Global Trends in Science and Technology

ISSN : 3079-5761
Volume 1, Number 4, 2025
https://doi.org/10.70445/gtst.1.4.2025.116-144

Block chain-Enabled Security and Privacy Solutions in Data Management

Hassan Raza[1], Tsendayush Erdenetsogt[2], Muhammad Mohsin Kabeer[3], Muhammad Shahrukh Aslam[4], Mazhar Farooq[5*]

[1]Washington University of science and technology, USA

[2]University of the Potomac, USA

[3]Gannon University

[4]Concordia University, USA

[5]Southern New Hampshire University

[1]hr968182@gmail.com, [2]Tsendayush.Erdenetsogt@student.potomac.edu, [3]Mohsinkabeer86@gmail.com, [4]shahrukhaslam81991@gmail.com, [5]Mazhar.farooq@snhu.edu

open access

Corresponding Author

Hassan Raza

hr968182@gmail.com

Article History:

Submitted: 03-11-2025

Accepted: 26-11-2025

Published: 30-11-2025

Keywords

Block chain, Data Management, Security, Privacy, Cloud Integration, Big Data, Scalability, and Cryptograph.

ABSTRACT

The block chain technology has become a potential solution to improving security, privacy, and trust on contemporary data management systems. Conventional centralized systems are easily breached, tampered with and unauthorized access makes it necessary to have decentralized systems that cannot easily be tampered with. Block chain offers immutability, transparency, and cryptographic security and smart contracts offer automated access control and auditing. Sensitive information is safeguarded using privacy-saving methods, such as encryption, a zero-knowledge proof, and decentralized identity schemes. Scalability and collaboration are further increased with integration with cloud and big data systems. This review identifies the uses of Block chain, challenges and future research direction, which shows that Block chain is capable of changing the way secure and privacy-conscious data management is achieved.

INTRODUCTION

The accelerated development of digital technologies has resulted in the increased volume, speed, and complexity of data created in fields like healthcare, finances, government, social media and Internet of Things (IoT). Data management has become an urgent need in organizations that aim at maintaining data storage, processing, sharing and analysis in a secure and efficient manner. Nonetheless, the conventional data management systems are mostly centralized and are prone to security breach, unauthorized access, tampering of data and privacy invasion [1]. The well-known data leaks and cyberattacks have also demonstrated the weaknesses of current security systems and the necessity to offer more solid, clear, and reliable measures. The Block chain technology has been found to be an up-and-coming paradigm to handle these issues by integrating the concepts of decentralization, immutability, transparency, and cryptographic security in the process of data management [2].

Initially created as the backbone technology of cryptocurrencies, Block chain has since become a flexible platform that can be used to store data securely, provide access control and share data in a distributed environment. Block chain makes use of single points of failure by removing the need to have one trusted authority, and because of this, it is especially helpful in handling sensitive and high-value information and resisting attacks. Two of the most important issues in the contemporary data management are security and privacy [3]. Even though organizations want to use data to benefit themselves in the form of analytics and decision-making, the organizations must take care of confidentiality, integrity, availability, and adherence to data protection in regulations. The solutions that are provided by Block chain have novel mechanisms like distributed ledgers, consensus protocols, cryptographic hashing, and smart contracts to implement data integrity, traceability, and controlled access [4]. Also, privacy-preserving methods such as encryption, anonymization, and zero-knowledge proofs can be used with Block chain to keep user identity and sensitive data secure without interfering with the data usability.

Although it has potential, there are also obstacles to the adoption of Block chain in data management. Problems of scalability, storage overhead, performance, interoperability and regulatory compliance should be thoroughly looked at. In addition, Block chain is frequently combined with off-chain storage systems, cloud platforms, and new technologies, which form complex structures, which have to be systematically analyzed [5]. The objective of the present review article is to outline Block chain-based access control and privacy in the field of data management. It also talks about how Block chain technology can be used to overcome the current security and privacy constraints, looks at major techniques and architecture described in the current research work, and discusses practical application of Block chain across different fields [6]. This review aims to provide useful information to researchers, practitioners, and policymakers looking to use Block chain to develop privacy-conscious data management systems by synthesizing existing development efforts, uncovering limitations, and outlining gaps in research to be addressed in future research efforts [7].

DETERMINANTS OF DATA MANAGEMENT SYSTEMS

Data management systems (DMS) are important systems that help organizations to gather, save, arrange, process and access data effectively. They are the foundation of the digital operations of the present time, enabling the applications of the enterprise resource planning to the cloud computing, big data analytics, and Internet of Things (IoT) environments. To the essence, the goal of data management systems is to be sure that the data is appropriate, accessible, dependable and safe during its lifecycle. Basic elements of a DMS normally contain databases, data storage frameworks, data models, query handling engines, and management interfaces that collaborate to provide the handling of structured and unstructured data [8]. The world has been typically characterized by centralized database management systems (DBMS) which provide well established means of ordering relational data in the form of schema, table and indices. These databases are very successful in offering a means of controlled access, data integrity constraints, and transactional operations with the features of Atomicity, Consistency, Isolation and Durability (ACID). Nevertheless, centralized systems fail to manage scale in cases of large-scale distributed data, since they tend to have challenges in the areas of single points of failure, susceptibility to cyberattacks, and lack of transparency among various stakeholders [9].

Distributed and cloud-based systems are also part of the modern data management to overcome these limitations. Distributed systems spread data to more than two nodes which improves fault tolerance, availability and scalability. Cloud-based solutions offer scalable storage and computing capabilities whereby organizations can handle large quantities of data without having to spend a lot of money to acquire the physical infrastructure [10]. However, these developments do cause security and privacy issues including unauthorized access, data leakage and challenges of following data provenance. The data management systems have important operations that involve data storage, retrieval, transformation, replication, and backup. Data storage is not only a process of containing raw data but also its permanence and availability. The retrieval operation, which is usually driven by query engines, should be effective and accurate particularly with real-time usage. Harmonization Data Data must be transformed and incorporated together with other sources, which is essential in analytic and decision-making. The data loss is mitigated through replication and backup measures that ensure that the business runs [11].

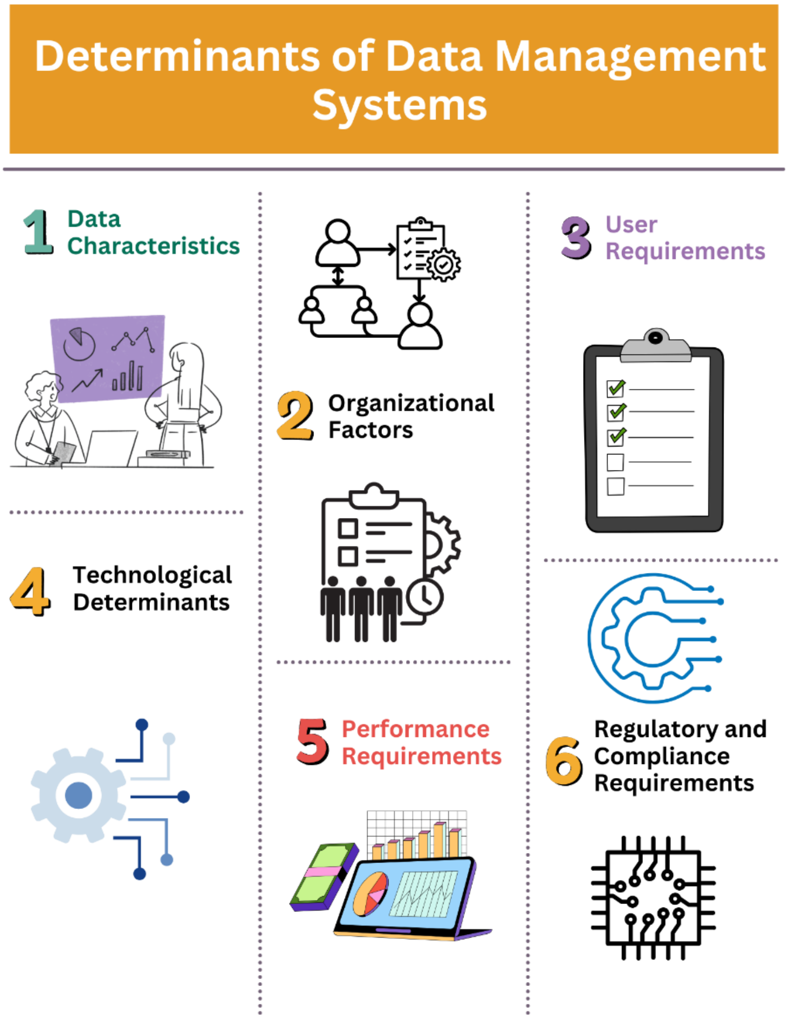
Determinants of Data Management Systems
1 Data Characteristics
2 Organizational Factors
3 User Requirements
4 Technological Determinants
5 Performance Requirements
6 Regulatory and Compliance Requirements

Figure 1. Determinants of data management systems

DMS design is being increasingly security and privacy-and-compliance-oriented. Cryptography, access control policies, authentication and auditing systems are usually used to safeguard confidential information. Furthermore, the constraints of regulatory policies like GDPR, HIPAA, and CCPA put heavy demands on data treatment, and therefore, secure and as-conformant data management systems are highly demanded. This knowledge of these basics forms the basis of analyzing the use of emerging technologies to improve the data in terms of security, privacy, and credibility namely Block chain [12]. The concepts of Block chain present decentralized designs, impossibility, and verifiability of transactions that are used to enhance the traditional DMS capabilities by filling the gaps present in centralized and distributed systems and allowing transparent and tamper-resistant data processes. This renders Block chain a very promising technology in the next-generation data management systems [13].

TRADITIONAL DATA MANAGEMENT SECURITY AND PRIVACY ISSUE

Although traditional data management systems are popular and well-developed, they have major problems with ensuring security and privacy. These systems are usually centralized systems and the data and information is stored and managed by one trusted authority or server. This architecture poses inherent vulnerabilities to the system because the system as a whole is vulnerable to cyberattacks, insider threats, and single points of failure. In this context where organizations depend on data to make the most important decisions, the impact of breaches or unauthorized access may be devastating, which may include financial loss, reputational harm, and legal sanctions [14]. Data breaches are one of the key issues in terms of security. Hackers can attack centralized databases containing a large amount of sensitive data, including personal identifiers, financial details and business proprietary data. After being compromised the breaches may reveal gigabytes of information. Conventional access control systems including role-based access control might not be adequate to guard against unauthorized access, in situations where credentials are stolen or insiders abuse their privileges [15].

Another issue of concern is data integrity. With a traditional system, unauthorized changes on the data can remain unknown and undermine reliability. With weak auditing and verification systems, it is hard to ensure that data is accurate, consistent and tamper proof. Moreover, distributed environments based on replication can be inconsistent in case weak synchronization protocols are used, or ill-intentioned nodes are trying to add the wrong data. There are other challenges of privacy preservation. With the organizations gathering and processing personal and sensitive information, user privacy is the most important thing to consider [16]. The centralized systems tend to make the user to have total trust on the managing authority, yet users do not have personal control in the manner their data is used, shared, or stored. Such procedures as data anonymization and encryption are used, but even these solutions might be inadequate to advanced attacks, such as re-identification or cryptanalysis [17].

Security and privacy risks are enhanced by the problems of scalability and interoperability. With the increase in data volumes, it is becoming more complex to ensure efficient, real-time access control in the distributed systems and in a secure manner. It is further complicated by the fact that the integration of various data sources and the implementation of uniform privacy policies are also required. Also, compliance with regulations creates difficulties [18]. Legal regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other regional privacy laws are stringent on the way data is supposed to be secured and handled. Lack of compliance may lead to heavy fines and penalties. Such restrictions reveal the necessity of innovative solutions that will optimize the security level, data integrity, and privacy without compromising accessibility or scalability. Decentralized ledger distributed across Block chain, cryptographic security, and intractable design are some of the promising solutions to these traditional vulnerabilities of data management. A combination of Block chain and other privacy-saving solutions can enable organizations to develop more powerful, transparent, and credible data management systems [19].

APPLICATIONS OF BLOCK CHAIN IN DATA SECURITY

The technology of Block chain has become an innovative source of improvement of security in the data management systems. A Block chain, at its simplest level, is a distributed registry storing entries of transactions or data on several nodes within a network, it is immutable, transparent and verifiable. In contrast to the traditional centralized databases, Block chain does not exclude the use of one authority to store the data or validate it, which dramatically decreases the chances of the single points of failure, the possibility of unauthorized access and data leakage. Such decentralization ensures that Block chain is especially applicable in the safe management of data in organizations and areas where the issue of trust is essential [20].

Data integrity is one of the security advantages of Block chain. A Block chain is made up of blocks which include cryptography hash of the prior block, and transaction data. Any change in the data would cause the hash to be changed and this would provide an instant notification to the network that there might have been tampering. This guarantees that the information stored on the Block chain is not manipulable and can be checked by any party [21]. The Block chain generated immutable record also leaves an auditable footprint, where organizations can trace the changes and gain access to history which is essential in regulatory compliance and accountability. Block chain also promotes access control and authentication. Access policies can be enforced automatically with the help of smart contracts that are self-executable code and stored in the Block chain. Such contracts also allow the definition of people who can read, write, or modify data and under what conditions, and intermediaries are not required, and human error is reduced. Also, Block chain-based identity management systems offer decentralized authentication and offer more control to users over their own credentials without compromising access to sensitive information [22].

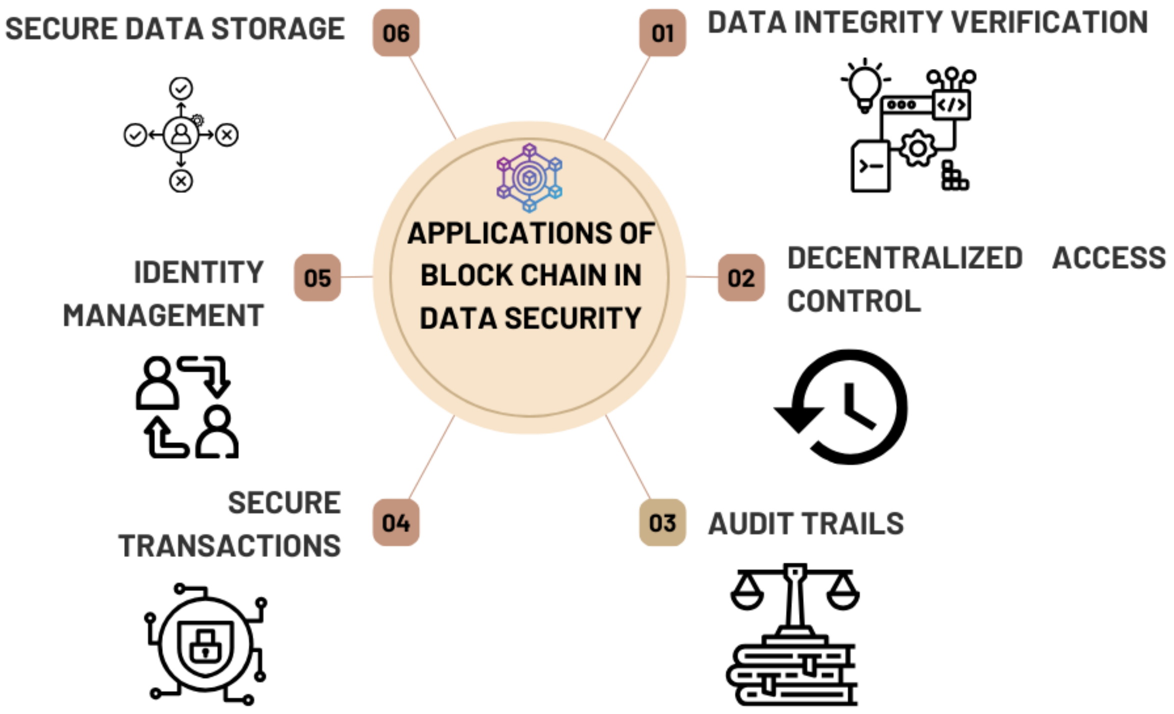
APPLICATIONS OF BLOCK CHAIN IN DATA SECURITY
01 DATA INTEGRITY VERIFICATION
02 DECENTRALIZED ACCESS CONTROL
03 AUDIT TRAILS
04 SECURE TRANSACTIONS
05 IDENTITY MANAGEMENT
06 SECURE DATA STORAGE

Figure 2. Applications of block chain in data security

Block chain may also enhance data exchange and cooperation between several participants. In the old fashioned systems, it used to be necessary to send copies of the data to a central server or use third-party mediators, which increased the possibility of leakage and unauthorized access. With Block chain, peer-to-peer data sharing is possible with data verification and confirmation of authenticity, which grants participants the ability to trust the data without violating privacy. Nevertheless, Block chain is in itself not a complete answer to total privacy [23]. Other methods like encryption, zero-knowledge proofs and pseudonymization are commonly combined with Block chain to make sure that sensitive data is held in secret, yet the ledger is transparent. The block chain is a critical component in the secure data management since it offers decentralization, tamper resistance, traceability, and automated access control. Its capability of increasing trust and security overcomes most of the weaknesses of traditional centralized systems and thus it can be used as a promising base on the next generation data management models. In conjunction with privacy-protective systems, Block chain can be used to help organizations store data, share and effectively manage it in a transparent and trustworthy way [24].

PRIVACY PRESERVATION METHODS BASED ON BLOCK CHAINS

One of the most important issues of modern data management is privacy preservation, particularly within the spheres where personal, financial, or medical information of the highest sensitivity is applied. The conventional centralized systems tend to fail in offering adequate privacy assurances because data is stored in a single repository and therefore is prone to breaches, theft, or other possible misuses. Block chain technology has provided a transparent and decentralized system, which has its own transparency problem with privacy [25]. To solve this, a number of Block chain-based privacy preservation schemes have been created, which integrated cryptographic schemes, architectural developments, and smart contract schemes. Encryption is one of the most popular techniques. The data on the Block chain can be encrypted with the help of the symmetric or asymmetric cryptographic algorithms. Encryption ensures that the data within the information is not accessed by a third party, yet those who are authorized can access the same when there is a need [26]. As an illustration, sensitive medical record or financial transactions can be easily transferred freely among the participants without subjecting the raw data to the whole network. Off-chain storage may also be used in conjunction with encryption where the encrypted version of the data is stored in the Block chain whereas the actual information is held in a non-Block chain location which helps to reduce exposure whilst preserving integrity [27].

Another method of maintaining privacy on Block chain network is pseudonymization and anonymization. Under these systems, distinguishing identities of users are substituted by pseudonyms or anonymized identities and transactions and data cannot be directly attributed to particular people. This is useful in maintaining privacy and yet permitting the Block chain to act as a transparent and verifiable registry. Zero-Knowledge Proofs (ZKPs) is a new somewhat advanced cryptographic privacy preservation. ZKPs give one side the opportunity to demonstrate to the other the truth of a specific statement without any further information being disclosed. ZKPs can be used in data management in Block chain to verify a transaction, give access permissions, or data authenticity without making any underlying sensitive data public. This is especially helpful to be used in the financial, healthcare, and identity management applications where confidentiality is the main priority [28].

Privacy-oriented Block chain systems also use the idea of ring signature and mixing schemes. Such techniques confuse the source of transactions or data postings by combining several transactions together, and hence it becomes hard to monitor the individual activity, and at the same time the transaction is legitimate. Besides, secure multi-party computation (SMPC) enables several parties to cooperatively compute a function on their inputs without divulging their inputs to the others [29].

ISSN : 3079-5761
Volume 1, Number 4, 2025
https://doi.org/10.70445/gtst.1.4.2025.116-144

Combined with Block chain, SMPC allows to process data collaboratively without compromising the privacy requirements. The privacy preservation methods based on block chains lead to greater security and confidentiality of data management systems providing both decentrality and high-level cryptographic measures. Encryption, pseudonymization, and zero-knowledge proving, ring signatures, and SMPC make organizations utilize the transparency and immutability of Block chain without sensitive information damage, building privacy-conscious and reliable data management systems. The strategies are the basis of creating the next generation secure and compliant data management systems [30].

SECURE DATA ACCESS AND CONTROL SMART CONTRACTS

Smart contracts refer to self-running code stored on a Block chain that execute rule and agreement mandates automatically between the parties without the involvement of intermediaries. Smart contracts are also important in data management in terms of securing access to data, integrity, and the enforcement of privacy policies. Smart contracts offer a decentralized and irreversible way of controlling access to, and manipulation or sharing of data, by implementing access control logic within the Block chain itself [31]. Automated access control is one of the main uses of smart contracts. Conventional access control systems like the role-based access control (RBAC) are based on the use of centralized servers and administrators which control the permissions. This leaves loopholes, such as insider threats, human errors, and possible manipulation. Smart contracts, in contrast, are automatic algorithms that run in accordance with set rules to make sure that the data is only shared with the authorized actors based on the set policies. As an example, within a healthcare system, a doctor can only receive the medical records of a patient after one has properly authorized them, and all the access events are recorded on the Block chain and can be audited [32].

Data integrity and accountability is also increased through smart contracts. All transactions with the data, including retrieving, modifying, or sharing information, can be documented as a Block chain transaction. Because Block chain operations are unchangeable and time-stamped, smart contracts offer an indication of the chain of all data-related operations, which is easier to trace unwarranted activities or any policy breach. This trait is especially useful in meeting the requirements of such regulations as GDPR or HIPAA, in which the evidence of the controlled access to and usage of data is necessary. Conditional data sharing is also another benefit [33]. Complex rules can be executed by creating smart contracts that regulate the sharing of data on when and how to share it. To illustrate, they can provide access to given datasets under certain conditions, like payment verification, multi-party consent or anonymization of sensitive data. This feature enables safe cooperation within distributed settings when multiple organizations have to share information without complete trust of each other [34].

In spite of their advantages, smart contracts have pitfalls like possible computer programming mistakes, security risks and scalability. Thus, to make sure of reliable implementation, detailed design, testing and auditing are crucial. Smart contracts offer a decent platform of safe data retrieval and management in Block chain-based data administration systems. They lessen the dependency on central authority, diminish the security threats as well as provide comprehensive visibility and privacy-aware data management practices by automating access policies, making compliance and maintaining immutable audit trails. The fact that they are integrated is a big improvement to the conventional centralized systems of access controls [35].

DECENTRALIZED IDENTITY AND ACCESS CONTROL

Decentralized Identity (DID) and access management is a new solution in the world of data management systems which is focusing on a crucial problem of identity verification, authentication and privacy of users. Conventional identity management systems assume the involvement of centralized authority, which can be a government database, corporate directory, or cloud service provider, to validate users as well as grant access privileges [36]. Although they are functional, these centralized models have a number of weaknesses, such as the presence of single points of failures, hacking, data breach and excessive collection of personal data. Conversely, decentralized identity systems take advantage of Block chain technology in order to offer secure and user-sovereign identity verification and access control that is not reliant on a single and trusted authority [37].

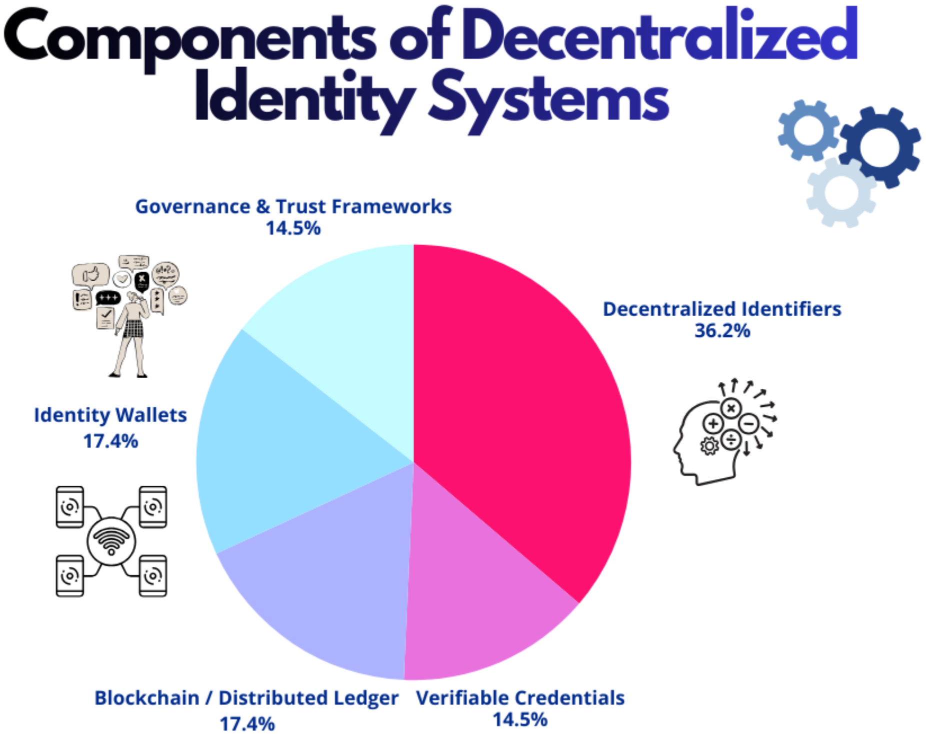

Figure 3. Components of decentralized identity systems

ISSN : 3079-5761
Volume 1, Number 4, 2025
https://doi.org/10.70445/gtst.1.4.2025.116-144

The concept of self-sovereign identity (SSI) lies at the centre of the concept of decentralized identity. SSI enables people to have complete ownership and control of their online personas, whereby verifiable credentials are stored using a Block chain or distributed register. Users will be able to share personal information selectively and that way they will not expose sensitive information which could be unnecessary. As an example, instead of disclosing all personal information to check the age or eligibility, a user can present cryptographic evidence that he satisfies the necessary requirements without disclosing any unnecessary information [38]. The mechanism of selective disclosure improves the privacy of the data and does not affect the authenticity and verifiability of the identity. Access management based on Block chain technology is a supplement of decentralized identity which guarantees a high degree of control over access to data in a safe and tamper-proof manner. Smart contracts are frequently used together with DIDs to automate the process of authorization by providing or withholding access under defined rules of access. Every access request will be recorded permanently in the Block chain forming a transparent audit trail that cannot be easily manipulated. It will be responsible and traceable, which is essential in terms of meeting privacy laws, including the GDPR, HIPAA, and CCPA [39].

Interoperability across platforms is also achieved in decentralized identity systems. Conventional identity solutions tend to be silo-ed and users have to use multiple credentials to use different platforms. The DID based on Block chain offers a universal, verifiable, and transportable identity which may be understood and trusted by various services and organizations. This not only makes the process of user easier but it also minimizes the administrative overhead and security vulnerability of password management and storing credentials in a centralized location [40]. In addition, the decentralized identity and access control are especially useful in distributed and collaborative ones, including healthcare, finance, and supply chains networks, which require many partners to communicate with each other safely without complete trust and trust in each other. These systems provide safe authentication, access control that is privacy-sensitive and greater autonomy, through combining immutability of a Block chain, smart contracts, and cryptographic mechanisms [41].

Access control on decentralized identity and Block chain identity offers a strong verification of identity, privacy-sensitive, and non-secret identity verification. These solutions overcome the fundamental limitations of centralized systems and introduce an important breakthrough in the current data management through the establishment of control over the digital identities of the users and the enforcement of access, which can be done automatically by means of immutable ledgers [42].

ISSN : 3079-5761
Volume 1, Number 4, 2025
https://doi.org/10.70445/gtst.1.4.2025.116-144

BLOCK CHAIN INTERACTION WITH CLOUD SYSTEMS AND BIG DATA

The development of Block chain technology in conjunction with cloud computing and big data is an important transformation in the contemporary data management. Big data infrastructures and cloud platforms have helped organizations to store and process large quantities of data in a structured and unstructured format effectively. Nevertheless, such systems tend to be based on centralized architectures that pose security, data integrity, privacy, and trust vulnerability. Decentralized and immutable ledger, Block chain provides new answers to these issues by increasing the level of transparency, accountability, and resistance to tampering in cloud-based, big data systems [43]. Among the major advantages of Block chain integration, there is an increase in data security. Conventional cloud-based applications by third parties are vulnerable to breaches, insider attacks, and unauthorized access because the data is stored in centralized servers controlled by the third parties. With the integration of Block chain, it is possible to store the data transactions in a decentralized registry that uses cryptographic security to guarantee immutability and tracking. Any intervention of finding a way to alter the data can be readily identified and all the process of data changes can be verified by all parties within the network, which enhances the credibility of the data integrity [44].

Block chain is also used in sharing data, which is secure and auditable, in distributed cloud and big data platforms. The traditional system may take longer to share information, involves middlemen and it may be prone to security lapses which is not the case with the new system. Using Block chain, peer-to-peer transfer of data can take place with verifiable evidences of authenticity, and various parties can retrieve shared datasets without undermining confidentiality [45]. Smart contracts also add to this functionality by automating access control, ensuring usage policies, and only performing transactions as per stipulated conditions. Block chain can enhance data provenance and quality in the framework of big data analytics. Big data systems tend to aggregate data on numerous sources, and it is difficult to verify the source and integrity of these data. Block chain also gives a secured data record of every data entry, so that analytics is done on validated information that cannot be tampered with. It is especially essential when it is used in the sphere of finance, healthcare, and supply chain management, where such incorrect or distorted data may lead to serious and unfortunate outcomes [46].

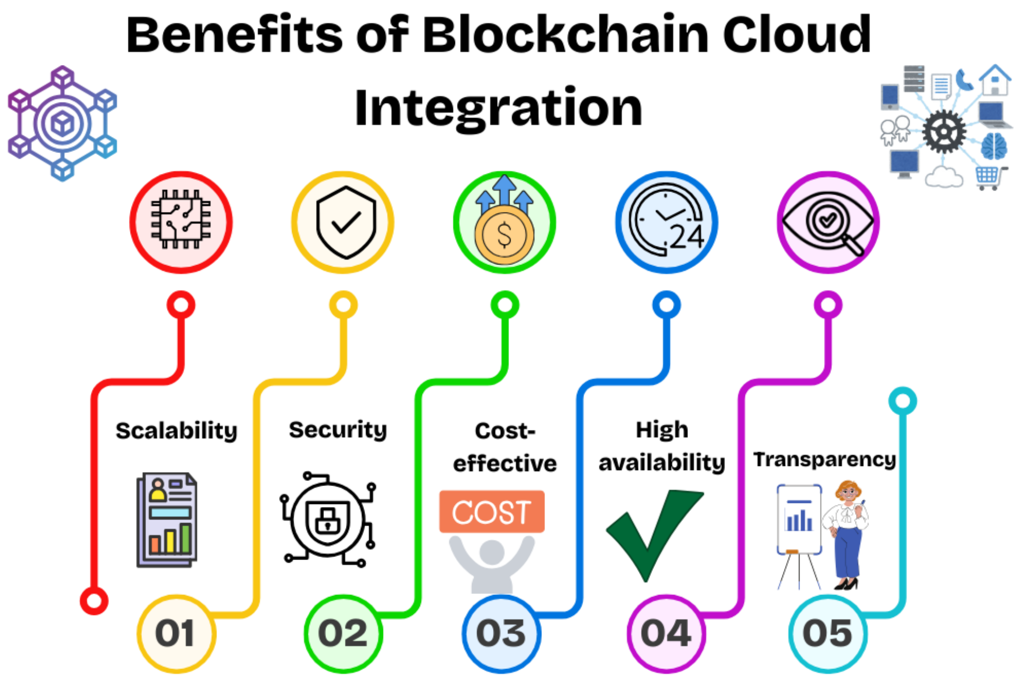

Figure 4. Benefits of block chain cloud integration

Block chain interoperability helps hybrid architecture, in which bulk data have been stored off-chain in cloud or distributed data stores, but the Block chain has metadata, transaction and access logs. The strategy helps resolve the shortcomings of Block chain in terms of scalability and capacity and maintain the advantages of security and transparency. Although it has benefits, using Block chain in combination with cloud and big data systems is associated with several issues, such as network latency, scalability, computational overhead, and heterogeneous platforms interoperability [47]. These issues are to be tackled carefully and optimized. The integration of block chain with cloud and big data systems also improves security, privacy, data integrity and trust, which offer a powerful framework of distributed data management. With the computational and storage power of cloud and big data increased with the decentralized verification and immutability of Block chain, organizations can create secure, transparent, and privacy-conscious data management ecologies that can be used in current digital applications [48].

STORAGE, SCALABILITY AND PERFORMANCE

Although the Block chain technology has a lot of benefits in terms of security, privacy, and trust in the handling of data, its application in large systems creates critical issues concerning its performances, scalability, and storage. These considerations are important in developing effective Block chain-powered data management systems, which may be able to accommodate real-life applications without reducing their usability or reliability. One of the aspects is performance;

especially where it is essential to process data quickly or almost in real-time [49]. The Block chain networks are usually based on consensus, including Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT) validation and confirmation of transactions. Although these mechanisms are necessary in the way of providing security and decentralization, they come with computational overhead and latency. As an illustration, Block chains that use PoW authentication like Bitcoin cannot be used in a high-throughput application, as it requires substantial computational power and time to verify transactions. Other consensus models (e.g. PoS or delegated consensus committees) offer faster confirmation of transactions but can present a trade-off in either decentralization or security [50].

The other important challenge is scalability. Due to an increase in the number of transactions and participants in a Block chain network, the network should be in a position to accommodate increasing volumes of data without compromising performance. The conventional Block chains keep a complete version of a ledger on each node and this might cause bottlenecks to processing and synchronization. Big data and IoT environments have high rates of transactions that may overwhelm Block chain networks, causing delays and low efficiency of the systems [51]. Some of the solutions found to enhance scalability through workload distribution and parallel processing of transactions include layer-2 solutions, shoring, and sidechains. In data management systems based on Block chain, storage is also something that should be considered. Block chains are also append-only, which means that with Block chains all the transactions and updates are permanently recorded on the ledger [52] though this guarantees permanence and traceability, it also leads to a lot of storage space in the long run. In case of large scale systems with large volumes of data, it is not viable to store complete datasets on-chain. The storage overhead can also be minimized with hybrid techniques, like off-chain storage, in which the bulk data is stored in external databases or distributed storage systems, whereas the Block chain is used to store hashes and metadata, which can be used to verify the integrity and verifiability of the data [53].

Performance and scalability are also influenced by network bandwidth and synchronization of nodes. The Block chain increases the size of each node needs to communicate and verify data, and in case it is not managed it can create congestion in the network and slow response time. In Block chain-based data management, such factors as performance, scalability, and storage are crucial. There is a need to have efficient consensus mechanisms, hybrid storage solutions and network optimization techniques to push the balance between security, decentralization and operational efficiency. These issues need to be addressed to implement Block chain solutions which are practical, scalable and can support modern data intensive applications in many areas [54].

ISSN : 3079-5761
Volume 1, Number 4, 2025
https://doi.org/10.70445/gtst.1.4.2025.116-144

THE DATA MANAGEMENT APPLICATIONS AND USE CASES OF BLOCK CHAIN

The Block chain technology has proved to have potential in revolutionizing the data management practices in many industries that have improved the security, privacy, transparency, and trust. It is decentralized, immutable, which solves the major weaknesses of centralized systems, allowing the storage of data safely, controlled access, and auditability. Consequently, Block chain has been implemented in various fields, all of which use its possibilities to address certain issues in data. Healthcare data management is one of the favorable applications [55]. Healthcare organizations create huge volumes of sensitive patient information including medical histories, lab reports, and imaging outcomes. In conventional systems of centralization, breaches, unauthorized access and data tampering are prone to occur. Block chain has the capability to save and operate patient records safely and ensure privacy during encryption or selective disclosure strategies. Smart contracts will be able to automate the control of consent so that only authorized staff or scientists will be able to access certain data. This solution does not only enhance data security but also facilitates the interaction between hospitals, laboratories, and insurance companies as well as ensuring that the patients have control over their personal data [56].

Block chain is used in the banking and financial industries to improve transparency of transactions, prevent fraud and compliance with regulations. Banking institutions are able to store their transactions on unchangeable block-chain records, which make them accurate and traceable, and they do not have to depend on intermediaries. Systems with Block chain also enhance sharing of data among banks and regulators, which facilitates quicker audits and minimizes the risks of operation. Moreover, privacy-saving algorithms, like the zero-knowledge proofs, enable the safe verification of transactions to be made without revealing any sensitive account data [57]. The advantage of the use of Block chain in the supply chain and logistics sector is accountability, traceability, and authenticity of goods. All the steps of the supply chain, such as the manufacturing of a product to delivery, can be traced on a Block chain, which will form a non-alterable history that can be trusted by the stakeholders. This will eliminate counterfeiting, increase transparency, and make it easier to make decisions basing them on real-time and reliable data [58].

Block chain can be used in the Internet of Things (IoT) to ensure secure information exchange between interconnected devices. The IoT systems produce a stream of data that can be easily manipulated and even accessed by unauthorized persons. The Block chain provides integrity of data and decentralized authentication of devices, minimizes security threats, and enhances reliability. The other uses are digital identity management, government records, protection of intellectual property, and cloud data security [59]. Block chain ensures data sharing, automated access on smart contracts and verifiable audit trails in all these areas and due to the decentralization, immutability, transparency, and programmable contracts, Block chain is a potent tool in enhancing data management in any sector. Block chain-based solutions are improving the privacy, security, and trust of sensitive data, and are changing the way sensitive data is stored, accessed, and shared and allowing organizations to create more resilient, efficient, and user-centric data ecosystems [60].

ANALYTICAL COMPARISON OF THE CURRENT SOLUTIONS BASED ON BLOCK CHAIN

A number of solutions have been developed as a result of the adoption of Block chain technology in data management and each is aimed at solving a particular security, privacy, and operational issue. These solutions should be put side by side in a comparative analysis to know their weaknesses, strengths, and applicability under various circumstances to allow organizations in choosing and applying the most effective frameworks. A significant portion of Block chain-based solutions is dedicated to public Block chains, including Ethereum and Bitcoin. Public Block chains are completely decentralized, and any person can become a node or a validator [61]. Their main strength is in the openness and inability to change anything, so every transaction can be checked and cryptography cannot be violated. Nevertheless, the public Block chains are characterized by such issues as the inability to scale, increased latency, and high computational expenses, particularly when it comes to handling large amounts of data. These are disadvantageous because they are not as good in real-time data management or in the enterprise level applications which demand high-speed transaction throughput [62].

Some of these drawbacks are overcome by private and consortium Block chains, including Hyperledger Fabric and Quorum, by limiting access to authorized parties. These networks are more decentralized and controlled and also provide higher speeds of transaction, reduced use of energy and more efficient consensus processes. Privacy management is also improved with private Block chains because sensitive information may be disclosed to trusted parties. Although that makes them appealing to enterprise use, they are not as transparent as the public Block chains and the trust relies on the governance of the consortium [63]. Hybrid Block chain removes the storage constraints of a traditional Block chain by storing data on- and off-chain. With such systems, Block chain is only stored with critical metadata or cryptographic hash, with bulk data stored in external databases or distributed storage systems. The solution increases the scalability and performance, yet the stored data integrity and verifiability. The hybrid solutions can be employed specifically in fields like healthcare, finance, and IoT when huge volumes of data are to be processed and shared safely without overwhelming the Block chain too much [64].

Privacy-preserving schemes are applied in other Block chain-based solutions, which include zero-knowledge proofs (ZKPs), secure multi-party computation (SMPC), and homomorphic encryption. These methods permit checking and calculation on the encrypted data without any sensitive information being revealed, overcoming the privacy issues of information sharing and analytics. Solutions based on ZKPs, such as allow organizations to prove transactions or other access controls without exposing the underlying data to ensure high privacy guarantees [65]. Block chain solutions range in terms of architecture, performance, privacy, and scalability. Public Block chains are more focused on transparency and decentralization with the issue of efficiency. Privacy and consortium Block chains are better in performance and privacy but are based on trusted management [66]. Privacy and Hybrid solutions provide a trade-off between the management of large, sensitive data. It is necessary to comparatively assess these solutions in order to reveal the most appropriate structure in relation to the particular organizational requirements, which guarantees the safety of information, its efficient processing, and the consideration of privacy issues [67]

RESTRICTIONS AND OPEN PROBLEMS

Although Block chain technology has proven to have enormous benefits in terms of safeguarding and privacy-conscious data management, there are also a number of limitations and unresolved issues that have to be resolved to provide the means of a viable and scalable implementation. These limitations are important to the researcher, developers, and organizations that want to use Block chain to develop contemporary data management systems [68]. Scalability is one of the most important challenges. Conventional Block chain networks, especially public block chains have been restricted in terms of the number of transactions that can be processed per second because of consensus system such as Proof of Work (PoW). With the growth in the number of users and transactions, the network is likely to become sluggish with lower throughput and an increase in operational expenses. Although newer consensus systems like Proof of Stake (PoS) or delegated consensus, high scalability, with decentralization and security, is a challenging trade-off, especially when the system is needed to process data in real-time or near real-time [69].

There are other issues related to storage and data management. Block chain as such is an append-only registry, and all the transactions are stored forever. This contributes to the speedy increase in the ledger volume, which puts storage and computation pressure on participating nodes. In case of large scale data management systems, it is not feasible to store all data on-chain. Some of the problems are addressed by hybrid solutions that keep metadata or cryptographic hashes on-chain but bulk data off-chain, which cause complexities in data availability, consistency, and integrity. The other important challenge is interoperability [70]. Companies tend to apply a variety of data management applications, cloud systems, and old systems. The standardization of heterogeneous environments and smooth communication protocols are necessary to integrate Block chain into those environments. In lack of the strategy of interoperability, Block chain solutions do not work in isolation and therefore reduce their efficiency in the real world of handling data [71].

The application of cryptographic and privacy-sensitive approaches does not eliminate the issue of privacy and confidentiality. By definition, public Block chains reveal the metadata of transactions, which in some cases can have patterns or sensitive information. Privacy might be improved with the help of more sophisticated solutions, e.g. zero-knowledge proofs, homomorphic encryption or secure multi-party computation, which add more computational complexity and might have an impact on performance. The regulatory and legal compliance is a changing issue [72]. The impossibility of editing or destroying personal data requested by the user may be a clash between Block chain and privacy laws such as the GDPR. To operate within the space of legal regulations and still enjoy the perks of Block chain, hybrid storage systems and privacy-saving mechanisms need to be designed with care [73].

Some Block chain applications raise energy consumption and resource efficiency issues, especially the PoW-based, which demand a high level of computation power and energy. Long-term data management application requires long-term sustainable Block chain designs. Although Block chain offers transformational advantages in the way it offers secure, transparent, and privacy-conscious data management, scalability, storage, interoperability, privacy, compliance, and resource efficiency issues still exist. Overcoming these constraints will play a critical role in coming up with implementable, strong, and generalizable Block chain-based data management systems. These obstacles need to be conquered through continuous research, optimization, and innovation that need to unlock the full potential of Block chain in the current data ecosystems [74].

FUTURE RESEARCH DIRECTIONS

The Block chain technology has proven to be very promising in maximising the level of security, privacy as well as trust in the data handling systems. Nevertheless, although it is associated with many benefits, there are various limitations and challenges which limit its full-scale adoption. As a result, the research study in Block chain-based data management of the future ought to aim at overcoming these limitations, maximizing system performance, and examining new usages to unachieve the full potential. Scalability and throughput optimization is one of the most important in the future research [75]. The existing Block chain systems, specifically the public Block chains, are limited to the ability to handle a high number of transactions because of the consensus algorithms such as the Proof of Work (PoW). Despite the fact that alternative systems, including Proof of Stake (PoS), delegated PoS, and Practical Byzantine Fault Tolerance (PBFT), have some improvements, it is difficult to balance between scalability, decentralization and security. Further studies might be done on hybrid consensus, paralleled transaction processing, and shards to allow high throughput and real time data management that could be used in enterprise and IoT applications [76].

The other significant course is the improvement of privacy-saving mechanisms. Although such methods as zero-knowledge proofs, secure multi-party computation, and homomorphic encryption provide high privacy, they come at the cost of increased computation time, and can potentially impact system performance. Studies should be conducted to create lightweight, efficient and scalable cryptographs protocols which ensure privacy without affecting the speed or usability [77]. A harmonious implementation of these methods into the Block chain-based data management systems will be essential in applications that process sensitive data including healthcare, finance, and personal identity management. Another essential field of research is interoperability and standardization. Adoption of Block chain in data management is commonly compromised by adoption of fragmentation networks, incompatible platforms, and the absence of standardized protocols. Future research may aim at creating interoperable designs that can enable seamless interconnection of various Block chain networks, cloud environments and legacy data environments. This will improve the usability of Block chain in an inter-organizational and inter-domain data managements setting [78].

It is also a priority to have sustainable Block chain solutions. Consensus mechanisms that consume a substantial amount of energy, including PoW, are also of a particular concern in terms of environmental impact and cost of operation. The investigation of the energy-saving consensus protocol and environmentally friendly Block chain structure will be crucial to the wide-scale usage in data management applications. Law and legal frameworks are a matter of consideration [79]. The fact that Block chain is immutable may contradict the legislation that demands the alteration or removal of data like GDPR. Further research might be conducted on the hybrid models and privacy-preserving approaches that would facilitate the compatibility of Block chain immutability with regulatory needs and allow managing the data that is compliant and secure at the same time [80]. Scalable, privacy-preserving, interoperable, energy-efficient, and regulatory-compliant Block chain solutions ought to be considered in future research. By focusing on these, academics can create the next generation of data management systems that realize all the potentials of Block chain and offer safe, reliable, and effective systems of various applications in many fields [81].

CONCLUSION

The Block chain technology has come as a revolutionary tool to decision-making in the data management systems that have persistently posed security, privacy, transparency, and trust as a challenge. Although traditional centralized data management structures are effective in managing storage and processing, they have fundamental weaknesses such as single points of vulnerabilities, vulnerability to cyberattacks, unauthorized access, data manipulation, and privacy breaches. With the growing dependence of organizations on digital data to make decisions, perform analytics, and collaborate across organizations, these vulnerabilities have been heightened, which makes more secure, decentralized and trustworthy solutions long overdue.

The analysis of the Block chain-based data management has shown that Block chain has some peculiarities that will directly tackle these limitations. The architecture of the system is decentralized, which gets rid of the reliance on one authority and thus lessens the risks of damaging the entire system or controlling it. Data integrity is guaranteed by immutable and tamper-resistant ledgers, whereas the authenticity of stored information is ensured by cryptographic security measures. The smart contracts integration will improve automated access to and control data, where pre-established rules may be used to determine the people who may access or manipulate data without human input. This enhances accountability as well as minimizes the possibility of errors or malicious practices.

Another advantage that Block chain-based solutions offer is privacy preservation. Encryption, pseudonymization, zero-knowledge proofs, ring signatures, and secure multi-party computation are the techniques that can enable organizations to ensure the confidentiality of sensitive data and benefit from transparency and auditability of Block chain. Moreover, decentralized identity (DID) systems enable people to have self-sovereign identity, which provides them with personal control over their own data and enables them to disclose it selectively when it is necessary. All these mechanisms improve the privacy of users, increase trust, and allow sharing data safely across platforms, especially in fields like healthcare, finance, IoT, and supply chain management.

The implementation of Block chain as a solution in cloud computing and big data systems also increases the range of its application. Hybrid architectures, where large datasets are stored off-chain with cryptographic references being held on-chain, address the shortcomings of storage and scalability of Block chain. The method maintains data integrity, makes it verifiable, and allows safe cooperation of numerous stakeholders without wasting network resources. Practical use in health care, financial, supply chain, and IoT shows that Block chain-based data management is practical and that organizations can use it to develop secure, auditable, and privacy-conscious data ecosystems. Block chain, though it has advantages, does not have its challenges. Scalability, performance and storage overheads are still critical issues especially in large scale and high transaction environments. There is a layer of complexity with network latency, computing power, integrating with legacy systems, and meeting regulatory standards like GDPR and HIPAA. Proof-of-Work-based systems are also a source of sustainability issues related to energy use. These constraints underscore the importance of research and innovation in optimising Block chain solutions, improving efficiency, and establishing standards that allow the easy integration of the Block chain solutions with the already existing data infrastructure.

Future research effort is in scalable consensus mechanisms, lightweight privacy-preserving protocols, interoperable frameworks, energy efficient designs and compliance oriented architectures. With these issues resolved, Block chain can become a holistic platform, which can be used to handle data management securely, reliably, and with scale. These innovations will enable the next generation where robust and efficient systems with the capability of integrated Block chain and flexibility and efficiency are integrated to facilitate the data-driven business of the future.

The application of Block chain-based data management is a paradigm shift that has never been experienced before and provides unprecedented benefits in terms of security, privacy, transparency, and trust. With Block chain, organizations can be confident in handling data by reducing the weaknesses of conventional systems as well as offering effective means of accessing, sharing and verifying secure data. Though the challenges exist, continuous research, development of new technology and implementation of hybrid is gradually combating these challenges. Finally, Block chain can transform the way data can be handled, stored and shared in industries, which will create a secure and privacy-conscious data environment that is trustworthy and responds to the needs of the data-hungry society of the present day.

REFERENCES

[1]. Babu JA, Patil S, Parameshachari BD, Rinaldi S, Balmuri KR, Hemalatha KL. Block chain enabled hybrid cryptographic algorithm for security and privacy preservation of electronic health records. ICT Express. 2025 Oct 1;11(5):945-50.

[2]. Saraswat B, Kumar A, Sharma S, Anand KB. Health chain-block chain based electronic healthcare record system with access and permission management. Measurement: Sensors. 2023 Dec 1;30:100903.

[3]. Dhinakaran D, Ramani R, Edwin Raja S, Selvaraj D. Enhancing security in electronic health records using an adaptive feature-centric polynomial data security model with blockchain integration. Peer-to-Peer Networking and Applications. 2025 Mar;18(2):7.

[4]. Pandey AK, Saxena R, Awasthi A, Sunil MP. Privacy preserved data sharing using blockchain and support vector machine for industrial IOT applications. Measurement: Sensors. 2023 Oct 1;29:100891.

[5]. Shakya S. Efficient security and privacy mechanism for block chain application. Journal of Information Technology. 2019 Dec;1(02):58-67.

[6]. Kumar A, Fahad M, Arif H, Hussain HK. Navigating the Uncharted Waters: Exploring Challenges and Opportunities in Block chain-Enabled Cloud Computing for Future Research. BULLET: Jurnal Multidisiplin Ilmu. 2023;2(6):1297-305.

[7]. Alzubi OA, Alzubi JA, Shankar K, Gupta D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. Transactions on Emerging Telecommunications Technologies. 2021 Dec;32(12):e4360.

[8]. Pavithra S, Pavani M, Harini D. IoT and Blockchain Security for Medical Data. Blockchain in Health Sciences. 2025 Aug 14:229-51.

[9]. Sutradhar S, Karforma S, Bose R, Roy S, Djebali S, Bhattacharyya D. Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems. 2024 Jan 1;4:49-67.

[10]. Jayasri R, Jayakumar D, Roselin SJ, Ramkumar MO. Plan of Block-chain Enabled Confirmed Key Management Protocol for Internet of Medical Things Development. In2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) 2022 Aug 17 (pp. 668-673). IEEE.

[11]. Ilambirai RC, Jame SL, Poornima PU. Block chain enabled data security using blowfish algorithm in smart grid network. Int. J. Data Sci. Artif. Intell. 2024;2(03):88-92.

[12]. Visuvanathan GE, Sayeed MS, Yogarayan S. BHFVAL: block chain-enabled hierarchical federated variational auto encoder framework for secure intrusion detection in vehicular networks. Scientific Reports. 2025 Dec 1.

[13]. Rana R, Bhambri P. Blockchain for Transparent, Privacy Protected and Secure Health Data Management. InSmart Healthcare Systems 2024 (pp. 33-43). CRC Press.

[14]. Srivastava R, Prashar D. A Secure Block-chain Enabled Approach for E-Heath-care System. In2021 International Conference on Computing Sciences (ICCS) 2021 Dec 4 (pp. 194-201). IEEE.

ISSN : 3079-5761
Volume 1, Number 4, 2025
https://doi.org/10.70445/gtst.1.4.2025.116-144

[15]. Saxena R. Blockchain-Enabled Secure Healthcare Data Management with Modified Gazelle Optimization and DLT-Trained RNN-BILSTM Approach. Jurnal Online Informatika. 2025 Nov 8;10(2):418-31.

[16]. Rao S, Gagan VS. Block Chain Enabled Digital Forensics. In2024 Recent Advances in Sustainable Engineering and Future Technologies (RASEFT) 2024 Dec 27 (pp. 54-59). IEEE.

[17]. Lodha L, Baghela VS, Bhuvana J, Bhatt R. A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring. Measurement: sensors. 2023 Dec 1;30:100904.

[18]. Kommineni KK, Ande P. Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks. International Journal of Intelligent Engineering & Systems. 2025 May 1;18(5).

[19]. Basha SM, Ahmed ST, Iyengar NC, Caytiles RD. Inter-locking dependency evaluation schema based on block-chain enabled federated transfer learning for autonomous vehicular systems. In2021 Second International Conference on Innovative Technology Convergence (CITC) 2021 Dec 9 (pp. 46-51). IEEE.

[20]. Arulmozhi B, Sheeba JI, Devaneyan SP. Revolutionizing COVID-19 Management: Block chain-Enabled Prediction and Secure Storage using Deep Learning Techniques. Procedia Computer Science. 2023 Jan 1;230:853-63.

[21]. Lawhale P, Kale SN. A Survey On Secure Architectures Using Hash Function Based On FPGA for Block Chain Enabled IoT Devices. In2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP) 2023 Apr 28 (pp. 1-6). IEEE.

[22]. Ismail M, Akram A, Naeem I, Saleem U, Mehmood KT, Iqbal R. EXPLORING THE POTENTIAL OF BLOCK CHAIN AND AI CONVERGENCE TO SECURE AND VERIFY IOT DATA TRANSMISSIONS IN HIGH-STAKES INDUSTRIES LIKE HEALTHCARE AND FINANCE. Spectrum of Engineering Sciences. 2025 May 16;3(5):447-67.

[23]. Uike D, Agarwalla S, Bansal V, Chakravarthi MK, Singh R, Singh P. Investigating the role of block chain to secure identity in IoT for industrial automation. In2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART) 2022 Dec 16 (pp. 837-841). IEEE.

[24]. Sahiti Yellanki V, Sah B. A Survey on Various Secure Access Control and Authentication in a Block Chain-Enable Cloud IoT. InExplainable IoT Applications: A Demystification 2025 Feb 14 (pp. 295-308). Cham: Springer Nature Switzerland.

[25]. Gudivaka RK, Basani DK, Grandhi SH, Gudivaka BR, Gudivaka RL, Kamruzzaman MM. A multilevel decentralized trust management-aware OS-GRU and S-fuzzy-based dynamic task offloading in block-chain enabled Edge-Cloud. Sustainable Computing: Informatics and Systems. 2025 Jun 1;46:101111.

[26]. Lakshmi TS, Muni NB, Reddy KM. Block chain enabled Secure Communication Framework for V2V and V2I Systems. Cuestiones de Fisioterapia. 2025 Jan 10;54(2):1466-74.

[27]. Meenakshi, Sharma P. A Blockchain-Based Solution for Enhancing Security and Privacy in the Internet of Medical Things (IoMT) Used in e-Healthcare. Blockchain and Deep Learning for Smart Healthcare. 2023 Dec 28:95-112.

[28]. Dai HN, Imran M, Haider N. Blockchain-enabled internet of medical things to combat COVID-19. IEEE Internet of Things Magazine. 2020 Oct 27;3(3):52-7.

[29]. Zhu L, Li F. Agricultural data sharing and sustainable development of ecosystem based on block chain. Journal of Cleaner Production. 2021 Sep 15;315:127869.

[30]. Indumathi J, Shankar A, Ghalib MR, Gitanjali J, Hua Q, Wen Z, Qi X. Block chain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (bc iomt u 6 hcs). IEEE Access. 2020 Nov 24;8:216856-72.

[31]. Indumathi J, Shankar A, Ghalib MR, Gitanjali J, Hua Q, Wen Z, Qi X. Block chain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (bc iomt u 6 hcs). IEEE Access. 2020 Nov 24;8:216856-72.

[32]. Baskaran G, Kannaiah SK, Ramanujam S. A secured authentication and DSM-KL ascertained performance optimization of a hybrid block chain-enabled framework for a multiple WSN. International Journal of Communication Systems. 2021 Nov 25;34(17):e4972.

[33]. Sivaganesan D. Block chain enabled internet of things. Journal of Information Technology. 2019 Sep;1(01):1-8.

[34]. Phansalkar S, Kamat P, Ahirrao S, Pawar A. Decentralizing AI applications with block chain. International Journal of Scientific & Technology Research. 2019;8(9):9.

[35]. Rajasoundaran S, Kumar SS, Selvi M, Ganapathy S, Rakesh R, Kannan A. Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. Wireless Networks. 2021 Oct;27(7):4513-34.

[36]. Bandaru VN, Visalakshi P. Block chain enabled auditing with optimal multi-key homomorphic encryption technique for public cloud computing environment. Concurrency and Computation: Practice and Experience. 2022 Oct 10;34(22):e7128.

[37]. Rahman MA, Abuludin MS, Yuan LX, Islam MS, Asyhari AT. EduChain: CIA-Compliant Block-chain forIntelligent Cyber Defense of Microservices inEducation Industry 4.0.

[38]. Ahmad N, George RP, Jahan R, Hussain S. Integrated IoT and Block chain for secured access and managing education data. In2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) 2022 Aug 11 (pp. 1201-1204). IEEE.

[39]. Qadeer S, Basheer Q, Qaseem MS. Home Automation Using Block Chain-enabled Cyber Physical System. InBlockchain Technology for IoE 2023 Sep 29 (pp. 261-274). CRC Press.

[40]. Reinhart S, Christopher R. Consumer Perspectives on Data Privacy and Transparency for Blockchain-Based Systems in the US Biotechnology Industry. Journal of Commercial Biotechnology. 2023 Dec 1;28(5).

[41]. Sharanya S, Prakash M, Senthilkumar J. Block chain enabled framework for industrial maintenance. InAIP Conference Proceedings 2024 Apr 2 (Vol. 3037, No. 1, p. 020023). AIP Publishing LLC.

[42]. Sharanya S, Prakash M, Senthilkumar J. Block chain enabled framework for industrial maintenance. InAIP Conference Proceedings 2024 Apr 2 (Vol. 3037, No. 1, p. 020023). AIP Publishing LLC.

[43]. Zuo Y, Dai C, Guo J, Guo Z, Xiao F, Jin S. Secure data sharing for autonomous vehicles in mobile blockchain networks. IEEE Network. 2024 Nov 20.

[44]. Abdallah M, Dobre OA, Ho PH, Jabbar S, Khabbaz MJ, Rodrigues JJ. Blockchain-EnaBlEd industrial intErnEt of things: AdvancEs, applications, and challEngEs. IEEE Internet of Things Magazine. 2020 Jun 25;3(2):16-8.

[45]. Veeraiah V, Preetham A, Karthikeyan P, Kumari PL, Mehta K, Kumbhkar M. Investigating the Role of Block Chain to Secure Identity in IoT for Industrial Automation. In2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) 2022 Apr 28 (pp. 245-249). IEEE.

[46]. Beloor V, Vijaykumar M, Swamy DR, Navneeth S. Block chain enabled Indian Agricultural supply chain using ISM DEMATEL approach. OPSEARCH. 2024 Oct 17:1-28.

[47]. Bhavya G, Swetha MS, Muneshwara MS, Anand R. Soft Computing Technique for Block Chain Enabled Secure Healthcare System. In2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) 2021 May 6 (pp. 305-310). IEEE.

[48]. Bindyashree CA, Basha SM. Trends and Challenges of Block Chain in Electronic Health Record System. In2023 4th International Conference on Smart Electronics and Communication (ICOSEC) 2023 Sep 20 (pp. 654-659). IEEE.

[49]. Das L, Lohani BP, Bhargava D, Sharma B. Data Security and Traffic Management Using Iot and Blockchain Application. InData Management and Security in Blockchain Systems 2024 Dec 26 (pp. 38-63). Bentham Science Publishers.

[50]. Joeaneke PC, Kolade TM, Val OO, Olisa AO, Joseph SA, Olaniyi OO. Enhancing security and traceability in aerospace supply chains through block chain technology. Journal of Engineering Research and Reports. 2024 Oct 4;26(10):114-35.

[51]. Raymond D, Kumar P, Gourshettiwar P, Werarathna I, Mankar D, Verma P. Blockchain Enabled Secure Data Sharing in Medical Sensors Networks: Concise Review. In2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI) 2024 Nov 29 (pp. 1-5). IEEE.

[52]. Banerji N, Debnath B, Bandyopadhyay K. Block-chain enabled secure smart IoT healthcare monitoring for COVID-19 patients. In2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon) 2022 Nov 20 (pp. 1-4). IEEE.

[53]. Yong G, Saw ST, Tang JN, Teng LY, Tang WZ, Ahmed S. The impact of Block chain-Based System on Goods Tracking and management in Industrial Environment. Digital Management Sciences Journal. 2024 Jun 30;1(2):91-105.

[54]. Wason R, Arora P, Nand P, Jain V, Kukreja V, editors. Blockchain-Enabled Solutions for the Pharmaceutical Industry. John Wiley & Sons; 2025 Jan 29.

[55]. Shah JK, Sharma R, Misra A, Sharma M, Joshi S. Blockchain-Enabled Communication Network Transforms Information Technologies: A Thematic Analysis. In2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT) 2023 Nov 23 (pp. 1286-1291). IEEE.

[56]. Haris RM, Al-Maadeed S. Integrating blockchain technology in 5G enabled IoT: A review. In2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT) 2020 Feb 2 (pp. 367-371). IEEE.

[57]. Senthilkumar G, Madhusudhan KN, Jeyasheela Y, Ajitha P. A novel blockchain enabled resource allocation and task offloading strategy in cloud computing environment.

Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije. 2024 Jun 27;65(3):973-82.

[58]. Salam S, Kumar KP. Survey on applications of blockchain in E-governance. Revista Geintec-Gestao Inovacao E Tecnologias. 2021 Jul 29;11(4):3807-22.

[59]. Liu S, Zhang Q, Liu H. Privacy protection of the smart grid system based on blockchain. InJournal of Physics: Conference Series 2021 Feb 1 (Vol. 1744, No. 2, p. 022129). IOP Publishing.

[60]. Khan MA, Abbas S, Rehman A, Saeed Y, Zeb A, Uddin MI, Nasser N, Ali A. A machine learning approach for blockchain-based smart home networks security. IEEE Network. 2020 Nov 17;35(3):223-9.

[61]. Toubi A, Hajami A. Data Manipulation in Wireless Sensor Networks: Enhancing Security Through Blockchain Integration with Proposal Mitigation Strategy. International Journal of Advanced Computer Science & Applications. 2024 Feb 1;15(2).

[62]. Mani C, Ajay C, Harish J, Logesh S, Santhosh N. Block chain and AI-empowered healthcare insurance fraud detection: An analysis, architecture and future prospects. InChallenges in Information, Communication and Computing Technology 2024 Dec 10 (pp. 421-425). CRC Press.

[63]. Wang H. IoT based clinical sensor data management and transfer using blockchain technology. Journal of ISMAC. 2020 Jul 8;2(03):154-9.

[64]. Antoney L, Augusthy TJ. Block chain accounting-the face of accounting & auditing in Industry 4.0. International Multilingual Journal of Science and Technology (IMJST). 2019;4(8):633-7.

[65]. Krishnadas A, Jarin T, John SP, Balogun BF, Addula SR. Analysis of Block Chain Based Technologies Employed in Inter-EV and Grid-EV Energy Trade. Digital Twin and Blockchain for Smart Cities. 2024 Oct 15:323-41.

[66]. Xia L, Sun Y, Swash R, Mohjazi L, Zhang L, Imran MA. Smart and secure CAV networks empowered by AI-enabled blockchain: The next frontier for intelligent safe driving assessment. IEEE Network. 2022 Mar 2;36(1):197-204.

[67]. Kaur J. Decentralized Finance (DeFi) and Blockchain Technology in Healthcare: A Promising Confluence for Enhanced Security, Data Interoperability, and Patient. InHarnessing Technology for Knowledge Transfer in Accountancy, Auditing, and Finance 2024 (pp. 126-149). IGI Global Scientific Publishing.

[68]. Balamurugan K, Azhagiri M, Vardhini PH, Jijo E, Parthiban L. Utilizing Blockchain and Interplanetary File System for Enhanced User Privacy in Secure Data Sharing. InBlockchain and IoT 2025 (pp. 42-60). Chapman and Hall/CRC.

[69]. Nassa VK, Varun VL, Chandra AS, Chakravarthi MK, Singh R, Verma D. Evaluation of block-chain transaction accuracy using neural network model. In2022 5th International Conference on Contemporary Computing and Informatics (IC3I) 2022 Dec 14 (pp. 357-361). IEEE.

[70]. Nesarani A, Ramar R, Pandian S. An efficient approach for rice prediction from authenticated Block chain node using machine learning technique. Environmental Technology & Innovation. 2020 Nov 1;20:101064.

[71]. Das D, Banerjee S, Mansoor W, Biswas U, Chatterjee P, Ghosh U. Design of a secure blockchain-based smart iov architecture. In2020 3rd International Conference on Signal Processing and Information Security (ICSPIS) 2020 Nov 25 (pp. 1-4). IEEE.

[72]. Omobude T, Uchenunu A, Asemah ES. CHAPTER SIXTEEN ADDRESSING FAKE NEWS AND MISINFORMATION IN NIGERIA THROUGH BLOCK CHAIN-ENABLED SOLUTIONS. Politics and Civic.:148.

[73]. Li M, Yu FR, Si P, Zhang Y, Qian Y. Intelligent resource optimization for blockchain-enabled IoT in 6G via collective reinforcement learning. IEEE Network. 2022 Aug 1;36(6):175-82.

[74]. Gai K, Choo KK, Zhu L. Blockchain-enabled reengineering of cloud datacenters. IEEE Cloud Computing. 2018 Nov 29;5(6):21-5.

[75]. Fayyaz F, Ghazal TM, Afifi MA, Abbas S, Al Hamadi H. Drones network security enhancement using smart based block-chain technology. In2022 International Conference on Cyber Resilience (ICCR) 2022 Oct 6 (pp. 1-6). IEEE.

[76]. Sharma DK, Khera A, Gupta KD, Dwivedi R. Blockchain Based Hybrid Framework for Identity Management in Healthcare. Advances in Computing Communications and Informatics. 2022 Jul 28;44:44.

[77]. Savitha M, Senthilkumar M. A unique secure multimodal biometrics-based user anonymous authenticated key management protocol (SMUAAKAP) based on block chain mechanism for generic HIoTNs. Theoretical Computer Science. 2023 Jan 4;941:77-90.

[78]. Shaikh AA, Riadhusin R, Subalakshmi R. Binary Whale Optimization Algorithm with Bidirectional Long Short-Term Memory Blockchain-based Privacy-Preserving for Healthcare Data in Internet of Things. In2025 3rd International Conference on Data Science and Information System (ICDSIS) 2025 May 16 (pp. 1-5). IEEE.

[79]. Mahavaishnavi V, Saravanan S, Anbalagan P. Blockchain-enabled Security for Medical Image Transmission: Prescription Data Hiding and Multi-secret Sharing-based Encryption. InTechTrends: Navigating the Frontier of Emerging Technologies 2025 Nov 11 (pp. 1-23). Bentham Science Publishers.

[80]. Chughtai ZA, Janjua JI. Block Chain Enabled Vehicle Documents Verification System. In2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC) 2025 Apr 10 (pp. 1-7). IEEE.

[81]. Manocha PS, Kumar R. Improved spider monkey optimization-based multi-objective software-defined networking routing with block chain technology for Internet of Things security. Concurrency and Computation: Practice and Experience. 2022 May 15; 34(11):e6861.