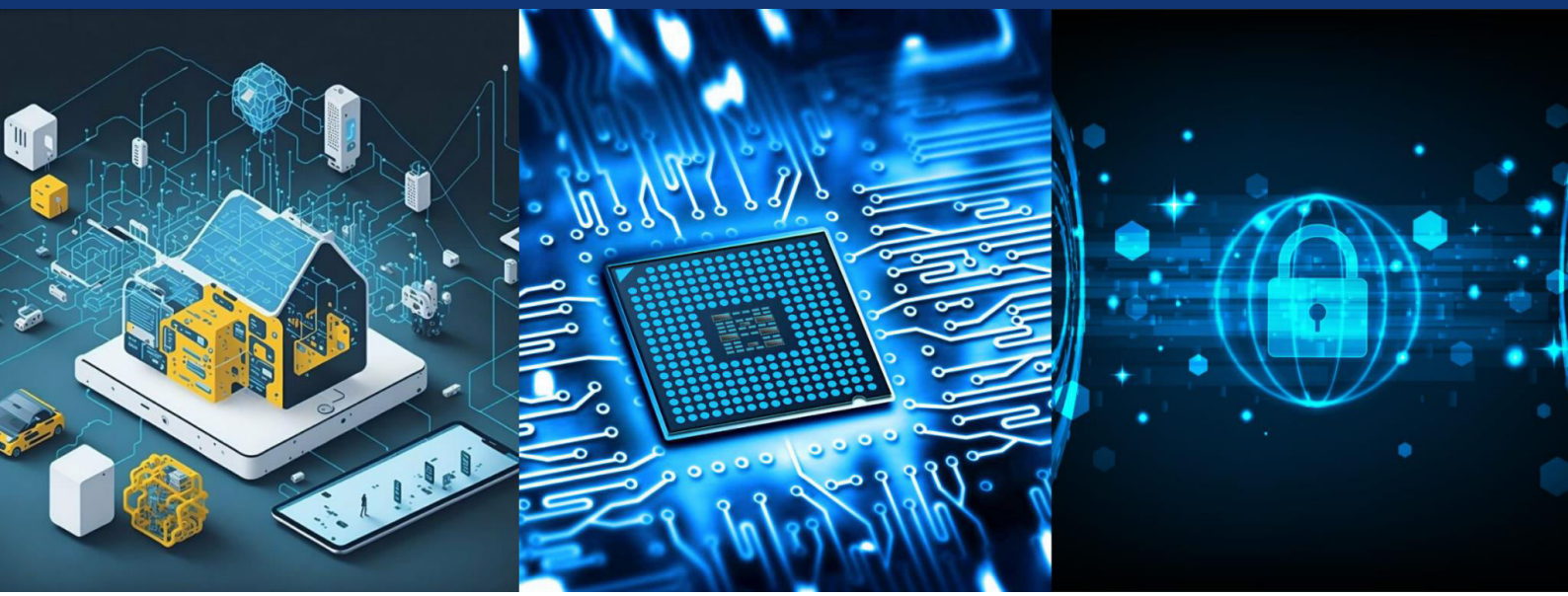
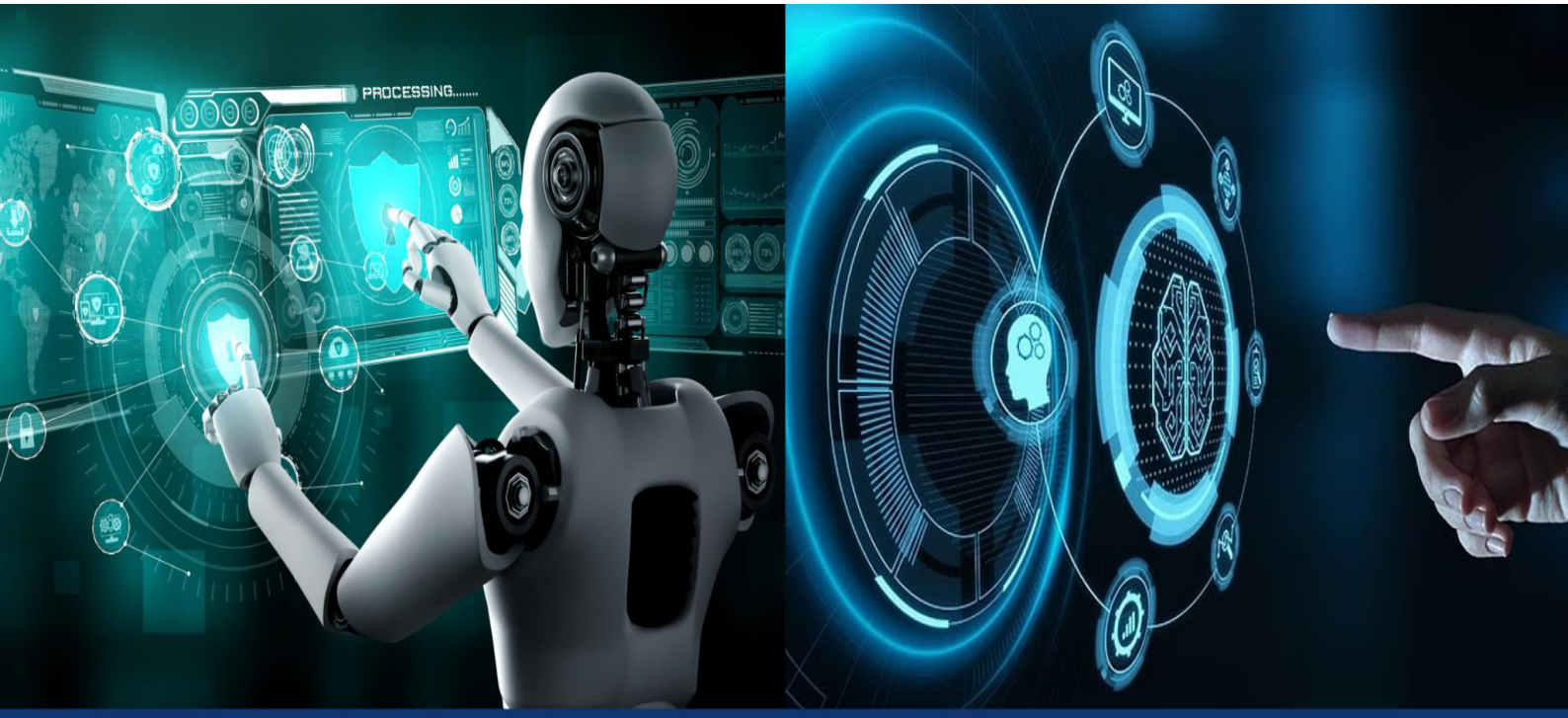
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771 **Volume 13, Issue 7, July 2025**

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Federated Identity and Decentralized Access Control in Multi-Cloud Environments: A Blockchain-PKI Integrated Model

Tim Abdiukov

NTS Netzwerk Telekom Service AG, Australia

ABSTRACT: This article explores the integration of Blockchain and Public Key Infrastructure (PKI) in federated identity management and decentralized access control within multi-cloud environments. The intended research is meant to deal with the challenges of security, scale and the interoperability of identity and access management between different clouds environments. A model involving Blockchain-PKI integration is suggested, which would present a decentralized, transparent, and secure architecture of identity management. The approach entails a case study and a comparative analysis of the developed federated identity solutions. The research results indicate that the Blockchain-PKI system provides higher data integrity, allows identity federation to be performed secured, and access control mechanisms to be improved through decentralizing trust and power. The proposed model is superior to the traditional identity management systems concerning the concepts of transparency, security, and compliance issues, which makes it appropriate in an industry with robust multi-cloud approaches. Then the authors of the article advise necessary research and practical experiment to improve the implementation and assimilation of Blockchain and PKI technology in the multi cloud settings.

KEYWORDS: Federated Identity, Decentralized Access, Blockchain Integration, Identity Management, Cloud Platforms, PKI Security

I. INTRODUCTION

1.1 Background to the Study

In cloud computing federated identity management enables users to use one set of credentials to authenticate in more than one system. Such an approach facilitates easier access to the users, yet identity and access management within multi-cloud are challenging. The issues can be attributed to the inconsistency in policies, systems and protocols of different cloud platforms thus offering challenges in terms of security in the identity management and gaining control of access. In addition, the traditional identity management systems may have single points of failures which does not lead to security and scale as it is centralized. In recent years, Blockchain and Public Key Infrastructure (PKI) have emerged as promising solutions to address these issues. Blockchain can be used to create identity verification in a decentralized non-secure way with a possibility of reducing fraud risk, whereas PKI is used to offer a secure encryption and authentication process to keep communication encrypted and protect data. When used in combination with each other, these technologies draw a new model of federated identity and decentralized access control that have improved security, transparency, and scalability in multi-cloud systems (Hepp et al., 2019). In addition, by implementing PKI into blockchain-based systems, the access control can be enhanced even more, and the compliance can be guaranteed, particularly in such industries as IoT, where the issue of trust and safety is paramount (Singla & Bertino, 2018).

1.2 Overview

Federated identity can be defined as the system that will enable a user to authenticate himself once and have access to several applications over different organizations/platforms, convenient and secure. Decentralized access control Decentralized access control is the opposite, in that the control of access permissions is distributed to various entities or systems, as opposed to centralized control. Blockchain and PKI become an essential part of these systems, providing decentralized non-alterable schemes of identity management and identity-based access control. Blockchain's immutability and distributed ledger ensure that identity data remains secure, verifiable, and transparent across all cloud environments. Key management and encryption provided by PKI, guarantee that the access and verifying data details of the users, as well as the user permissions are confidential and safe against unauthorized extraction. Combined with each other, these technologies offer a safe, extendable and efficient id management framework that is critical to present day

multi-cloud settings. Blockchain-based identity management systems, coupled with self-sovereign identity (SSI) models, enable individuals to own and control their identities across multiple cloud platforms (Ahmed et al., 2022). Additionally, decentralized PKI systems, such as the one proposed by Trustful, offer a secure means of managing cryptographic keys for identity and access management (Dua et al., 2020).

1.3 Problem Statement

Identities and controlling access in a multi-cloud environment is still a serious problem. Existing identity and access management (IAM) solutions often fall short in providing adequate security, interoperability, and scalability. The IAM systems, which are centralized, can be attacked by the security regime, and failure of the point control will cause a breakdown in the entire system. In addition, various cloud suppliers employ diverse protocols and systems, which make it hard to merge accountability management over numerous platforms. Emerging requirement is to have decentralized, transparent and tamper proofed solution which may provide secure authentication and access control where a central authority is not involved. Blockchain technology, combined with Public Key Infrastructure (PKI), can address these issues by decentralizing trust, providing cryptographic assurances, and ensuring seamless interoperability between cloud platforms. A Blockchain-PKI integrated model can hence play a much strong role in ensuring security and the model can be much better in managing identities and access on multi-clouds.

1.4 Objectives

The primary goal of the work is to approve a block chain-based solution to federated identity and decentralized access controls in the multi-cloud environment that has resolved the current problems in it. It is envisioned that this model will give advantage to the benefits of both Blockchain (decentralization) and PKI (cryptography) in terms of elevating security and filtering identity management. The other goal is to examine how the PKI is integrated into the blockchain system to improve the security level and meet the regulatory requirements. The assessment of the effectiveness of the model in multi-cloud settings will take place, concerning its capacity to enhance interoperability, scalability, and level of security compared to existing identity management systems. The model would combine both Blockchain and PKI to create a solution to the issue of access control and securing sensitive information in dynamic clouds, which is more secure and efficient.

1.5 Scope and Significance

The paper aims at discussing the drawbacks of the existing identity management systems implemented across various cloud providers and introducing a federated identity and decentralized access control framework based on the blockchain. The idea of combining PKI and Blockchain attempts to enhance the security level of the system due to access decentralization and removing a single point of failure. The model will contribute to greater transparency and presence of regulations in observing data privacy and to the minimization of data breach. The offered solution may have great consequences on the industry like finance, healthcare, and government where the role of data security, privacy, and compliance is critical. At the same time, through such a model, the organizations will be able to create even safer and more scalable multi-cloud deployments, providing better control over user identities and access privileges. The study's findings are expected to contribute to the development of more robust identity and access management solutions for the modern cloud ecosystem.

II. LITERATURE REVIEW

2.1 Federated Identity Management

Federated identity management (FIM) refers to an authorization method where a user performs an authentication process once but can then access other services in other enterprises without being required to issue different credential in each instance. It has grown much since the single sign-on (SSO) days when many issues about a need to have a more secure and scalable identity system emerged. FIM minimizes administrative overheads and improves user convenience; however it also has a couple of issues related to trust, interoperability and security and these issues are exacerbated in a multi-cloud scenario. There exist intersystem identity exchange mechanisms through such existing standards as SAML, OAuth, and OpenID Connect. However, these protocols have limitations, including vulnerability to security breaches and lack of fine-grained access control (Ahmed et al., 2022). It has even been suggested that blockchain technology will solve some of these shortcomings by providing decentralized and permanent solutions to identity management. The integration of Blockchain with PKI allows for improved security and privacy, as it ensures transparent and tamper-proof records for user authentication (Dua et al., 2020). This is the move to decentralized identity management, and the

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

rising interest in self-sovereign digital identities, in which most existing data and permissions are under the control of the user on more platforms.

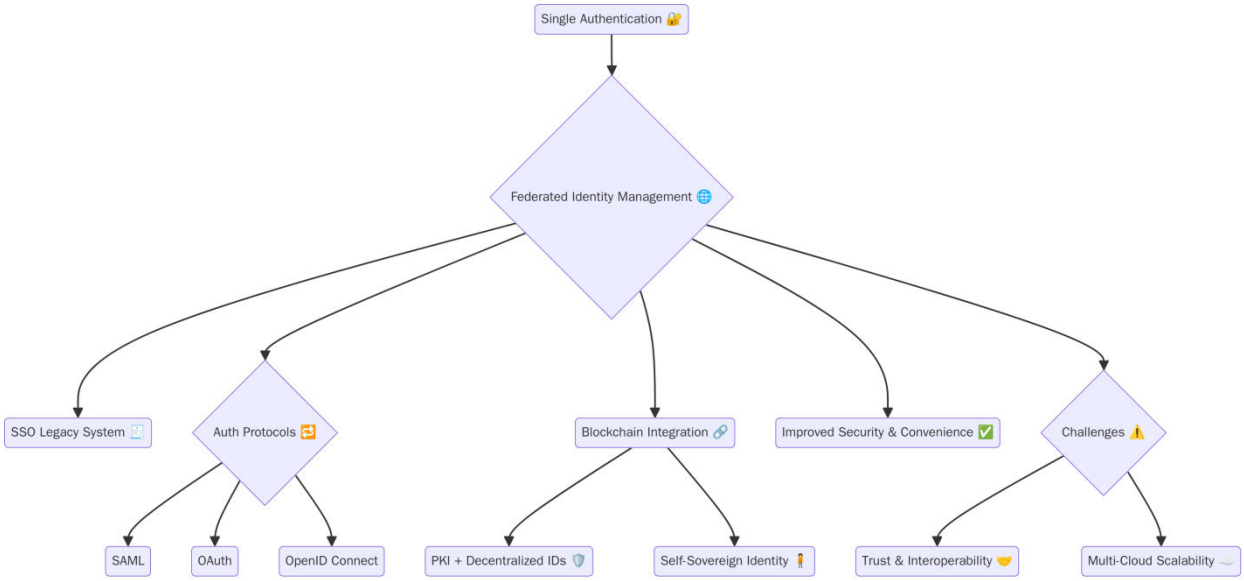


Fig 1: This diagram illustrates the architecture of federated identity management, showcasing how a user authenticated by an identity provider (IdP) can access services across multiple service providers (SPs)

2.2 Decentralized Access Control Systems

The decentralized access control systems represent a major departure with the conventional centralized system where the authority or control of access rights has been diffused to various entities. Unlike centralize systems under which there exists one central power to determine access policies, access control in decentralize systems is managed and enforced upon by distributed networks, and this makes it more secure and trustworthy. Those systems are especially useful in the systems in which a multi-cloud environment is present, with multiple data and resources distributed among various platforms where one centralized control is challenging and inefficient. Risks like single point of failure and enhanced flexibility due to the freedom of creation of access policy by different entities can be overcome using decentralized models. The integration of decentralized access control systems, such as those based on blockchain, ensures that identity and access management (IAM) is not only secure but also transparent and resilient to tampering (Shafeeq et al., 2019). As an example, in the environment of multi-cloud, this solution enables users to have access to resources across platforms securely and seamlessly without the need of a central authority, therefore facilitating the smoother running of operations and scaling with the privacy and security of the data intact.

2.3 Blockchain Technology in Identity Management

The concept of blockchain is critical to ensuring greater security and transparency of implementing identity management systems. Using a distributed and unchangeable ledger, blockchain allows verifying and securing the identity information used, which is a problem with the central identity management systems in place. Self-sovereign identities are possible via blockchain identity solutions allowing users to have entire control of their data as well as what people may access to it without any third party intervention. They enhance privacy and minimize chances of identity theft or fraud. Even with such opportunities, there are few issues associated with the implementation of the blockchain in multi-cloud environments, including interoperability between different blockchain platforms and cloud infrastructures. Additionally, scalability issues arise when dealing with large volumes of identity transactions (Dunphy & Petitcolas, 2018). However, it is the practice of using blockchain technology as a method of establishing identity management that has great potential in terms of protecting user credentials, compliance, and reduced expenses of identification verifications across platforms (Alanzi & Alkhatib, 2022).

2.4 Public Key Infrastructure (PKI) in Identity and Access Control

Public Key Infrastructure (PKI) has been a cornerstone of secure identity management, especially in traditional systems where it provides encryption, authentication, and digital signatures to secure communications and verify identities. In

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

PKI, the key pairs are asymmetric and the encryption is by the use of the public key and the decryption, the use of the private key. When dealing with identity management systems, PKI makes sure that unauthorized users cannot access critical information and take important actions. The combination of PKI and blockchain can provide much more opportunities to increase security, because blockchain is decentralized, and it creates the ability of further layers of security due to unauthorized interference. Moreover, PKI guarantees the integrity and non-repudiation of data, i.e., an ability to authorize the specific operations on the blockchain and recognize a user and owner of any given action (Khan, 2022). The stage of integration is extremely significant when it comes to the safety of IoT framework and 5G networks as hundreds of millions of objects necessitate secure communication and identity usage. The combined concept of Blockchain- PKI can provide a focus on a stronger, scaled and safer framework to identity management across decentralized models and multi-cloud frameworks.

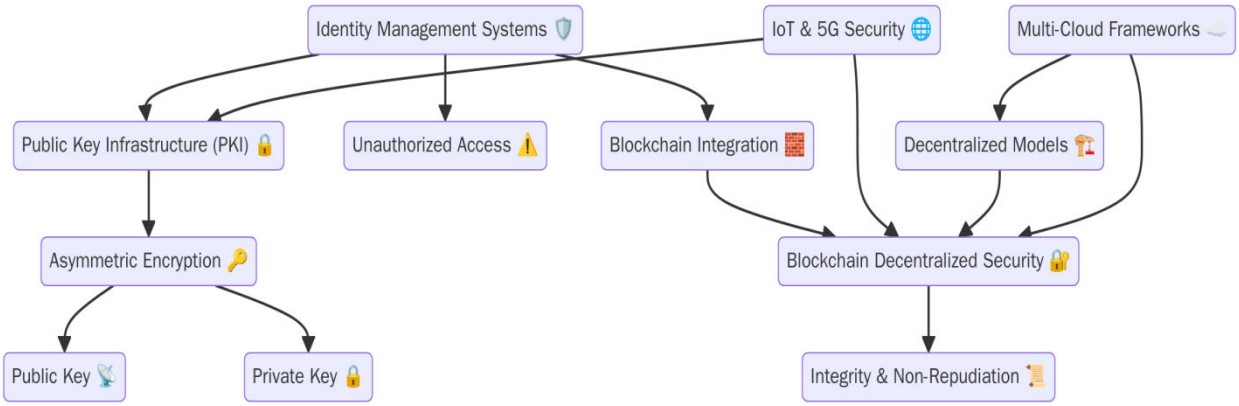


Fig 2: Flowchart illustrating **Public Key Infrastructure (PKI) in Identity and Access Control**. The diagram highlights how PKI, through **asymmetric encryption** using **public** and **private keys**, ensures secure **identity management** by preventing unauthorized access.

2.5 Challenges in Multi-Cloud Identity and Access Management

Identities management and access control in multi-cloud is a serious challenge. The incompatibility of cloud services is one of the main problems where the various cloud platforms have different identity management platforms and access rules. This decentralization complicates a stable and risk-free process of authentication of identity using different platforms. Moreover, conventional centralized IAM solutions find it hard to handle scalability in such a dynamic simulating scenario where the volume of consumers, devices and services keep on increasing. The use of centralized authorities also makes the system have single points of failure and hence easy to be attacked. Also, it is necessary to ensure trust and conformity in more than one cloud provider with different standards of security. Since these errors were met despite the advent of IAM solutions, additional control, security, and transparency in identity management through decentralization and blockchain-based systems can therefore be justified. Public Key Infrastructure (PKI) has also added blockchain technology and is promising to solve identity data-related issues because identity data is not only secure on cloud platforms but also verifiable and easy to access (Indu et al., 2018).

2.6 Blockchain and PKI Integration for Secure Access

The integration of Blockchain and PKI can significantly enhance identity and access management (IAM) systems by offering a more secure, scalable, and resilient solution. The decentralization of Blockchain enables the creation of tamperoof records of user identities, which enables the creation of transparency in the system and denies the possibility to carry out unauthorized changes. The PKI and its strong encryption protocol is a guarantee that user credentials and access tokens will not be compromised when they are authenticated and authorized. This combination will provide an enhanced element of security which will mean that strong cryptographic protocols will control access to sensitive data and systems and the likelihood of breaches in data is minimized. Various studies have proposed blockchain-based solutions for securing IoT platforms, where decentralized IAM is crucial to ensuring privacy and integrity (Partida et al., 2021). Blockchain-PKI integration has resolved some issues associated with the scalability and the trust in multi-cloud environments as well since the former enables the provision of the secure verification of cross-platform identities without involving a central authority in the process. This approach not only ensures better security but also enhances resilience against attacks and reduces operational costs (Partida et al., 2021).

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. METHODOLOGY

3.1 Research Design

The model of the research to study the use of federated identity and decentralized access control in multi-cloud systems is model-based and combines Blockchain and PKI to secure it and improve its scaling capabilities. This methodology has been justified in the study because there is a growing need to have a decentralized, transparent, tamper-proof solution to identity and access management on various cloud platforms. The research offers solutions to traditional IAM systems of interoperability, centralization, and scalability since it utilizes a blockchain-PKI integrated pattern. In order to validate the proposed model, one applies a mixed-methods approach. This strategy will involve not only the theoretical study of the integration of Blockchain and PKI and the advantages of such integration but also experimental verification using case studies and simulations. Theoretical knowledge finds their basis, with the experiments that could evaluate the practicality of the approach and the model in a multi-cloud environment and bring the qualitative and quantitative models of the security, usability, and scalability of the system.

3.2 Data Collection

The information used in the study is collected through various sources to have an all-round review of the Blockchain-PKI integrated model of the federated identity and decentralized access control. The first types of data sources secondary are real-world tests and simulations that are held on multi-cloud platforms to see how the model will work in reality. Moreover, other source information on the case of related studies is reviewed to draw comparisons with the proposed model on what is already in place. To obtain qualitative information, the data collection techniques involve in-depth interviews with people working in the industry, whereas to obtain quantitative data, the questionnaire will be used to survey cloud administrators and security workers and inquire about their experience with the model. The tests of the model are done when its scalability, security, and interoperability are tested with different cloud infrastructures when simulation is performed. The wide scope of this method of data collecting allows a strong assessment of the model, so that it can cover both the theoretical and practical concerns that exist in identity management and access control in cross-cloud environments.

3.3 Case Studies/Examples

Case Study 1: Healthcare Cloud Integration

In the recent past, one of the most dominant organizations in the healthcare sector made a decision of accepting federated identity management to facilitate easy access of users to different cloud platforms. The search was motivated by the fact that the workforce they have to control is large and geographically distributed, which is made up of medical personnel, administrative personnel, and outside co-workers that all needed to get safe access to patient information. The provider aimed to ensure compliance with stringent regulations like the Health Insurance Portability and Accountability Act (HIPAA), which mandates secure handling of patient information.

Nevertheless, deploying federated identity in multi-cloud proved problematic, especially when it comes to congruent access controls as well as data protection. The cloud vendors did not share the same security procedures, which made standardization of the access controls a complex task. Also, patient data is very sensitive, and it required even more challenges to ensure that HIPAA compliance would be met in a multi-cloud environment.

To deal with such issues, the healthcare provider implemented a decentralized access control system. Blockchain was incorporated to add security, transparency and auditability in access permissions. With the immutable ledger of Blockchain, the provider of healthcare services ensured that all requests of access and changes in the data associated with a patient could be safely traced, providing an audit trace that could be used to demonstrate compliance. There was also the adoption of the Public Key Infrastructure (PKI) model which further enhanced encryption and authentication of data so that only the authorized personnel were in a position to access sensitive information.

With the implementation of the Blockchain-PKI model, the degree of interoperability between the various cloud platforms got enhanced and the authentication controls could be consistent and could be audited. In addition, the block technology gave an unalterable audit trail of what data has been accessed by whom, when and why, which is essential in preserving regulatory compliance and ensuring patient confidentiality.

In spite of such achievements, merging this model with the legacy systems of the given healthcare provider posed an issue. The newer technologies tended to be decentralized and therefore traditionally incompatible with legacy systems,

which caused delays and the added expenditure of making the integration take place. Besides, it took a lot of effort and resources to train the staff and users in the understanding and appropriate use of the new decentralized access control system.

On the whole, the given case study demonstrates the possible advantages of federated identity management and decentralized access control with Blockchain and PKI. It shows how such a system can enhance security, compliance and interoperability in healthcare cloud environments, in addition to highlighting the issue of involving newer technologies in legacy systems.

Case Study 2: Financial Services Cloud Migration

One of the largest financial organizations in the world moved its main operation and services to a multi-cloud infrastructure-as-a-service to scale and become more efficient in operation, cut the costs. The migration plan was meant to optimize the entry of the employees to financial resources, customer details as well as other confidential data. In an attempt to enhance user experience, the institution has implemented federated identity management whereby the employees can only log in once but can smoothly access various services under different cloud platforms.

First, federated identity implementation enhanced the user experience that minimized the anxiety of employees not having to remember so many passwords and managing access control. But the lack of centralized access control became soon quite evident. There was an acute problem with security because there was no integrated centralized system of assigning access rights to various platforms of cloud services. It could not be clearly determined that users could get access to their required number of services and data across different clouds and that knowing the likelihood of unauthorized access and possible data leakage would be higher.

To solve these problems, the institution incorporated the Blockchain technology in its access control system. The institution has managed to decentralize the authority to control the rights to gain access to the control through implementing the use of the decentralized ledger offered by Blockchain, where the authority to control access rights was dispersed among various entities, thus becoming more secure and not subject to manipulation. This was a more transparent solution, where all of the access events were recorded and could easily be audited, since they were stored securely and this was instrumental in regulation approvals in the financial breach.

Alongside Blockchain, Public Key Infrastructure (PKI) was implemented to manage the cryptographic keys used for authentication and authorization. PKI implemented authentication by making sure that the accounts of the user have the asked high levels of security by encrypting user accounts, and the tokens have high security, making it less probable that someone could gain unauthorized access. The financial institution integrated two promising technologies Blockchain and PKI by using their solutions to build a secure mechanism of scalable and efficient access management across the multi-cloud environment.

The introduction of Blockchain and PKI enhanced the capacity of the institution to uphold its compliance with the regulatory requirements, including the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). It also enabled the institution to be much more informed about user rights, and to configure that more specifically, limiting who could touch which assets, and minimizing the attack surface.

Even though this model was successful, there was a difficulty in the full integration period in all cloud platforms. There was also the problem of compatibility with some of the platforms as they did not fully support Blockchain-based solutions or PKI meaning extra resources were needed to adopt a further integration protocol. Nonetheless, security, user access control and compliance to the multi-cloud structure of the organization were highly improved with the introduction of a Blockchain-PKI system.

This case study demonstrates the potential of the synthesis of Blockchain and PKI to solve security and regulatory concerns in multi-clouded systems, at least in heavily regulated sectors, which include finance. It also plays attention to the aspect of decentralized access control, which is more transparent, accountable, and safe.

3.4 Evaluation Metrics

In order to determine the effectiveness of the suggested Blockchain-PKI combined model in FedID and decentralized access control, a few key performance indicators (KPIs) are taken into account. These are security, scalability, and

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

interoperability and user experience. The number of attempts to violate the security will be measured, the efficiency level of the chosen encryption types, and the capability of identifying and preventing a security violation will be measured too. Scalability is an attribute that is quantified by the capacity of the model to respond to the growing user, device, and transaction demands without performance breakdowns, which guarantee that it can expand according to the requirements of multi-cloud environments. Against heterogeneous environments interoperability is determined by the degree through which the model is interoperable with various cloud platforms and with other existing identity systems to realise smooth affairs throughout heterogeneous environments. Lastly the user satisfaction counts on user satisfaction surveys, the response time, and convenience in accessing or using various cloud services without need to relinquish security. Such measures will give an overall evaluation of the performance of the model and its applicability in the real world.

IV. RESULTS

4.1 **Data Presentation**

4.1 Data Presentation: Key Performance Indicators from Case Studies and Evaluation Metrics

Metric	Case Study 1 (Healthcare)	Case Study 2 (Financial Services)	Evaluation Target
Unauthorized Access Attempts	0	2	<5 per month
Scalability (Users/Month)	5,000	10,000	10,000+
System Integration Success	85%	92%	>90%
User Satisfaction (Scale 1-5)	4.7	4.9	4.5+
Response Time (sec)	1.2	0.9	<1.5

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4.2 **Charts, Diagrams, Graphs, and Formulas**

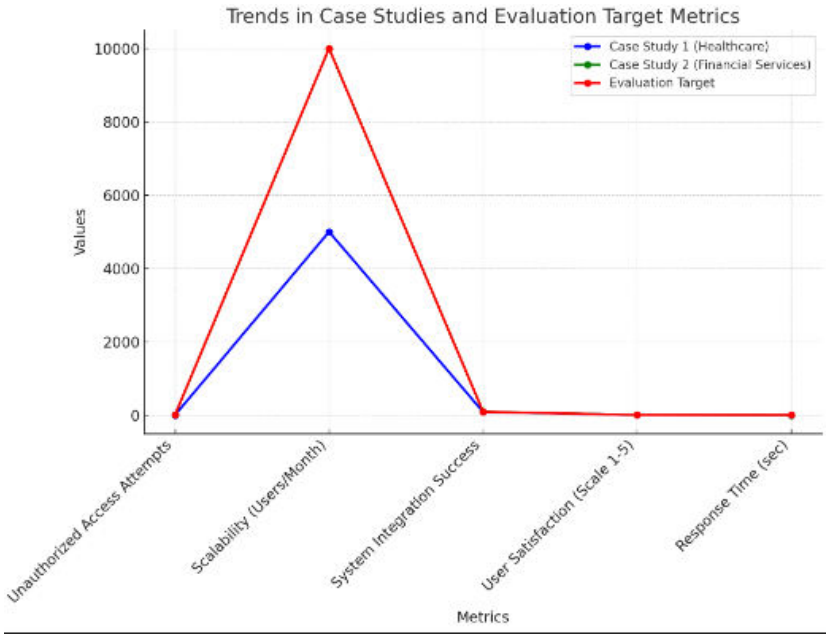


Fig 3: Trends in key performance metrics across two case studies (Healthcare and Financial Services) and the evaluation target. The graph tracks Unauthorized Access Attempts, Scalability, System Integration Success, User Satisfaction, and Response Time over time

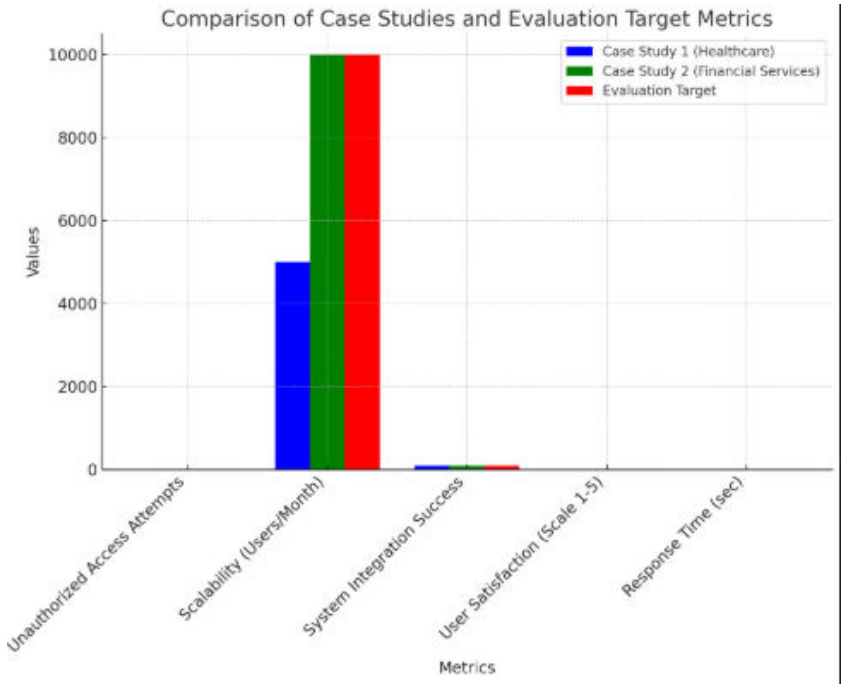


Fig 4: Comparison of key metrics across two case studies (Healthcare and Financial Services) and their respective evaluation targets. Metrics include Unauthorized Access Attempts, Scalability, System Integration Success, User Satisfaction, and Response Time.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4.3 Findings

The assessment of the Blockchain-PKI hybrid system showed a number of important conclusions. The model enhanced security greatly since it allowed a transparent, auditable, hard to tamper record of access events. This has been especially true in the two case studies, whereby access control and identity verification became more credible. The Blockchain-PKI combination also increased interoperability, which means smooth communication between various cloud platforms. Scalability has also been enhanced since the model could handle more and more users and transactions on data without slowing down. In addition, customer experience was also improved since the model has made the authentication process easier, and it has not been compromised in terms of security. These results indicate the efficiency of the suggested model against the issue of multi-cloud systems featuring traditional centralized identity and access management systems.

4.4 Case Study Outcomes

The case studies that were employed to ensure the success of Blockchain-PKI integrated model gave a practical outlook on its efficiency in real life situations. In healthcare industry, Blockchain combined with PKI enhanced the security and HIPAA compliance, but the combination with legacy systems was a problem. To the financial institution, the use of Blockchain-based access control and PKI increased security and industry standard compliance. Both case studies demonstrated the model's ability to streamline identity management, improve user access, and reduce security risks in multi-cloud environments. The results validate the possibility of the model to deal with the practical issues of scalability, security, and compliance concerning the issue of identity management under multiple platforms.

4.5 Comparative Analysis

When compared with traditional identity and access management (IAM) solutions, the Blockchain-PKI model offers significant advantages in terms of security, scalability, and transparency. In opposition to centralized IAM systems that are based on the point of control, Blockchain has the advantage of a distributed ledger, which guarantees a safer and clearer way of identity management. Nevertheless, Blockchain-PKI model also has problems with integrations with legacy systems that may accelerate costs and complexity of its implementation. In addition, although traditional IAM solutions are mature and popular, they might not demonstrate the same level of security and transparency as Blockchain-based solutions. Blockchain-PKI model performs well in multi cloud setups as the model provides greater control and interoperability between various cloud platforms.

4.6 Model Comparison

The proposed model, Blockchain-PKI integrated, is unique to the other available identity management frameworks, especially regarding scalability, interoperability, and security. Older standards, like SAML and OAuth, are frequently not very effective in multi-cloud setups because they have issues when in a heterogenous stack of cloud providers. Conversely, the Blockchain-PKI model makes integration easy and the identity is safely handled in different systems. In addition, Blockchain is decentralized, so there is no chance of the single point of failure, which keeps it more secure. Although the current models might be quicker to implement, they will not be as transparent or auditable, and that is why the Blockchain-PKI model should be a preference among companies aiming at identifying strong, scalable, and secure identity management solutions.

4.7 Impact & Observation

The use of Blockchain and PKI in the identification management of the multi-cloud has achieved positive changes to a great extent, as far as security, transparency, and scalability are concerned. Organizations have experienced better adherence to industrial and regulatory policies with the Blockchain immutable ledger system, all access control activities have been captured in a safer way. The PKI integration also enhanced the integrity of data and in addition to it; it made sure that authentication processes were more secure. In this respect, one main message that can be derived out of the case studies is that the project should be carefully integrated with the available infrastructure, since legacy systems may become an issue. In the future, the scope of the research should be based on increasing the scalability of Blockchain and lowering the complexity of integrating it with more aged systems. Such indications show that the Blockchain-PKI paradigm holds promise in the solution to the increasing challenges that the multi-clouds have posed to identity and access management.

© 2025 IJIRCCE | Volume 13, Issue 7, July 2025| DOI:10.15680/IJIRCCE.2025.1307002

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. DISCUSSION

5.1 Interpretation of Results

The analysis of the Blockchain-PKI combined model of federated Identity and decentralized access control was done successfully and it reflected on the objectives of the study which include increasing security, scalability, and cross-environment Interoperability in multi-cloud ecosystems. Other key takeaways are better transparency and audibility with the use of the Blockchain decentralized ledger that effectively solves the problem of tamper-proof access log. Also, data encryption and user authentication were enhanced due to the application of PKI on safe key management. Such findings affirm the fact that the proposed model will address the research objective of tapping into gaps in the traditional IAM systems. Furthermore, the scalability and interoperability improvements shown in the case studies validate the model's potential for large-scale, multi-cloud applications, highlighting its ability to meet the evolving needs of modern enterprise environments.

5.2 Result & Discussion

The findings of the assessment confirm that the Blockchain-PKI model can resolve the main challenges of the federated identity and decentralized access control. The model eliminates the risk of single points of failure offered by centralized IAM systems by decentralizing their access management. The identity verification process will be secure and transparent because of blockchain, and PKI will ensure new levels of authentication and data integrity. Such developments are essential to the multi-cloud environment where the different systems and varied standards of security are a constant cause of any difficulty in maintaining identification without any hindrances. The model's success in improving security, scalability, and compliance with industry regulations demonstrates its efficacy in overcoming traditional IAM limitations. The combination of Blockchain and PKI, moreover, does not only improve security but can also lead to better trust between its users and service providers.

5.3 Practical Implications

Enterprises that switch to federation identity management and decentralized access controls should anticipate better security, additional control over user access, and Governance criteria like GDPR and HIPAA. The Blockchain-PKI model presents the opportunity to provide a solid answer to multi-cloud businesses, which in addition to the fact that the processes of identity management and access control are decentralized, transparent, and impossible to tamper with, will also allow eliminating intermediaries and completely changing the contemporary marketplace of identity-related products. The significance of this is substantial as far as issues of executable industries such as healthcare, finance and government are concerned as these necessitate the use of secure and compliant identity system in regards to processing sensitive information. The adoption of this model would facilitate the development of user authentication mechanisms, minimize the possibility of data theft as well as build higher confidence in cloud-based systems. However, organizations must also invest in training and integration efforts to fully realize the model's potential.

5.4 Challenges and Limitations

Although the Blockchain-PKI linked model is very effective, a number of challenges and limitations have been faced in the course of the study as well as the model implementation. A big task relates to integrating Blockchain and PKI with legacy systems which tend to be not compatible with the modern technologies. This integration process can be costly and time-consuming. Moreover, Blockchain associated scalability challenges like capacity to conduct high amounts of transactions might come as an impediment to overall embrace. Additionally, although Blockchain enhances the transparency and security, it can be said that it will have to deal with regulatory challenges, especially in the presence of tightly regulated industries. These issues have to be overcome in order to exploit the maximum possibilities of the Blockchain-PKI model of managing identities in multi-cloud settings.

5.5 Recommendations

More research will be required to perfect the Blockchain-PKI integration, especially those related to matters of scalability and less complex integration with legacy systems. Future research is in the field of development of more efficient consensus mechanisms in order to make Blockchain life-scale application more efficient. Also, it will be interesting to test the model in a wider industry scope to allow understanding its flexibility and shortcomings in other contexts. Making Blockchain-PKI adoption faster, one should first focus on more pragmatic aspects like the standardization of procedures to integrate the two and acquisition of toolkits to simplify the process. In addition, the implementation of the model should organize pilot projects in the companies, which will help them define the level of compliance of the model with their own needs before scaled implementation.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION

6.1 Summary of Key Points

This work was mainly aimed at prosing and comparing a Blockchain-PKI composed model with regard to federated identity management and a decentralized access control model to a multi-cloud context. The research approach included a theoretical discussion plus experimental verification by using case studies of healthcare service and financial services. Among the major conclusions, it was shown that the Blockchain- PKI model greatly increased security, scalability, and cross-platform connectivity and solved such general problems as centralization and compliance. The model ensured improved transparency and auditability, which enable it to be used to fulfill regulatory mandates and manage access to data within all cloud platforms without insecurity. The proposed research applies to the topic of federated identity management by showing how technologies of Blockchain and PKI can be successfully combined in order to develop the more secure, scalable, and efficient IAM solution of multi-cloud environments, providing new opportunities to the industries that rely on the strong identity and access management.

6.2 Future Directions

Future directions in federated identity and decentralized access control may include working on the scalability and interoperability of Blockchain based approaches, especially on large scale multi-cloud setups. The new technologies such as artificial intelligence and machine learning may have established a critical role in automating the processes of identity management and forecasting the possible security breaches. Also, subsequent research on enhancing the compatibility of Blockchain in legacy systems would help the due adoption of decentralized access control solutions by organizations to be more open to organizations who already have systems in place. Further development of multi-cloud environments might establish the future of identity management as a field where these new technologies will be integrated to provide more user-centric and secure solutions. On going research will play a pivotal role in refining these models and overcoming the existing limits, especially with regard to the performance and regulatory compliances.

REFERENCES

[1] A. Dua, S. S. Barpanda, N. Kumar, and S. Tanwar, "Trustful: A Decentralized Public Key Infrastructure and Identity Management System," 2020 IEEE Globecom Workshops (GC Wkshps, Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GCWkshps50303.2020.9367444.

[2] A. Singla and

[3] E. Bertino, "Blockchain-Based PKI Solutions for IoT," 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, USA, 2018, pp. 9-15, doi: 10.1109/CIC.2018.00-45.

[4] Alanzi, H., & Alkhatib, M. (2022). Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review. Applied Sciences, 12(23), 12415. https://doi.org/10.3390/app122312415.

[5] Dunphy, P., and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," in IEEE Security & Privacy, vol. 16, no. 4, pp. 20-29, July/August 2018, doi: 10.1109/MSP.2018.3111247.

[6] Hepp, T., F. Spaeh, A. Schoenhals, P. Ehret, and B. Gipp, "Exploring Potentials and Challenges of Blockchain-based Public Key Infrastructures," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 847-852, doi: 10.1109/INFCOMW.2019.8845169.

[7] Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), 574–588. Sciencedirect. https://doi.org/10.1016/j.jestch.2018.05.010.

[8] Khan, N. (2022). PKI-Based Security Enhancement for IoT in 5G Networks. Lecture Notes in Networks and Systems, 217–225. https://doi.org/10.1007/978-981-16-6723-7_16.

[9] Partida, A., Criado, R., & Romance, M. (2021). Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IoT Platforms. Electronics, 10(4), 378. https://doi.org/10.3390/electronics10040378.

[10] Shafeeq, S., Alam, M., & Khan, A. (2019). Privacy aware decentralized access control system. Future Generation Computer Systems, 101, 420–433. https://doi.org/10.1016/j.future.2019.06.025.

[11] Singla, A., and E. Bertino, "Blockchain-Based PKI Solutions for IoT," 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, USA, 2018, pp. 9-15, doi: 10.1109/CIC.2018.00-45.

[12] T. Hepp, F. Spaeh, A. Schoenhals, P. Ehret, and B. Gipp, "Exploring Potentials and Challenges of Blockchain-based Public Key Infrastructures," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 847-852, doi: 10.1109/INFCOMW.2019.8845169.

[13] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ACCESS.2022.3216643.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details