शोध आलेख / Research Article

ब्लॉकचेन तकनीक का उपयोग करके स्वास्थ्य संबंधी सूचना विनिमय प्रणालियों की सुरक्षा और गोपनीयता

Security & Privacy of Healthcare Information Exchange System Using Blockchain Technology

गरिमा माथुर[1], अंजना पांडेय[2], सचिन गोयल[3]

Garima Mathur[1], Anjana Pandey[2] , Sachin Goyal[3]

[1]Dept of CSE, UIT RGPV, Bhopal,

[2, 3] Dept of IT, UIT RGPV, Bhopal,

[1]garima41mathur@gmail.com, [2]anjanapandey@rgtu.net, [3]sachingoyal@rgtu.net

सारांशः

रोग ग्रस्त व्यक्तियों की संख्या में निरंतर वृद्धि के साथ, स्वास्थ्य सेवा प्रदाताओं को नियमित आधार पर स्वास्थ्य सुरक्षा डेटा की बढ़ती संख्या का प्रबंधन करने की आवश्यकता है। जैसे–जैसे सूचना की मात्रा हर साल बढ़ेगी, अस्पतालों और क्लीनिकों के लिए सूचनाओं को संसाधित करना और स्टोर करना कठिन हो जायेगा। स्वास्थ्य सेवा संगठनों द्वारा प्रबंधित डेटा में बीमा दावा डेटा और IOT उपकरणों से एकत्र किए गए जैसे कई प्रकार के डेटा शामिल हैं। उचित चिकित्सा सेवाओं को सुनिश्चित करने के लिए एक सुरक्षित सूचना साझा करने की रणनीति होना महत्वपूर्ण है जो स्वास्थ्य सेवा प्रदाताओं और उनकी कवर की गई संस्थाओं दोनों के रिकॉर्ड की शुद्धता को सत्यापित करने की अनुमति दे सके। इसमें ब्लॉकचेन तकनीकी लाभकारी रूप से उपलब्ध है, क्योंकि इसका एक मुख्य लाभ डेटा अखंडता है। जब जानकारी को रिकॉर्ड और एन्क्रिप्ट किया जाता है, तो उसका आदान–प्रदान करना या उसे हटाना असंभव हो जाता है। ब्लॉकचेन का उपयोग करने का एक अन्य लाभ उन लोगों के समूहों के लिए है जो एक दूसरे पर भरोसा नहीं करते हैं, लेकिन फिर भी एक विश्वसनीय तृतीय–पक्ष को शामिल किए बिना डेटा साझा करना चाहते हैं, उनके लिए ब्लॉकचेन सबसे उपयुक्त समाधान होगा। इस पत्र में, हमने बताया है कि ब्लॉकचेन की कार्यप्रणाली, स्वास्थ्य देखभाल में इसकी आवश्यकता और ब्लॉकचेन प्रौद्योगिकी का उपयोग करके जैव चिकित्सा और स्वास्थ्य सूचना विनिमय प्रणाली में सुरक्षा और गोपनीयता कैसे प्राप्त की जा सकती है।

Abstract:

With an ongoing increase in sick person numbers, healthcare providers need to manage an increasing number of healthcare data on a regular basis. As the information volume will increase each year, it turns into tougher for hospitals and clinics to process and store information. Data managed by healthcare organizations include insurance claim data and data gathered from IOT devices. For ensuring proper medical services it is important to have a secure information sharing strategies that can permit both healthcare providers and their covered entities to verify the correctness of record. This is in which blockchain is available in beneficial, as one of its main advantages is data integrity. When information is recorded and encrypted, it becomes impossible to exchange or do away with. Another advantage of using blockchain is for those groups of people who don't trust one another but still want to share data without including a trusted third-party for them blockchain would

be most appropriate solution. In this paper, we have explained the working of blockchain, its need in healthcare and how security and privacy can be achieved in biomedical and healthcare information exchange system using blockchain technology.

मुख्यशब्दः ब्लॉकचेन, बायोमेडिकल, स्वास्थ्य सेवा, Distributed Ledger, क्रिप्टोग्राफिक हैश।

Keywords : Blockchain, biomedical, healthcare, Distributed Ledger, cryptographic hash.

प्रस्तावना

ब्लॉकचेन एक ऐसी तकनीक है जो जानकारी को पीयर–टू–पीयर (P 2 P) आधार पर स्टोर और आदान–प्रदान करने में सक्षम बनाती है। ब्लॉकचैन तकनीक द्वारा रिकॉर्ड को तीसरे पक्ष की आवश्यकता के बिना सुरक्षित रूप से साझा किया जा सकता है

ब्लॉकचैन प्रौद्योगिकी की कई अवधारणाओं में ट्रुस्ट्–एन्फोर्केद सिक्युरिटी को प्राथमिक माना जाता है। एल्गोरिथ्म में ब्लॉकों की एक अनंत श्रृंखला होती है जो इसे अधिक सुरक्षित बनाती है और हमलावरों के लिए इसे बदलना मुश्किल बनाती है।

सबसे सरल शब्दों में, ब्लॉकचेन कंप्यूटर के एक समूह द्वारा प्रबंधित अपरिवर्तनीय रिकॉर्ड का एक क्रम है जिसे किसी एक सिस्टम द्वारा नियंत्रित नहीं किया जाता है। सूचना के इन ब्लॉकों को क्रिप्टोग्राफिक हैश की मदद से एक साथ जोड़ा जाता है।

इसके बारे में असाधारण बात यह है कि ब्लॉकचैन नेटवर्क का कोई केंद्रीय अधिकार नहीं है। इसमें डेटा सभी के लिए खुला है क्योंकि इसमें डेटा विकेंद्रीकृत है। इसमें जो लोग शामिल हैं, वे अपनी गतिविधियों के लिए जिम्मेदार हैं और जो लोग इस पर आधारित हैं वे अपने स्वभाव से पारदर्शी हैं।

प्रेरणा

ब्लॉकचेन में, डेटा सभी के लिए एक आम डेटाबेस के रूप में मौजूद होता है। ब्लॉकचैन डेटाबेस किसी एक स्थान पर स्टोर नहीं होता है; रिकॉर्ड खुले और आसानी से सत्यापित किए जाते हैं। हैकर्स इस जानकारी को बदल नहीं कर सकते क्योंकि इसका कोई केंद्रीकृत संस्करण उपलब्ध नहीं है। नीचे ब्लॉकचेन की प्रशंसा के कुछ कारण दिए गए हैं–

- यह अपने स्वभाव से विकेंद्रीकृत होता है क्योंकि यह एक सिस्टम के पास नहीं होता है।
- यह क्रिप्टोग्राफिक रूप में जानकारी स्टोर करता है।
- यह डेटा को अपरिवर्तनीय बनाता है, ताकि कोईभी ब्लॉकचेन के अंदर की जानकारी से छेड़छाड़ न कर सके।
- ब्लॉकचेन के अंदर के डेटा को ट्रैक किया जा सकता है क्योंकि यह पारदर्शी है।

ब्लॉकचैन में दो विरोधाभासी विशेषताएं हैं यानी यह पारदर्शी और निजी दोनों है। इसमें किसी व्यक्ति की पहचान केवल उनके private address से दर्शाई जाती है और complex क्रिप्टोग्राफी के माध्यम से कवर की जाती है।इस प्रकार, यदि आप किसी भी तरह किसी व्यक्ति के लेन देन के इतिहास को देखेंगे तो आप "ऐलिस sent 1 BTC" के बजाय "0x5eFd6F7c79447eAaCD0c13B4AE17c8F64188ddC5" sent 1 BTC देखेंगे।

इसलिए, भले ही व्यक्तिगत पहचान छिपी हुई हो, हम अभी भी उनके public address के पते का उपयोग करके किए गए लेनदेन का निरीक्षण कर सकते हैं।

ब्लॉकचेन तकनीक की एक और सबसे महत्वपूर्ण विशेषता इसकी अपरिवर्तनीयता है, जिसका अर्थ है कि एक बार ब्लॉकचेन में कुछ हो जाने के बाद, इसे बदला नहीं जा सकता है। क्या आप कल्पना करपाएंगे कि यह धनसंबंधी प्रतिष्ठानों के लिए कितना महत्वपूर्ण होगा? केवल क्रिप्टोग्राफिक हैश के कारण ब्लॉकचेन को यह गुण मिलता है।

b. ब्लॉकचेन तकनीक एक distributed ledger के रूप में

ब्लॉकचैन रिकॉर्ड्स की लिंक की गई सूची है, जिसे ब्लॉक, टाइम–स्टेप के रूप में जाना जाता है और एक क्रिप्टोग्राफ़िक हैश मान के माध्यम से जुड़ा होता है जो एक संरक्षित और अपरिवर्तनीय तरीके से तय किया जाता है [1, 2]। इसकी एक निरंतर बढ़ती हुई सूची है जहाँ हर नए ब्लॉक को अंतिम में जोड़ा जाएगा। प्रत्येक नया ब्लॉक क्रिप्टोग्राफ़िक हैश मान [3] के माध्यम से अपने पिछले ब्लॉक की ओर इंगित करता है। ब्लॉकचैन में ब्लॉक एक वितरित (पी 2 पी) नेटवर्क में सॉर्ट किए जाते हैं। प्रत्येक नोड में दो कुंजियाँ होती हैं [4]। एक का उपयोग संदेशों को encrypt करने के लिए किया जाता है (अर्थात एन्क्रिप्शन के लिए) जिसे सार्वजनिक कुंजी के रूप में जाना जाता है और अन्य का उपयोग संदेशों को decrypt करने के लिए किया जाता है (अर्थात डिक्रिप्शन के लिए) जिसे निजी कुंजी के रूप में जाना जाता है जो इसे समझने के लिए नोड की अनुमति देता है। केवल सही निजी कुंजी संबंधित निजी कुंजी के साथ एन्कोड किए गए संदेशों को हटा सकती है। इस तरह एक ब्लॉकचेन की स्थिरता, अपरिवर्तनीयता और immutability को प्राप्त किया जा सकता है [6]। इसे asymmetric क्रिप्टोग्राफी के रूप में जाना जाता है।

ब्लॉकचैन के प्रत्येक ब्लॉक को क्रिप्टोग्राफ़िक हैश की सहायता से एक साथ जोड़ा जाता है जो क्रिप्टोग्राफ़िक हैश फ़ंक्शन जैसे SHA256 द्वारा उत्पन्न होता है। यह ब्लॉक की anonymity, कॉम्पैक्टनेस और अपरिवर्तनीयता की भी गारंटी देता है [7]।

हर बार एक नोड लेनदेन करता है इसे पहले हस्ताक्षरित किया जाता है और फिर आगे पुष्टि के लिए नेटवर्क को सूचित किया जाता है। लेन–देन की प्रामाणिकता और अखंडता सुनिश्चित करने के लिए प्रत्येक लेनदेन पर एक निजी–कुंजी द्वारा हस्ताक्षर किए जाते हैं। नेटवर्क लेनदेन में जो फैलाया जाता है और जिसे वैध माना जाता है, उसे पहले व्यवस्थित किया जाता है और फिर कुछ विशिष्ट नोड्स द्वारा ब्लॉक में पैक किया जाता है, जिसे खनिक के रूप में जाना जाता है जब नेटवर्क स्पष्ट समझौते प्रणालियों का उपयोग करता है, उदाहरण के लिए, proof-of-stack और proof-of-work.

खनिकों को कैसे चुना जाता है और ब्लॉक में क्या जानकारी होनी चाहिए, यह समझौते पर निर्भर करता है सहमति प्रोटोकॉल आखिरकार तय करते हैं कि खनिकों का चयन कैसे किया जाना चाहिए और इसमें क्या डेटा होना चाहिए। चयनित ब्लॉकों को फिर पूरे नेटवर्क में प्रेषित किया जाता है, स्वीकृत नोड्स फिर पुष्टि कराते हैं कि क्या इस ब्लॉक में वैध लेनदेन शामिल हैं और साथ ही यह सत्यापित करता है कि यह श्रृंखला में पिछले ब्लॉक को संदर्भित करता है या इसके संबंधित हैश के उपयोग से नहीं। इसके अलावा अगर दोनों स्थितियां संतुष्ट हैं तो ब्लॉक नोड द्वारा श्रृंखला में जोड़ दिया जाता है अन्यथा यह नोड को छोड़ देता है।

c. स्वास्थ्य सेवा में ब्लॉकचेन की आवश्यकता

ब्लॉकचैन को स्वास्थ्य सुरक्षा प्रणाली [8] में अविश्वसनीय क्षमता माना जाता है। चिकित्सा सेवाओं को बेहतर बनाने के लिए प्राधिकरण को सूचना के प्रशासन को सौंपा जाना चाहिए और विभिन्न प्रणालियों को जोड़ने की इसकी क्षमता इलेक्ट्रॉनिक स्वास्थ्य रिकॉर्ड की सटीकता को बढ़ा सकती है। इस तकनीक का उपयोग दवा के नुस्खे के साथ–साथ आपूर्ति श्रृंखला प्रबंधन, गर्भावस्था और किसी भी संवेदनशील जानकारी के लिए किया जा सकता है। अन्य चिकित्सा सेवा क्षेत्र जो ब्लॉकचेन इनोवेशन द्वारा लाभान्वित हो सकते हैं, वो हैं; आपूर्तिकर्ता मान्यता, क्लिनिकल चार्जिंग, कॉन्ट्रैक्टिंग, क्लिनिकल रिकॉर्ड ट्रेड, क्लिनिकल प्रीइमिनीयर आदि।

एक रोगी–संचालित पद्धति को सशक्त बनाने के लिए चिकित्सा सेवा प्रशासन बदल रहे हैं।

ब्लॉकचेन–आधारित चिकित्सा सेवा रूपरेखाएँ गोपनीयता को बेहतर बनाने में सहायक हो सकती हैं और साथ ही रोगी की सूचनाओं की निर्भरता को भी बढ़ा सकती हैं क्योंकि अब रोगियों के पास उनके चिकित्सा सेवा रिकॉर्ड का अधिकार हो सकता है।

रोगियों की नैदानिक जानकारी का भंडारण चिकित्सा सेवा में महत्वपूर्ण है। ये जानकारी असाधारण रूप से संवेदनशील हैं और इस तरीके से डिजिटल हमलों के लिए एक आदर्श उदाहरण है। सभी संवेदनशील जानकारी के बारे में सुनिश्चित करना अनिवार्य है। एक और परिप्रेक्ष्य जानकारी पर कमान है, जो रोगी द्वारा अधिमानतः किया जाएगा। इस प्रकार, मरीजों की चिकित्सा सेवाओं की जानकारी को साझा करना और प्राप्त करना एक और उपयोग है। ब्लॉकचेन प्रौद्योगिकी हमलों के विरुद्ध बेहद शक्तिशाली है, और अभिगम नियंत्रण के लिए विभिन्न तकनीकों को देता है। नतीजतन, ब्लॉकचेन चिकित्सा सेवा की जानकारी के लिए एक सभ्य संरचना देता है।

व्यक्तिगत नैदानिक जानकारी के लिए, सार्वजनिक के बजाय निजी ब्लॉकचेन का उपयोग करना अधिक उचित होगा।

II. साहित्य समीक्षा

ब्लॉकचेन तकनीक पर आधारित बायोमेडिकल और स्वास्थ्य सेवा सूचना विनिमय प्रणाली की सुरक्षा और गोपनीयता के लिए किए गए पूर्व शोधों को नीचे दिखाया गया है।

[10] केंद्रीय प्राधिकरण पर निर्भर न होते हुए भी ब्लॉकचेन प्रौद्योगिकी, विकेंद्रीकृत और वितरित पर्यावरण को सशक्त बनाने के साथ रोगी के केंद्रित डेटा की सुरक्षा पर ध्यान केंद्रित करता है। क्रिप्टोग्राफिक मानकों का उपयोग लेनदेन को सुरक्षित और विश्वसनीय बनाता है। आजकल, क्रिप्टोकरेंसी के प्रसार के कारण, ब्लॉकचेन तकनीक असाधारण रूप से लोकप्रिय हो गई है। एक क्षेत्र जहां ब्लॉकचेन तकनीक में बड़ी संभावनाएं हैं, वह चिकित्सा सेवाओं की आवश्यकता है, क्योंकि चिकित्सा सेवा ढांचे से निपटने के लिए और अलग–अलग रूपरेखाओं को संबद्ध करने के लिए एक अधिक रोगी–केंद्रित तरीके की आवश्यकता होती है और इलेक्ट्रॉनिक स्वास्थ्य सेवा रिकॉर्ड्स (ईएचआर) की सटीकता में भी सुधार होता है। इस पत्र का उद्देश्य स्वास्थ्य सेवा में ब्लॉकचेन के परिचय और अनुप्रयोग पर प्रकाश डालना है।

[11] यह कार्य एक loss-less compression एल्गोरिदम BAQALC प्रस्तावित करता है जो ब्लॉकचैन लागू FASTQ और FASTA दोषरहित compression के लिए उपलब्ध है जो डीएनए अनुक्रमण डेटा की विशाल मात्रा के भंडारण और विनिमय को सक्षम करता है। प्रस्तावित BAQALC एल्गोरिथ्म न केवल उच्चतम compression प्रदर्शन दिखाता है, बल्कि डीएनए डेटा को अपरिवर्तनीय भी बनाता है। यह पत्र पांच पुराने रोगों के लिए विभिन्न compression एल्गोरिदम के compression अनुपात की तुलना करता है और परिणाम दिखाता है कि BAQALC में उच्चतम compression राशन है और साथ ही सुरक्षित भंडारण मंच भी प्रदान करता है।

[13] [14] द्वारा आईओटी और ब्लॉकचैन संचालित स्वास्थ्य सेवा के मामले के अध्ययन को दर्शाया गया है। मनुष्य को आजकल जिस बुनियादी क्षमता की आवश्यकता है, वह है, प्रभावी रूप से पहचानने, महसूस करने और कार्य करने के लिए स्वास्थ्य, और इस तरह, यह व्यक्ति के विकास में उपयोग किए जाने वाले एक आवश्यक घटक के रूप में कार्य करता है, फिर भी प्रकृति के अलावा लोगों के साथ एक जगह है। रोगी की जांच करते समय, चिकित्सक को व्यक्तिगत स्वास्थ्य के बारे में प्रत्येक विवरण को लिखना चाहिए। इस तरह मापे गए डेटा को नोट करने से मानवीय त्रुटि हो सकती है। इंटरनेट से संबंधित उपकरण, जो रोगी की स्थिति को मापते हैं, कुछ समस्याओं को हल कर सकते हैं।

हर बार अस्पताल जाने वाले मरीज को डॉक्टर के पिछले मेडिकल रिकॉर्ड से गुजरना पड़ता है। जोड़े गए उपकरणों का उपयोग करके, सभी डेटा सीधे उसके / उसके PHI (Personal health information) में स्टोर किए जाते हैं। हालांकि डॉक्टरों को अभी भी रोगी की जांच करने की आवश्यकता है लेकिन इस विशेष उपकरणों की मदद से मरीजों की स्थिति की लगातार निगरानी की जा सकती है और यह उनका समय भी बचाएगा। इसी तरह, पहनने योग्य गैजेट्स विशेषज्ञों और वैज्ञानिकों को बीमारियों की बेहतर समझ के लिए अधिक महत्वपूर्ण जानकारी दे सकते हैं, हर दिन स्पष्ट चीजों की जांच करके, ताकि हम किसी भी घटना को होने से रोक सकें और जीवन को बचा सकें।

एक निरीक्षण प्रणाली और IOT उपकरणों के उपयोग के साथ, बड़ी मात्रा में डेटा का भंडारण संभव है, जिसके परिणामस्वरूप रोगी के इलेक्ट्रॉनिक स्वास्थ्य रिकॉर्ड को अद्यतन किया जा सकता है [14] । ब्लॉकचेन प्रौद्योगिकी की अपरिवर्तनीयता विशेषता, उपयोगकर्ता को रोगी के डेटा को अपरिवर्तनीय रखने के साथ–साथ पूरी तरह से संरक्षित चिकित्सा इतिहास प्रदान करने की अनुमति देती है। उपयोगकर्ता सही क्रेडेंशियल्स का उपयोग करके किसी भी समय कहीं से भी अपनी रिपोर्ट तक पहुंच सकते हैं और इससे न केवल समय की बचत होगी बल्कि संस्थानों के बीच मेडिकल रिकॉर्ड के हस्तांतरण की लागत भी कम होगी।

एक और मुद्दा केंद्रीयकृत प्रणाली है क्योंकि केंद्रीकृत नियंत्रण में कई डाउनसाइड हो सकते हैं जो संस्थानों के बीच सहयोग करना मुश्किल बनाते हैं। दूसरी ओर, ब्लॉकचेन विकासवादी, सराहनीय और बहुत नई तकनीक है। ब्लॉकचेन पर डेटा की इस बड़ी मात्रा को स्टोर करना एक मुद्दा है। हालाँकि, इस डेटा की प्रतिकृति अभी भी प्राथमिक चिंता बनी हुई है। बिग डेटा तकनीक इस समस्या का सबसे उपयुक्त समाधान होगा। ब्लॉक चेन के साथ–साथ बड़े डेटा का उपयोग करना इसे और अधिक शक्तिशाली बनाता है, उदाहरण के लिए ब्लॉकचेन डीबी [13] [14]।

[15] इंटरनेट ऑफ थिंग्स (IOT) और ब्लॉकचैन के मेडिकल उपयोग के मामले के एक केस स्टडी को दर्शाया गया है, जो ब्लॉकचैन आधारित इंटरनेट ऑफ थिंग्स मॉडल का प्रस्ताव करके स्वास्थ्य रिकॉर्ड के अविश्वसनीय भंडारण के मुद्दे पर एक जवाब देने का इरादा रखता है, जहां एक मरीज के रूप में चल रही जानकारी पुनर्स्थापनात्मक स्थिति को एक जैव–सेंसर के माध्यम से एकत्र किया जाता है और इसे ब्लॉकचेन में एकत्रित्त करता है। इन पंक्तियों के साथ अपरिवर्तनीय डेटा संग्रहण उत्पन्न किया जा सकता है। एक स्मार्ट अनुबंध द्वारा अंतिम बीमा क्लिनिक बिल को बीमा कवरेज के साथ निर्धारित किया जा सकता है। यह बाहरी आपूर्तिकर्ताओं की आवश्यकता को कम करेगा और एक सीधी रूपरेखा (पारदर्शी प्रणाली) बनाएगा।

यह पत्र डिस्चार्ज किए गए रोगियों के रिकॉर्ड के विवरण को बचाने के लिए Interplanetary document framework के उपयोग का भी प्रस्ताव करता है, बाद में वास्तविक ब्लॉक श्रृंखला पर भार को कम करता है। आम तौर पर यह निश्चित रूप से रोगियों और विशेषज्ञों को एक रोगी की आवश्यकता के लिए त्वरित प्रतिक्रिया के साथ एक संरक्षित और सीधी स्थिति बनाकर लाभान्वित करेगा।

[16] यह कार्य स्वास्थ्य सेवा में ब्लॉकचेन के अनुप्रयोग पर केंद्रित है। ब्लॉकचेन ने इसी तरह इलेक्ट्रॉनिक उपयोगों (ईएचआर) में सहमति रखने से लेकर क्लेम प्रोसेसिंग तक को व्यवस्थित करने तक कई उपयोग मामलों के माध्यम से चिकित्सीय प्रशासन डेटा की विश्वसनीयता और सरलता को सुधारने के लिए एक चरण के रूप में एकत्र किया है। लेखक इसी तरह ब्लॉकचेन के मूल को दर्शाता है और स्वास्थ्य उद्योग के अंदर इस प्रौद्योगिकी के वर्तमान और भविष्य के उपयोग को दर्शाता है।

[17] हाई–थ्रूपुट डीएनए अनुक्रमण तकनीक में तेजी से विकास और जीनोम–अनुक्रमण की लागत में कमी के बाद, ब्लॉकचेन तकनीक का उपयोग करके अपरिवर्तनीय डीएनए अनुक्रम डेटा ट्रांसमिशन में एक बड़ी प्रगति हुई है। आनुवंशिक उद्योगों में। हालांकि, डीएनए अनुक्रमण के लिए आवश्यक लागत और समय में कमी अभी भी डेटा की इतनी बड़ी मात्रा के प्रबंधन का मुद्दा है। साथ ही, इतनी बड़ी मात्रा में डीएनए अनुक्रम डेटा की सुरक्षा और प्रसारण अभी भी एक मुद्दा है। यह विचार शोधकर्ताओं और स्वास्थ्य सेवा उपयोगकर्ता दोनों के लिए भावी पीढ़ी जैव सूचना विज्ञान प्रणालियों के लिए एक सुरक्षित भंडारण मंच प्रदान करने के लिए है। सुरक्षित डेटा साझाकरण रणनीतियाँ, जो डेटा की सटीकता की पुष्टि के लिए अपने सुरक्षित पदार्थों के साथ स्वास्थ्य सेवा प्रदाताओं को अनुमति दे सकती हैं, उचित चिकित्सा सेवाओं को सुनिश्चित करने के लिए महत्वपूर्ण हैं। इस पेपर में, यह स्वास्थ्य सेवा डेटा को सुरक्षित करने के लिए ब्लॉकचेन तकनीक के अनुप्रयोगों के बारे में सर्वेक्षण किया गया है, जहां रिकॉर्ड की गई जानकारी को एन्क्रिप्ट किया गया है ताकि इसे घुसना या हटाया जाना मुश्किल हो जाए, क्योंकि ब्लॉक–चेन तकनीक के प्राथमिक लक्ष्य डेटा को अपरिवर्तनीय बनाना है।

[18] स्वास्थ्य सेवा अपने मुख्य कामकाज के लिए इंजीनियरिंग और प्रौद्योगिकी के कई क्षेत्रों को शामिल करता है। रोगियों के इलेक्ट्रॉनिक स्वास्थ्य रिकॉर्ड का उपयोग रोगियों के चिकित्सा इतिहास को स्टोर करने और उन्हें उपयोगकर्ता के लिए आसानी से उपलब्ध और उपभोग योग्य बनाने के लिए किया जाता है। यह डेटा साइबर हमलों और दुर्भावनापूर्ण गतिविधियों के लिए भी प्रवृत्त है। ब्लॉकचैन का एक प्रूफ–ऑफ–स्टेक कार्यान्वयन एक विकेन्द्रीकृत स्वास्थ्य प्रबंधन प्रणाली तैयार करने का प्रस्ताव है जो 256–बिट एन्क्रिप्शन का उपयोग करके सुरक्षित और सुरक्षित होने के अलावा अस्पतालों के बीच अंतः क्रियाशीलता प्रदान करता है। यह एक सुरक्षित वातावरण में डेटा को संभालने की बेहतर गति के साथ पर्याप्त विकेन्द्रीकरण प्रदान करता है, स्वास्थ्य सेवा प्रणाली के लिए निजी ब्लॉकचैन नेटवर्क में संबंधित सभी उपयोगकर्ताओं के लिए सूचना तक आसानी से पहुंच प्रदान करता है।

III. स्वास्थ्य संबंधी आंकड़ों के प्रबंधन में समस्याओं की पहचान

स्वास्थ्य सेवा वातावरण में ब्लॉकचेन प्रौद्योगिकी के अनुप्रयोगों की एक विशाल श्रृंखला है। इसका उपयोग रोगी के स्वास्थ्य सेवा रिकॉर्ड्स, औषधीय आपूर्ति श्रृंखला के प्रबंधन के सुरक्षित रूप से आदान–प्रदान के लिए किया जा सकता है और यह जेनेटिक शोधकर्ता के जेनेटिक कोड को अनलॉक करने के लिए बहुत मददगार हो सकता है। सुरक्षित एन्क्रिप्शन एल्गोरिदम की मदद से घुसपैठियों से रोगी के रिकॉर्ड को रोकने के लिए ब्लॉकचैन तकनीक पहले से ही महत्व प्राप्त कर रही है।

आजकल सबसे प्रसिद्ध ब्लॉकचैन की औषधीय सेवाओं के आवेदन हमारी महत्वपूर्ण नैदानिक जानकारी को संरक्षित और सुरक्षित रखने के लिए है क्योंकि सुरक्षा को स्वास्थ्य प्रणाली में एक बड़ा मुद्दा माना जाता है। वर्ष 2009 और 2017 के बीच में, 176 मिलियन से अधिक रोगी रिकॉर्ड्स को सूचना विराम में उजागर किया गया था। अपराधी वीजा और बैंकिंग डेटा के साथ–साथ स्वास्थ्य सेवा रिकॉर्ड भी ले गए।

ब्लॉकचेन में रोगी के डेटा को अपरिवर्तनीय, विकेन्द्रीकृत और पारदर्शी रखने की क्षमता है जो इसे सुरक्षा अनुप्रयोगों के लिए एक नवीन अतिप्रवाह बनाता है। इसके अलावा, चूंकि ब्लॉकचेन में एक विरोधाभासी विशेषता है, अर्थात यह पारदर्शी होने के साथ–साथ निजी भी है। यहां व्यक्ति की पहचान सुरक्षित और जटिल कोड के साथ कवर की गई है जो नैदानिक जानकारी की सुरक्षा सुनिश्चित कर सकता है। इस तकनीक के विकेंद्रीकृत विचार भी रोगियों, विशेषज्ञों और चिकित्सा सेवा प्रदाताओं को

समान डेटा तेजी से और सुरक्षित रूप से रखने की अनुमति देता है। स्वास्थ्य सुरक्षा में कुछ डेटा सुरक्षा से संबंधित मुद्दे नीचे दिए गए हैं

- **समस्या 1: नैदानिक परीक्षणों की सूचना सुरक्षा**

किसी भी दवा के अनुमोदन या अस्वीकृति के लिए नैदानिक परीक्षणों का उपयोग किया जाता है या हम कह सकते हैं कि इसका उपयोग किसी विशेष दवा की प्रभावशीलता को निर्धारित करने के लिए किया जाता है। शोधकर्ता हमेशा परीक्षणों के परिणामों, गुणवत्ता विश्लेषण आदि से संबंधित जानकारी एकत्र करने और रिकॉर्ड करने में रुचि रखते हैं। प्रत्येक शोधकर्ता स्पष्ट परीक्षा के लिए उत्तरदायी होता है, जिससे हर किसी को नियंत्रित करना मुश्किल हो जाता है। यह जानकारी तब किए गए शोध के पूरे परिणाम को बदलने के लिए आसानी से बदलने में या कवर करने में सक्षम होगी।

- **समस्या 2: रोगी डेटा प्रबंधन**

स्वास्थ्य बीमा पोर्टेबिलिटी और जवाबदेही अधिनियम (HIPAA) रोगी के डेटा गोपनीयता को कड़ाई से नियंत्रित करता है, और उम्मीद करता है कि PHI (Personal health information) बिल्कुल सुरक्षित हो। किसी भी मामले में, PHI के साथ पहचाने जाने वाले एक अन्य मुद्दे: कुछ समय के लिए, रोगियों को अपने नैदानिक रिकॉर्ड बाहरी लोगों को देने की आवश्यकता होती है (उदाहरण के लिए दवा की दुकानों के साथ होती है, जब उन्हें बाहरी लोगों से दवा खरीदनी पड़ती है)। तो, कैसे ब्लॉकचैन आंशिक पहुंच के साथ–साथ डेटा की सुरक्षा प्रदान कर सकता है?

IV. स्वास्थ्य सुरक्षा में डेटा सुरक्षा मुद्दों के लिए समाधान

• यह युग हर किसी को डिवाइस में पंजीकृत किसी भी रिपोर्ट की वैधता साबित करने की अनुमति देता है। यह लेन–देन के रूप में रिकॉर्ड जोड़ने और सभी सिस्टम नोड्स द्वारा जानकारी को मान्य करने के माध्यम से अस्तित्व का प्रमाण प्रदान करता है। जैसा कि ऊपर उल्लेख किया गया है, ब्लॉकचेन अपरिवर्तनीय डेटा रिकॉर्ड करता है। यह एक्सचेंज के प्रकार के अंदर रिकॉर्ड जोड़ने और सभी फ्रेमवर्क हब द्वारा डेटा को अनुमोदित करने के माध्यम से उपस्थिति का प्रमाण देता है। जैसा कि ऊपर सत्यापित किया गया है, ब्लॉकचेन अपरिवर्तित जानकारी को रिकॉर्ड करता है। यह सुविधा नैदानिक परीक्षणों के डेटा को अपरिवर्तनीय बनाने की अनुमति देती है और इसे संशोधित करना मुश्किल बनाती है। 2016 में कैम्ब्रिज विश्वविद्यालय के दो विशेषज्ञों ने यह देखने के लिए एक जांच की कि कैसे ब्लॉकचेन नैदानिक प्राथमिकताओं की उपस्थिति का प्रमाण प्रदान कर सकता है। मूल कोड के साथ सिस्टम द्वारा उत्पन्न कोड की तुलना करने के बाद वे इस निष्कर्ष पर पहुंचे कि डेटा बदला गया है या नहीं। यह SHA256 की अनूठी विशेषता है जो हर बार एक अद्वितीय हैश बनाता है जब सूचना में परिवर्तन किया जाता है।

• प्रत्येक PHI ब्लॉक के लिए, ब्लॉक चेन रोगी की आईडी के साथ एक हैश# जेनरेट करती है।। एक एपीआई का उपयोग करके, प्रत्येक और प्रत्येक इकाई को रोगी के व्यक्तित्व को उजागर किए बिना आवश्यक डेटा मिल सकता है। एक मरीज यह निर्णय ले सकता है, कि किसको प्रवेश देना है और यह प्रवेश पूर्ण होगा या आधा। इसके अलावा, यदि रोगी को इस बारे में निश्चित नहीं था कि वह क्या कर रहा है या नहीं, तो वे स्पष्ट बाहरी लोगों को सेट कर सकते हैं जिन्हें PHI साझा करने के लिए अपनी सहमति देने की आवश्यकता होगी। ब्लॉकचैन में स्वास्थ्य सेवा के साथ–साथ विभिन्न उद्योगों में उपयोग की पहली दर है।

ब्लॉकचेन को एक लिंक की गई सूची के रूप में देखा जा सकता है जिसमें डेटा और एक पॉइंटर होता है जहां प्रत्येक ब्लॉक संरचना की तरह एक श्रृंखला में अपने पिछले एक की ओर इशारा करेगा।

हैश पॉइंटर कुछ भी नहीं है, एक पॉइंटर है जो केवल अपने पिछले ब्लॉक के पते के साथ–साथ पिछले ब्लॉक के हैश मान को भी रखता है। यह एक छोटा सा बदलाव है, जो ब्लॉकचेन को अविश्वसनीय रूप से भरोसेमंद और अन्वेषण करता है।

अब कल्पना कीजिए, अगर कोई हमलावर ब्लॉक, n* में निहित जानकारी को बदलने का प्रयास करता है, तो nt ब्लॉक में मामूली बदलाव स्वचालित रूप से हैश फ़ंक्शन के गुण के कारण n-1 वें ब्लॉक में एक कठोर बदलाव करेगा। इसी तरह n-1th ब्लॉक में बदलाव (n-2)th ब्लॉक के डेटा को बदलने के लिए मजबूर करेगा और इसी तरह, चेन को पूरी तरह से अलग बना देगा। ब्लॉकचेन की इस गुण को अपरिवर्तनीयता के रूप में जाना जाता है।

आइए हम हैशिंग प्रक्रिया के एक उदाहरण पर विचार करें। इस गतिविधि के लिए, हम SHA–256 (सिक्योर हैशिंग एल्गोरिथम 256) का उपयोग कर रहे हैं।

Table 1. Hashing Process

Input	Hash
Hello	185f8db32271fe25f561a6fc938b2 e264306ec304eda518007d176482 6381969
Bye	128901223aac8df3b89cd75d7 ec644f 9924ed9dcd01e0c65 ae99334a3cf9273a

उपरोक्त उदाहरण से यह स्पष्ट है कि आपकी जानकारी कितनी भी बड़ी या कम क्यों न हो, हमारे पास हमेशा एक निश्चित 256–बिट लंबाई आउटपुट होगा। यह तब और महत्वपूर्ण हो जाएगा जब हमें भारी मात्रा में सूचनाओं का सामना करना होगा। इसलिए, इनपुट के बजाय हैश को याद रखना आसान हो सकता है और साथ ही हम इसका ट्रैक भी रख सकते हैं। क्रिप्टोग्राफिक हैश के बारे में एक दिलचस्प तथ्य यह है कि इनपुट में एक छोटा सा बदलाव भी हैश मूल्य में एक बड़ा बदलाव कर सकता है इस गुण को Avalanche effect के रूप में जाना जाता है।

आइए एक उदाहरण पर विचार करके इसे देखें:

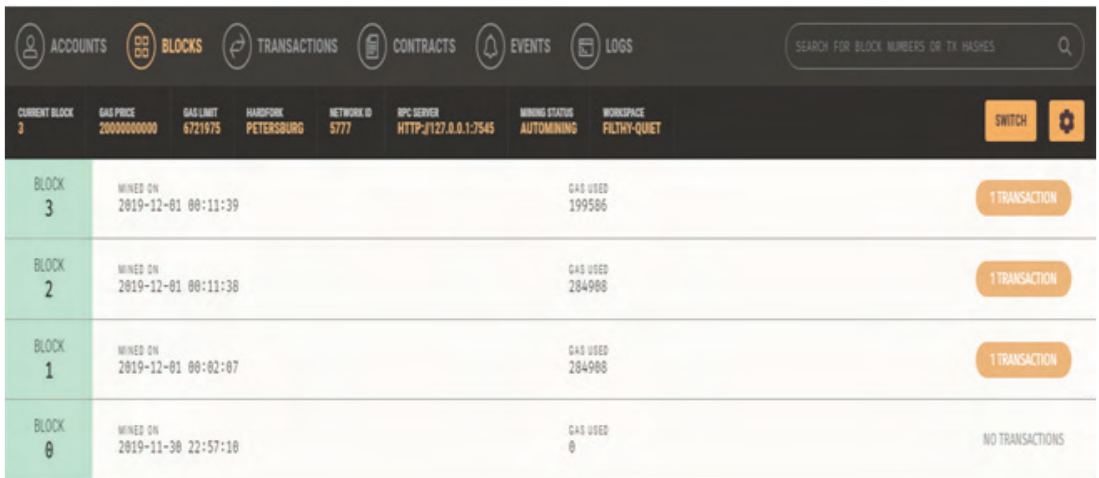
Table 2. Avalanche effect in Hashing Process

Input	Hash
Hello	185f8db32271fe25f561a6fc938b 2e264306ec304eda518007d1764 826381969
hello.	2cf24dba5fb0a30e26e83b2ac5b9e 29e1b161e5c1fa7425e730433629 38b9824

उपरोक्त उदाहरण से यह स्पष्ट है कि इनपुट में एक छोटा सा बदलाव भी हैश मूल्य में एक बड़ा परिवर्तन कर सकता है। चित्र 1 ब्लॉकचेन की संरचना की तरह एक जुड़ी हुई सूची को दर्शाता है, जहां प्रत्येक ब्लॉक में डेटा होता है और एक संकेतक अपने पिछले एक की ओर इशारा करता है।हमने अपना काम दिखाने के लिए गनाचे प्राइवेट (Ganache private) ब्लॉकचैन टूल का इस्तेमाल किया है।

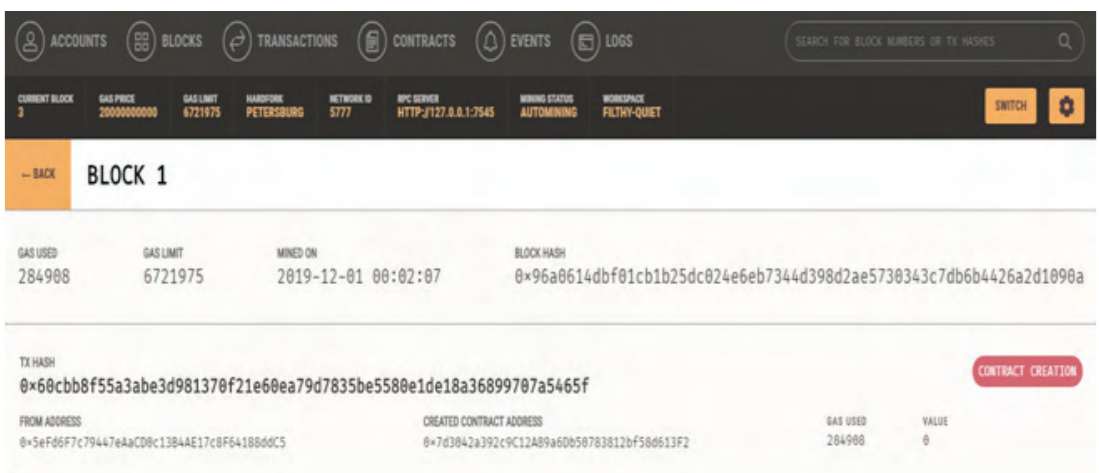
Ganache तेजी से एथेरियम और कॉर्डा वितरित अनुप्रयोग विकास के लिए एक व्यक्तिगत ब्लॉकचेन है। आप पूरे विकास चक्र में Ganache का उपयोग कर सकते हैं; आपको एक सुरक्षित और नियतात्मक वातावरण में अपने dApps को विकसित, परिनियोजित और परीक्षण करने में सक्षम बनाता है।

Ganache दो प्रकार में आता है: एक UI और एक सीएलआई। Ganache UI एक डेस्कटॉप एप्लिकेशन है जो एथेरियम और Corda तकनीक दोनों का समर्थन करता है। कमांड–लाइन टूल, Ganache-Cli (जिसे पहले TestRPC के नाम से जाना जाता था), एथेरियम पर विकास के लिए उपलब्ध है।



चित्र 1. Ethereum एक्सचेंजों का पूर्वावलोकन

ब्लॉक 1 के बारे में पूर्ण विवरण चित्र 2 में दिखाया गया है जैसे हैश मान, स्रोत पता, खनन समय आदि



चित्र 2 Ethereum ब्लॉक का विस्तृत पूर्वावलोकन

V. निष्कर्ष :

रोगी की जांच करते समय, चिकित्सक को व्यक्तिगत स्वास्थ्य के बारे में प्रत्येक विवरण को लिखना चाहिए। इस डेटा को नोट करने से मानवीय त्रुटि हो सकती है। इंटरनेट से संबंधित उपकरण, जो रोगी की स्थिति को मापते हैं, कुछ समस्याओं को हल कर सकते हैं।हर बार डॉक्टर अस्पताल जाने वाले मरीज के पिछले मेडिकल रिकॉर्ड से गुजरना पड़ता है। उपकरणों का उपयोग करके, सभी डेटा को सीधे मरीज के EMR (Electronic Medical Record) में स्टोर किया जा सकता है। हालांकि डॉक्टरों को अभी भी रोगी की जांच करने की आवश्यकता है लेकिन अब यह अपना समय बचाएगा। इस विशेष उपकरणों की मदद से हम मरीजों की स्थिति की लगातार निगरानी कर सकते हैं। इसी तरह, पहनने योग्य गैजेट्स विशेषज्ञों और वैज्ञानिकों को बीमारियों की

बेहतर समझ के लिए अधिक महत्वपूर्ण जानकारी दे सकते हैं, हर दिन स्पष्ट चीजों की जांच करके, ताकि हम किसी भी घटना को होने से रोक सकें और जीवन को बचा सकें।एक निगरानी प्रणाली और IoT उपकरणों के उपयोग के साथ, बड़ी मात्रा में डेटा का भंडारण संभव है, जिसके परिणामस्वरूप रोगी के इलेक्ट्रॉनिक स्वास्थ्य रिकॉर्ड को अद्यतन किया जा सकता है [14]। ब्लॉकचेन प्रौद्योगिकी की अपरिवर्तनीयता विशेषता, उपयोगकर्ता को रोगी के डेटा को अपरिवर्तनीय रखने के साथ–साथ पूरी तरह से संरक्षित चिकित्सा इतिहास प्रदान करने की अनुमति देती है। उपयोगकर्ता सही क्रेडेंशियल्स का उपयोग करके किसी भी समय कहीं से भी अपनी रिपोर्ट तक पहुंच सकते हैं और इससे न केवल समय की बचत होगी बल्कि संस्थानों के बीच मेडिकल रिकॉर्ड के हस्तांतरण की लागत भी कम होगी।इस पत्र में, हमने ब्लॉकचेन की कार्यप्रणाली, स्वास्थ्य सेवा में इसकी आवश्यकता और ब्लॉकचेन प्रौद्योगिकी का उपयोग करके जैव चिकित्सा और स्वास्थ्य सूचना विनिमय प्रणाली में सुरक्षा और गोपनीयता कैसे प्राप्त की जा सकती है, के बारे में बताया है।

VI. Table of the Hindi terminology used %

Blockchain	ब्लॉकचेन
Biomedical	बायोमेडिकल
Cryptographic hash	क्रिप्टोग्राफिक हैश
Cryptographic currency	क्रिप्टोकरेंसी
Database	डेटाबेस
Decentralized	विकेंद्रीकृत
Distributed	वितरित
DNA sequence	डीएनएअनुक्रमण
Hackers	हैकर्स
Healthcare	स्वास्थ्य सेवा
Input	इनपुट
IOT (Internet of things)	आईओटी
output	आउटपुट
Peer-to-Peer	पीयर–टू–पीयर
Security	सुरक्षा
Technology	तकनीक
Transparent	पारदर्शी

References:

[1] Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: Th e Foreseeable Impact on Society and Industry. Computer 2017, 50, 18–28.

[2] Roehrs,A.; da Costa, C.A.; da Rosa Righi, R.;Alex, R.; Costa, C.A.; Righi, R.R. OmniPHR: A distributed architecture model to integrate personal health records. J. Biomed. Inform. 2017, 71, 70–81.

[3] Sleiman, M.D.; Lauf, A.P.; Yampolskiy, R. Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency सिस्टम . In Proceedings of the 2015 International Conference on Cyberworlds (CW), Visby, Sweden, 7–9 October 2015; pp. 332–336.

[4] Aumasson, J. Serious Cryptography: A Practical Introduction to Modern Encryption; No Starch Press: San Francisco, CA, USA, 2017.

[5] Ferguson, N.; Schneier, B. Practical Cryptography, 1st ed.; John Wiley & Sons, Inc.: New York, NY, USA, 2003.

[6] Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.

[7] National Institute of Standards and Technology. Secure Hash Standard (SHS); Federal Information Processing Standards Publication: Gaithersburg, MD, USA, 2012.

[8] European Coordination Committee of the Radiological. Blockchain in Healthcare; Technical report; European Coordination Committee of the Radiological: Brussels, Belgium, 2017.

[9] Wüst, K.; Gervais, A. Do you need a Blockchain? IACR Cryptol. ePrint Arch. 2017, 2017, 375.

[10] Marko Hölbl, Marko Kompara, Aida Kamišali´c and LiliNemecZlatolas. "A सिस्टमatic Review of the Use of Blockchain in Healthcare". MDPI, journal, 10 October 2018.

[11] Seo-Joon Lee, Gyoun-Yon Cho, Fumiaki Ikeno and Tae-Ro Lee. "BAQALC: Blockchain Applied Lossless EfficientTransmission of DNA Sequencing Data for NextGeneration Medical Informatics". Appl. Sci. 27 August 2018, 8(9), 1471

[12] LichengWanga, XiaoyingShen a, Jing Li b, Jun Shao c, Yixian Yang. "Cryptographic primitives in blockchains". Elsevier Journal of Network and Computer Applications 127 (2019) 43–58.

[13] BigchainDB: A Scalable Blockchain Database, T McConaghy, R Marques, A M¨uller, D De Jonghe, T. T McConaghy, G McMullen, R Henderson, S Bellemare, A Granzotto, June 8, 2016, ascribe GmbH, Berlin Germany, https://www.bigchaindb.com/whiteपेपर/bigchaindb-whiteपेपर.pdf

[14] BigchainDB features, https://www.bigchaindb.com/features/

[15] TusharDey, ShwetaSunderkrishnan, ShauryaJaiswal, Prof. NehaKatre ," HealthSense: A Medical Use Case of Internet of Things and Blockchain" . Proceedings of the International Conference on Intelligent Sustainable सिस्टमs (ICISS 2017) IEEE Xplore Compliant.

[16] Angraal,S.;Krumholz,H.M.;Schulz,W.L. Blockchain Technology: Applications in HealthCare. Circ.Cardiovasc. Qual. Outcomes2017,10,e003800

[17] G. Mathur, A. Pandey and S. Goyal, "Immutable DNA Sequence Data Transmission for Next Generation Bioinformatics Using Blockchain Technology," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170715.

[18] Sagar V., Kaushik P. (2021) Ethereum 2.0 Blockchain in Healthcare and Healthcare Based Internet-of-Things Devices. In: Dave M., Garg R., Dua M., Hussien J. (eds) Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences. Algorithms for Intelligent सिस्टमs. Springer, Singapore. https://doi.org/10.1007/978-981-15-7533-4_17.

अन्तर्ज्ञान

"शान्त मन से ही कई चमत्कारिक खोजों और आविष्कारों ने जन्म लिया है। मन की इस अवस्था में, ब्रह्मांड के सभी रहस्य अनायास प्रकट होते हैं, जैसे स्क्रीन पर चित्र। "

. . . अम्मा श्री माता अमृतानंदमयी देवी

तात्विक सिद्धान्तों की खोज का कोई तार्किक तरीका नहीं है। केवल अंतर्ज्ञान (intuition) का तरीका है, जो दिख रहा है उसके पीछे पड़ी व्यवस्था के प्रति एक भावना से उद्दीप्त होता है। वह रहस्यवादी भावना है। यहाँ सभी कला और सभी विज्ञान के सत्य बीज कण निहित हैं। जिस किसी में भी ऐसी भावना का अभाव है, वह आश्चर्यभरे समाधान पाने में सक्षम नहीं है और डर की स्थिति में रहता है, वह मृत व्यक्ति की भांति है। यह जानने के लिए कि वास्तव में हमारे लिए जो अभेद्य है वह वास्तव में विद्यमान है और श्रेष्ठतम प्रज्ञान एवं परम सौंदर्य के रूप में प्रकट होता है, जिनके केवल स्थूल रूप ही इंद्रियों की सीमित शक्ति से दिखाई देते हैं। यह ज्ञान, और यह भावना ही सच्ची धार्मिकता का मूल आधार है। केवल इस संदर्भ में, मैं अपने आप को प्रगाढ़ धार्मिक लोगों में शुमार करता हूँ।

. . . अल्बर्ट आइंस्टीन आध्यात्मिकता पर