[1,3]Keesara Sravanthi
[2] P Chandrasekhar

An Efficient Multi-User Groupwise Integrity CP-ABE(GI-CPABE) for Homogeneous and Heterogeneous Cloud Blockchain Transactions

Abstract: - As the size of medical data grows exponentially, safeguarding Electronic Health Records (EHR) via cloud blockchain transactions becomes increasingly critical. This paper presents the Multi-User Groupwise Integrity Ciphertext-Policy Attribute-Based Encryption (GI-CPABE), an efficient framework designed to ensure robust data security. By implementing an Improved Ciphertext-Policy Attribute-Based Encryption (ICP-ABE), the GI-CPABE framework is designed to be compatible with both homogeneous and heterogeneous cloud environments, providing secure access that is role-specific and reliable. A distinctive feature of this framework is its role-based access control mechanism, which efficiently assigns user access rights and roles based on multi-user group attributes, considered as integrity measures. An experimental setup was established on a real-time cloud server, simulating a cloud based EHR system. Test data, mimicking real-world EHRs, was generated and subjected to encryption and decryption processes, evaluating the time efficiency of these operations. The proposed GI-CPABE framework demonstrated optimized storage utilization by calculating the overhead of encrypted data, ensuring data integrity through defined attribute-based policies, and enabling secure, controlled access to medical data. Furthermore, a comparative analysis was conducted to ascertain the effectiveness of the proposed framework against existing models. The implementation of access control mechanisms exhibited robust enforcement of access controls tailored to different user roles such as healthcare providers, patients, and administrators.

Keywords: Group integrity, group access control ,Cloud data security, encryption, Blockchain, medical data.

I. INTRODUCTION

Healthcare institutions, including hospitals and general practitioners, must adhere to the imperative of implementing robust health-care systems. This entails the management of health-related data within electronic health records (EHRs), comprehensive databases housing individuals' health information. Health-related data encompasses conditions, medications, medical imagery, and personal particulars, such as names, ages, genders, weights, and billing details. Given the sensitivity of this information, safeguarding it against unauthorized access remains a paramount challenge in healthcare systems. Thus, a central concern today is ensuring the secure transmission of medical data without compromising patient confidentiality. Advancements in Information and Communication Technology (ICT) facilitated by Health Information Technology (HIT) have the potential to significantly enhance the management of patients' treatment. The secure use and transmission of essential health information enabled by HIT contributes to improved medical decisions and more effective therapy. Healthcare institutions have greatly benefited from the introduction of Electronic Medical Records (EMRs) and Electronic Health Records (EHRs) [1-3]. An Electronic Medical Record (EMR), compiled by a single healthcare provider, contains a comprehensive summary of a patient's health data, including medical conditions, test results, physician notes, and radiological reports. It's possible for a patient to have multiple EMRs from various hospitals or doctors' offices. In contrast, the Electronic Health Record (EHR) contains a patient's health information from multiple healthcare providers. EHRs offer numerous advantages, including enhanced healthcare comprehension, increased patient engagement, improved efficiency and cost savings, enhanced treatment quality and outcomes, and better care coordination. The use of electronic health records can help reduce unnecessary or redundant tests and lab procedures. For instance, a study estimated potential savings of $183,586 over two years by preventing 11,790 unnecessary test requests using digital systems. Additionally, electronic health records can reduce overhead expenses. These computerized systems not only enhance the quality of care and service but also reduce costs, minimize unnecessary appointments, and improve patients' access to online prescription services.

[1] *Corresponding author: Keesara Sravanthi, Research Scholar, Department of computer science and Engineering, GITAM, Vizag, AP, India.Emailid:sravanthireddy.k8@gmail.com

[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,Telangana, India.

EHRs can streamline pharmacy operations and reduce the time spent on traditional prescription writing. Moreover, they can be employed for various administrative tasks, reducing costs related to lab/test result delivery charges, online billing requests, appointment scheduling, and updates.In recent months, Bitcoin has garnered significant attention from both the commercial and academic sectors. Blockchain technology, the underlying technology that enables Bitcoin and other cryptocurrencies to function, is central to this phenomenon. The blockchain uses an integrated data structure within the network to record all transactions, setting itself apart with the immutability of stored records, achieved through a combination of consensus and cryptography [4-8]. The term "Distributed Ledger Technology (DLT)" is commonly used for this technology due to data distribution across a network of nodes. This article provides a detailed analysis of blockchain and its distinctions from traditional database systems, along with its actual utility and potential, based on academic research. The findings will assist practitioners and academics in choosing the most suitable technology for their specific use cases. The article also examines recent works using a recommended decision tree to evaluate the successful implementation of blockchain technology in relevant problem areas. Blockchain technology is evolving to establish a decentralized ecosystem where third parties have no control over transactions and data. It involves a series of blocks maintained by all nodes in the network, known as the blockchain. These blocks store transactions, and each block is cryptographically linked to the previous one by providing a hash value. This creates a permanent data storage system where new blocks can only be added to the end of the chain, preventing updates or deletions of existing transactions. Various blockchain-based systems have emerged to enable the secure distribution of digital assets among untrusted users [9].Leveraging blockchain technology provides the opportunity to create a public ledger containing decentralized digital information accessible from any internet-connected computer [10].

Within this database, each data block forms part of a chain comprising numerous data bits, collectively referred to as the database chain. The blockchain introduces a pioneering shared digital record accessible to untrusted parties [11], especially advantageous in healthcare where decentralized data transfer ensures the integrity of health information [12]. The versatility of blockchain technology extends to various applications [13] within the healthcare sector. One substantial benefit lies in its ability to reduce the complexities and costs associated with data reconciliation while facilitating swift access to real-time health applications.The Medical Health Record (MHR) encompasses a diverse array of documentation accumulated over time by healthcare specialists. These records include directives for medication and treatment management, X-rays, test results, and various other health-related details. Traditionally, healthcare professionals have been responsible for organizing and overseeing these records. However, the advent of online data storage has empowered patients to manage their Personal Health Records (PHR) independently. Third-party organizations offer cost-effective online storage solutions to facilitate this process. Scientifically, electronic health records (EHRs) pertain to patient data stored in a digitized format, covering everything from basic allergies to transaction records at healthcare institutions, medications, and treatment histories.Online storage providers utilize patient data from electronic health records to compile diverse medical information, aiding in the identification of patients in need of medical attention. EHR systems are meticulously designed to ensure the security and accuracy of patient data, effectively mitigating the risk of losing vital medical history. Additionally, EHR systems enhance accessibility, alleviate the burden of data duplication, and substantially reduce the likelihood of data loss [14]. Conventional patient records demand extensive human labor. When a patient visits a clinic or hospital, their records must be located and transported to the appropriate department before the examination can commence, posing a risk of mishandling. Fig. 1 illustrates the traditional medical record system.The maintenance and exchange of health records are paramount responsibilities in the healthcare system, with severe consequences if the security of health data is compromised [15], potentially leading to patient fatalities due to integrity breaches. Given the sensitive and private nature of electronic health records [16], ensuring their security is of utmost importance. Blockchain technology has gained prominence in recent years due to its adaptability compared to alternative solutions. However, concerns persist over the potential theft or lawful access of data stored on other servers depending on the circumstances [17]. The existing medical data management system lacks guarantees regarding the integrity and reliability of patient data, particularly within medical institutions [18]. Medical data loss and hacking are persistent threats, resulting in data security breaches, violations of personal privacy, and other challenges. In a centralized environment, most medical data remains vulnerable to threats like tampering and hacking, risking data leakage and loss [19].

Blockchain's ability to maintain an unchangeable distributed ledger of transactions makes it a promising solution for addressing security concerns associated with cloud-based systems. Blockchain is a decentralized, unalterable database of transactions. This research's most significant contribution is the use of the SHA256 cryptographic hashing method to enhance patient data security, rendering it extremely difficult for attackers to reverse the hashing process and access the original data. SHA 256's enhanced security is attributed to its verified key, capable of validating or matching dynamic passwords against acquired authentication, thereby improving security.The maintenance and exchange of health records are pivotal responsibilities within the healthcare system, with consequences for the security of health records being even more dire than in other systems. Loss of integrity can profoundly impact a patient's life and, in extreme cases, result in fatality. Safeguarding the confidentiality of electronic medical records is of utmost importance. In comparison to other alternatives, blockchain technology has gained popularity due to its adaptability. However, when data is stored on other servers, concerns about theft or lawful use may arise. Medical data, vital for patient diagnosis and treatment, is considered highly sensitive and confidential by the medical community. Patient data is compartmentalized to protect patient confidentiality, with various controls governing its distribution and lifecycle events.The transmission and exchange of medical data outside of medical institutions are strictly prohibited, except in cases where patients request access to their own medical records. This complex web of restrictions severely hampers the sharing and trading of medical data, diminishing its overall utility. The existing medical data management system, primarily designed for healthcare organizations, lacks guarantee of the accuracy and reliability of patient data. Inevitable risks of data loss and hacking persist, subjecting the acquired data to security concerns and privacy breaches [20]. Centralized storage of medical data in healthcare institutions makes it susceptible to various risks, including intentional tampering and hacking, leading to the potential leakage or loss of medical data, among other adverse outcomes. In contrast, blockchain technology is emerging as a promising solution to address security vulnerabilities inherent in cloud-based systems due to its ability to maintain an ever-expanding, immutable, and cost-effective ledger of distributed data.Blockchain is a decentralized and immutable database that is becoming increasingly popular and versatile in various sectors, with significant implications for the healthcare industry. Similar to Electronic Medical Records (EMRs), Ethereum Blockchain technology offers potential cost savings, data security, and accessibility improvements. Modern technological advancements are reshaping many aspects of human life, including healthcare, as technology continues to advance. Blockchain technology offers significant advantages in terms of security, user experience, and other healthcare sector aspects. However, most Electronic Medical Records (EMR) systems currently lack the capability to exchange patient health information, resulting in interoperability challenges within the healthcare system. Blockchain technology is being leveraged to facilitate the management and transfer of EMRs to address this issue. Currently, patient information is securely distributed among various institutions, hospitals, and insurance companies, with no central database access point. However, this is expected to change in the near future. Patients who record their health information on a blockchain may have the option to grant access to their electronic health data to other parties, preventing unauthorized tampering. In essence, blockchain serves as a distributed ledger for sharing and trading health information among involved parties [21]. In this context, authorized organizations can access the blockchain for inspection and block validation, in contrast to public blockchains like Bitcoin. Each authorized user can monitor their health data through their own anonymous account, enhancing data transparency and personal data management. Although blockchain technology offers improved data transparency and self-management for patients, it presents challenges in the administration of personal medical data and services. This research proposal aims to advance blockchain-based homomorphic encryption algorithms to enhance the efficiency and security of regulating and accessing health record information.

The proposed method reduces administrative burdens while safeguarding the confidentiality of sensitive data during the distribution of Electronic Medical Records (EMR) on an open platform, benefiting both parties. A blockchain ledger is characterized by its tamper-proof and publicly verifiable attributes. There are three types of blockchains in blockchain technology: public, consortium, and private blockchains. Public blockchains are accessible to all participants, with distributed access to ledger information. Private blockchains are exclusively used by private organizations and are not accessible to the general public. Consortium blockchains are similar to private blockchains and are established based on organizational norms that define blockchain accounting, reading, and writing rights. In the current medical data management system primarily designed for medical organizations, there is no assurance of the integrity and reliability of patient data. Unfortunately, the loss or hacking of medical data are inherent risks that must be acknowledged, leaving acquired data perpetually vulnerable to data security concerns and personal privacy breaches, among other challenges. The centralized nature of medical data storage within medical institutions exposes it to various risks, including potential tampering and hacking, which may lead to data leakage or loss, among other adverse outcomes [22]. Blockchain technology is emerging as a promising solution to address these security vulnerabilities inherited from cloud-based systems.

It offers a distributed and immutable database structure. A notable feature of this study is the proposed SHA256 cryptographic hashing algorithm, which significantly enhances the security of patient data by making it nearly impossible for an attacker to reverse the hashing process and recover the original data. SHA256's enhanced security is attributed to its use of a verified key, which can confirm or match the dynamic password against acquired authentication, thus fortifying security. A blockchain comprises an ever-expanding collection of linked blocks, secured through encryption, forming a single chain of transactions. Each block includes a timestamp, transaction data, and a cryptographic hash of the previous block. The data in each block must be maintained in a way that prevents retrospective amendments without affecting subsequent blocks, ensuring data integrity. Blockchain networks are typically peer-controlled and adhere to specific protocols for interactions and block validation. While blockchain records are not infallibly accurate due to the possibility of forks, they are inherently secure by design. Efforts are underway to develop distributed computing systems with high Byzantine fault tolerance. In recent years, the general public and the mainstream media have shown a growing interest in blockchain technology. Blockchain is often hailed as the fourth wave of computer technology, with profound implications, surpassing its association with the Bitcoin cryptocurrency. Blockchain, in its most basic form, serves as a novel data structure for information storage, combining existing technologies in innovative ways to ensure network integrity and reduce the need for trust. It facilitates peer-to-peer transactions without intermediaries, extending beyond tangible assets to include intangible assets like sensitive information. Digital ledger technology, commonly known as blockchain technology, offers a method to store individual transactions in a distributed chain of blocks without the need for a trusted third party. Blockchain ensures immutability through the use of public and private keys, enhancing integrity, accountability, and to some extent, privacy [23]. Public blockchains are open to anyone who wishes to participate, typically operating without authorization. They rely on the financial incentives of honest participation, such as mining rewards, to deter malicious actors. However, a defensive mechanism, Byzantine Fault Tolerance, is still required to guard against malevolent participants and maintain the blockchain's functionality, depending on consensus rules [24]. Information and access to patient records are essential in the healthcare industry. Paper-based records offer benefits such as less labour and physical storage. On the other hand, EHRs provide improved patient safety, easier access to clinical data, reduced medical costs, fewer medical errors, and better support for decision-making. As a result, 90% of medical facilities have adopted EHR systems to allocate healthcare resources efficiently. However, the e-healthcare system presents specific challenges, including privacy, confidentiality, and security of medical information. To address these challenges, the healthcare sector currently uses cloud computing in digital technology to outsource data. The cloud provides practical facilities for easy exchange of information and access to patient records. Sharing and accessing data requires an effective privacy and security mechanism to prevent vulnerabilities. Stakeholders must use data while upholding confidentiality to protect it from third-party or enemy threats. Accessing information from any location has led to the storage of e-health information in the cloud, which provides numerous benefits. However, health data requires special consideration for security and privacy. To protect privacy, one must prevent data tampering, spoofing, and disclosure, which pose a danger to data privacy. The alteration of data is vulnerable to threats that benefit ineligible users. These threats have the potential to cause harmful modifications to both reputation and information. Furthermore, authorized parties may have their right of access to their own data revoked. The key distinction between public and private blockchains lies in the authorization of network participants, the execution of the consensus mechanism, and the management of the shared ledger. Public blockchains are more widely accessible to a broader audience, while private blockchains have stricter access controls. Public blockchain networks are open to individuals and organizations free of charge, providing an open invitation for participation. It is common practice to incentivize network participation to attract additional users. Notably, Bitcoin represents one of the largest and most extensively used publicly accessible blockchain networks, particularly in terms of transaction volume [25]. Despite its relatively recent inception, blockchain technology has attracted a diverse array of industries, including finance, government, energy, and healthcare. This article delves into the use of blockchain technology in the healthcare sector and offers recommendations for further research. Ongoing research in this field is progressing rapidly, leading to the discovery of several state-of-the-art blockchain-based use cases across various domains. Examples include electronic medical data sharing, remote patient monitoring, medicine supply chain, and various other applications.

As a final point of discussion, we focus on recognizing the limitations of previously explored methodologies and propose open research challenges and potential avenues for future research to conclude the discussion. To ensure that the attributes on the key would be encrypted to the cypher text's decryption, the key was encrypted. To establish adaptability, smart contracts were hired and a bench for access control was brought into being. Each data allocation appeal demanded interacting with smart contract transactions. Access control and fine-grained control are put into action in a block chain-based data safety sharing architecture [26].

Originally, they used a multi-level authorization center in collaboration with a hierarchical attribute model to implement a hierarchical attribute-based encryption architecture. By allocating user attributes, this approach enabled adjustable and precise access control [27]. A methodology to allow secure data sharing while safeguarding patient privacy was built into the cryptographic model. Through the use of a Empowerment Approach, This method was successfully implemented on-demand revocation, fine-grained access control, and access control. Additionally, the role-based and proxy signature-based models also Highlighted the delegation mechanism. The Blockchain-Based Security Sharing Technique (BSSPD), A technology that empowered use of fine-grained access control for personal data [28]. Instances of cipher text-policy attribute-based encryption, like IPFS, blockchain, and CP-ABE, were put to use with regard when working on this algorithm. To enhance the scheme, the data exchange for DO was encrypted and preserved on IPFS [29]. Data security initiatives must be established in order to assure the safe storage of Malicious assaults on data and unlawful breach could endanger the data that electronic health records stores. To ensure privacy in the cloud of e-health, policies are implemented based on the adversary model. If cloud servers are considered unreliable entities, private information may be exposed. Adversaries in such scenarios may distribute the data to unauthorized parties, although they may not alter it. Therefore, multiple privacy requirements, including authenticity, auditing, and integrity, must be met by the cloud. To guarantee secure data storage, accountability, discretion, confidentiality, non-repudiation, and data security measures must be implemented [30]. Access permission was pre-defined for patients through smart contracts, ensuring secure data sharing. The content and access control model were jointly designed to maintain privacy in the data sharing process, and the extraction signature model was applied. [31] developed a fine-grained blockchain structure for data sharing in IoT, using a consensus technique as a Byzantine fault tolerance model. The IoT data was encrypted before being added to the smart contract model. To achieve fine-grained sharing, an attribute encryption model was used, and access permission was pre-defined for patients. Various stakeholders store medical data and information. However, cloud networks bear the burden of hosting unlimited amounts of data, providing highly efficient and affordable storage, as well as excellent access processing. Nevertheless, the privacy and security of medical information are at risk when multiple users access data from various locations on a large network. Moreover, most medical data has restricted access and is highly confidential. Therefore, storing data on external servers inevitably weakens security, especially with public access to health information [32].

II. RELATED WORKS

In the United States, healthcare providers routinely maintain and exchange patients' Electronic Health Records (EHRs) through regional Health Information Exchange (HIE) organizations. In contrast, some countries in Europe, Australia, Singapore, and Estonia have adopted the concept of a national or universal Electronic Health Record (EHR). In these regions, healthcare providers, such as those in Estonia, are responsible for maintaining patient information and transmitting specified data to a national EHR system. This approach enables data from various healthcare providers to be accessed and shared through a unified national platform, benefiting both patients and healthcare professionals for medical research [33]. The adoption of Health Information Technology (HIT) has been on the rise, with doctors and nurses increasingly incorporating it into their practices. The surge in the adoption of Electronic Health Records (EHRs) in the United States can be attributed to initiatives like the United States Centers for Medicare and Medicaid Services' incentives program. Between 2005 and 2018, the utilization of EHR systems by office-based practitioners significantly increased. According to the American Medical Association, 79.7 percent of office-based practitioners were using certified EHR systems [34]. The adoption of EHR capabilities by office-based clinicians in the US has led to increased patient engagement, as per surveys conducted by the National Center for Health Statistics in 2013. In 2014, 57.0% of clinicians electronically communicated health information with their patients, up from 46% the previous year. Additionally, there was a 30 percent increase in doctors using encrypted communications with their patients in 2014 compared to 2013. Certified EHR systems were extensively used in over 90% of hospitals, particularly large hospitals with 400 or more beds, at the time of this publication [35].

[36] examined the adoption of blockchain technology, considering technological, organizational, and environmental factors, utilizing innovation theory. Their research highlighted the key benefits of blockchain, such as anonymity, immutability, and transparency. Complexities, interoperability, data security, innovation, and relative advantages were identified as the main technical factors influencing the adoption of blockchain technology. Organizational factors, such as company size, regulatory environment, market dynamics, industry competition, and government support, were also deemed important. The study emphasized the significance of organizational attributes in driving adoption. The acquisition of new resources, integration of assets, development of new capabilities, and increased regulatory requirements necessitate significant high-level management support. Organizational Readiness (OR) refers to the internal resources that organizations can use to adopt blockchain technology, including human resources, financial management, and infrastructure.

Engaging management and staff in embracing the change due to these attributes enhances organizational readiness. They identified standards related to authentication, interoperability, clinical data exchange, and mobile health as central issues within the healthcare industry. The study also examined blockchain limitations and concerns, including the absence of standards, decentralized storage, security vulnerabilities, key management, scalability, and Internet of Things overhead. Deloitte Insights outlined five adoption hurdles that companies must address before deploying blockchain technology [37]. These include the time required for blockchain setup, the need for cooperation to enhance transaction processing speed, a lack of standardization, the complexity and cost associated with blockchain solutions, and legal and regulatory issues. Regulatory concerns were identified as a significant barrier to further investment in blockchain technology by CEOs in a recent study. [38] studied the diverse applications of blockchain technology in non-financial sectors. The study specific applications for blockchain which have the prospects to succeed, that includes the digitally signing contracts and communications, strive against the forged medications in pharmaceutical industry, and smart healthcare systems. It has been specifically of consequence how block-chain technology has contributed to safeguard the confidentiality and privacy of health care data, which includes sensitive patient information. Blockchain technology has improved the standards of safe exchange and medical records archiving without any outside assistance.[39] Explored various fields and industries where blockchain can be effectively applied beyond the realm of banking. Blockchain technology has the capacity to be effectively utilized in various crucial domains which include employing digital signatures for contracts and communications, combating the proliferation of fake medications, and implementing intelligent healthcare systems. By making use of blockchain technology, long-established enterprises may Save and transmit information faster and safer without any aids from other groups. Electronic medical records (EMRs) enhance mobility, availability and directness which upgrades access for medical professionals, along with the raising chances of fraudulent movement by unsanctioned individuals. Security and confidentiality policies are required for healthcare data, with patient health record security starting with confidentiality. Owing to the deftness with which EHRs have made data fabrication anyone can now effortlessly create fraudulent with honest claims by forging records. Blockchain has the potential to address several significant challenges in healthcare. In the case of traditional Electronic Health Records (EHRs), gaining access to health records involves a complex process. Data is centralized within healthcare organizations and is under their control. A more transparent and reliable system is needed to transform the healthcare sector, offering benefits such as increased transparency and reliability among all users.

The Blockchain-Based Clinical Records Secure Capacity and Clinical Benefit System, developed by [40], utilizes blockchain technology for distributed storage of personal clinical data, leveraging properties like decentralization, immutability, and irrefutability. Similarly, [41] has created a blockchain-based security management system for the Internet of Things architecture, utilizing Ethereum transactions as a backend. This model ensured high security, availability, privacy, and security. [42] developed a decentralized security architecture for the Internet of Things using blockchain technology, offering more efficient network threat identification. However, it had a longer recovery time in case of system disruptions. [43] designed a Searchable Encryption for Electronic Health Record Sharing based on blockchain. This model involved a complex logic-based index for EHRs and required moving the index to the blockchain for widespread distribution, with data owners retaining control. [44] developed a Robust Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain Technology.

Their blockchain technology ensured data integrity and access control during log transactions, with cloud servers securing stored patient EHRs. However, the model needed practical simulation for protocol testing in a real-world setting.[45] presented a method that employs blockchain for access control in a personal health record system, ensuring privacy protection. The model integrates the tamper resistance feature of blockchain and uses proxy re-encryption and cryptographic algorithms to uphold system privacy. Additionally, the model incorporates attributes such as tamper resistance, revocability, consent, and auditability to enhance performance. [46] modeled a Blockchain-based Distributed Key Management Architecture (BDKMA) for access control in the Internet of Things model. The structure of this model was utilized for fog computing to reduce latency, with multiple blockchains operating. To achieve cross-model domain access, we utilized cloud technology. Additionally, we implemented the blockchain model to fulfill the requirements of extensibility, granular auditability, decentralization, high scalability, and maintaining privacy access control. We also developed various system operation models, such as authorization assignment nodes and group access models, to support the system. Our system achieved extensibility by incorporating dynamic transaction collection duration changes for different structures. This algorithm significantly improved the system's performance and scalability in terms of network size. [47] created a blockchain-based system that provides secure mutual authentication. They integrates both blockchain and attribute signatures for message authentication, terminal authentication, and authentication of gateway codes.

Additionally, BSeIn applies the encryption process for multiple receivers to provide confidentiality. Smart contracts were used to scale the request process, and they worked together to accomplish it. A model was used to safeguard user privacy during data retrieval. The data owner encrypted the address and decryption key of the shared data using the ABE-CP model and specific access policies. To distribute keys and publish information, the data owner utilized blockchain technology. [48] devised an effective data sharing strategy on blockchain by distributing data to users who adhere to the access rules. Lastly, a searchable encryption model was implemented to tackle the complexity of cypher text queries. The researchers used an approach that involved sharing data without involving data owners in data queries. They introduced the CP-ABE algorithm for data encryption and successfully improved data security during the sharing process. [49] presented a model for EHR interoperability based on the blockchain model, which uses blockchain-based smart contracts powered by Ethereum for complex data complication and delicate access control. The researchers also applied more sophisticated cryptographic methods for the security process. This model compiles references to data hashes. The team utilized an original approach to improve security and privacy, incorporating two additional schemes. The first scheme involved the use of homomorphic encryption for query processing, while the second scheme utilized differential privacy for data anonymization. To compile small, encrypted records and store keys, the team employed the proxy re encryption method over a blockchain. They also utilized smart contracts for access control and the roles of third parties on the blockchain, in addition to patients, resulting in an enhanced degree of decentralization. [50] created the blockchain-based health data consent approach, utilizing smart contracts to represent individual consent and empower data seekers. To further enhance security and privacy, the team added two additional schemes to the original approach: homomorphic encryption for query processing and differential privacy for data anonymization. The records were securely stored in the cloud using blockchain technology. [51] presented a blockchain-based EHR data sharing model that utilized a dynamic consent approach, incorporating the Access Matrix (ADA-M) and Data Use Ontology (DUO). DUO modeled users' specific consent, while ADA-M specified the questions in a data request. The Ethereum blockchain was utilized to estimate various data sharing scenarios. BPDS, an electronic medical record, was utilized to accumulate the actual digital health record. Indexes were securely stored in an interference-proof alliance blockchain. This approach significantly reduced the complexity of medical data leakage. The different centers for authorizations were improved by integrating the Fabric blockchain approach to address the high decryption costs faced by IoT users. Additionally, the High-complexity partial decryption model utilized smart contracts on the blockchain to reduce user overhead. To ensure historical data traceability, blockchain was employed, and a function that meets data restriction security requirements was implemented. Furthermore, performance was enhanced by adding a hierarchical attribute-based cryptographic model. [52] developed the AuthPrivacyChain cloud system, which is a blockchain-based access control model with privacy protection. Initially, the node's account address was used in this system. Due to its unique features and decreased data access control permission, blockchain data was accumulated while being encrypted. Subsequently, an authorization process for access control was created, which includes both revocation and authorization. This model was developed here and is dependent on EOS (Enterprise Operation System) safeguards to ensure privacy. The strategy involves encrypting access control rights and accumulating them in the blockchain model, which successfully safeguards user privacy. Additionally, this model ensures accessibility, resource accountability, and resists several internal and external pressures while maintaining accountability for resources, integrity, and outside assaults. The researchers presented a blockchain-enabled model for data privacy. The algorithm [53] provides a guarantee of confidentiality for user data in smart cities, and stakeholders involved in smart contracts are made aware of this. Subsequently, data owners are encouraged to share their information with stakeholders or third parties while ensuring compliance with various requirements of the European Union General Data Protection Regulation (EU GDPR), including access, sharing, and deletion with the data owner. Electronic Health Records (EHRs) are a collection of smart, systematized patient health records that include laboratory test results, sensitive information, and other documents. These records offer added benefits such as accessibility, accuracy, and efficiency, in addition to high comparability to traditional health records. The proposed mechanism suggests a three-way approach to safeguard data by combining security procedures such as Diffie-Hellman cryptography, Advanced Encryption Standard, and Hellman key exchange. [54] presented a data security improvement through a cloud computing algorithm. The encryption algorithms protect the data stored in the cloud, and the Diffie Hellman Key exchange makes the key ineffective, thereby preventing any unauthorized transmission. The implementation of advanced encryption standards and the utilization of file distribution and the SHA1 algorithm, as presented by [55], have successfully safeguarded cloud data from hackers. While distributing files through servers may pose security issues, the authentication procedure is fortified by hash-code files, which restrict access to authorized personnel only. This approach effectively addresses security concerns, including error localization, data security, and integrity. As a result, it has proven to be an effective measure against malicious attacks involving server collusion and modification. The analysis presented shows that our proposed method has outperformed other methods. [56] introduced a secure erasure cloud storage method that utilized proxy reencryption and the advanced encryption standard algorithm. This resulted in a more secure cloud storage server. The tactic has benefited a decentralized system, as proxy reencryption saves time and aids in data re-encryption while reducing memory consumption in a distributed setting. The system stores data using a hybrid version of distributed erasure code. The proxy re-encryption scheme enables sharing of cloud-based information and facilitates its retrieval. It employs erasure encoding to encourage sharing through a dispersed system. The distributed erasure code manages storage and allows consent for data in the cloud. In [57] presented a cloud data security mechanism that uses the Advanced Encryption Standard (AES) for computing. They modeled security with the cloud platform as a service (PaaS) in mind and used AES as the secret key for a more efficient encryption algorithm with a strong security system. Heroku uses a PostgreSQL-based PHP application[58].

III. Proposed model

This section presents a novel data security framework that utilizes a multi-user role-based access control technique to assign user access control rights and roles on the organizational business function. Each group's attributes are considered as integrity measures, and policies are defined using these attributes. In this work, multi-user groupwise integrity CP-ABE(GI-CPABE) is proposed to improve the effectiveness of handling multi-users in real-time applications.

A. Multi-Modal EHR Hash:

```
# Step 1: Initialization
x0, μ0, η = CalculateInitialValues(H, P, b)
keys = H, b
# Step 2: Chaotic Coordinates Generation
for i in len(M):
    for j in len(N):
        x, y = x0, y0
        for k in len(M * N):
            x = 3.965 * x * (1 - x)
            y = 3.965 * y * (1 - y)
        xi_prime = floor(x * 1e14) % M + 1
        yi_prime = floor(y * 1e14) % N + 1
        # Use xi_prime and yi_prime as chaotic coordinates
# Step 3: Nonlinear Scrambling
for i in len(M):
    for j in len(N):
        p = (a1 * i^2 + b1 * j) ^ xi_prime % M + 1
        q = (a2 * i + b2 * j^2) ^ yi_prime % N + 1
        # Use p and q for nonlinear scrambling
# Step 4:  Image Byte data
for i in len(M):
    for j in len(N):
        Genprime[i][j] = f(i, j)  # Use the nonlinearly byte data
# Step 5: Image Diffusion
s1 = floor(((key1 / x0) + (key2 / η)) * 50)
s = s1 + M * N
for i in range(M * N):
    ai = A[i]  # Use chaotic values
# Step 6: Chaotic Sequence Generation
for i in range(M * N):
    b[i] = IterateLogisticMap(x0, μ0, M * N)
# Step 7: Cyclic-Shift Function for Image Diffusion
for i in range(M * N):
    ci = floor(b[i] * 1e3) ^ Genprime[i] % 8
    D[i] = circshift(Genprime[i], ci)
# Step 8: Final Ciphertext Generation
for i in range(M * N):
    if i == 0:
        C[i] = Genprime[i] ^ Genprime[M * N - 1] ^ A[i] ^ B[i] ^ D[i]
    else:

        C[i] = Genprime[i] ^ C[i - 1] ^ A[i] ^ B[i] ^ D[i]
```

Initialization (Step 1): In this step, initial values x0, μ0, and η are calculated using the CalculateInitialValues function.

Chaotic Coordinates Generation (Step 2): This step involves generating chaotic coordinates xi_prime and yi_prime through the iteration of a logistic map equation. The coordinates are computed for various combinations of i and j within specified ranges.

Nonlinear Scrambling (Step 3): The generated coordinates xi_prime and yi_prime are used in nonlinear scrambling operations. Formulas involving a1, a2, b1, and b2 are applied to the coordinates, resulting in values p and q used for further processing.

Image Byte Data (Step 4): In this step, the array Genprime is populated with byte data obtained from a function f(i, j) applied to image coordinates i and j. This data likely represents information from an input image.

Image Diffusion (Step 5): Image diffusion is applied using variables like key1, key2, and A. The diffusion process involves calculations and iteration over a range of values, with the goal of dispersing and mixing the image data.

Chaotic Sequence Generation (Step 6): Chaotic sequences are generated using the logistic map function IterateLogisticMap. The generated sequences are stored in the array b and are likely used for introducing additional complexity into the encryption process.

Cyclic-Shift Function for Image Diffusion (Step 7): A cyclic-shift function is applied to the Genprime data based on values derived from the b array. This step likely involves rearranging or shuffling the image data to increase its security.

Final Ciphertext Generation (Step 8): In the final step, the ciphertext C is generated. This is achieved by applying various XOR operations involving the Genprime, A, B, and D data. The result is stored in the C array, which represents the encrypted or obfuscated output of the input image data.

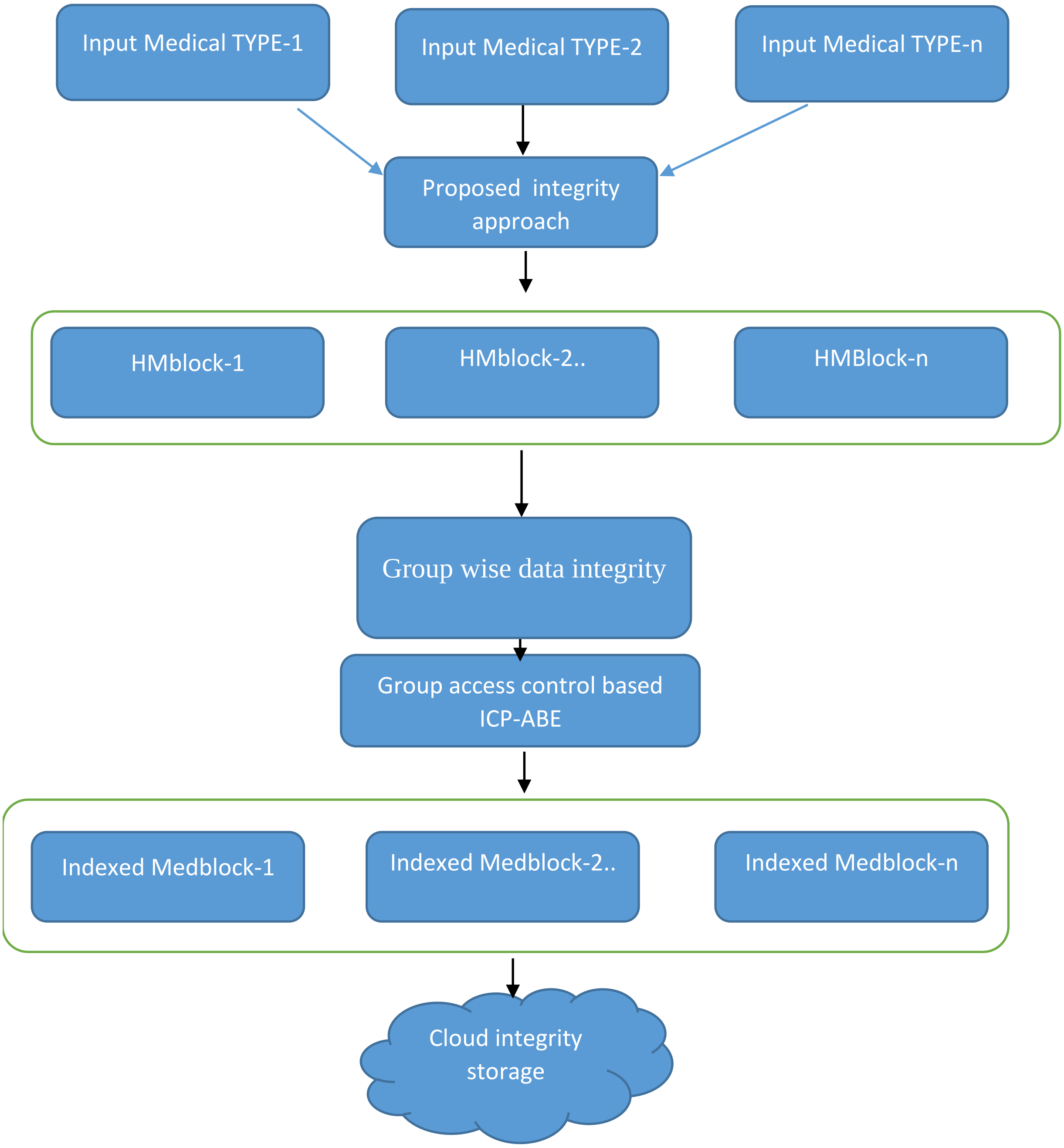


Figure 1: Overall GCP-ABE Framework

The proposed framework incorporates CP-ABE (Ciphertext-Policy Attribute-Based Encryption), a counterpart to KP-ABE (Key-Policy Attribute-Based Encryption), offering adaptability and serving as a core component in numerous other systems. Group users are permitted to pick anyone attribute or several other attributes from the list provided.

A. The framework comprises the subsequent stages:

Step 1: Initialization of Group-Wise Attributes

Applying the optimal integrity method, the framework inaugrates each group's features during the intial phase. The integrity algorithm uses and ideal hash function to ensure data security and integrity. Additionally, it provides group characteristics that are suitable for the best CP-ABE scheme, enabling attribute-based encryption to be accessed for the safe and adaptable access control.

Step 2: Grouping of Files

On using a compression feature, the framework adequatelly integrates files. By arranging files and reducing their size, the compression feature improves storage.

Step 3: Policy Definition for Each Group

The framework creates access policies for each set of files and characterisitics. Due to their integrety value, the properties are covered. These properties highlight the needs to be fullfilled so as to gain access to files in each group.The group qualities's are applied to carry out safguarding regulations.

Step 4: Generation of Unique Group ID

The framework generates a unique group ID for every set of files so as to make the implementation of ICP-ABE (Improved Ciphertext-Policy Attribute-Based Encryption) effortless.As a means to access the and enforce access contorl regulations , this ID is used as a sample.

Step 5: Secure Storage in the Cloud

Every set of file is encryted, generally with the help of an encrypter and securely placed in a cloud storage system.Encrypted data is safeguarded, ensuring the secrecy and integrity of the data, involving the compressed group of files and related properties.

Step 6: Decoding of Data Using Cipher Text and Policies

The framework enables lawful users to decode stored information using the correct access policies and correct cypher text when they need to access the information.Users are able to decrypt the data regain the authentic files by meeting the rules and regulations, ensuring safe and regulated data access.

B. Group wise data integrity:

This section introduces a novel approach for ensuring data integrity at the group level. A combined approach to integrity verification has been devised, calculating a distinct hash for each data encoding and decoding step. This method utilizes a series of complex mathematical transformations on the input data, as illustrated in Figure 2. Figure 2 describes the overall framework of group wise block chain data security using integrity and encryption models. These transformations play a crucial role in the computation of the hash value, ensuring the integrity and security of the data throughout the encoding and decoding processes.

```
1. Set the varibles, cloud_medical_data and blockchain.

2.For all groups of files in cloud_medical_data, follow these steps
    -A new block with different is to be created.
    -Assign the hash value of the latest block in the blockchain as the new identifier for the preceding block.
              - Set the block data to the current group of files and the block timestamp to the current time.
    - Compute the hash value of the block using a cryptographic hash function and save it within the block.
    -Append the data to the blockchain.

3.Divide the block data into k portions of equal size.

4.For each segment within the set of k, continue to.
     -Ensure the block data is of a consistent size by padding if needed.
    -Secure the block data by applying a symmetric encryption algorithm with a confidential key.
```

- Compute the hash of the encrypted block data using a cryptographic hash function, and then place it in the body.

-Append the securely encoded block information to the blockchain.

5. Iterate through steps 2 to 4 for every set of files within cloud_medical_data.

6. Safeguard the blockchain through a secure backup to mitigate the risk of data loss or unauthorized alterations.

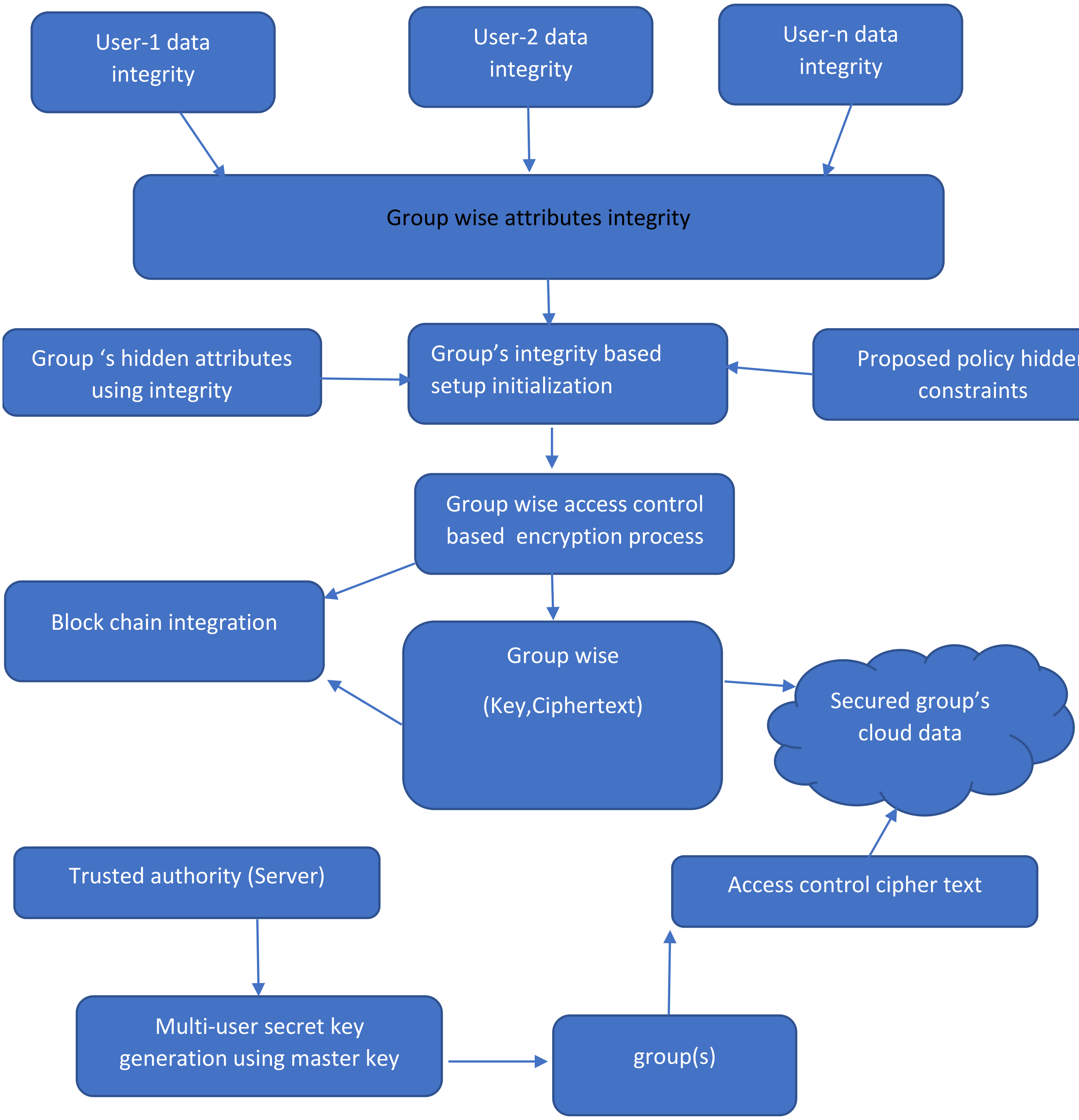

User-1 data integrity
User-2 data integrity
User-n data integrity
Group wise attributes integrity
Group 's hidden attributes using integrity
Group's integrity based setup initialization
Proposed policy hidden constraints
Group wise access control based encryption process
Block chain integration
Group wise (Key,Ciphertext)
Secured group's cloud data
Trusted authority (Server)
Access control cipher text
Multi-user secret key generation using master key
group(s)

Figure 2: Dynamic group integrity based CP-ABE Encryption Model for block chain framework

C. Multi-User Secret Key Generator:

1.*Multi-User Secret Key Generators* (MUSKG) are of great help during many situations, especially when it is to guarantee safe communication and data exchange among numerous parties. One of the benefits and scenario in which MUSKG can be useful are mentioned:

2. *Secure Communication*: In an environment involving numerous users, ensuring secure communication is crucial. MUSKG creates unique secret keys for each user, considering their roles or characteristics, enabling secure sharing of data and facilitating communication among users.

-

Calculate E P = P ⊕ H1(K2, σ k).
- Calculate K1' = ∏(ui^fi) = h^(K1f(α , P)), and K2' = ∏(vi^fi) = h^(K2f(α , P)).
- Issue the proto-ciphertext Cproto = {E P, K1', K2'}.
- An encryptor randomly chooses σm and σk in {0,1}^lσ.
- Define the access policy P.
- Invoke the method Proto_Encrypt to obtain Cproto = {E P, σk, K1', K2'}.
- Calculate rm = Hash(P, M, σm).
- Calculate Rm = (g^α)^(rm) = g^(αrm).
- Calculate K1m = (K1')^(rm) = h^(K1f(α, P)rm).
- Calculate K2m = (K2')^(rm) = h^(K2f(α, P)rm).
- Calculate C σ m = H2(e(g, h)^(rm)) ⊕ σ m, and Cm = H3(σ m) ⊕ M.
- Output the ciphertext C = {E P, σk, Rm, K1m, K2m, Cσm, Cm}.
- KeyGen_k accepts the master keys pair {MSK, MPK} and a random number ru as input.
- It returns a partial key su_k along with the access policy {Au,k} for a user u.
- Define the access policy Au,k for the user u.
- Calculate f(α , Au,k) = ∏(x + H4(i))^(1 - ai,k).
- Calculate su_k = (1/K1)^(1/N) ∏(j ≠ k) PRF_jk(ru) / f(α , Au,k).
- Output {su_k, Au,k}.

The protocol begins with "Step PE1," where a semi-trusted assisting cloud calculates an access policy denoted as P, which consists of a series of parameters p1, p2, up to pn. This access policy is used to define a polynomial function f(x, P), where each coefficient fi corresponds to different powers of x, and it has a degree of at most n.In "Step PE2," the cloud computes E(P), which is the result of combining the access policy P with another parameter, H1(K2, σk). Additionally, it calculates two values, K1' and K2', by raising specific elements to the powers determined by the polynomial function f(x, P). These values are used for further encryption.A proto-ciphertext Cproto is issued, containing E(P), K1', and K2'.In the "Encrypt phase," the process is carried out by an encryptor who selects random values σm and σk. With the help of a semi-trusted helping cloud, the cipher creator formulates an entry protocol P and addresses it as the Proto_Encrypt function. Through this method, a proto-ciphertext Cproto with E(P), σk, K1', and K2' is generated. Then, by using a hash function on P, M (the plaintext message), and σm, the encryption determines rm. In addition to calculating Rm, K1m, and K2m—all aiding in the encryption process—it also makes use exponentiation with K1' and K2'. According with these computations, Cσm and Cm are acquired, that generate the ciphertext components by combining data from group elements and using extra hash functions. At last, the ciphertext C is assembled, including E(P), σk, Rm, K1m, K2m, Cσm, and Cm.

Setup:

A pairing-friendly elliptic curve's group G is created randomly following the selection of a security parameter. Within G, select a generator (g) at random.

- Compute g^x, it being the master public key (MPK) corresponding to a randomly generated number x
- Compute g^y, that refers to the master secret key (MSK) in the context of a provided random number, y.

Key Generation:

- Select a series of attributes A.
- To find g^z, that is the user's public key (UPK), pick a random number z.
- Calculate the user's secret key (USK) as (g^x)^z * (g^y)^(Hash(A)).

Encryption:

- decipher the set of files, select a combination of group characteristics A.
- Pick an integer r randomly and compute g^r, the encryption key.
- With the help of the encryption key and the collection of attributes A, encrypt the group files m. The graphical illustration of the ciphertext is (g^r, m*(g^r) ^(Hash(A))).

Decryption:

- Using the secret key of the user,compute (g^r)^(Hash(A)).
- To obtain the original set of files, divide the ciphertext by the calculated value.

Step 1: Initialization of Groupwise Attributes and Data Files

During this phase, the data files and the collection of group-specific attributes are initialized. he data files contain the information requiring encryption and storage on the blockchain, with these attributes representing the characteristics or qualities associated with each category.

Step 2: Compute Integrity for Each Group Attributes List

At this phase, the computation of the integrity for each group's attribute list is carried out. Utilizing a suitable approach or method to ensure the precision, reliability, and security of attributes is integral to the integrity assessment.

Step 3: Perform Indexing Approach

During this phase, the data is effectively arranged and supervised using an indexing method. Indexing facilitates the quicker and more convenient retrieval of specific data items from the group list.

Step 4: For Each File in the Group List

The actions below are taken for every file in the group list:

Step 5: Perform ICP-ABE Scheme

The information within the file is safeguarded through the utilization of the ICP-ABE (Enhanced Ciphertext-Policy Attribute-Based Encryption) system. By employing this method, access control based on attributes becomes feasible; decryption of a file is only permitted when the user's attributes align with the access policy designated for that specific file.

Step 6: Add Hash and Encoded Data to the Blockchain

The encoded information of the file and the approximated hash value are added to the blockchain. While the encoded data ensures the safety and secrecy of the contents of file , the hash value serves as a unique identification and integrity check for the file.

Step 7: Store in Cloud Server

A cloud server stores the completed blockchain, containing both hash values and encoded file contents. The hash value serves as a distinctive identifier and integrity verification for the file contents. To guarantee the availability and integrity of data, the cloud server provides a scalable and secure setting for the storage and retrieval of blockchain information.

D. *Generating Unique-ID*

The "generateUniqueId" function is designed to create a distinctive identifier for a file based on its size, the timestamp of its latest modification, and its file path. The function operates in the following manner:

The UniqueId variable is initialized with a null value. The function, within a try-catch block, generates a distinctive data string that characterizes the file. This is achieved by concatenating the file location, size, and the most recent modification timestamp. The ProposedHash() function is subsequently employed, with the expectation that it will generate a 4096-bit message digest. An unspecified hashing algorithm is employed to hash the data string, aiming to produce the digest. Following this, the resulting hash is transformed into a hexadecimal character representation, establishing the intended unique identification for the file. This is accomplished as the code iterates through the hash, converting each byte into a string of hexadecimal charactersFurthermore, it ensures the consistent length of the hexadecimal representation for each byte by adding a leading '0' when necessary. In conclusion, the resultant hexadecimal string is assigned to the variable uniqueId. The code outputs the stack trace and handles the exception in case of a NoSuchAlgorithmException. Ultimately, the function yields the uniqueId, which serves as the distinct identifier for the file and is derived from its size, last modified timestamp, and file path. The resulting unique ID can serve various purposes, such as system indexing or file identification.

```
function generateUniqueId(filePath, fileSize, lastModified):
    uniqueId = null
    try:
        // Concatenate file path, size, and last modified timestamp
        data = concatenate(filePath, fileSize, lastModified)
        // Create a 4096 bit message digest
        digest = ProposedHash();
hash = digest.digest(data.getBytes())
hexString = ""
for byte b in hash:
hex = convertToHexString(b)
hexString += hex.length() == 1 ? '0' : ''
hexString += hex"
        // Set the generated unique ID
        uniqueId = hexString
    catch NoSuchAlgorithmException e:
        e.printStackTrace()
    return uniqueId
```

IV. EXPERIMENTAL RESULTS

A. *Infrastructure Setup:*

To duplicate the cloud-based Electronic Health Record (EHR) system, establish a Java environment on a live cloud server. A feasible approach is to utilize a cloud service provider like Google Cloud Platform (GCP), Microsoft Azure, or Amazon Web Services (AWS).

B. *Data Generation:*

Generate sample data resembling an Electronic Health Record (EHR), ensuring it includes diverse health-related information such as treatment records, patient demographics, medical histories, and sensitive details like prescribed medications and diagnoses.

C. Encryption and Decryption Algorithms:

Data Encryption:

Implement the selected encryption algorithm(s) on the generated Electronic Health Record (EHR) data.

Record the duration required to complete encryption for individual data pieces.

Data Decryption:

Decrypt the EHR data using appropriate decryption algorithm(s).

Measure the time it takes to perform decryption for each piece of data.

D. Overhead Measurement:

Calculate the overhead for each piece of encrypted data. This involves determining the size difference between the ciphertext (encrypted data) and the original plaintext (unencrypted data).

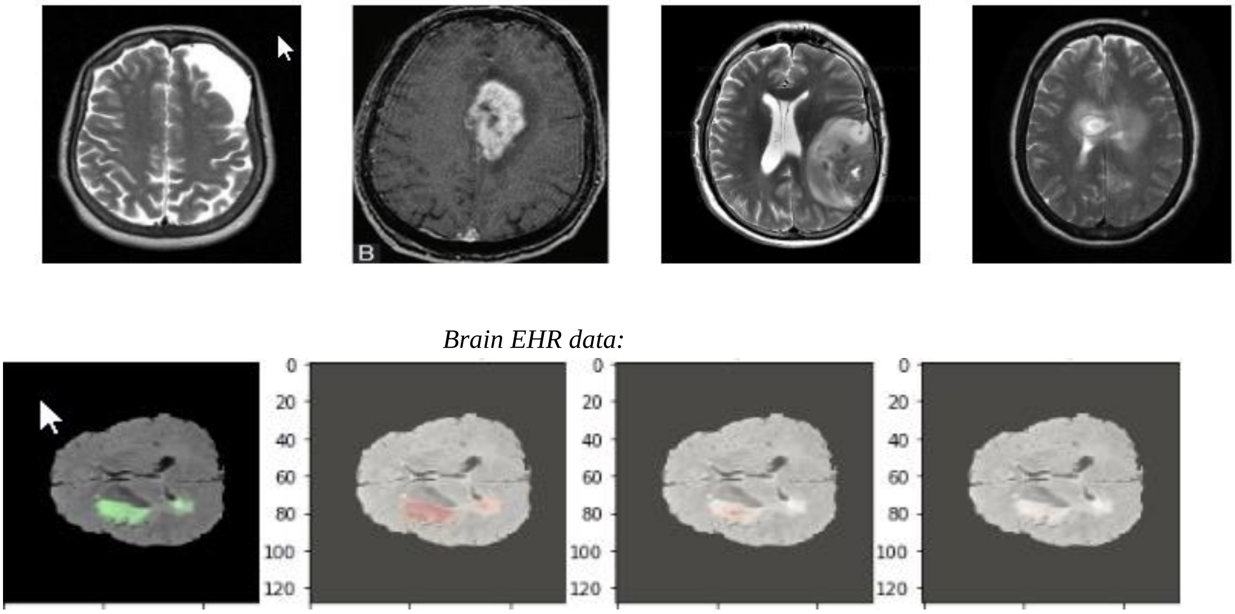
E. Access Control Implementation:

Implement access control mechanisms to ensure that only authorized entities can access and modify the EHR data on the blockchain. Define roles and permissions for different user types (e.g., healthcare providers, patients, administrators) and evaluate how well the system enforces these access controls.

F. Transaction Throughput Testing:

Simulate a load on the system by sending a high volume of transactions (e.g., EHR updates, queries) to the blockchain. Measure the number of transactions the system can handle per second (transaction throughput).

Analyze the impact of encryption/decryption on transaction throughput.



Sample EHR data:Brain EHR data1

Brain EHR data:

Figure 3: Sample brain tumor HER records

SpinalCord EHR data

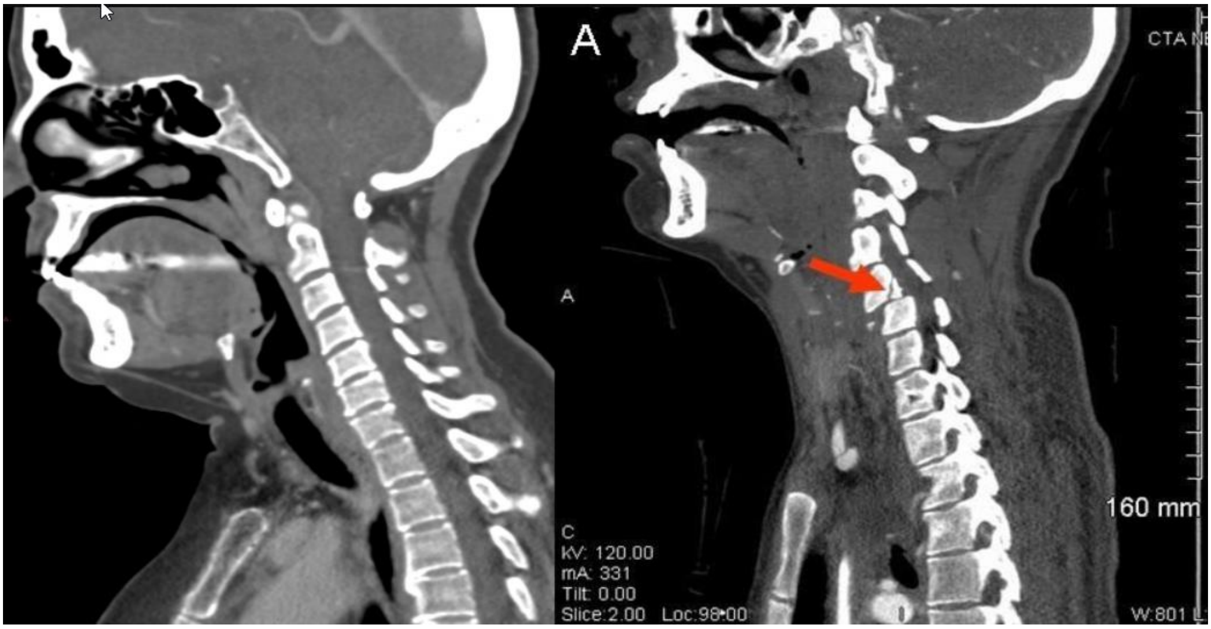


Figure 4: Sample spinal cord 3D image

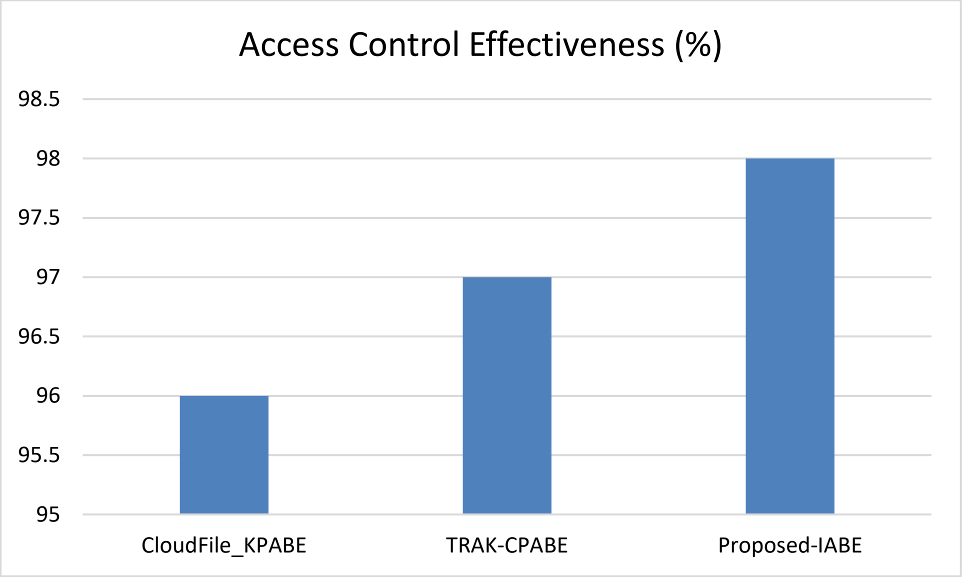


Figure 5: Comparative Evaluation of Proposed Access Control Efficiency Against Existing Models for Blockchain Multi-User Cloud Data Security.

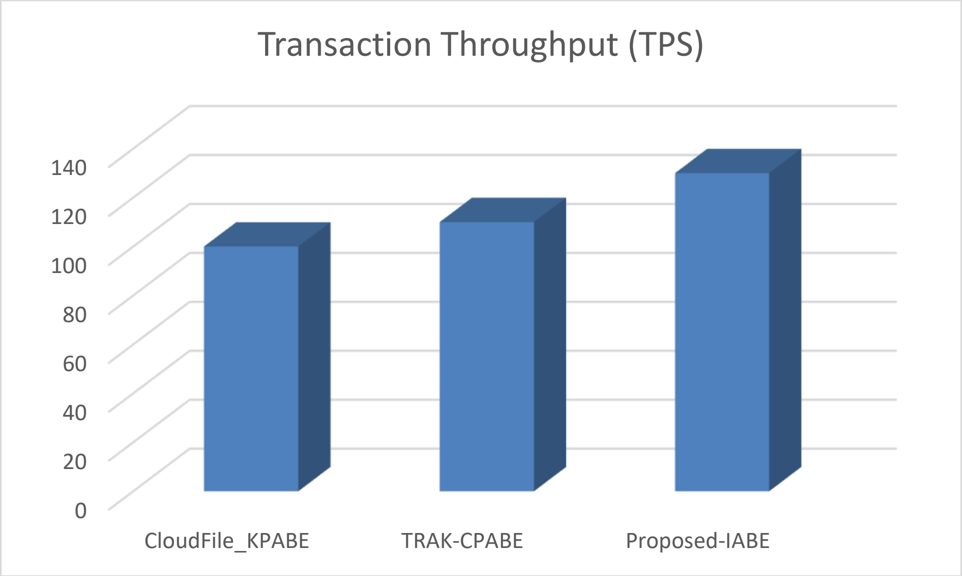


Figure 6: Comparative Evaluation of Proposed transaction throughput (TPS) Against Existing Models for Blockchain Multi-User Cloud Data Security.

G. Salt and pepper noise

Table 1: Comparative analysis of three different Attribute-Based Encryption (ABE) schemes -- CloudFile_KPABE, TRAK-CPABE, and Proposed-IABE in handling salt and pepper noise, across various groups.

Group No	*CloudFile_KPABE*	*TRAK-CPABE*	*Proposed-IABE*
10	0.80269	0.76738	0.918134
20	0.702066	0.64543	0.892846
30	0.787163	0.730372	0.82514
40	0.905333	0.948311	0.948495
50	0.934487	0.920195	0.944699
60	0.697838	0.866959	0.932965
70	0.603412	0.782376	0.793362
80	0.72793	0.839403	0.913018
90	0.877123	0.61297	0.906717
100	0.867721	0.882841	0.925247

Table 1, describes the Comparative analysis of three different Attribute-Based Encryption (ABE) schemes -- CloudFile_KPABE, TRAK-CPABE, and Proposed-IABE in handling salt and pepper noise, across various groups. for various Medical data.

Table 2: Comparative analysis of proposed IABE model to traditional approaches Cloudfile_KABE and TRAK-CPABE using average encryption and decryption runtime(ms) with different group size for medical 3D spinal data

Group No	*CloudFile_KPABE*	*TRAK-CPABE*	*Proposed-IABE*
10	2234	2105	2017
20	2405	2077	2047
30	2464	2138	2037
40	2392	2440	2197
50	2490	2143	2131

Table 2, describes the Comparative analysis of proposed IABE model to traditional approaches such as Cloudfile_KABE and TRAK-CPABE for runtime computation of encryption and decryption process for Input 2d Medical data. In the table, proposed-IABE approach has better average runtime(ms) of the conventional methods with different communication group sizes. Here, each group is constructed from the subset of attributes in the IABE scheme.

Table 3: Comparative analysis of proposed IABE model to traditional approaches Cloudfile_KABE and TRAK-CPABE using average encryption and decryption runtime(ms) with different group size for medical 3D brain data

Group No	*CloudFile_KPABE*	*TRAK-CPABE*	*Proposed-IABE*
10	2172	2061	2051
20	2030	2423	2008
30	2172	2279	2151
40	2218	2287	2079
50	2021	2315	2020

Table 3, describes the Comparative analysis of proposed IABE model to traditional approaches such as Cloudfile_KABE and TRAK-CPABE for runtime computation of encryption and decryption process for Input 2d Medical data. In the table, proposed-IABE approach has better average runtime(ms) of the conventional methods with different communication group sizes. Here, each group is constructed from the subset of attributes in the IABE scheme.

Table 4: Comparative analysis of proposed IABE model to traditional approaches Cloudfile_KABE and TRAK-CPABE using average encryption and decryption runtime(ms) with different group size for medical 2D brain data

Group No	*CloudFile_KPABE*	*TRAK-CPABE*	*Proposed-IABE*
10	2257	2034	2020
20	2422	2102	2082
30	2016	2419	2006
40	2479	2313	2254
50	2213	2315	2088

Table 4, describes the Comparative analysis of proposed IABE model to traditional approaches such as Cloudfile_KABE and TRAK-CPABE for runtime computation of encryption and decryption process for Input 2d Medical data. In the table, proposed-IABE approach has better average runtime(ms) of the conventional methods with different communication group sizes. Here, each group is constructed from the subset of attributes in the IABE scheme.

A good hash function exhibits what's known as the avalanche effect, where a small change to the input should result in a drastic change in the output. Ideally, flipping a single bit of the input should result in each bit of the output flipping with a 50% probability. Collision resistance is a property of a hash function that it is hard to find two different inputs that hash to the same output. Every bit of the hash output should depend on every bit of the input, to make it difficult to find two distinct inputs that hash to the same value.

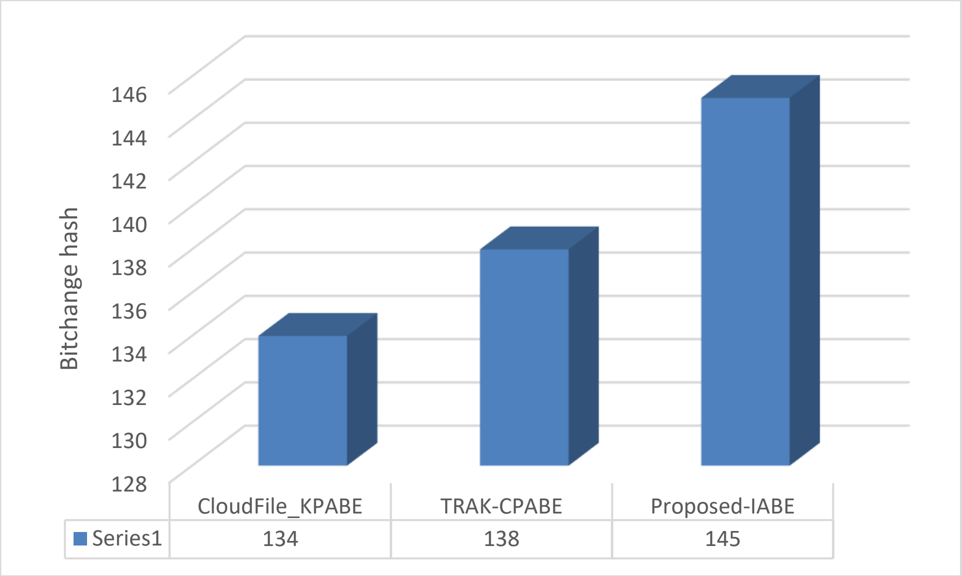


Figure 7: Comparative analysis of proposed IABE model to traditional approaches Cloudfile_KABE and TRAK-CPABE using average bit variation with different group size for all medical data

V. CONCLUSION

This study introduced a complete framework to improve data security in medical applications hosted on the cloud. The system included initiating group-specific attributes with an optimal integrity algorithm, effectively organizing files using compression functions, defining access control policies, creating unique group IDs, encoding with encryption for secure storage in cloud systems, and decoding data using cipher text and access policies. By using attribute-based encryption and the groupwise integrity Ciphertext-Policy Attribute-Based Encryption (GICP-ABE) scheme, the system ensures secure and adaptable access control for medical data. The results from the experiment showed that the suggested framework is more efficient and effective when compared to conventional methods. The system tackles the difficulties of maintaining the integrity of group data, handling data of variable sizes, and ensuring secure group access to medical data in cloud environments. The suggested method plays a role in improving the security, confidentiality, and integrity of medical data, opening avenues for enhanced blockchain-based medical applications on the cloud.

REFERENCES

[1] M. Kumaresan, R. Gopal, M. Mathivanan, and T. Poongodi, “13 - Amalgamation of blockchain, IoT, and 5G to improve security and privacy of smart healthcare systems,” in Blockchain Applications for Healthcare Informatics, S. Tanwar, Ed., Academic Press, 2022, pp. 283–312. doi: 10.1016/B978-0-323-90615-9.00015-3.

[2] Mrs. U. Chelladurai, Dr. S. Pandian, and Dr. K. Ramasamy, “A blockchain based patient centric electronic health record storage and integrity management for e-Health systems,” Health Policy and Technology, vol. 10, no. 4, p. 100513, Dec. 2021, doi: 10.1016/j.hlpt.2021.100513.

[3] A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, “A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF),” Neuroscience Informatics, vol. 2, no. 1, p. 100030, Mar. 2022, doi: 10.1016/j.neuri.2021.100030.

[4] I. Taloba et al., “A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare,” Alexandria Engineering Journal, vol. 65, pp. 263–274, Feb. 2023, doi: 10.1016/j.aej.2022.09.031.

[5] X. Yang, J. Wang, W. Xi, T. Tian, and C. Wang, “A blockchain-based keyword search scheme with dual authorization for electronic health record sharing,” Journal of Information Security and Applications, vol. 66, p. 103154, May 2022, doi: 10.1016/j.jisa.2022.103154.

[6] K. Hasan, M. J. M. Chowdhury, K. Biswas, K. Ahmed, Md. S. Islam, and M. Usman, “A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks,” Computer Networks, vol. 211, p. 109004, Jul. 2022, doi: 10.1016/j.comnet.2022.109004.

[7] L. Lodha, V. S. Baghela, J. Bhuvana, and R. Bhatt, “A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring,” Measurement: Sensors, vol. 30, p. 100904, Dec. 2023, doi: 10.1016/j.measen.2023.100904.

[8] J. Sengupta, S. Ruj, and S. Das Bit, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” Journal of Network and Computer Applications, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[9] M. Ali, L. Tang Jung, A. Hassan Sodhro, A. Ali Laghari, S. Birahim Belhaouari, and Z. Gillani, “A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security,” Alexandria Engineering Journal, vol. 64, pp. 749–760, Feb. 2023, doi: 10.1016/j.aej.2022.10.056.

[10] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, “A lightweight blockchain and fog-enabled secure remote patient monitoring system,” Internet of Things, vol. 22, p. 100691, Jul. 2023, doi: 10.1016/j.iot.2023.100691.

[11] S. Barbaria, H. Mahjoubi, and H. B. Rahmouni, “A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case,” Procedia Computer Science, vol. 219, pp. 1436–1443, Jan. 2023, doi: 10.1016/j.procs.2023.01.433.

[12] N. Sharma and R. Rohilla, “A novel Hyperledger blockchain-enabled decentralized application for drug discovery chain management,” Computers & Industrial Engineering, vol. 183, p. 109501, Sep. 2023, doi: 10.1016/j.cie.2023.109501.

[13] S. Tiwari, N. Dhanda, and H. Dev, “A real time secured medical management system based on blockchain and internet of things,” Measurement: Sensors, vol. 25, p. 100630, Feb. 2023, doi: 10.1016/j.measen.2022.100630.

[14] 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.

[15] Garrido, L. J. Ramírez López, and N. B. Álvarez, “A simulation-based AHP approach to analyze the scalability of EHR systems using blockchain technology in healthcare institutions,” Informatics in Medicine Unlocked, vol. 24, p. 100576, Jan. 2021, doi: 10.1016/j.imu.2021.100576.

[16] M. S. Rahman, M. A. Islam, M. A. Uddin, and G. Stea, “A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges,” Internet of Things, vol. 19, p. 100551, Aug. 2022, doi: 10.1016/j.iot.2022.100551.

[17] R. Mukta, H. Paik, Q. Lu, and S. S. Kanhere, “A survey of data minimisation techniques in blockchain-based healthcare,” Computer Networks, vol. 205, p. 108766, Mar. 2022, doi: 10.1016/j.comnet.2022.108766.

[18] N. Deepa et al., “A survey on blockchain for big data: Approaches, opportunities, and future directions,” Future Generation Computer Systems, vol. 131, pp. 209–226, Jun. 2022, doi: 10.1016/j.future.2022.01.017.

[19] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, “A Survey on Role of Blockchain for IoT: Applications and Technical Aspects,” Computer Networks, vol. 227, p. 109726, May 2023, doi: 10.1016/j.comnet.2023.109726.

[20] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A survey on the adoption of blockchain in IoT: challenges and solutions,” Blockchain: Research and Applications, vol. 2, no. 2, p. 100006, Jun. 2021, doi: 10.1016/j.bcra.2021.100006.

[21] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, “A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine,” Healthcare Analytics, vol. 3, p. 100192, Nov. 2023, doi: 10.1016/j.health.2023.100192.

[22] P. Hegde and P. K. R. Maddikunta, “Amalgamation of Blockchain with resource-constrained IoT devices for healthcare applications – State of art, challenges and future directions,” International Journal of Cognitive Computing in Engineering, vol. 4, pp. 220–239, Jun. 2023, doi: 10.1016/j.ijcce.2023.06.002.

[23] S. Mohan M and L. Sujihelen, “An efficient chain code for access control in hyper ledger fabric healthcare system,” e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 5, p. 100204, Sep. 2023, doi: 10.1016/j.prime.2023.100204.

[24] H. Naser Alsuqaih, W. Hamdan, H. Elmessiry, and H. Abulkasim, “An efficient privacy-preserving control mechanism based on blockchain for E-health applications,” Alexandria Engineering Journal, vol. 73, pp. 159–172, Jul. 2023, doi: 10.1016/j.aej.2023.04.037.

[25] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, “Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey,” Computers & Security, vol. 97, p. 101966, Oct. 2020, doi: 10.1016/j.cose.2020.101966.

[26] H. Malik, T. Anees, M. Faheem, M. U. Chaudhry, A. Ali, and M. N. Asghar, “Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions,” Internet of Things, vol. 23, p. 100860, Oct. 2023, doi: 10.1016/j.iot.2023.100860.

[27] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, “Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications,” Journal of Information Security and Applications, vol. 56, p. 102673, Feb. 2021, doi: 10.1016/j.jisa.2020.102673.

[28] M. Sookhak, M. R. Jabbarpour, N. S. Safa, and F. R. Yu, “Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues,” Journal of Network and Computer Applications, vol. 178, p. 102950, Mar. 2021, doi: 10.1016/j.jnca.2020.102950.

[29] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, “Blockchain and Smart Healthcare Security: A Survey,” Procedia Computer Science, vol. 175, pp. 615–620, Jan. 2020, doi: 10.1016/j.procs.2020.07.089.

[30] Keshta et al., “Blockchain aware proxy re-encryption algorithm-based data sharing scheme,” Physical Communication, vol. 58, p. 102048, Jun. 2023, doi: 10.1016/j.phycom.2023.102048.

[31] D. Ramesh, R. Mishra, P. K. Atrey, D. R. Edla, S. Misra, and L. Qi, “Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage,” Alexandria Engineering Journal, vol. 68, pp. 205–226, Apr. 2023, doi: 10.1016/j.aej.2023.01.012.

[32] Singh Chouhan, M. Sanaullah Qaseem, Q. Mohammed Abdul Basheer, and Ms. Asma Mehdia, “Blockchain based EHR system architecture and the need of blockchain inhealthcare,” Materials Today: Proceedings, vol. 80, pp. 2064–2070, Jan. 2023, doi: 10.1016/j.matpr.2021.06.114.

[33] T. Benil and J. Jasper, “Blockchain based secure medical data outsourcing with data deduplication in cloud environment,” Computer Communications, vol. 209, pp. 1–13, Sep. 2023, doi: 10.1016/j.comcom.2023.06.013.

[34] J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, “Blockchain for healthcare systems: Architecture, security challenges, trends and future directions,” Journal of Network and Computer Applications, vol. 215, p. 103633, Jun. 2023, doi: 10.1016/j.jnca.2023.103633.

[35] E. M. Adere, “Blockchain in healthcare and IoT: A systematic literature review,” Array, vol. 14, p. 100139, Jul. 2022, doi: 10.1016/j.array.2022.100139.

[36] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, “Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0,” Internet of Things and Cyber-Physical Systems, vol. 3, pp. 309–322, Jan. 2023, doi: 10.1016/j.iotcps.2023.05.006.

[37] S. Singh, S. Kumar Sharma, P. Mehrotra, P. Bhatt, and M. Kaurav, “Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives,” Materials Today: Proceedings, vol. 62, pp. 5042–5046, Jan. 2022, doi: 10.1016/j.matpr.2022.04.998.

[38] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, “Blockchain technology in the healthcare industry: Trends and opportunities,” Journal of Industrial Information Integration, vol. 22, p. 100217, Jun. 2021, doi: 10.1016/j.jii.2021.100217.

[39] S. Singh, B. Pankaj, K. Nagarajan, N. P. Singh, and V. Bala, “Blockchain with cloud for handling healthcare data: A privacy-friendly platform,” Materials Today: Proceedings, vol. 62, pp. 5021–5026, Jan. 2022, doi: 10.1016/j.matpr.2022.04.910.

[40] Tomar, N. Gupta, D. Rani, and S. Tripathi, “Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system,” Internet of Things, vol. 23, p. 100849, Oct. 2023, doi: 10.1016/j.iot.2023.100849.

[41] X. Xiang and X. Zhao, “Blockchain-assisted searchable attribute-based encryption for e-health systems,” Journal of Systems Architecture, vol. 124, p. 102417, Mar. 2022, doi: 10.1016/j.sysarc.2022.102417.

[42] EL Azzaoui, P. K. Sharma, and J. H. Park, “Blockchain-based delegated Quantum Cloud architecture for medical big data security,” Journal of Network and Computer Applications, vol. 198, p. 103304, Feb. 2022, doi: 10.1016/j.jnca.2021.103304.

[43] 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.

[44] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” Journal of Information Security and Applications, vol. 50, p. 102407, Feb. 2020, doi: 10.1016/j.jisa.2019.102407.

[45] Z. Liu, S. Wang, and Y. Liu, “Blockchain-based integrity auditing for shared data in cloud storage with file prediction,” Computer Networks, vol. 236, p. 110040, Nov. 2023, doi: 10.1016/j.comnet.2023.110040.

[46] Y. Gao, A. Zhang, S. Wu, and J. Chen, “Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing,” High-Confidence Computing, vol. 2, no. 4, p. 100084, Dec. 2022, doi: 10.1016/j.hcc.2022.100084.

[47] G. Zhang, Z. Yang, and W. Liu, “Blockchain-based privacy preserving e-health system for healthcare data in cloud,” Computer Networks, vol. 203, p. 108586, Feb. 2022, doi: 10.1016/j.comnet.2021.108586.

[48] Sheela and C. Priya, “Blockchain-based security & privacy for biomedical and healthcare information exchange systems,” Materials Today: Proceedings, vol. 81, pp. 641–645, Jan. 2023, doi: 10.1016/j.matpr.2021.04.105.

[49] M. R. Dorsala, V. N. Sastry, and S. Chapram, “Blockchain-based solutions for cloud computing: A survey,” Journal of Network and Computer Applications, vol. 196, p. 103246, Dec. 2021, doi: 10.1016/j.jnca.2021.103246.

[50] Z. H. Mohammed, K. Chankaew, R. R. Vallabhuni, V. R. Sonawane, S. Ambala, and M. S, “Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records,” Measurement: Sensors, vol. 26, p. 100706, Apr. 2023, doi: 10.1016/j.measen.2023.100706.

[51] Y. Zhang, X. Wei, J. Cao, J. Ning, Z. Ying, and D. Zheng, “Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, Part A, pp. 8350–8361, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.015.

[52] M. Chen et al., “Blockchain-Enabled healthcare system for detection of diabetes,” Journal of Information Security and Applications, vol. 58, p. 102771, May 2021, doi: 10.1016/j.jisa.2021.102771.

[53] H.-B. How and S.-H. Heng, "Blockchain-Enabled Searchable Encryption in Clouds: A Review," Journal of Information Security and Applications, vol. 67, p. 103183, Jun. 2022, doi: 10.1016/j.jisa.2022.103183.

[54] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, and E. Oropallo, "Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem," Technovation, vol. 120, p. 102480, Feb. 2023, doi: 10.1016/j.technovation.2022.102480.

[55] M. A. Saberi, M. Adda, and H. Mcheick, "Break-Glass Conceptual Model for Distributed EHR management system based on Blockchain, IPFS and ABAC," Procedia Computer Science, vol. 198, pp. 185–192, Jan. 2022, doi: 10.1016/j.procs.2021.12.227.

[56] Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "ChainSure: Agent free insurance system using blockchain for healthcare 4.0," Intelligent Systems with Applications, vol. 17, p. 200177, Feb. 2023, doi: 10.1016/j.iswa.2023.200177.

[57] Pampattiwar and P. Chavan, "Chapter 4 - Security and privacy facets of electronic health record," in Unleashing the Potentials of Blockchain Technology for Healthcare Industries, M. M. Ghonge, P. N., A. Das, Y. Wu, and O. Pal, Eds., Academic Press, 2023, pp. 59–75. doi: 10.1016/B978-0-323-99481-1.00006-7.

[58] N. Parekh and R. Mangrulkar, "Chapter 5 - Enabling blockchain architecture for health information exchanges," in Unleashing the Potentials of Blockchain Technology for Healthcare Industries, M. M. Ghonge, P. N., A. Das, Y. Wu, and O. Pal, Eds., Academic Press, 2023, pp. 77–93. doi: 10.1016/B978-0