International Journal of Theoretical & Applied Computational Intelligence
https://ijtaci.com

Research Article

IoT-Enabled Cloud Storage Data Access Control Model Based on Blockchain Technology

Hayder Sabah Salih[1], Mohammed Hasan Ali[2*] and Muhammad I. Khan[3,4]

[1]Head of the Quality Assurance and Performance Evaluation Division at the College of Law- Mustansiriyah University in the Iraqi Ministry of Higher education and Scientific Research, Baghdad, Iraq

[2]College of Technical Engineering, Imam Ja'afar Al-Sadiq University, Al-Muthanna, Iraq

[3]School of Engineering, University of Warwick, Warwick Coventry CV4 7AL, United Kingdom

[4]AIDA Lab Prince Sultan University Riyadh, Saudi Arabia

*Crossponding author. Mohammed Hassan Ali (email. mohammed.hasan@sadiq.edu.iq)

https://orcid.org/0000-0001-7963-0918

Received: 22/7/2025; Accepted: 27/8/2025; Published: 17/9/2025

https://doi.org/10.65278/IJTACI.2025.14

Abstract: Cloud-based data access control security systems (CSDA) are the most versatile and elegant choice for SMEs and mid-sized enterprises. Storage, The idea of "the cloud" refers to the use of remote servers and data centers maintained by a third party, in this example, an internet service provider. There is no longer a need to invest in specialized data storage facilities due to the availability of on-demand data storage infrastructure with elastic storage capacity and variable storage prices. Authentication of Internet of Things devices is crucial for establishing that linked gadgets are what they claim to be. To reduce the likelihood of malicious behavior, access control regulates the access to the resources under the conditions. For cloud storage to function, at least one data server must be connected to the internet. Data supplied over the internet to a data server might be stored in "the cloud," where a copy of the data is kept. When necessary, the user may access this information through a web-based interface. The major issues with cloud computing are related to people's expectations of privacy and data security. Cryptography and other security methods may help keep personal information safe and secure. The data is separated into smaller bits by using a cloud storage service that relies on blockchain technology (BT). Then, it disperses this additional security over the network. Blockchain features, including hashing, private key encryption, and transaction ledgers, make this possible. CSDA-BT cloud storage is a new approach to archiving data and other digital artifacts in the cloud. Files may

be accessed and viewed from any location with an internet connection. The cloud has several benefits, including easy accessibility, backups, and high availability. To stay competitive while becoming closer to their customers, cloud storage businesses must work on lowering pricing and making storage faster. Cheap data storage enables novel forms of expression.

Keywords: Blockchain technology; Data access; Cloud storage; E-business; IoT; Security

1. Introduction

Users can access data stored in the cloud over a network, backed up and made available via a remote storage system, often the internet [1]. Cloud data storage is often purchased on a per-use, monthly basis. Data is stored on huge computer servers in cloud services accessible to users via the web [2]. Content may be uploaded, stored, and retrieved from a distant location. When using cloud storage, readers can access files from any location with an internet connection [3]. If a hard drive fails or other hardware malfunctions occur, visitors can access the data on the cloud to recover it [4]. The local storage on physical drives can be backed up with this service. The web interface of the cloud service provider is usually the end-user gets to them [5]. Before starting the service, cloud resources can be supplied to the users that select their storage capacity [6]. Cloud service providers use several large data facilities worldwide [7]. When a client orders cloud storage from a provider, the provider is responsible for ensuring the safety of the customer's data, providing enough storage space, servers, and computing resources, and ensuring the data is available and sent through a network [8]. Accessing data stored in the cloud using standard storage protocols and APIs or exporting the data to another location [9]. Cloud storage has several benefits as a replacement for costly and inconvenient on-premises storage area networks. However, organizations are wary of or restrict their usage of cloud storage because of flaws, particularly in public services [10].

In a blockchain, information is recorded, not to be altered, hacked, or manipulated. To explain the blockchain, one must understand that every machine in the network has an identical copy of the ledger [11]. Blockchain is the most common type of system built on a peer-to-peer network. Users can join or quit this open-source operating system anytime [12]. Cryptocurrencies, media streaming, cloud storage, and more may benefit from this technology. There are several benefits to using blockchain technology on its own and combined with other technologies [13]. Cloud computing can address key security and privacy concerns combined with blockchain technology. There is no central location where blockchain may be kept because it is decentralized [14]. Hence, it's stored on several computers and servers throughout the network. The individual computers or other devices that make up a network are called nodes. Put another way. There is only one blockchain for every node on a network [15]. Cloud storage can also benefit from blockchain technology. Many advances have been made in such networks' security, speed, uptime, and scalability [16]. Peer-to-peer networks like this would enable individuals who require additional storage capacity to rent space from other users' devices. In light of its information-era security, blockchain has been hailed as the next generation of financial technology [17]. Security is provided through authentication, encryption, and the production of a hash value for virtual currency exchanged among peers [18]. Blockchain storage might be a more affordable, secure, and trustworthy alternative to cloud storage [19]. Centralised cloud storage providers ensure data security by making multiple copies of the data and storing them in multiple data centres [20]. Blockchain technology improves the integrity, security, transparency, and traceability of information sent through a business network, saving businesses money by creating new efficiencies [21].

Several industries might benefit from blockchain technology, including tourism, healthcare, banking, and education [22,23]. Blockchain technology benefits multi-step transactions that need verification and traceability [24,25]. It may safeguard transactions, decrease compliance expenses, and speed up data transfer. For example, a product's origin may be verified using blockchain technology.

The main contributions of this article are:

- The capacity to obtain data from IT systems at any given time is known as data access. Users can access this data and its location in a manner allowed by the organization that has it.
- Cloud computing is a rapidly evolving technology with numerous benefits that are expected to continue growing in the future. The use of cloud computing reduces the financial burden of growth. For both consumers and hosts, cloud computing will be a win-win situation.
- Data can be safely and quickly transferred across platforms using blockchain technology. Real estate ownership, title, and other records might potentially benefit from the technology.
- The proposed method for CSDA-BT Blockchain technology produces a record of every transaction that cannot be changed. Fraud, hacking, data theft, and other forms of data loss are all rendered impossible with this secure digital database. The immutable ledger created by blockchain technology is a permanent record of all transactions.

The remainder of the study consists of a discussion of state of the art in the field of CSDA-BT in section 2. The proposed approach in section 3, section 4 exhibits experimental results and analysis. Finally, research is concluded in section 5.

2. Discussed blockchain-based cloud storage data access control algorithm

Premkamal et al. [26] discussed how the cloud can hold a significant amount of data, making it the best choice for outsourcing big data. Currently known techniques of data duplication based on encrypted data schemes do not provide granular control over who may access the duplicated data. This work provides an improved attribute-based access control system with safe duplication to improve large data storage in the cloud-enhanced attribute-based access control with secure deduplication (EABAC-SD). Furthermore, the technique reveals that data owners are not qualified, ownership rights have been revoked, and they cannot contribute data. According to performance studies, EABAC-SD technology is more efficient.

Qi et al. [27] proposed that the Industrial Internet of Things (IIoT) presents a potential opportunity for developing digitalised industrial systems. IoT participants may identify goods using radio frequency identification, a key component of IIoT. This study suggests a secure industrial data access management strategy for cloud-enabled IIoT. Cloud-aided IIoT data access control is designed to enforce fine-grained access controls and item-level data security. Several optimisation strategies have been proposed to enhance the efficiency of computer service providers while maintaining item-level data security. Xu et al. [28] introduced a breakthrough fine-grained access control strategy based on the Cypher and attribute-based encryption (CP-ABE) method, enabling cloud storage to keep its data safe and secure. After comprehensively investigating the CP-ABE algorithm's underlying theory, an envelope-based control system for fine-grained cloud storage is developed. An algorithm is devised to implement the new scheme development process. Simulated findings demonstrate that the proposed data access control technique may increase encrypted search performance and enable fine-grained access in cloud storage environments. Peng et al. [29] Growing WSNs transmit massive volumes of data to a central server, necessitating access control measures to keep the information safe. To better store, manage, and use data from large-scale WSNs, big data (BI) systems are deployed. Traditional access control methods will significantly impact the

performance of (WSN-BI) big data systems. First, this article examines the standard access control strategy's data processing flow, time complexity, and impact on system performance in large data systems. The suggested approach has considerably improved test performance, even in the same test environment and security policy. Chandel et al. [30] detailed the cloud's advantages have opened the road for widespread use. However, there are several security and privacy dangers associated with cloud-based storage, which data owners must be mindfully aware of. Some academics have suggested using Attribute-based encryption (ABE) to safeguard sensitive information. The cloud has numerous advantages, but security remains a significant concern. Data privacy and access control may be ensured with the AES-CP-IDABE advanced encryption standard, cypher text, and attribute-based encryption. The proposed approach was faster in execution, encryption, and decryption than the current ABE method.

Mubarakali et al. [31] discussed how Personal Health Records (PHRs) are increasingly being used as a trading platform for medical data. Protection and data security issues arise when PHR is deployed in a distributed computing architecture, and it may be used to identify trusted cloud servers and flag them as such. In addition, the PHR framework has many customers and data owners who may place a substantial computational and administrative burden on the framework's pieces, limiting the PHR information's accessibility and usefulness. An attribute-based Health Record Protection method has been developed to address the problems raised in the preceding paragraph by providing information access control confidentiality, credibility and secrecy.Xu et al. [32] proposed when it comes to large-scale Internet of Things (IoT) devices, the cloud offers a cost-effective and flexible alternative for data storage and administration (CSPs). However, various data security and privacy problems must be solved for the strategy to be widely used. For example, data confidentiality in the IoT cloud may be protected using attribute-based block ciphers, giving fine-grained access control over encrypted data. However, some security issues can't be addressed by existing attribution-based solutions, such as stolen or leaked user secret keys, owing to various causes.

Agrawal et al. [33] introduced access control mechanisms for mobile cloud environments that may be made more secure by using dynamic features of mobile devices. Mobile network issues, such as dropped calls, must be addressed immediately. The suggested method enables access control and data secrecy using dynamic characteristics encryption. When a network connection fails, the mobile agents work in pairs to fix the problem. Using the anonymous key-issuing technique to disperse the secret key safeguards the user's confidentiality. We put the method to the test in a production-ready mobile cloud setting and examine the data we collect. Susilo et al. [34] detailed that cloud computing is a paradigm shift that may dramatically cut the prices of hardware and software resources in computer infrastructures. As a result of this ease of use, businesses have effectively used cloud storage for internal data sharing. Initially, it appears that keeping the shared data on the cloud in plain text and encrypting it with adequate access control is acceptable. However, to prevent unwanted access to the shared data, it must be encrypted and kept in cipher text with proper access controls. Unfortunately, there may be evil workers who desire to depart from the mandated sharing rules. Chen et al. [35] prepared to dynamically re-encrypt data access control in cloud computing storage to improve security, shield user privacy, and solve the problems of low data access control accuracy and high energy consumption caused by current methods. The relationship between data nodes is shown by constructing an access control tree grounded in the data preparation. Controlling who has access to data stored in the cloud requires key generation, encryption, re-encryption, decryption, and the dynamic re-encryption method for data security state transition.

Khalid et al. [36] discussed that cloud service providers must establish a secure data storage, sharing, and retrieval framework to deliver trustworthy services to end users. Data computation in real-time and

decision delay are two of the cloud service's challenges. With this idea, fog computing places cloud capabilities at the network's periphery. So, this research aims to characterize and categorize different privacy-protecting and access-control systems in the fog computing environment and to convey their value in this context. Alshammari et al. [37] detailed when it comes to data storage. Cloud computing is revolutionary because it eliminates the need for extra gear, which may be expensive, cumbersome, and need additional room. Large volumes of data may be cost-effectively stored on the cloud. As a result, only legitimate people may access the data, which is protected from those who are not. However, this method cannot solve the problem of trust. These researchers aim to find the most practical solution to T-RBAC approaches' trust issues by investigating the roles and tasks of trustworthiness evaluation. They suggest a multifaceted trust model that uses a cryptographic T-RBAC to protect the confidentiality and integrity of information kept in the cloud.

Security difficulties, cost management, and lack of resources knowledge are the most pressing issues for cloud computing. Many people don't know what blockchain is or how it works, and this is a major obstacle to its widespread adoption in industries other than banking. Investing and exploring new ideas are being hindered by it as well.

3. Relevant work in the field of cloud storage data access control using blockchain technology

Individuals are permitted access to firm data only if they do this for the company they claim to represent. In other words, access control restricts how data may be used. For data security, bunting argues that two-factor authentication and permission are crucial. Security measures prevent access to data and data processing systems. In a data breach, they help reduce the possibility of information being accessed without proper authorization. Because many small firms collaborate to share processing power and storage space, blockchain provides a safe and inexpensive cloud storage method. As a result, organizations contributing computer power can be compensated, and cloud storage expenses can be reduced.

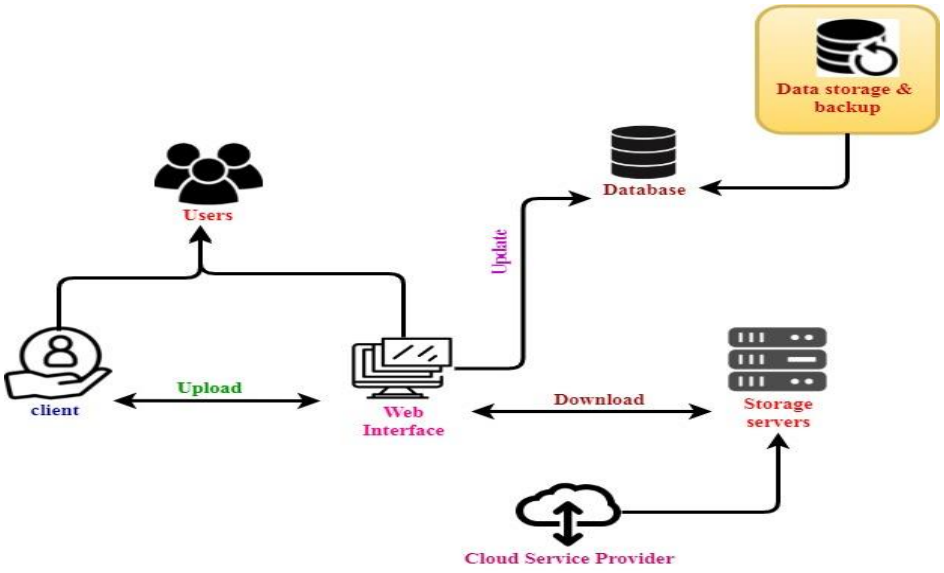

Figure 1: Cloud storage data access

Figure 1 shows that any person purchasing or paying for service is considered a customer. Clients may include businesses and other organizations. On the other hand, clients seem to have a contractual agreement with the supplier. A user is a person who uses, abuses, or puts anything into action. A computer user is a person that uses a computer for work. A person with a substance abuse issue is an example of an end-user.

A data transfer occurs when you send data from your device to another device over the internet, another user's computer, or a network location. Using a file transfer software may send files straight from the computer to the recipient's computer via the server. Data is transferred from the computer to the Internet through uploading. Even clicking on a link on a web page transmits a little data to the web server. The computer is getting data from the Internet when it is downloading. This web app may access data and programs on a remote server from the local machine. Once the content is downloaded from a web server, a user's web browser acts as a client by making it possible for them to engage with it.

A database is any organized data stored digitally, often on a computer. The process of managing a database often involves the usage of a database management system. Accessing and processing the data may be done quickly and easily with this method. The services and solutions a cloud computing company offers are useful for both businesses and individuals. Their services, including virtual hardware, software, and infrastructure, might be rented from and managed by this service provider. This is possible to employ a storage server to keep digital data, files, and services safe and easily accessible. On the server, various data sizes may be stored and accessible via the Internet or shared network. Small to large volumes of data can be kept on the server and accessible over the Internet or a network shared by other computers. A file server is another term for a storage server. Storage is storing the data in a secure area that can be accessed at a moment's notice. This is best to keep just the functioning versions of the files in the cloud. Backing up data is storing additional copies of the files outside of where they are already stored.

$$m = \sqrt{I+1} \times \int \log\ (i) \pm (I) \qquad (1)$$

The Eq. (1) denotes m for cloud storage performance, I for data storage, log is the logarithmic function for download, i for a web interface. Megabyte second is the most fundamental storage performance metric. Typical hard disc drive seeks times are reported in milliseconds, and rotational latency may be computed using the drive's spindle speed. Visitors may monitor the cloud resources using metrics to verify that all components connect properly. It is common for cloud performance measures to be based on input/output operations per second, file system caching, and auto-scaling.

$$Z = \int (\alpha + \beta) \sum \tan^{-1}\ (\theta) + e^{l} \frac{l}{e-1} \qquad (2)$$

Eq. (2) says Z for the impact of cloud data access, α is the mathematical function for data users, $\tan^{-1}$ for trigonometric function in backup, θ for mathematical function in the update, β for mathematical function in data shared, e for services, l for storage. Cloud computing enables constant access to data and its related analytics. Enterprises might use this method to accelerate new goods or services to market and quickly execute changes. This is a must in sectors that undergo fast change to remain competitive. In the cloud, data, and analytics are always available. Enterprises might use this method to accelerate goods or services to market and execute changes more quickly. This is a need in today's fast-paced business environments.

$$j = \frac{1}{L} \sum \max_{2}(L) \div \iint L \qquad (3)$$

Eq. (3) denotes j for storage data service, $\max_{2}$ maximum for users, L for storage. Having a safe place to save important company information is crucial to success. Files related to accounts payable, cost reporting, and other processes must be stored securely. Records, such as budgets and procedures, must continue to be easily accessible. Storage management refers to the processes and tools optimizing data storage capacities. By adopting these practices, businesses may save on IT expenses while storing more

data on their current infrastructure, gaining efficiencies in data retrieval, security, and compliance with data retention rules.

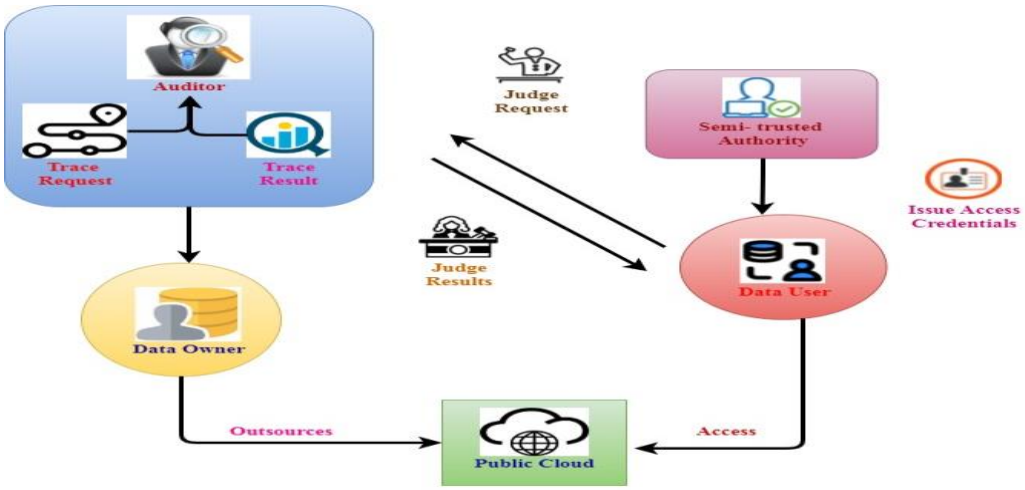

Figure 2: Cloud storage data access control

Figure 2 shows data in the company; owners are responsible for the quality of one or more data sets. Several actions fall under this umbrella, such as ensuring definitions are in place, addressing data quality concerns, and reporting on data quality. An auditor's responsibility is to perform an audit, which may be either an individual or a business. To work as an auditor, one has to be accredited by a recognized body or have other qualifications deemed enough by that body. For example, White Hat Gross Man published a report explaining a vulnerability that might allow an attacker to obtain cookies and possibly website passwords. Family members or friends may send a letter to a court before the sentence to describe a defendant's character. It is also common for victims to write similar letters describing how the defendant's acts harmed them. Human resource management, facility management, supply chain management, accounting, customer service, marketing, drafting of CAD designs, research and content creation, engineering, and diagnostics are typical tasks businesses outsource. A third-party supplier manages the infrastructure and provides on-demand computing services. It is a public cloud model. In a public cloud, anybody may purchase and use computer resources. Several people use a public cloud simultaneously. "access" refers to a person's ability to enter or depart a certain location. Roads leading to major highways are an example of access points. An individual's right of access refers to their ability to use, speak with, or approach another individual. An example of access is being granted permission to enter a restricted place. It includes login or identifying numbers, security keys, tokens and techniques, technology, and equipment used to confirm a person's identity, as well as access rights and the use of services, all of which are examples of authentication mechanisms.

$$C = \cos\ (K) \div (\int \sin\ (\beta) \frac{\pi}{2} \times \frac{1}{3}) \qquad (4)$$

Eq. (4) denote C for public cloud performance, $\cos$ is the trigonometric function for access, K for outsources, β is the mathematical function for request, π for the mathematical function for data usage. According to the author of a new book on corporate design, public clouds offer an advantage over their internal equivalents in security, stability, and flexibility. On the other hand, private cloud services may be less secure and dependable than public cloud services. Contrary to what was stated above, private or enterprise clouds are employed by enterprises with a high value on data security and compliance.

$$k = \iint \cos^{-1}(g) \div \sum(N) \qquad (5)$$

Eq. (5) says k for the development of tracing requested, $\cos^{-1}$ is the trigonometric function for auditor, g for semi-trusted, N for judge result. Tracing is a software engineering technique that uses special logging to keep track of a program's execution. System administrator logs fall into a linguistic grey area because they record software-to-use or operating-system events that are relevant only to system administrators. Tracing the execution of code throughout a distributed system is crucial for keeping tabs on bugs and improving performance, particularly in systems where new services are constantly being added.

$$U = \sqrt{1 - T} \times \frac{1}{(V-1)} \sum V \qquad (6)$$

Eq. (6) denotes U for data owner, T for tracing, V for monitoring. People or groups that make decisions about just data is used and who have access to it are called data owners. Even if homeowners don't often access their data, it is their responsibility to ensure its safety and security. To be a Data Owner, a person must be a senior business member. Because of this, they must be given power and the funding or resources necessary to carry out data cleansing.

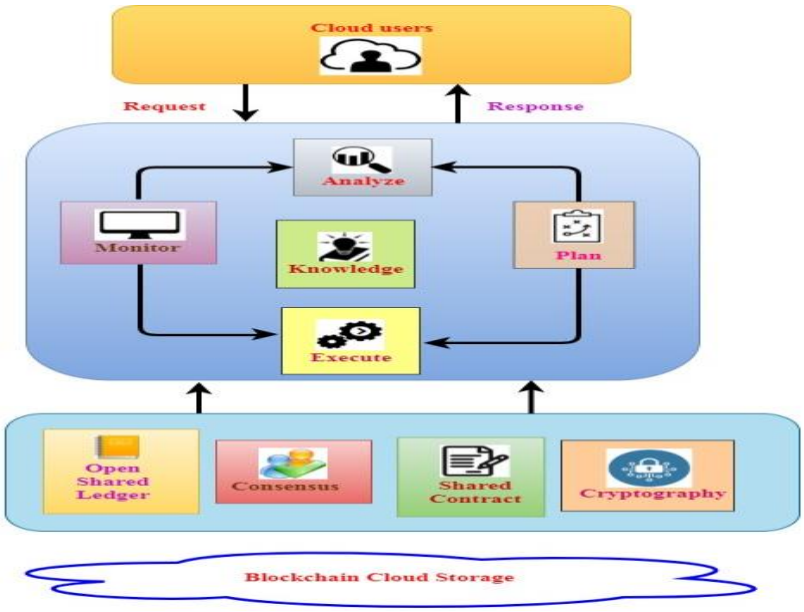

Figure 3: Blockchain using cloud storage

Figure 3 illustrates that the cloud is utilised for offsite replication, recovery procedures, communication, terminal emulators, software development and evaluation, big data analytics, and customer-facing internet applications. These are just a few of the numerous purposes of cloud computing for enterprises of all sizes and industries. Medical diagnosis is one instance of an analysis. Analyze a fossil substance, a language or a word, or an action to determine its morality to determine the constituents or nature of the investigated entity. The output device of a computer monitor is a picture or text display. The display, electronics, case, and power supply are the most common parts of a monitor. A plan may be defined as a paper, plan, or diagram that outlines the next step. An example of a plan is a list of activities that must be completed to complete a project. Learning, understanding, or being aware of something is a form of knowledge. Learning the alphabet is an example of knowledge. An example of knowledge is the capacity to locate a certain place. Being informed or aware of something is a state of awareness of certain information or circumstances. Work execution is carrying out scheduled maintenance work while following a predetermined timetable. The maintenance professionals should do the given task. All work should be done under-acknowledged,

under-acknowledged good maintenance practices: Independent computers record, share, and sync transactions in their electronic ledgers using distributed ledger technology.

Append-only mode is used to link blocks of data together on the blockchain. Consensus is defined as an agreement reached by a group. By reaching an agreement on the contents of a document via a process called consensus, a group may increase the likelihood that all its members understand and support the same decision. Non-affiliated third parties' benefit from contracts in which the seller or any of its subsidiaries or affiliates are parties, as well as any retained business. In contrast to conventional banking systems, cryptocurrency does not depend on banks for transaction authentication. Using this decentralized system, everyone in the globe may send and receive monetary transfers. All bitcoin transactions are recorded in a public ledger, and cryptocurrency holders hold them in digital wallets.

$$Y = \frac{1-O}{t} \times \log\ (t) \div \sum O \qquad (7)$$

Eq. (7) denoted Y for cloud user services, and $\log$ is the logarithmic function for a response, O for execution, t for a plan. Third-party providers host infrastructure, platforms, or software in the cloud, then make it available to customers online. All one needs to access cloud services is a device with a file system, an internet signal, or a virtual private network. Computing in the "cloud" makes it possible for a single computer to access the collective resources and databases of many other computers connected to a network. In addition, cloud computing allows users to save them on remote databases instead of relying on local hard drives or storage devices to keep the files and data.

$$v = \frac{\delta u}{\delta H} \pm \int \frac{\pi}{2} \times (u - H) \qquad (8)$$

The Eq. (8) says v for shared contract strategy, δ is the mathematical function for analysis, π is the mathematical function for knowledge, u for execute, H for cloud users. Pre-design through post-construction is when an organization's contract strategy must be considered to complete all major objectives. If there is ever a disagreement, it is better to have a contract that specifies the terms agreed upon and the extent of services provided, for the obvious reason that the terms and conditions have been clearly spelt out and agreed upon by all parties.

$$s = \int \sin^{-1}\ (\theta) + \sqrt{1 - X} \pm \widehat{M} \qquad (9)$$

Eq. (9) denotes for development of blockchain cloud storage, $\sin^{-1}$ is the mathematical function for cryptography, M for users, X for the database. A blockchain is a distributed digital ledger stored on computers worldwide, and these records are stored in a form that prevents them from being altered in the future. For enterprises developing blockchain applications, third-party providers may create and administer cloud-based networks for them. Blockchain technology's burgeoning realm, these third-party services are a relatively new phenomenon.

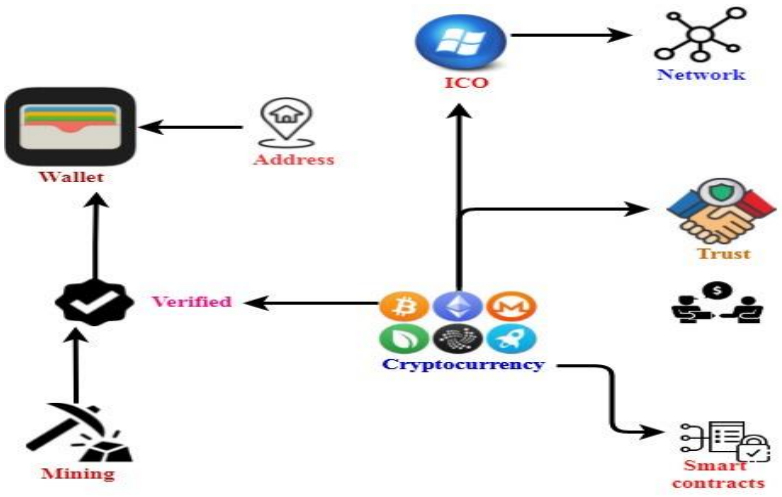

Figure 4: Blockchain technology

Figure 4 shows that Users may store and manage their Bit, Ether, and other cryptocurrencies in a blockchain wallet. It is possible to send cryptocurrencies and convert them back into the user's native currency using a cryptocurrency wallet. A blockchain address resembles an email address in that it is a unique string of numbers and characters. An address on the network that may only be used once is called a "destination address." Every time someone wants crypto, they should be given a different address. Verifying your identity is an important step in preventing identity theft and ensuring that no one else but you has access to credit card information. Depending on the degree of verification you pick, the user will access additional services and larger trading limits. An initial coin offering (ICO) does not include the sale of any actual shares. Instead of a bitcoin token, ICO businesses provide a blockchain token that is essentially a piece of the company. When you buy a well-known current token, such as a cryptocurrency, users often receive an equal amount of new tokens in return. An app's distributed ledger and smart contract services are hosted on the blockchain. Blockchain network administrators and end-users may both be consumers of apps. Chaining blocks guarantees that the content of a block is always reliable. Every machine on your network will verify a transaction using the blockchain, for instance, a payment statement. Blockchain transactions record, verify and settle all aspects of the transaction within seconds across every node. In the event of a validated change being recorded on one ledger, it is simultaneously recorded on the other.

Compared to traditional financial sectors, cryptocurrencies do not depend on banks for transaction authentication. Using this decentralized system, everyone in the globe may send and receive monetary transfers. All bitcoin transactions are recorded in a public ledger, and cryptocurrency holders hold them in digital wallets. It means smart contracts are blockchain-based computer programs that run only when specific conditions are met. By eliminating the need for a third party or lengthy procedure, automated contracts provide clarity for all parties involved. Mining verifies each blockchain transaction while using bitcoins or any other cryptocurrency. It comprises many bitcoins, each with a unique data code for a single block. The term "chain" refers to the linkages between the various blocks.

$$F = \sqrt{Q} * \max_{2}(\pi) \pm \sum \tan(\theta) \qquad (10)$$

The Eq. (10) denotes F for blockchain processing, tan trigonometric function for trust, $\max_{2}$ Maximum for contract, π is the mathematical function for ICO, $and\ \theta$ is the mathematical function for Q in mining. In a blockchain, information is recorded, not to be altered, hacked, or manipulated. The ledgers of all participants in the blockchain are identical, and each individual possesses a copy of that ledger.

$$G = \sqrt{(a+b)} \div (\alpha + \beta) \int \min_{2}(a) \qquad (11)$$

The Eq. (11) says G for blockchain in the smart contract, α is the mathematical function for data storage, β for the mathematical function in smart storage, $\min_{2}$ for minimum in currency, a for data, b for address. In other words, smart contracts are blockchain-based computer programs that run only when certain conditions are met. By eliminating the need for a third party or lengthy procedure, automated contracts provide clarity for all parties involved.

$$P = \frac{R}{S} + \sqrt{(q)} \times \sum \operatorname{csc}(\theta) \qquad (12)$$

The Eq. (12) says $P$for blockchain in data mining, csc is the trigonometric function for wallet, θ is the mathematical function for verified, q for address, R for outsources, S for storage. Bitcoin transactions are secured and verified using Blockchain mining, a peer-to-peer computing process. Blockchain miners contribute transaction data to the global public ledger of prior transactions maintained by bitcoin. Mining is the process of verifying transactions.

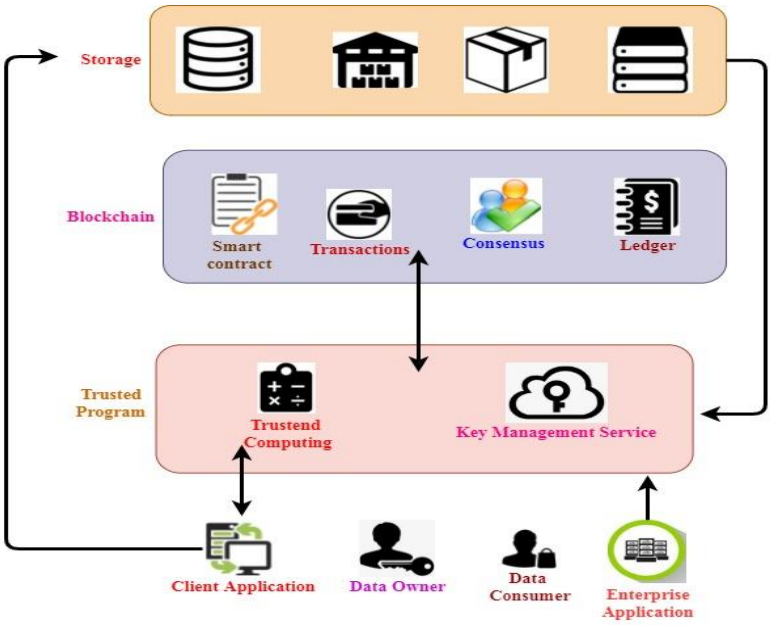

Figure 5: Blockchain storage and control

Figure 5, shown in Storage, is a permanent home for the software, operating system, and files. Because computers depend on storage systems to store and retrieve data, the speed at which the system can boot up, load, and access data is directly correlated to the storage system's capacity. Changing, hacking, or cheating the blockchain is extremely difficult, if not impossible. As previously stated, a blockchain is a distributed digital database of copied transactions. Data detailing a transaction is sometimes referred to as "data information." This data type is always dated, numerical, and relates to larger items. Orders, invoices, and payments are a few common business transactions. An agreement reached by a group is a consensus. Consensus may be shown in a bill's text, which is agreed upon by both republicans and democrats. An approach to decision-making that aims for broad consensus among the group participants. A general journal of accounts records financial activities that should appear on an income and balance sheet. Journal entries

in the accounting ledger can contain money in the bank, accounts receivable, money invested, money to be paid out, and money from customers.

Trusted computing means many methods and ideas for improving computer security by changing the hardware and software that support it. Key encryption and other sensitive data can be stored in a computer's sealed storage. Protecting cryptographic keys from loss or improper use is a primary goal of key management servers (KMS). KMS platforms and other important management technologies govern the creation, distribution, usage, storage, archiving, and deletion of encryption keys. Using the client-server paradigm, jobs or workloads are divided between service providers as servers and users as clients who request resources or services from the service providers as servers. Large software systems developed for use in a corporate setting, such as industry-government, are called enterprise applications (EA). A computer-based information system must include enterprise architecture software to function properly.

$$m = \sqrt{(1 - C)} * \sum \frac{1}{2}(\alpha + \beta) \qquad (13)$$

The Eq. (13) denotes m for data storage in blockchain, α is the mathematical function for contracts, β for the mathematical function for transactions, C for the ledger. Thanks to blockchain storage, it's possible to store files in a blockchain manner using people's idle, hard drive space worldwide. In addition, it can alleviate many of the issues that plague central cloud storage by using local technology.

$$X = \int \cos(\pi) + \iint f(A)dx \qquad (14)$$

Eq. (14) states that X represents a trusted program, where cos is the trigonometric function for blockchain, π is a mathematical constant for transfer, f is the data owner, $and\ A$ represents computing. Trust is the confidence in the capability of a machine or sensor to perform predictably, safely, and reliably in a certain situation. Electronic certificates, digital signatures, and cryptography are the main methods for establishing confidence in computer systems.

$$O = \sum(n) \iint \log\ (D) \div \int (D) \qquad (15)$$

The Eq. (15) denotes O for blockchain application, and log is the mathematical function for the data owner, D for the data consumer. Financial services, healthcare, government, travel, and hospitality are just a few areas where blockchain technology may be used. The financial services industry is one of the first areas to use blockchain technology innovatively.

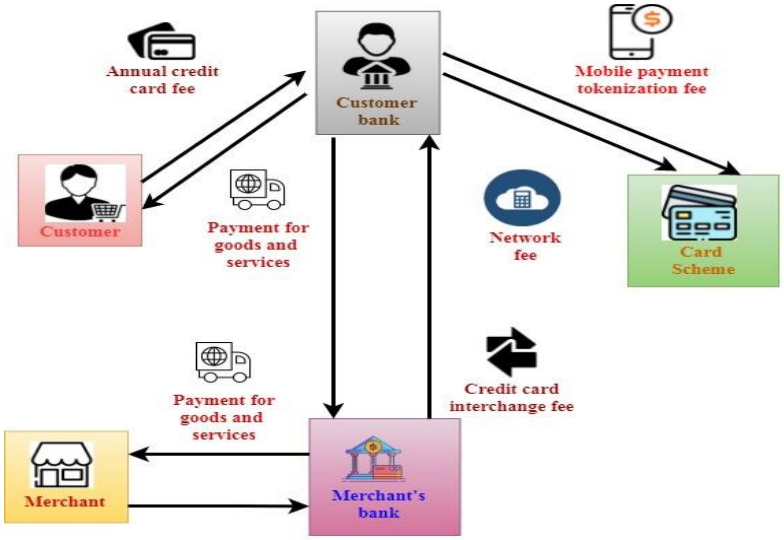

Figure 6: Blockchain in algorithmic control

A banking institution, seen in Figure 6, is defined as a business that accepts deposits and makes loans to customers. Banks provide more than deposit accounts and lend money; they also manage assets, trade currencies, and provide safe deposit boxes. Banks may choose from several different sizes and shapes. Many types of banks exist, including retail, commercial or corporate, and investment banks. An individual who purchases goods or services from a business is called a "customer." The term "client" describes a person looking for a business to provide them with a professional service. There are several definitions of what it means to be a trader. There has been a long history of industry, business, and trade merchants. Multinational enterprises' foreign financing is handled by merchant banks, financial institutions, and organizations specializing in this type of financing. When compared to other sorts of financial organizations, these stand apart. Therefore, they aren't able to interact with the public.

Merchant banks may also handle other overseas transactions. American Express, union pay, and card are well-known card schemes. Cardholders, merchants, and acquiring banks are the primary participants in the card scheme process. Membership, transaction, or other fees, assessments, or charges that the Network imposes on the Bank, as the issuer of the Credit Cards, are referred to as Network Fees here. It is common practice to trade goods and services for money or other forms of value. After all, the parties have agreed to the conditions. Payments are normally issued. All modes of payment, including cash, check, wire transfer, credit card, and debit card, are accepted. Every time someone uses a credit or debit card in their business to buy something, the merchant's bank account needs to pay an interchange charge. The card-issuing bank's fees cover payment processing charges, fraud and bad debt costs, and the risk associated with approving the payment. In addition, the credit card company automatically charges you an annual fee to keep your credit card account open.

$$Y = \int \sum(r) \div \frac{\pi}{2} \times \frac{W}{z} \tag{16}$$

Eq. (16) denoted Y for mobile payment tokenization fee, π is the mathematical function for card scheme, r for network fee, W merchant, z for a customer. This innovative payment mechanism uses a unique identification number known as a 'token' instead of sensitive debit or credit card information during a digital transaction. As a result, online transactions are more secure, as the user no longer has to disclose their credit card information.

$$J = \int \sum E * \log\ (\emptyset) \pm \frac{\pi}{2} \tag{17}$$

Eq. (17) says J for credit card merchant service fee, log is the logarithmic function for a bank, $\emptyset$ for mathematical function in a customer bank, π in mathematical function for card interchange, E for goods services. For instance, customers may see service charges from banks charging fees not part of their network or vendors charging fees for using a credit card to pay. Customer service fees or maintenance costs may also be referred to as follows.

$$p = \int \sin\ (\theta) \times \sqrt{(N+1)} \tag{18}$$

The Eq. (18) denotes p for collecting payment for goods service; sin is the trigonometric function for blockchain, θ is the mathematical function for service, N for a customer. Involves the transfer of products from one party to another, whether it is a supplier, a buyer, or another entity. The point at which the flow of products comes to an end to be delivered to the intended receiver. The site where products or services are delivered or consumed is known as the "place of supply. In other words, it's where the recipient of an item or service has registered to get it.

Figure 7 denotes the end-user may usually access them using the cloud service provider's web interface. Users define their storage capacity, prepared before the service can supply cloud resources. It's possible that protecting data in the cloud is the same as protecting it in a conventional data center. Verification and recognition, security systems, decryption, secure destruction, error detection, anonymization, and so on are all examples of data protection technologies that might be employed in cloud computing.

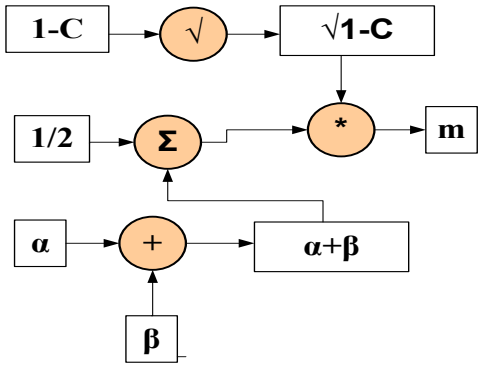

Figure 7: Flow diagram of the client data storage in cloud access

4. Experimental analysis of cloud storage data access control algorithm

Analytical data can be accessed using a cloud-based analytics application. All of the accessible data sources, data formats, processing techniques, computing infrastructure, approaches to address, and storage infrastructure may be seen via a single interface. Cloud analytics is an excellent match for multinational firms since it facilitates increased sharing and cooperation among personnel. In the cloud, employees may effortlessly share data and work on real-time analytics from any location on the planet. It means that even if the wrong people get their hands on the data, they won't use it if the encryption keys are still secure. Data stored in the cloud is particularly vulnerable to a compromised provider, account, or system, so this is especially important. An important part of compliance is where an organization's data is located, which can be accomplished through data storage management. Documentation, automation, redaction, and governance tools are among the guidelines for compliance. Compliance can also be achieved by storing data in an immutable manner.

4.1 Comparison of secret key computation time

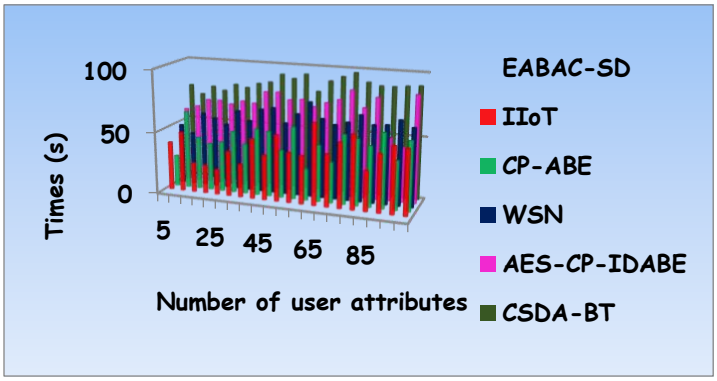

Figure 8: Comparison of secret key computation time

Figure 8 shows that integers are commonly used in computer encryption as a key. Random number and pseudo-random generators are sometimes used to create keys, and data generated using a pseudo-random generator seems random to the naked eye. Symmetric, or secret-key, encryption relies on a piece of information or parameter to encrypt and decode messages. In cryptography, there are two kinds of keys public and private. A set of guidelines referred to as the key distribution procedures can make this possible, or more parties interacting via an unsecured network can share a secret key in this fascinating area of cryptography.

4.2 Inconsistency of the Task Scheduling Framework

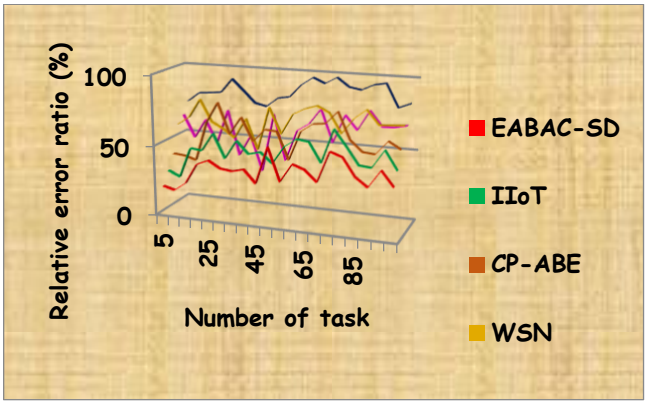

Figure 9: Relative error of the task schedule framework

Figure 9 shows that a task scheduling algorithm collects rules and policies for allocating tasks to the most appropriate resources to maximize performance and resource efficiency. Scheduling challenges include finding the best possible timetable for various objectives, diverse machine settings, and the unique qualities of the works themselves. The user may choose whatever number of jobs and as many parallel computers as they like. The environments page provides an in-depth look into machine environments. Round-robin scheduling is used when numerous jobs have the same priority. However, if more urgent work arises, it will take precedence. They halt the current work and move on to something of higher priority. An example of this scheduling technique is a barcode scanner.

4.3 Number of changes of searching files

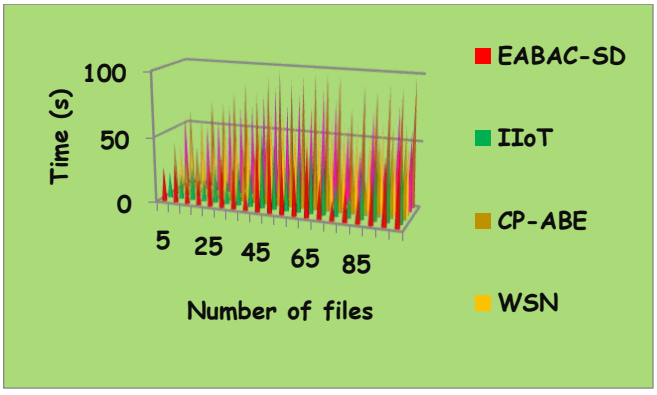

Figure 10: Number of changes in searching files

According to users, Figure 10 shows indexing choices can slow down file explorer. If users wish to address this issue, remove huge directories with many nested folders and files from the index. An easy-to-

navigate search engine can locate files and folders based on their name, save the date, or size. The computer and apps can quickly identify material by searching for keywords or common attributes like the date a file was generated in a digital index like a book's index. Files may be found by opening the file explorer and then using the search bar that appears to the right of the address bar. The search tools tab opens when users click within the search area.

4.4 The number of security policies

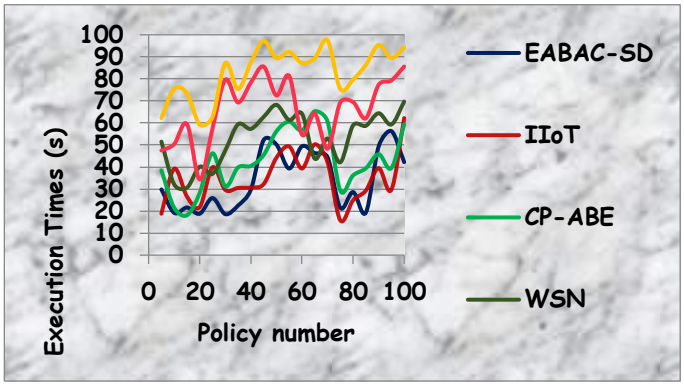

Figure 11: Number of security policies

Figure 11 shows clearly that a company's security policies are the rules, regulations, and protocols it has established to protect its information systems and the data inside them. Organizations with well-established security policies are more protected than those that do not. Conformance to security policies is vital for large-scale critical cyber infrastructures. The complexity of these systems necessitates an automated method, the risk of insider assaults, and the potential speed of an attack on a system. To put it another way: A security standard is an established common language, and it is supposed to be used consistently, as a rule, a guideline, or a definition, according to the definition provided by the International Organization for Standardization. To enhance the safety and security of information technology, specific requirements are necessary.

4.5 Communication of the data owner

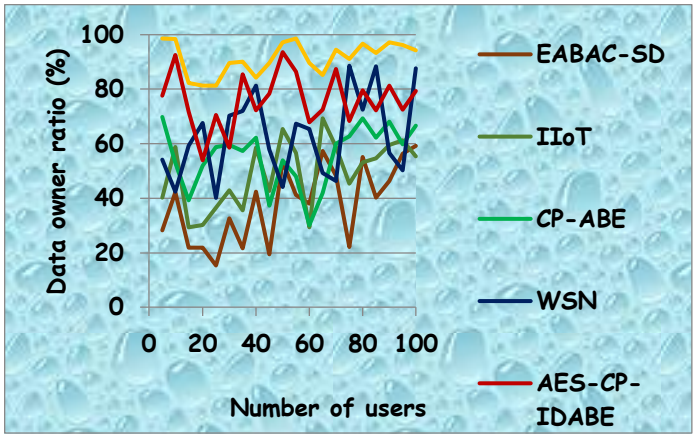

Figure 12: Communication of the data owner

Figure 12 states that they are responsible for ensuring that the information assets in their functional areas are accessible to those who need them. Data Owners can manually review and approve each access request

or develop a set of rules to determine who is authorized to access data based on their business role, support responsibilities, or other factors. Simply put, the data steward's job is to help the end users. This person is responsible for gathering, evaluating, and reporting data-related concerns and difficulties. Subject matter or line-of-business assignments are typical ways data stewards are appointed. In addition, a data steward is responsible for storing and disseminating sensitive information inside the company. This duty becomes more important when a company's data includes confidential information that might fall into the wrong hands.

4.6 The computation time of key generation

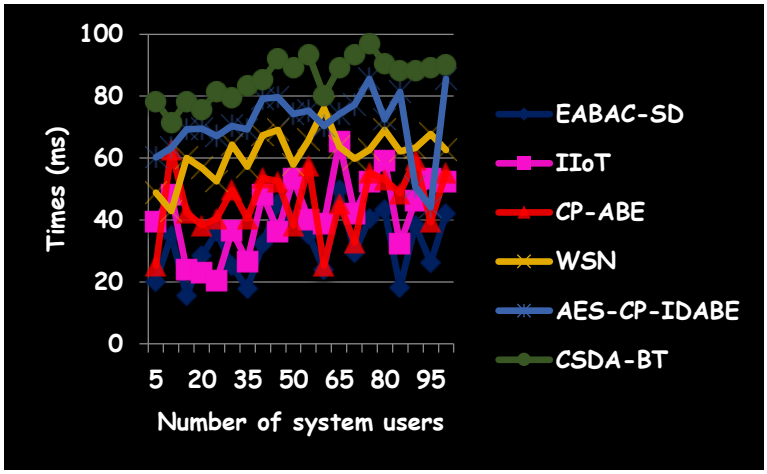

Figure 13: Computation time of key generation

Figure 13 refers to thinking, solving, and programming in a computational manner. There are several ways to generate cryptographic keys, encrypted and decoded using a key. The throughput of any encryption operation is determined by dividing the entire encrypted text by the encryption time. Adding up or calculating with a computer is known as computing, and adding up receipts is one form of calculating. Every goal-oriented activity that relies on benefits from or is created by computers is called computing. The process includes algorithm research and development and hardware and software design. Science and technology are intertwined with the humanities and the arts.

5. Conclusion

Cloud storage allows data to be stored on remote servers and accessed online. Regarding data management, users often pay a monthly or per-consumption cost. Cloud computing has enabled students to access resources from any device, at any time, from anywhere. The university's website is a hub for both application and online study. Since the advent of cloud computing, institutions can now store vast amounts of data securely in the cloud without incurring the time and expense of building specialised data centers. An analytic algorithm in the cloud is applied to data stored in a private or public cloud to provide a result of interest. Cloud analytics uses flexible cloud computing and advanced analytic tools to identify data patterns and derive new insights. Technology that uses the internet to store data and information alters how businesses operate. There is no limit to the amount of data stored on the cloud.

Funding: No specific funding received for this research.

Data Availability: This article used no external data.

Conflicts of Interest: No conflict of interest is stated by the authors.

Authors contributions. Conceptualization: HSS MHI; methodology: HSS, MHI, MIK validation: MHI, MIK; writing—original draft preparation, HSS, MHI; writing—review and editing: MHI, MIK; visualization: HSS, MHI; supervision: HSS, MH; The authors had approved the final version.

AI usage declaration: Grammarly Premium was used solely for proofreading and improving linguistic quality.

References

1] Xiong, S., Ni, Q., Wang, L. et al., (2020). "SEM-ACSIT: Secure and efficient multiauthority access control for iot cloud storage". *IEEE Internet of Things Journal*, 7(4), 2914-2927.

[2] Anilkumar, C., and Subramanian, S. (2021). "A novel predicate based access control scheme for cloud environment using open stack swift storage". *Peer-to-peer Networking and Applications*, 14(4), 2372-2384.

[3] Shiny, S., and Jasper, J. (2022). "Decentralized access control technique with multi-tier authentication of user for cloud storage". Peer-to-peer Networking and Applications, 15(1), 13-27.

[4] Yang, Y., Chen, Y., Chen, F. et al., (2022). "Identity-based cloud storage auditing for data sharing with access control of sensitive information". *IEEE Internet of Things Journal*, 9(13), 10434-10445.

[5] Ezhilarasi, T. P., Sudheer Kumar, N., Latchoumi, T. P. et al., "A Secure Data Sharing Using IDSS CP-ABE in Cloud Storage". *Lecture Notes in Mechanical Engineering*, Singapore, Springer Singapore, 1073-1085, 2021.

[6] Dhal, K., Rai, S. C., Pattnaik, P. K. et al., (2022). "CEMAR: a fine grained access control with revocation mechanism for centralized multi-authority cloud storage". *Journal of Supercomputing*, 78(1), 987-1009.

[7] Riad, K., Huang, T., and Ke, L. (2020). "A dynamic and hierarchical access control for IoT in multi-authority cloud storage". *Journal of Network and Computer Applications*, 160, 102633.

[8] Prince, P. B., and Lovesum, S. P. J. (2020). "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system". *SN Computer Science*, 1(5).

[9] Bhise, A. S., & Toushif Latif, P. M. (2019). "Secure cloud storage system by integrating trust with role based access control and cryptographic algorithm". *In Techno-Societal 2018: Proceedings of the 2nd International Conference on Advanced Technologies for Societal Applications* 2, 87-97. Cham: Springer International Publishing.

[10] Ning, J., Huang, X., Susilo, W. et al., (2020). "Dual access control for cloud-based data storage and sharing". *IEEE Transactions on Dependable and Secure Computing*, 1-1.

[11] Verma, O. P., Jain, N., and Pal, S. K. (2020). "Design and analysis of an optimal ECC algorithm with effective access control mechanism for big data". *Multimedia Tools and Applications*, 79(15-16), 9757-9783.

[12] Xue, K., Xue, Y., Hong, J. et al., (2017). "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage". *IEEE Transactions on Information Forensics and Security*, 12(4), 953-967.

[13] Ahuja, R., and Mohanty, S. K. (2020). "A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage". *IEEE Transactions on Cloud Computing*, 8(1), 32-44.

[14] Huang, Q., Yang, Y., and Wang, L. (2017). "Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things". *IEEE Access*, 5, 12941-12950.

[15] Sookhak, M., Yu, F. R., Khan, M. K. et al., (2017). "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues". *Future Generation Computer Systems*, 72, 273-287.

[16] Li, F., Liu, B., and Hong, J. (2017). "An efficient signcryption for data access control in cloud computing". *Computing*, 99(5), 465-479.

[17] Wang, R. (2017). "research on data security technology based on cloud storage". *Procedia Engineering*, 174, 1340-1355.

[18] Lan, C., Li et al., (2017). "A new security cloud storage data encryption scheme based on identity proxy re-encryption". *International Journal of Network Security*, 19(5), 804-810.

[19] Hong, J., Xue, K., Xue, Y. et al., (2020). "TAFC: time and attribute factors combined access control for time-sensitive data in public cloud". *IEEE Transactions on Services Computing*, 13(1), 158-171.

[20] Fan, K., Wang, J., Wang, X. et al., (2017). "A secure and verifiable outsourced access control scheme in fog-cloud computing". *Sensors*, 17(7), 1695.

[21] Hu, C., Li, W., Cheng, X. et al., (2018). "A secure and verifiable access control scheme for big data storage in clouds". *IEEE Transactions on Big Data*, 4(3), 341-355.

[22] Li, J., Chen, X., Chow, S. S. et al., (2018). "Multi-authority fine-grained access control with accountability and its application in cloud". *Journal of Network and Computer Applications*, 112, 89-96.

[23] Lin, C., He, D., Huang, X. et al., (2018). "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0". *Journal of Network and Computer Applications*, 116, 42-52.

[24] Fu, X., Nie, X., Wu, T. et al., (2018). "Large universe attribute based access control with efficient decryption in cloud storage system". *Journal of Systems and Software*, 135, 157-164.

[25] Zhong, H., Zhu, W., Xu, Y. et al., (2018). "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage". *Soft Computing*, 22(1), 243-251.

[26] Premkamal, P. K., Pasupuleti, S. K., Singh, A. K. et al., (2021). "Enhanced attribute based access control with secure deduplication for big data storage in cloud". *Peer-to-peer Networking and Applications*, 14(1), 102-120.

[27] Qi, S., Lu, Y., Wei, W. et al., (2021). "Efficient data access control with fine-grained data protection in cloud-assisted IIoT". *IEEE Internet of Things Journal*, 8(4), 2886-2899.

[28] Xu, Q. (2020). "Research on data access control algorithm based on fine-grained cloud storage". *International Journal of Grid and Utility Computing*, 11(4), 468.

[29] Peng, J., Zhou, H., Meng, Q. et al., (2020). "Big data security access control algorithm based on memory index acceleration in WSNs". *EURASIP Journal on Wireless Communications and Networking*, 2020(1).

[30] Chandel, S., Yang, G., and Chakravarty, S. (2020). "AES–CP–IDABE: A privacy protection framework against a dos attack in the cloud environment with the access control mechanism". *Information*, 11(8), 372.

[31] Mubarakali, A., Ashwin, M., Mavaluru, D. et al., (2020). "Design an attribute based health record protection algorithm for healthcare services in cloud environment". *Multimedia Tools and Applications*, 79(5-6), 3943-3956.

[32] Xu, S., Yang, G., Mu, Y. et al., (2019). "A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance". *Future Generation Computer Systems*, 97, 284-294.

[33] Agrawal, N., and Tapaswi, S. (2019). "A trustworthy agent-based encrypted access control method for mobile cloud computing environment". *Pervasive and Mobile Computing*, 52, 13-28.

[34] Susilo, W., Jiang, P., Lai, J. et al., (2022). "Sanitizable access control system for secure cloud storage against malicious data publishers". *IEEE Transactions on Dependable and Secure Computing*, 19(3), 2138-2148.

[35] Chen, X., Zeng, D., Pang, S. et al., (2021). "Cloud computing storage data access control method based on dynamic re-encryption". *Security and Communication Networks*, 2021, 1-10.

[36] Khalid, T., Abbasi, M. A. K., Zuraiz, M. et al., (2021). "A survey on privacy and access control schemes in fog computing". *International Journal of Communication Systems*, 34(2).

[37] Alshammari, S. T., Albeshri, A., and Alsubhi, K. (2021). "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services". *Symmetry*, 13(3), 492.