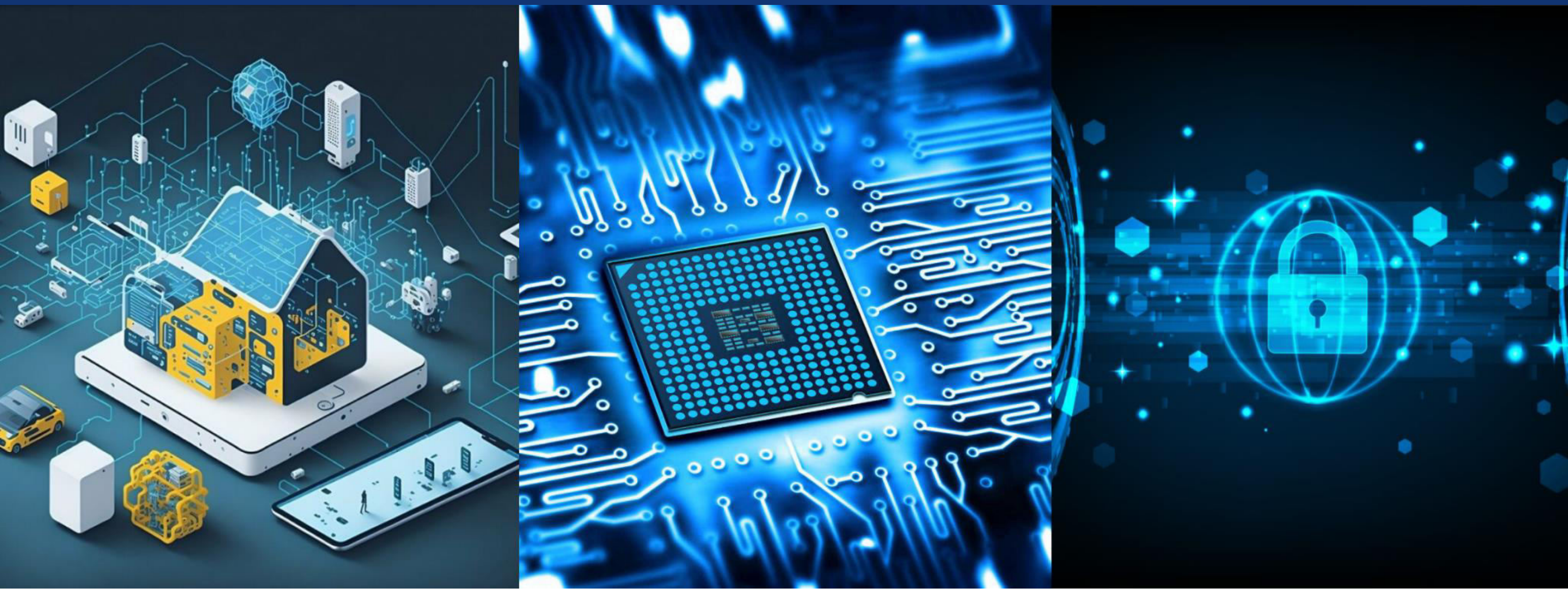
IJIRCCE

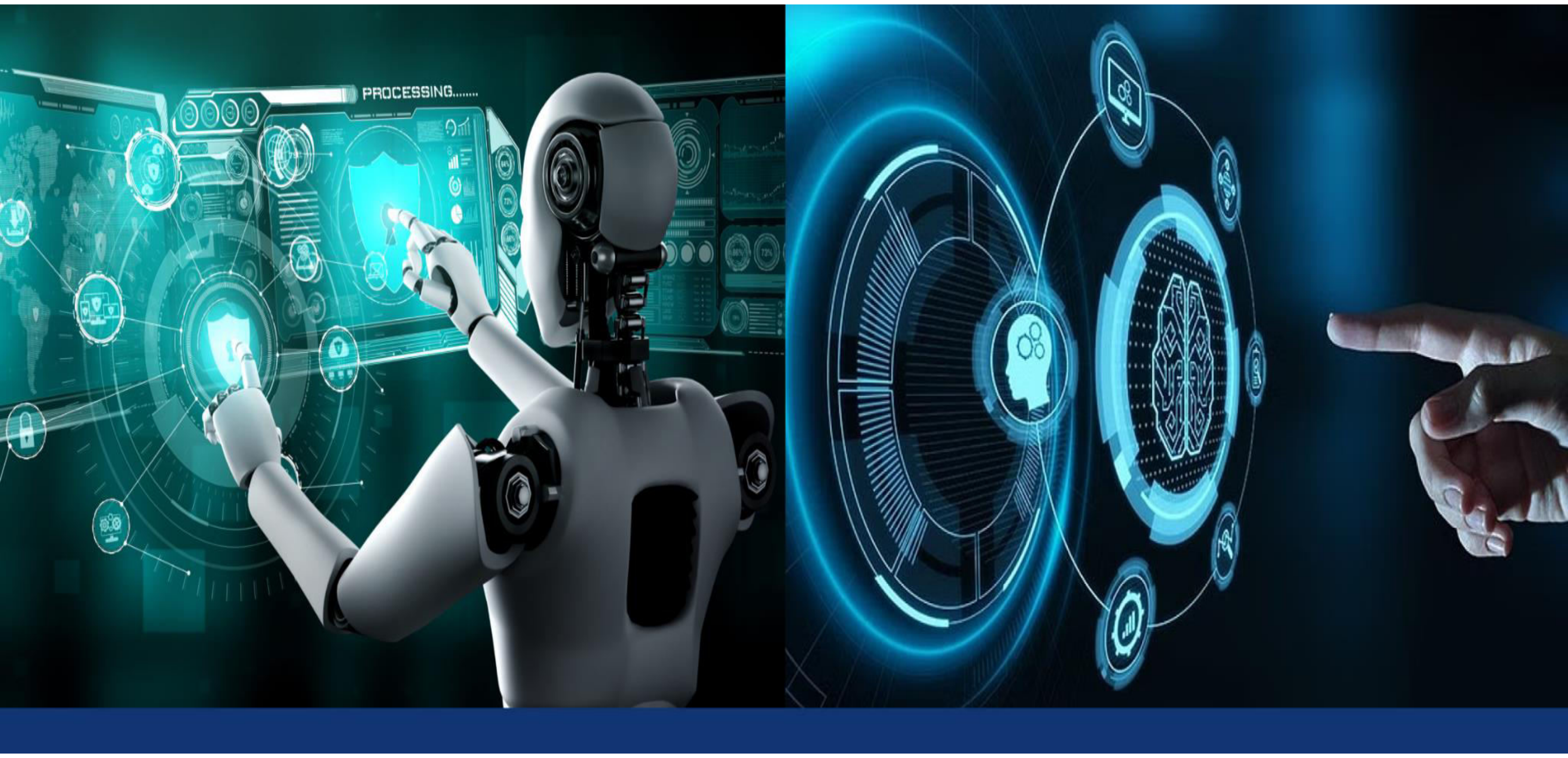
ISSN(O): 2320-9801

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 3, March 2025

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303133

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)

Data Security in Communication using Blockchain and Key Based Protocols

P.Sathiyapriya, R.Ashokkumar, E.Vishal, R.Suganesh

Assistant Professor, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

ABSTRACT: Satellite communication plays a vital role in developing the global communication networks. Satellite communication network has gained a lot of attention recently as a solution to mitigate the limitations of terrestrial networks because it has less stability and coverage. There are lot of inconvenience in it, such as low data processing capacity, storage and limited security. Illegal access became the challenging one. Data processing capacity is minimal, storage and security are constrained due to satellite physical limits in terms of available power and area, and the data may be exposed to alteration or contamination by intruders.

Since satellite communication has become more crucial in the development of global communication networks, there have been worries regarding its security. In this project, a satellite communication network is suggested the QKD protocol, which is based on authentication and privacy protection. An architecture comprising of both traditional through a wireless heterogeneous network has been built to achieve this goal. Registration, authentication, and revocation are used to carry out the communication. The satellite will send the acquired data to the terrestrial base station based device accesses control system.

I. INTRODUCTION

1. Overview

With the fast improvement of PC organisations and correspondence innovation, satellite correspondence has become one of the most significant and promising exchange information technologies, given its intrinsic advantages of long-range mobile communication, the cost-effectiveness of multicast and broadcast systems, wide coverage area, and high flexibility. Satellite correspondence frameworks empower the sending and getting of data around the world, offering web access, TV, phone, radio, and other regular citizen and military tasks, through the satellite organisation correspondence system.

1.2 Cloud Data:

Cloud data refers to the storage, management, and processing of data in a cloud computing environment, where data is stored on remote servers accessed over the internet instead of on local devices or on-premises servers. This approach offers numerous benefits, including scalability, accessibility, reliability, and cost-effectiveness. Firstly, cloud data storage provides scalability, allowing businesses to easily expand or shrink their storage capacity based on demand. With traditional on-premises solutions, scaling storage often involves purchasing and configuring additional hardware, which can be time-consuming and costly. In contrast, cloud storage services offer elastic scalability, enabling organizations to increase or decrease storage capacity instantly, based on their needs, without the need for upfront investment in infrastructure.

Additionally, cloud data is highly accessible from anywhere with an internet connection, enabling seamless collaboration and remote access to data for employees, partners, and customers. This accessibility fosters greater flexibility and productivity, as users can retrieve and share data from any location and device, facilitating remote work and collaboration across geographically dispersed teams.

- **Cloud Server Application**

Cloud server applications, a cornerstone of modern computing, revolutionize the way businesses deploy, manage, and scale their software solutions. These applications leverage cloud computing infrastructure to deliver services and functionality over the internet, eliminating the need for organizations to maintain physical servers on-premises. Cloud server applications offer numerous advantages, including flexibility, scalability, reliability, and cost-effectiveness.

Flexibility is a hallmark of cloud server applications, enabling developers to deploy and update software quickly and easily. With cloud-based platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), developers have access to a wide range of services and resources, such as virtual machines, databases, storage, and networking capabilities. This flexibility allows organizations to tailor their infrastructure to meet specific requirements and adapt to changing business needs without the constraints of physical hardware.

Scalability is another key benefit of cloud server applications. Cloud platforms offer auto-scaling capabilities that automatically adjust resources based on demand. This means applications can seamlessly handle fluctuations in traffic and workload without manual intervention. Whether experiencing sudden spikes in user activity or gradual growth over time, cloud server applications can scale up or down dynamically, ensuring optimal performance and user experience.

Reliability is inherent in cloud server applications due to the redundant infrastructure and built-in fault tolerance mechanisms of cloud platforms. Cloud providers operate data centers across multiple geographic regions, offering high availability and resilience to hardware failures, natural disasters, and other disruptions. Additionally, cloud services often include features like data replication, automated backups, and load balancing to enhance reliability and minimize downtime.

Cost-effectiveness is a compelling reason for businesses to adopt cloud server applications. By leveraging cloud infrastructure on a pay-as-you-go model, organizations can avoid hefty upfront investments in hardware and infrastructure maintenance. Instead, they pay only for the resources they consume, reducing operational costs and improving budget predictability. Moreover, cloud server applications enable efficient resource utilization, allowing organizations to scale infrastructure up or down as needed, further optimizing costs.

II. SYSTEM ANALYSIS

Existing System:

There are several advantages to satellite communication as well as risks. Security solutions that minimize security risks and safeguard satellite networks should be developed via cryptographic algorithms. The primary consideration in any communication is security, hence the conventional security methods include DES and AES (Advanced Encryption Standard). Elliptic curve cryptography (ECC), Triple-DES, Blowfish, hash algorithms, and (Data Encryption Standard), among others.

Limitations:

- The increasing computer power of attackers and eavesdroppers is making encryption techniques less dependable.
- Static authentication is used by many of these systems, which only authenticates the user or device once at the start of each session.
- Does not prevent man-in-the middle attack and fails to prevent a collision attack.

- Does not provide backward and forward secrecy as the attacker can gain the ID of the devices, then sniff other values from the current session to find the previous and future secret keys.
- Initialization and computation cost high.

Proposed System:
Geostationary earth orbit (GEO), medium earth orbit (MEO), and low
earth orbit (LEO) are the three kinds of orbits characterised by Cloud server height (LEO). GEO satellites, for example, remain stationary in relation to the earth&#39;s surface, resulting in less Doppler shift and a reduced likelihood of transmission outages than non-GEO satellites. GEO satellites operate at very high altitudes (35,786 km) and provide the most comprehensive coverage. GEO satellites are selected in our suggested protocol because to their low outage probability and vast coverage.

Expected Merits:
The expected merits of using Geostationary Earth Orbit (GEO) satellites in our proposed protocol include their ability to maintain a fixed position
relative to the Earth&#39;s surface, which results in minimal Doppler shift and a lower risk of transmission outages compared to satellites in other orbits. GEO satellites, operating at an altitude of 35,786 km, offer extensive coverage, making them ideal for wide-area communication and monitoring. This high altitude ensures that GEO satellites can cover large portions of the Earth&#39;s surface at once, providing reliable and consistent service with a lower probability of outages, which is a significant advantage over other orbit types like Medium Earth Orbit (MEO) and Low Earth Orbit (LEO) satellites.

III. SYSTEM REQUIREMENTS

Hardware Requirements:

- Processors: intel® core™ i5 processor 4300m at 2.60 ghz or 2.59 ghz (1 socket, 2 cores, 2 threads per core), 8 gb of dram
- Disk space: 320 gb
- Operating systems: windows® 10, macos*, and linux*

Software Requirements:

- Server side : python 3.7.4(64-bit) or (32-bit)
- Client side : html, css, bootstrap
- Ide : flask 1.1.1
- Back end : mysql 5.
- Server : wampserver 2i
- Os : windows 10 64 –bit or ubuntu 18.04 lts "bionic beaver

Software Description:
Python

Python is a general-purpose interpreted, interactive, object-oriented, and high- level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language.

Python is currently the most widely used multi-purpose, high-level programming language. Python allows programming in Object-Oriented and Procedural paradigms. Python programs generally are smaller than other programming languages like Java. Programmers have to type relatively less and indentation requirement of the language, makes them readable all the time. Python language is being used by almost all tech- giant companies like – Google, Amazon, Facebook, Instagram, Dropbox, Uber… etc. The biggest strength of Python is huge collection of standard libraries which can be used for the following:

- Machine Learning
- GUI Applications (like Kivy, Tkinter, PyQt etc.)
- Web frameworks like Django (used by YouTube, Instagram, Dropbox)
- Image processing (like OpenCV, Pillow)

- Web scraping (like Scrapy, BeautifulSoup, Selenium)
- Test frameworks
- Multimedia
- Scientific computing
- Text processing and many more.

Tensor Flow:

Tensor Flow is an end-to-end open-source platform for machine learning. It has a comprehensive, flexible ecosystem of tools, libraries, and community resources that lets researchers push the state- of-the-art in ML, and gives developers the ability to easily build and deploy ML-powered applications.

Tensor Flow provides a collection of workflows with intuitive, high-level APIs for both beginners and experts to create machine learning models in numerous languages. Developers have the option to deploy models on a number of platforms such as on servers, in the cloud devices, in browsers, and on many other JavaScript platforms. This enables developers to go from model building and training to deployment much more easily.

Keras:

Keras is a deep learning API written in Python, running on top of the machine learning platform TensorFlow. It was developed with a focus on enabling fast experimentation.

- Allows the same code to run on CPU or on GPU, seamlessly.
- User-friendly API which makes it easy to quickly prototype deep learning models.
- Built-in support for convolutional networks (for computer vision), recurrent networks (for sequence processing), and any combination of both.
- Supports arbitrary network architectures: multi-input or multi-output models, layer sharing, model sharing, etc. This means that Keras is appropriate for building essentially any deep learning model, from a memory network to a neural Turing machine.

Pandas:

pandas is a fast, powerful, flexible and easy to use open source data analysis and manipulation tool, built on top of the Python programming language. pandas is a Python package that provides fast, flexible, and expressive data structures designed to make working with "relational" or "labeled" data both easy and intuitive. It aims to be the fundamental high-level building block for doing practical, real world data analysis in Python.Pandas is mainly used for data analysis and associated manipulation of tabular data in Data frames. Pandas allows importing data from various file formats such as comma-separated values, JSON,Parquet, SQL database tables or queries, and Microsoft Excel. Pandas allows various data manipulation operations such as merging, reshaping, selecting, as well as data cleaning, and data wrangling features. The development of pandas introduced into Python many comparable features of working with Data frames that were established in the R programming language.

NumPy:

NumPy, which stands for Numerical Python, is a library consisting of multidimensional array objects and a collection of routines for processing those arrays.

Using NumPy, mathematical and logical operations on arrays can be performed. NumPy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

Matplotlib:

Matplotlib is a comprehensive library for creating static, animated, and interactive visualizations in Python. Matplotlib makes easy things easy and hard things possible. Matplotlib is a plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK. lay a prominent role in monitoring and controlling external devices.

IV. LITRETURE SURVEY

Title : Secure Federated Learning Across Heterogeneous Cloud and High- Performance Computing Resources - A Case Study on Federated Fine-tuning of LLaMA 2

Author : Zilinghan Li; Shilan He

Concept : Federated learning enables multiple data owners to collaboratively train robust machine learning models without transferring large or sensitive local datasets by only sharing the parameters of the locally trained models. In this paper, we elaborate on the design of our Advanced Privacy-Preserving Federated Learning (APPFL) framework, which streamlines end-to-end secure and reliable federated learning experiments across cloud computing facilities and high-performance computing resources by leveraging Globus Compute, a distributed function as a service platform, and Amazon Web Services. We further demonstrate the use case of APPFL in finetuning a LLaMA 2 7B model using several cloud resources and supercomputers.

Limitation : Federated learning offers significant advantages by allowing multiple data owners to collaboratively train machine learning models while maintaining data privacy, as only the parameters of the locally trained models are shared rather than the full datasets. However, one of the primary limitations of federated learning is the complexity and scalability of managing and coordinating the communication and computations across different cloud computing facilities and high- performance computing resources. Ensuring the secure and efficient transfer of parameters, as well as the seamless integration of various cloud platforms and services, poses technical challenges that must be addressed for successful deployment of federated learning models at scale.

References : Li, Zilinghan, et al. "Secure Federated Learning Across Heterogeneous Cloud and High-Performance Computing Resources-A Case Study on Federated Fine-tuning of LLaMA 2." *Computing in Science & Engineering* (2024).

Title : COCAME: A Computational Offloading in Cloud Assisted Mobile Environments Structure to Enhance Performance and Energy

Author : R. Aishwarya; G. Mathivanan

Concept : The widespread popularity and affordability of smart mobile devices provide users with a fantastic interface. However, inherent hardware limitations, encompassing storage, CPU, and power consumption, pose challenges. The utilization of various services significantly drains the limited battery capacity of these devices. Complex mobile applications, constrained by restricted resources, suffer from diminished performance and power capacity, making battery enhancement a formidable challenge. Leveraging cutting-edge technologies can potentially boost device sales by 5% annually. It is crucial for infrastructure and application developers to address energy and performance challenges. In the realm of Mobile Cloud Computing, computational offloading plays a pivotal role in enabling high-computational apps on smartphones, potentially improving power efficiency and performance. Despite numerous advancements in computational offloading structures and methodologies, existing frameworks struggle to accurately assess the added burden of relocating application components during runtime. To enhance both performance and energy efficiency, the proposed COCAME approach focuses on strategically transferring minimal instances of computationally intensive application components at runtime.

Limitation : Smart mobile devices offer excellent user interfaces due to their popularity and affordability, but they face significant hardware limitations, such as storage, CPU power, and battery capacity. These limitations are further compounded when users run multiple services, which quickly drain the battery. Complex mobile applications, restricted by these resources, often experience poor performance and limited battery life.

References : Aishwarya, R., and G. Mathivanan. "COCAME: A Computational Offloading in Cloud Assisted Mobile Environments Structure to Enhance Performance and Energy." *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2024.

Title : An Efficient Privacy-Preserving Ranked Multi-Keyword Retrieval for Multiple Data Owners in Outsourced Cloud

Author : Dong Li; Jiahui Wu

Concept : With the widespread use of cloud storage technology by individuals and organizations, data providers usually send their data to cloud for storage to reduce memory pressure, and allow the users to retrieve these data, which has become the trend of rapid data retrieval. To guarantee the data confidentiality, several research works have been developed on encrypted cloud data for ranked multi- keyword retrieval. Nevertheless, most of these schemes are disabled since they cannot resist keyword guessing attacks. Moreover, the ranked top- K search results obtained by the subscriber from the encrypted cloud data are inaccurate. To overcome these drawbacks, we design a novel and efficient privacy-preserving ranked multi- keyword retrieval scheme (named as PRMKR) in this paper. With PRMKR, the data and the inverted indexes which belong to the data provider can be securely transferred to the cloud server. In addition, a registered subscriber can request accurate retrieval services without compromising his/her trapdoor information to the cloud server. Specifically, we design an encryption searchable plugin-in server and lower dimensional inverted indexesvector for data owners, which can further guarantee data confidentiality of the data owner and improve search efficiency, respectively. Our rigorous security proof demonstrates that PRMKR can withstand keyword guessing attacks. Finally, experimental evaluations confirm that PRMKR has decent computational and communication efficiency.

Limitation : Despite the advancements in cloud storage and the development of encrypted cloud data retrieval schemes, there are still some limitations. Many existing schemes are vulnerable to keyword guessing attacks, which can compromise data security. Furthermore, the search results for ranked top-K queries on encrypted cloud data are often inaccurate, affecting the reliability of the retrieval process. These challenges make it difficult to ensure both the confidentiality of the data and the accuracy of search results. While the PRMKR scheme addresses these issues by securely transferring data and inverted indexes to the cloud and providing accurate retrieval without exposing sensitive information, it still faces the challenges inherent in maintaining high search efficiency and security under evolving attack strategies.

References : Li, Dong, et al. "An Efficient Privacy-Preserving Ranked Multi- Keyword Retrieval for Multiple Data Owners in Outsourced Cloud." IEEE Transactions on Services Computing (2023).

Title : Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network

Author : Adnan Shahid Khan

Concept : A lightweight multifactor mutual authentication protocol for Cell- Free communication using ECC-based Deffie Hellman (ECDH). This scheme utilizes timestamping, one-way hash function, Blind-Fold Challenge scheme with public key infrastructure. The proposed cryptosystem integrates with blockchain technology using proof of staked (POS) as a consensus mechanism to ensure integrity, non- repudiation and traceability. The proposed scheme can enforce the mitigation of several major security attacks on communication links such as spoofing attacks, eavesdropping, user location privacy issues, replay attacks, denial of service attacks, and man-in-the-middle (MITM) attacks, which is one of the significant features of the scheme. Furthermore, this scheme contributes to reducing authentication, communication, and computational overheads with an average of 32.8%, 52.4% and 53.2% better performance respectively as compared baseline authentication protocols.

Limitation : Despite its promising features, the lightweight multifactor mutual authentication protocol for Cell-Free communication using ECC- based Diffie-Hellman (ECDH) has some limitations. One potential drawback is the reliance on public key infrastructure (PKI), which can introduce complexities in key management and certificate handling, especially in large-scale deployments. Additionally, while the integration of blockchain technology using proof of stake (PoS) enhances security through consensus mechanisms, it may also result in increased latency due to the need for frequent block validation and mining processes. Furthermore, although the protocol significantly reduces authentication, communication, and computational overheads, its performance may still be impacted in environments with limited resources or in scenarios where high-frequency transactions are involved. Finally, while the scheme mitigates several security threats, it does not eliminate all possible attack vectors, particularly those related to advanced quantum computing threats in the long term.

References : Khan, Adnan Shahid, et al. "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network." *IEEE Access* 11 (2023): 20524-20541.

Title : Securing Smart Grid Data With Blockchain and Wireless Sensor Networks: A Collaborative Approach

Author : Saleh Almasabi

Concept : The rapid advancement of grid modernization and the proliferation of smart grids have engendered a critical need for cyber-physical security. Recent cyber-attacks targeting grid infrastructure, notably leading to substantial blackouts in Ukraine, underscore the vulnerabilities and potentially catastrophic consequences of such incursions. These attacks, whether stemming from cyber threats such as Denial of Service (DOS), False Data Injection Attacks (FDIA), or complex cyber-physical manipulations, emphasize the imperative of robust cybersecurity protocols in smart grid operations. This research investigates a pivotal approach to fortify and safeguard smart grid systems by integrating blockchain technology with wireless sensor nodes. By leveraging a Proof of Authority (PoA) Ethereum Blockchain framework, the study delves into the transformative capabilities of Blockchain within Supervisory Control and Data Acquisition (SCADA) networks. Specifically, it examines configurations across IEEE 14-bus, 30-bus, and 118-bus topologies.

Limitation	:	While the integration of blockchain technology with smart grids offers promising advancements in cybersecurity, there are several limitations that need to be addressed. The implementation of blockchain, especially with a Proof of Authority (PoA) framework, can introduce latency due to the processing and validation of transactions, potentially affecting the real-time performance of smart grids. Additionally, the scalability of blockchain in large-scale grid systems, such as those with 118-bus topologies, poses challenges due to the computational power required and the network overhead. Another limitation is the complexity of integrating blockchain with existing SCADA systems, which may involve significant upgrades to infrastructure and protocols. Furthermore, while blockchain can enhance security, it is not immune to all types of cyber-attacks, and the need for continuous updates and improvements in cybersecurity measures remains crucial to safeguard smart grids from evolving threats.
References	:	Almasabi, Saleh, et al. "Securing smart grid data with blockchain and wireless sensor networks: A collaborative approach." IEEE Access (2024).

V. CONCLUSION

Blockchain provides a decentralized, immutable ledger that ensures data integrity, transparency, and tamper-proof records, making it ideal for securing communication channels. Combined with key-based protocols such as Public Key Infrastructure (PKI), which enable robust encryption and authentication mechanisms, this dual approach addresses common vulnerabilities in traditional communication systems, including data interception, unauthorized access, and data manipulation.

The adoption of this hybrid security model ensures that communication networks are resilientto attacks like man-in-the-middle, replay, and phishing. Furthermore, blockchain's inherent transparency and traceability capabilities make it easier to track and audit communication events, enhancing accountability.

While challenges like scalability, energy consumption, and integration complexities remain, the potential benefits—such as higher trust, privacy, and data sovereignty—make blockchain and key-based protocols a promising solution for securing modern communication infrastructures. Future advancements in these technologies will likely mitigate current limitations, making them even more effective in protecting sensitive data in various sectors.

REFERENCES

1. S. Liu, Z. Gao, Y. Wu, D. W. K. Ng, X. Gao, K.-K. Wong, et al., "LEO satellite constellations for 5G and beyond: How will they reshape vertical domains?", *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 30-36, Jul. 2021.
2. M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities", *IEEE Netw.*, vol. 35, no. 2, pp. 244-251, Mar. 2021.
3. B. Al Homssi, A. Al-Hourani, K. Wang, P. Conder, S. Kandeepan, J. Choi, et al., "Next generation mega satellite networks for access equality: Opportunities challenges and performance", *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 18-24, Apr. 2022.
4. X. Lin, S. Cioni, G. Charbit, N. Chuberre, S. Hellsten and J. Boutillon, "On the path to 6G: Embracing the next wave of low Earth orbit satellite access", *IEEE Commun. Mag.*, vol. 59, no. 12, pp. 36-42, Dec. 2021.
5. X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6G: Architectures applications and challenges", *IEEE Internet Things J.*, vol. 9, no. 1, pp. 437-461, Jan. 2022.
6. M. M. Azari, S. Solanki, S. Chatzinotas, O. Kodheli, H. Sallouha, A. Colpaert, et al., "Evolution of non-terrestrial networks from 5G to 6G: A survey", *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2633-2672, 4th Quart. 2022.
7. X. Hou, J. Wang, Z. Fang, Y. Ren, K.-C. Chen and L. Hanzo, "Edge intelligence for mission-critical 6G services in space-air-ground integrated networks", *IEEE Netw.*, vol. 36, no. 2, pp. 181-189, Mar. 2022.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com