£×¤7UñoOþÉš©½&l€¬d%cìüÅ,5¶ü´…"Ù';
E €U-• ¹|° šµË^ßv4Ù00>…Î¡0ºf¤-?®[æÎ‹(_(l-
ñ$×Àº0Q 3¾qÇKÓ+t• §€q‡V|ˆ.¯á cYPÕÁ¾
ÏÐy1—^Èì<}<¢wU.4¯Hve½eÐúØÉí~ÕÖh—}@Y·¹Úîúç°• Ñ•E
Éù7Z¢0ˆ¾c)Ëù ó¿*ói
• ìœNïÕ}|Ô_ä¶÷Éº7•€SÊ>…í«öx4Ñ• è`ýnùÞŸý:
¶ë¬£• Uq‰8é>îõÂ_~TfZÃõP8ÄŠDû·r• šëbØ.vîm¤oÙ-• ß7`U
=È¶ðsÄE €*{Ìòå• Þ Œ™Â|ˆR¦!ñdÔ›1ënø÷OÐýšœ- y^u¹a€-
R‰3«[œØ‹½:•}E˜±ÃÂCw¹"³J&é¦´Iºô• äÁ5ÏysÿT ãÿ¦ ÅÞUs³ò -=
KÐ• À€·ˆ,j¶‰0çMÐX²7g [–ÝE
€iyl•xÿûª{-zS• ûÉfzÏ• ÷·l'• ^7 Â¦ºxè2Ø-0Ëž,œdù,&• eâ-
0éþÖ#O§Ã|+À1lo]ÂaÑðgà U%]]%à,¼œ-6

Table 2 outlines the generation of the master key during the setup stage of the suggested encryption framework. This key is constructed by combining the integrity, policy space, and attribute space as part of the encryption procedure.

Table 3: Public Key:

Eò;.)Y¾V• Øvzý'Ãöèœõ>¿oí11 àvð• Ë*aÑ"üœÚ',Š^ýÍ4.ZÀø-^
'$Þ• E j0rÆt'þ§¾þ¨,´¢ôåE €¡Î[¾J4 ³–Lì"Ïã`• õÃçw³
ÖãëDÞhnÝN¤º…´ bšÑ:,…jÑŠÿÙË• +Oé?ÊÀæig3>¢™
ðÍÖ\¶R{·• ³¤„D[: §êFM >v
.•|ô%xzö•‡ê¿í³'öÊˆÂƒbÝìƒÖ)E HjgBšp-žÔ¶ÿä€ ¼1 E €X
1šÚ}ÆêÏ4ÀDÍ
KÖLØŽy!'Ð<HfÔiÝ}l6€ËWþûmÇÞgûAÉÖ¸»Þ÷¼ðÙÊ:„fjA£`z
®ƒ FŒFõÒgê?íÆ-«ÄË¾Û• âÖcéE_WúZË—ªý£-@Š¹–E „JØ
– óó\«A ITN®Aa‹E €báŠY™
àV
(O±Û#'lsÝH|ã½Ë¡ÆË2M*·
#u¤Ëw%Üi¶é€Óø"ÂÝ«òG,J0V å,-
xc˜w½È4ŒêDÌßìì|«ömH›½º iO¬‰´&Ó¸
4½ß¿Ø‡PóOª«ÕÖœ»r&E Åñ2 Ï¯• ªE aqwÏlÝUE
€RåNíu>@Ç}ƒû ´¸¡zàü—-Y• ù"°*é• ƒ²ÚoÍÒ•
/4• `}• Þiÿ#u§º„4L§My°A´.I-hÍí„™…§Ö7@-
Åw˜IÀ"#, ®T"˜pšã,øt¼µ"À• uá‰tñ»Ã@Ê¿Ü»
Ô»x$ÆÀ_ÉLÏùƒE !Nƒ•k4LÌ³¾• Ý…kŽycè-ÿE €• â—
zñ• 9Yö'#9Sð¾NFòù6.W
œyæ‰‰éÂ]PœM¸bµâeˆO4öþÜ?l ^úH ‹yAÔr'?^¢Š@|—
¥ôŸ8ÓõÎhqu0Y§Ëv¥r|Jq«Ä[ú†Ü©`ÿL¥?¸
¿ªÌãCÓ&A]ÜRHN²‰vêN3E ôSfP&ê'»‹åê†=yÀP
E €UižÒWgE^[\{¨l"¨Kêôñ‡aAx%™¬(ŽØ/ ,mô¬ˆ®òï€¹
¡ªaES3e™š5wº2p1«>ŠË ‰`¼NleÅd)œ¤°
ì»<¬• Ô}L_º¦• ¬çÂð%• ,A }üa¬9³3‰êã,Û°šE
U• Ì¼20\>>oÓ!KT"§‰E €
5_Ÿ'SÂÒþ2Þœ†±Ès†0ƒEŸ´Å/Yˆœ'·Ö&a\ìS¡
°
Yûbmg4Ò×\$• îW@›åšE>¸Ô+x¼Ha¤Xïúý]2~É¨o/×Ñ?ý,Æ°ŽÃY
ùa3Q"˜Çf6½Ù€Sñ}Âºá.†‹b• u"¿¡E A-³åbŸ±… iø^Ë?ä™• ©E
€œŸÜT95aH,Ì¶Ðh—
¯ø…)ï£,LeÌ[$øK±•¬Æ÷±4-‹þöçK{• ªÐÎº,• 4$ÂÆSÆ("²• c'/*9S
~žhuû¸žàª•Q$á7ðÙÝa»…gÈîEš÷Ê? ßØ°šùþ
ˆÎßgªQƒ‹ºÅmkE j˜ºâ&'ÖÄbw3²NN'• E €,¾ñºh®• -
!A‡'Š®×• C~Ê~#¢Þí«2Ý`²öz™å³• ÈÇ?q%PIà ËÙt…ì6pÖ×¹Ë]

Ÿ‹é(îS?Q³CofD^øjHÔ8ù„“™ó'V7Öy€°ô7tÅ3|ÜƒÎ¤Vf• .¿éK%Žô
¡K¾ÑÍ'T\E =UøÙ½¡7}-êª'æ,ÍAï:'¹E €põ„Oœ ò• 'W‰7{6
ù¹B\¹ÈÂø¿ÐZ•
,:õÅT¬®ühƒp+FßQtT¯†ÃÉÎÇ%¤¬Ìm=j*o`ƒ————————
D;'F³X¬üî————————————————————
tí• |¹ôºïÏ÷çO6ù…Ï@£®• |ìÝâ<½kî'CH¿JÂ½Š ±o©é†c™————
ÿ¬œ¯E ¦Ù-þÖ3ªT˜o\%¡k¶E €3®R Ý‡g—
ë»IðÂP·Ë¨ªO´XÇ¨10NœŸ©ïM®Þlu'GÂ»ŽÍEAÆÿru——————
ã5ÒÔ· ìIã`:d#Ý_,Å™ Ð——————————————————
µ³!3,„˜'dKÔGv#ýÖÑ^zçœ2|oØ ðxÍ‡#J_éÞ• .YHü_• ®kêâ%TÎê
éKD»J_E +içÎº"0öÖL&A}¹ÎÈr©E €7'Z?®@ E9kŸ.×{Ýáy2¬
¤BÔVÝ¦òa• Ì,‡Ê
?ÇÖÜ4¼†Úš_É1
• 5 c¤èoL£{Ï4MèÁ]A°XZ×3>ìÐùÓt"• oó• É-üÃ«ÈrC
ˆÿ©ì¿pVäÕ3IòrneŸ¦ÐÊ`×Ì
Ç-à·• E }——————————————————~• ¡)—
¿ƒcÞ´J¢Êh/
E €½&âéÅ½‹¹?BºÜ`×gVMš|_ü™®ºö• æ3n8OV‰œu:%+ –
É¹ iüL9i »———————————————————————
¨ù§' Ì¤$M`ºr úèŽ¶?æèš+96/s,rïöXbË• ZÜ• ¸•)Ö¾Ùg‹¦~h@å
‹`þó˜Ýö—èöE].Œ´Ú9Ú•=•í-¦š———————————
zé³‰lE €s30˜–å§I(©v™q~ŸTt+?µúNqÿsá#Üú2ÞâCÆ¼ûç———
‹rŸX~€CI\Em+ oÚp'MS‹¹Ïzå×²&˜z~KT-
£ØQqm€Ü‰[G¿,ž,ò½XEuHCÚã3·IW§4 –;Ø![• SÓË~ã£2E }Ü
`VMõƒîá¬E
€‰¯ÙÖsäa"`å"ø¬ÿÍjÂøñÂZÎjÀ;Õ,{ñC,• &5hà^*À¶÷-
ß6• ýµ·²>(ñ ¦®MW³.OÐ
yÍröÏ§ÀEAb\ÿè¤ÛQ/?µT¢)˜ï±çÑDq;ú[]?¼• -
:/`\$%½œŽoÑ`¨W-K_E ‹J‹yh'ãpö"Dk,þÖîèE
€EgŽ0÷E¼ð'JÉ• «ñ• ÁEXðË÷È/"Açäë'“-(Å¥—»ï–
ÇuwqX!Q¥&Ïƒ\áÓÄ-€;îU‰¤Lâ¦• Óë• fzm'©A———————
o¾V@ý… ×xù^Xï¡`ç) • [ûi©O½ëÎòB ƒS+Øë>Übã™)wGHE
C¡Š½ûMü ýkVgjÍ —a• ÂE €XxRs'Åw¬ Ò˜sB,ˆÕ¶`†• $J«N]ë
dÎ ˆ“Ú¬CØ3ˆÐÌþÎv|:,´ë¦Wœ_yv#ö/¾s• ?Û‡Î` Ñ~h=,ì˜û—
2çíÊÑ/~wÚ,ÛëïÅn
«ÿHØ«uqˆ#4_bj(€Š——————————————›ÑëiD
Yä6E ^ +'½cóÚºI®[‹Ò "E €#cJd$A-• Q…• `"Üu³Ú
ÿþñ[%-›#Á‹½ Ü^¡öäÅhn ————————————
&Ž• å™Ö_X¬z™D¶\nÈC1Kê¢ñw4GùoQÐ» c°ŸÐÇÁëÓv7Š.‹
OÕ"wÂÛ%
û———————————————6×Ë• 5—
ÑÁ\æâVà • Þ7Æ€K<¤;E]$õ¨õŽRežsã³1¼…_ÀE €-
5vxåJšÎõ˜>ð8¼‰~Ø¹ÐÞŸË>¹õdóÀB,„—âP~tQEôájøm‰´• £•íBÎ
W¬;X©ŽÌ#h´õéº/ëko•<Pï§"–ÊøºQë#ŽÑža ÒÃhÈ}jE
{ºC?ÕÖì±Ë³~ù« ï ØHu0E €šêYÕ±P——————————
$–I/ßêðpT—————————————————2ÁEä Å¥U
• ž
?„,ö‡IÁán}2×ÔU|$7»• Ð• çé9á³á™Ð=l·IÛ;R`+Éi——————
o§¤º-Ýdú«}Øea€Arh—)äA• Èq6‡tz}ªŒ uhœÆ>ž¾±0AÑö†7"E
%//T|¶m >¹Ø~D×¶Ê ÕE
€¢Ÿ²¯"š:C• ¶ Ó]• (ôsçxXHçTv›À˜ÓþÞÂCÁ_• ™,"ŸGzÆq• {þ
¯-M³M„¦ÁÜ+k–Wj€Ê -·ñ*———————————————
Ðü *bÍU¶
QÕLan-º¸F"‹NáÍ´½V/–Z¿I*„#yD.ÍXkNª¡E
heBŸ~¬ŠvŒâùrˆàNoÑüsE €\S———————————————
í#fK-é#øÎ…€ µ£Z8ËÿXÆ¥¶·'/H8"wü¾ââIr4g3¢ÁJ÷•
¨^E¥·1|7¶\NñƒY\Â/Àæ+1t°4{×2vugòÜx •Í——————
X¶¢Þ¾bÈë²ß!-òšãG³
S &- `®-,®E X
Z™¯ÏlÀ¸h"ùb™¯ÄÜZ¯E €€XK>«;ñ«Fÿ Í?¾“ÄK• <™µ
ú,ªJ————————————————————————
úÉîëšœþ×ær*tòK~KFëG•©Ô'›RÞÔM‰¶ØÙ
[ŸCöÐÞ`Ñ¢¯X/p—
{ÝÈ¯K7• @ýG™»‡îÐ• ³ògÊzž˜?œÿbFàƒIìëlï âK3wQ&tDLºE
+ÿMãÓ{|ÜáÖÉ«•RÁPƒE €X*U$\———————————————
+„È¿ôáTT-
ÚŒuPªÃN‰¿zÛ6e/ÖÜÛop½ÔÈ~'\ZLJ¬ì6µNÎU‹JÄdzûùåBJˆ|ó,
Ö‰Ùwø" ã"ŒË–Ð¸`·Ã¼¡ü0Jê®• |}ÔØJüœåBÒ,6÷°Gk¦ÅL¡Ä#
ñKw;„gæ¥WE
hâlž{®Lõ·Œ• ———————————————————3;ƒ¬E
€oê
H‰yJµGeöÆz&• Q‹múdOEzÞ¥Ø

Table 3 provides information on the public key value associated with the input data, generated during the encryption process within a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) framework. In CP-ABE, the public key is crucial for enabling secure, policy-based access to encrypted data. This public key is typically generated based on a set of attributes and policies, ensuring that only authorized users who satisfy these conditions can decrypt the data.

Table 4: Sample Encrypted Data for the medical data in block chain framework

%-©òØÅRÿC>«§ÌeSŠ<\,ü§"• {ÌeÔv k• î&oª±œ@Çvpë+Xåp¼
²Çvpë+Xåp¼óØ*û}zÇvpë+Xåp¼óØ*û}zÇvpë+Xåp¼óØ*û}zàÝ
%¹—…";ªÁÁœoS«Mšµv^nŒ¡Ûi'™• |ËR°Të¬êel#ÌàÏVY;š
8E,ÃñäË«ÀºöuèˌF=ícâî]3–XÀ"ôC• »%œÑuP@sq¦"!
ë'í),/Ãàˆ¹ñb“)7CØ‰ ë
OŒ£NØé¡´‹p@-(Ü-¨çî±[<———————————————
——————————————————————————
:g• • •
ó——————————————————*€Oé_ ‰ÿõªÅ
õâ`ìkÃË)¨-f`¾jzt€Ñ)Ç| ¦|MLF————————————
éIséÑøÀ¼nêø½ó?Àp\D,————————————————
b"á• J?Ð³f9Ç'4
‡ÚÂJÞ}§—î¡/o¬…sU:Æ=;Gº(¥'Y;KWmr_¹$ ·ÒQiU%¯€ZEÇá‹
ëÃd=4' ò7v×ààÉ¤~f8f1——————————————————íô
ê‰ÕQ¤Ë+â>Œ1
äïë{_¼ëÓò‰I¼Øn\ÕQnŠ• ´‹— @äˆûF«• Ÿa——————
ÆùVÒï<.Ú ê1êµÖåPþ}ŽÑãuëˆ™«Ú÷]Œ¼————————————
ã·³p.V———————————————————————
© ìòê=$ääB6Á©®"æÎ;• >• 'Bkx‡SF _;ÊbíŽkù4jÓ
8dŽ—¾C8• <G/—ðF¼æF×———————————————
"Öx>m¤çLûœ—âÜkB…ÿ]Ü• Ÿï——————————————
ÛúDÁ
/g_E@˜ã›Y6¼!)"èw§€þFt• ®w
¶k¥Æèômh°…¨•Xß7\¢ûY^K'®¬„ÁþEóÁK¿,Þàšv^®_H¼ö4RHöc
——————————————
-Å»¹Õ¾Yo'úqð0ÀÃOá¢qå,ïCº¬OvãEÃÜOª4§}-Sg)®ï————
´n.%r—D=upGPqŸÒ‰>ò
'Ì2u:º• fê$`©o,ÏÖ
)<ÛÔkÃ$¸T#¸vòº!t&• ì
GTWa_ê[!šfÉ¯"Õ)«‹¾Åê½UÀ™—
¼^"nïïº[Ó|o,^Oi."0¶r/XÐWÜr¬|–
ÑŸ`çÊã¤i£è§r^ïSçòxTó+´• aƒ'%•
h-Gµž¹Cö°%b%?Æïhè<™æÏEÅãTßèÁ7…•*Y• ÌA9ÁŒ'Í;óÁ»"Ì
õ&"'ŒñtÎè1• š@Qh§¤z@ÌÝdA'ºÿÐ"µ×Á$©ûÂ9ÒÐ'Â^´â€
Çýâ¶,,;5Òµ
¹ôç?ç• Ÿ¡¯P• ñ†@nnØÄšâzB"• /ð—Ô!°àQÖ#šý‡tX~• †J————
"5 ÿ• Àw1o8lªˆ ¾·• PRË™¶=EÝIq˜•PgÞçÈRE¤Æ("lŠ• –
ÍAž_¬KðAª@Qs˜÷0c@…fS%mZÜ×Ý]-Ô‹gKy• '¤¶#ó+²r×/\ B
ñâáZ¥I[ÓJª£M%Ü• ŒïýÐ¶'

§,fáúaŒ^KŸôìb-°A]†R• E/• “Õ àíÉ————————————
¸ëmªÇz\›ó‘—————————————————————————
kÒiU
û®±»âGkk‰Å›•B¦*ÁïLO~ö¾--ÅÅJ3fBåež*¦^Á¬ÉLiÖÇø©»Âö
Ÿ
A»œµÿjÍŽ×F -
-¡y‘ñ Ð.éBÀ_å• ¶´¼}+s‹¾£`§
ŽþÀÉÔê¼ØNÊ,k€¸½QÁ}y”#TTpcç ²4Õ–·ˆôÚþC.wÚ›ÖHˆ• V\Ž
:Ü£Íg´ô‰~.,úôXÏ“V·ãë,¦?>†˜}†ÛV©‹•~BØqÝ†IW‰Õçdº•“Í¹{`l
u:D”šˆªñÞd|-/• ívr³ê´‘šD^• ¨¤sÂ4–èŸQÄ6Úk”÷Ëfº-
KJèÊËcG4X¢@`ç÷2~¢Òu zZ'‡ùƒGÎ;þ—
.»Õ%w:,ÑçÍÓž-• Èm-_ÝH?‰1• ¨œ<• ‘Ø ¤3}RºÛÓ\´j“Ž¬ƒ2r——
:î`Ýd/ï6]¶&ÁCÞ¾§Î:R'Ð9Ÿd«êB`%„üÍ
W·gP¯O`RÊ T”
*óø;v?zHN@xj–
zzNÌôüß————————————————————'ÿ†–
Z~EƒËWtÿð¾ÔúÙ¾BñÜ½C¹_Ô¶<ÀHÍúú• ,ÿûƒ»ºÎ˜}^±3‡(Ðžh
ÕQþÎÈåSÃóVº ´”€ž-…¸9¶zèt¢+Ì+• ŒÎÂ‰UÄé1Büm§#Y4<ð•
dÿ,u-šÏŽÄ&€:]Có• u@hB¡îpQ¤» *L—Æ9õº±-™ÌE£ÚwÁ
“øLç1GL£PÝ±þ’…ßõ»ðG¥¯ÃÎ¼àK|E• E³<k• ¯óDç-²Ç¶ÁÆèH7
P\a¤ž½N@• ³ÀRQ¨¹«\<ZŒ
õ°þÎ.©þòÕAG³”tO—Eè@@ÚœÄO-íŠÍþú‡âNBrn&2en—Ø,ƒkí –
Sš=ØuÁDì«E=iÉÂ°4·£ÏçäÀ• «¸[–Í• u• …–[E=ä²€,i f
H÷_èèÛz"t¯-T-¤/rsöŠ<ÏÕ9ÔúKˆõVÅ>¹5Pá4K8-
z)îó(îÄ5æì¹a×=Ï×HÚåRîEq ²‰ÉûV‹ž[\þ'v¡RhéÓS~E’ÿ$¤Šƒ}
Ì!ÁGÿ´ç©ÖoÄ»VnŒÒXD8Ø²ýÎÁî¼Ô[®• ‘¡îQnô———————————
n+mv°+’é¦löD©ÆT• • Õ,‹¸XŒ#QF}Í-je›À£¨——————————
j¶ü§^¹%R|øéÂŒ—|Å.†öm¥ucî å Îp<·———————————————
¼Ð¢Â9p————————————————————_xñØ• • -
Q†‡Àê5ñt¾›³ƒê7KDu×0o/hÿ>¤p*Ã¹˜ª@þœYNžð#—
åX:>uè‘ÁÎÉ”šËå„à³«RkóZÑ'Å½:›:©çyícyO,§Áñ_oÕWúO_)ŽêL
A /£B¢;(j5ˆB%¶ÊÈúˆùZ‡!—• 9|´ûrR<-s
nr¦ã¥˜@µMÓÖ/,Zj·
UÐ-=!Ð7RGLpß}‡ÞkCo6%#Õ{°gS¨Ä„ƒ———————————
O…——————————————————Ï‹×zžýë¯:ŸöÚÕÚ1¾
xÈ¹ÿ^dxH'ë¡hºµ³LÕI-{ÁçÌÄ'Å³9{P q«ï\Ž¿à

Ù‡A‘O†1KA–€ÝÛåths˜
UÈµPŒÆYci6Iˆ À †NpX·îÊsy-Ÿ¡îëê¨¦+.*žbu!4H‡lSSÝ

Table 5: Sample medical record integrity value using non-linear chaotic model

43kdf6f0e3c484845873da6ed4c3f30822ee90d9f0ff42252b11f16275e0965e2845f055b4da97f2d1f0a7774cf28bb4770043515cd6a91a0e1b5597782a26e9259732e2e1c7b81f5299904e418b8d707ece5b18393e4c2b155d9220c5a4c1ea64346dedc247900d8f22dfc5b9051edff241f2319322a76aaff7a0fe7405b6eb568280a7d9220c5a4c1ea64346dedc247900d8f22dfc5b9051edff241f2319322a76aaff7a0fe7405b6eb568280a79326caffcb8727487f9a671c8843a29727c113d37ffe8bb738c222c2f93ba48e22f6bae97584c85139ff6c482aa62be9cda2c8a8fa65749ec49893a6440df99d1bf8081b19d5f23233bff2b340de98669h7h

Table 5, describes the integrity value of the proposed model on sample input EHR record.

Figure 5: Performance evaluation of average hash bit variation of proposed blockchain security framework with existing models using 2048 hash bit.

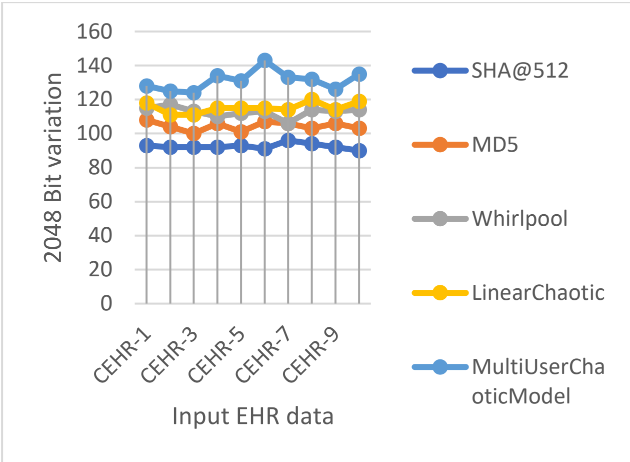

Figure 6: Performance evaluation of average hash bit variation of proposed blockchain security framework with existing models using 4096 hash bit.

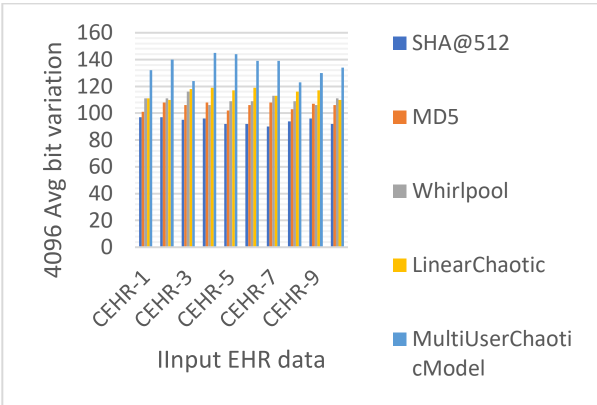

Table 6: Performance evaluation of average runtime(ms) of proposed blockchain security framework with existing models using 2048 hash bit.

CEHR Transactions	***SHA 512***	***MD5***	***Whirlpool***	***Linear Chaotic***	***MultiUserChaoticModel***
CEHR-1	4086	3999	4040	4016	3398
CEHR-2	4279	3997	4153	4055	3075
CEHR-3	3808	4192	4256	4033	3132
CEHR-4	4169	4195	4082	3852	2946
CEHR-5	4052	4238	4100	3836	3321
CEHR-6	3933	3862	4082	4037	3204
CEHR-7	4168	4088	4011	4083	3212
CEHR-8	3863	4067	3890	4289	3275
CEHR-9	4122	4269	4018	3890	3309
CEHR-10	3838	3809	3890	3958	3366
CEHR-11	4269	4120	4137	4010	2953
CEHR-12	3819	4054	3971	4006	3285
CEHR-13	3882	4249	4277	3831	3263
CEHR-14	3838	4291	4231	4140	3382
CEHR-15	4107	3822	3825	3983	3270
CEHR-16	3819	4037	4282	3831	3285
CEHR-17	3990	4225	4104	3895	3255
CEHR-18	3886	4148	4250	4170	3147
CEHR-19	4104	4270	4013	4215	2983
CEHR-20	4052	4292	3995	4088	3386

Table 7: Performance evaluation of average runtime(ms) of proposed blockchain security framework with existing models using 4096 hash bit.

CEHR Transactions	*SHA 512*	*MD5*	*Whirlpool*	*Linear Chaotic*	*Multi-user Chaotic Model*
CEHR-1	4246	4120	4250	3907	3087
CEHR-2	4036	3885	4239	3833	3340
CEHR-3	3873	3884	4114	3922	3297
CEHR-4	4283	3812	3987	3844	3387
CEHR-5	3928	3818	4129	4094	3213
CEHR-6	3911	4169	4016	4052	3203
CEHR-7	3987	4126	4085	4231	3415
CEHR-8	4205	4042	4101	4207	3095
CEHR-9	4271	4289	3919	3963	3152
CEHR-10	4210	3869	3983	4274	3340

5. Conclusion

The emergence of cloud storage solutions tailored to the healthcare domain has introduced a paradigm shift in data protection and computational security. Leveraging blockchain-based data structures and advanced memory management, these solutions have shown great promise in addressing the security challenges posed by larger media files and diverse data formats. This proposed data security framework, based on a role-based access control technique, offers a novel approach to bridge the gap between users and access permissions. Specifically designed for the cloud blockchain mechanism, our framework departs from the conventional use of standard integrity-checking algorithms and instead employs a unique hybrid non-linear dynamic algorithm, enhancing the variability of hash bits during blockchain construction. In this pproach, each medical data transaction undergoes rigorous processing and is added to the blockchain with specialized security blocks for hashing and encryption, thereby bolstering the overall security measures. The encryption method, based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE), grants users the flexibility to select attributes from a predefined set, enhancing the system's adaptability and usability. Moreover, proposed non-linear chaotic function-based hash algorithm and advanced attribute-based encryption model are used to address the challenges inherent in traditional blockchain frameworks when dealing with large cloud datasets. This dynamic-sized hash verification and encryption framework operates effectively in real-time cloud computing environments, as evidenced by experimental results that demonstrate its superiority over conventional blockchain frameworks in safeguarding medical data.

References

[1] Mrs. U. Chelladurai, Dr. S. Pandian, and Dr. K. Ramasamy, “A Blockchain based Patient Centric EHR Storage and Integrity Management for e-Health Systems,” Health Policy and Technology, p. 100513, May 2021, doi: 10.1016/j.hlpt.2021.100513.

[2] X. Qin, Y. Huang, Z. Yang, and X. Li, “A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing,” Journal of Systems Architecture, vol. 112, p. 101854, Jan. 2021, doi: 10.1016/j.sysarc.2020.101854.

[3] H. Li and T. Jing, “A Ciphertext-Policy Attribute-based Encryption Scheme with Public Verification for an IoT-Fog-Cloud Architecture,” Procedia Computer Science, vol. 174, pp. 243–251, Jan. 2020, doi: 10.1016/j.procs.2020.06.080.

[4] M. B. Taha, C. Talhi, and H. Ould-Slimanec, “A Cluster of CP-ABE Microservices for VANET,” Procedia Computer Science, vol. 155, pp. 441–448, Jan. 2019, doi: 10.1016/j.procs.2019.08.061.

[5] M. Xie, Y. Ruan, H. Hong, and J. Shao, “A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices,” Future Generation Computer Systems, vol. 121, pp. 114–122, Aug. 2021, doi: 10.1016/j.future.2021.03.021.

[6] K. Sowjanya, M. Dasgupta, and S. Ray, “A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems,” Journal of Systems Architecture, vol. 117, p. 102108, Aug. 2021, doi: 10.1016/j.sysarc.2021.102108.

[7] Z. Zhang, W. Zhang, and Z. Qin, “A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted cloud computing,” Future Generation Computer Systems, May 2021, doi: 10.1016/j.future.2021.04.022.

[8] Y. Su, Y. Li, K. Zhang, and B. Yang, “A privacy-preserving public integrity check scheme for outsourced EHRs,” Information Sciences, vol. 542, pp. 112–130, Jan. 2021, doi: 10.1016/j.ins.2020.06.043.

[9] S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C.-M. Chen, “A secure blockchain-based e-health records storage and sharing scheme,” Journal of Information Security and Applications, vol. 55, p. 102590, Dec. 2020, doi: 10.1016/j.jisa.2020.102590.

[10] Z. Wang, C. Cao, N. Yang, and V. Chang, “ABE with improved auxiliary input for big data security,” Journal of Computer and System Sciences, vol. 89, pp. 41–50, Nov. 2017, doi: 10.1016/j.jcss.2016.12.006.

[11] H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, “Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments,” Journal of Parallel and Distributed Computing, vol. 148, pp. 46–57, Feb. 2021, doi: 10.1016/j.jpdc.2020.10.002.

[12] K. Sheela and C. Priya, “Blockchain-based security & privacy for biomedical and healthcare information exchange systems,” Materials Today: Proceedings, May 2021, doi:

10.1016/j.matpr.2021.04.105.
[13] T. Benil and J. Jasper, “Cloud based security on outsourcing using blockchain in E-health systems,” Computer Networks, vol. 178, p. 107344, Sep. 2020, doi: 10.1016/j.comnet.2020.107344.
[14] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, “Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain,” Information Sciences, vol. 485, pp. 427–440, Jun. 2019, doi: 10.1016/j.ins.2019.02.038.
[15] P. Deshmukh, “Design of cloud security in the EHR for Indian healthcare services,” Journal of King Saud University - Computer and Information Sciences, vol. 29, no. 3, pp. 281–287, Jul. 2017, doi: 10.1016/j.jksuci.2016.01.002.
[16] M. Sangeetha, P. Vijayakarthik, S. Dhanasekaran, and B. S. Murugan, “Fine grained access control using H-KCABE in cloud storage,” Materials Today: Proceedings, vol. 37, pp. 2735–2737, Jan. 2021, doi: 10.1016/j.matpr.2020.08.542.
[17] L. D. Serbanati, “Health digital state and Smart EHR systems,” Informatics in Medicine Unlocked, vol. 21, p. 100494, Jan. 2020, doi: 10.1016/j.imu.2020.100494.
[18] S. Banerjee et al., “Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment,” Journal of Information Security and Applications, vol. 53, p. 102503, Aug. 2020, doi: 10.1016/j.jisa.2020.102503.
[19] S. Badr, I. Gomaa, and E. Abd-Elrahman, “Multi-tier Blockchain Framework for IoT-EHRs Systems,” Procedia Computer Science, vol. 141, pp. 159–166, Jan. 2018, doi: 10.1016/j.procs.2018.10.162.
[20] R. Sarma, C. Kumar, and F. A. Barbhuiya, “PAC-FIT: An efficient privacy preserving access control scheme for fog-enabled IoT,” Sustainable Computing: Informatics and Systems, vol. 30, p. 100527, Jun. 2021, doi: 10.1016/j.suscom.2021.100527.
[21] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K.-K. R. Choo, “Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment,” Computer Standards & Interfaces, vol. 54, pp. 3–9, Nov. 2017, doi: 10.1016/j.csi.2016.05.002.
[22] M. B. Taha, C. Talhi, and H. Ould-Slimane, “Performance Evaluation of CP-ABE Schemes under Constrained Devices,” Procedia Computer Science, vol. 155, pp. 425–432, Jan. 2019, doi: 10.1016/j.procs.2019.08.059.
[23] K. Sethi, A. Pradhan, and P. Bera, “Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation,” Journal of Information Security and Applications, vol. 51, p. 102435, Apr. 2020, doi: 10.1016/j.jisa.2019.102435.
[24] S. Banerjee, B. Bera, A. K. Das, S. Chattopadhyay, M. K. Khan, and J. J. P. C. Rodrigues, “Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT,” Computer Communications, vol. 169, pp. 99–113, Mar. 2021, doi: 10.1016/j.comcom.2021.01.023.