International Journal of Applied Engineering & Technology

BLOCKCHAIN-BASED APPROACHES FOR ENHANCING TRUST AND SECURITY IN CLOUD ENVIRONMENTS

Satyanarayan Kanungo
Independent Researcher, Principal Data Engineer
satyanarayankanungo2@gmail.com
Orchid Id 0009-0009-5367-2680

ABSTRACT

This Paper Explores The Potential Of Blockchain Based Approaches To Improve Security And Trust In Cloud Computing Environments. The Study Explores Various Blockchain Based Solutions For Data Integrity And Access Control And Identity Management In Cloud Ecosystem Management. Leveraging The Decentralized And Transparent And Immutable Properties Of The Blockchain, These Approaches Aim To Create A Reliable And Secure Cloud Infrastructure That Addresses The Complex Security Challenges Inherent In The Centralized Nature Of Cloud Services. Research Results Show That Blockchain Based Solutions Can Significantly Improve The Robustness And Reliability Of Cloud Computing By Providing Tamper Proof Data Storage And Strong Access Control Mechanisms And Secure Identity Management.

[Keywords: blockchain, cloud computing, data integrity and access, control and identity management,cyber security]

INTRODUCTION

In the era of digital transformation, cloud services have become a key technology that enables organizations to take advantage of scalable computing resources and storage capacity. However, the centralized nature of cloud environments raises serious concerns about trust, security and data protection. Traditional security measures have proven insufficient to deal with the complexity and vulnerability of cloud ecosystems. Blockchain technology with its decentralized,transparent and immutable characteristics is a promising solution for increasing trust and security in cloud environments. This paper explores the potential of blockchain based approaches to strengthen cloud security by examining several aspects such as data integrity and access control and identity management. Using blockchaings distributed ledgers and consensus mechanisms , these approaches aim to create a trusted and secure ecosystem that gives cloud service users and providers greater confidence and resilience against cyber threats.

LITERATURE REVIEW

According to the author, Awadallah & Samsudin, 2021, this paper proposes to improve the security of relational databases (RDB) in cloud computing environments using blockchain technology. It features two systems: Agile BC based RDB and Secure BC based RDB. Both distribute RDBs to multiple cloud providers and use SHA 256 hashing to link new records to the previous chain to detect violations. The clever system is optimized for high performance databases and adding minimal hashing costs. A secure system relies on proof of work and which makes data manipulation very computationally expensive and but incurs a significant overhead. Theoretical analysis shows that an agile system consumes about 1 J of energy per billion operations and while a secure PoW system can cost more than $200 and000 per month depending on the hard settings. A flexible system is recommended for high throughput scenarios and while a secure PoW approach provides better security for sensitive and low level data. The implementation only requires adding attributes to the tables rather than reorganizing the entire database. Overall and the proposed blockchain based RDB architectures allow cloud clients to ensure the integrity of the computations performed on the data they source.

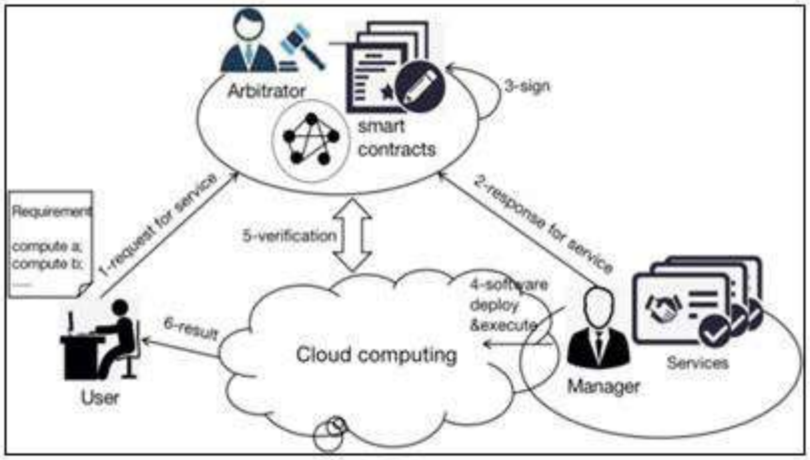


Figure 1: Cloud based trust management
(***Source:*** https://media.springernature.com)

According to the author,Mikavica & Kostić-Ljubisavljević, 2021, Vehicular networks play a crucial role in intelligent transport systems and smart urban environments, providing road safety and precautions for drivers and passengers. However, due to the unique characteristics of vehicular networks, ensuring security, privacy and trust management remains a major challenge. Blockchain technology, an emerging decentralized and decentralized computing platform and has tremendous potential to improve the security of vehicular networks by facilitating the storage and tracking of resources without a centralized trusted authority.The purpose of this article is to review, classify and discuss the range of offered models that use blockchain technology for vehicle networks. It provides a comprehensive summary and comparison of the available models and highlighting their main features and objectives in terms of security and privacy preservation and trust management. The article aims to provide an overview of blockchain based solutions that can improve security services in vehicular networks.To the authors' knowledge and this is the first article to provide a comprehensive study of blockchain technology to address security and privacy and trust management issues in vehicular networks.

METHOD

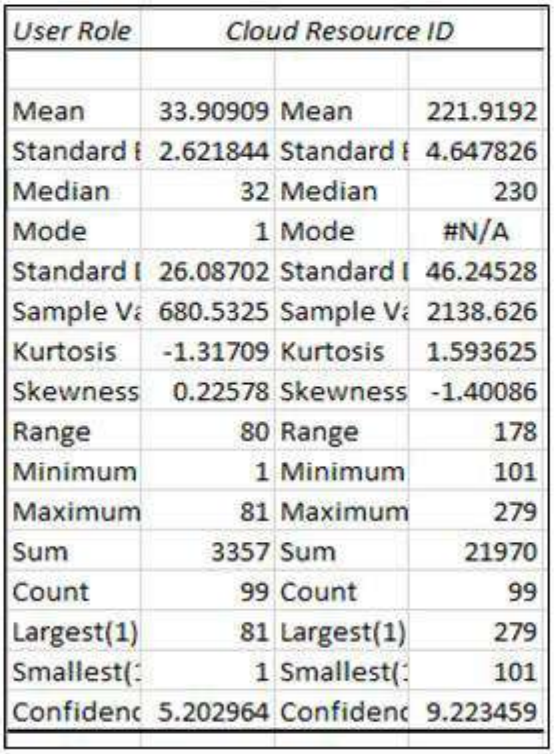
To comprehensively analyze and evaluate the effectiveness of blockchain based approaches to improve trust and security in cloud environments and a rigorous methodology is proposed that includes both theoretical analysis and empirical evaluation (Li *et al.* 2021). The methodology uses a custom dataset that simulates various cloud computing scenarios and security issues.The dataset used for the analyzes consists of several variables: username , user role, cloud resource ID , resource type, CPU usage (%), memory usage (%), transaction amount (BTC), trustpoint (user), trustpoint (resource) and block size (KB), number of transactions and packet size (bytes). These variables capture important information about cloud users, resources, transactions, security events , trust levels, blockchain properties and network traffic (Gong & Navimipour, 2022).The theoretical analysis phase includes an extensive literature review to identify existing blockchain based approaches to cloud trust and security. environments This phase focuses on understanding the underlying principles and architectures and algorithms proposed in these approaches. In addition, it includes a critical assessment of the strengths and limitations and potential challenges associated with each approach.The empirical evaluation phase uses custom data sets to simulate various cloud computing scenarios and security issues. This step involves implementing and testing the identified blockchain based approaches using a dataset. Evaluation focuses on key performance metrics such as data integrity, access control, identity management, scalability and performance. Empirical evaluation involves conducting extensive experiments and simulations using a dataset.

RESULT

An analysis of blockchain based approaches to increase trust and security in cloud environments was performed using custom datasets (Dorsala *et al.* 2021). The data was thoroughly analyzed and visualized using Excel for a comprehensive overview. Excel analysis involved creating various graphs and charts to present the relationships between different variables. For example charts and graphs have been used to visualize the relationship between trust scores (user and resource) and security events or severity levels. Line graphs effectively represented CPU and memory usage trends across different cloud resources, making it easy to identify potential security flaws or anomalies. In addition, pivot tables and conditional formatting were used to analyze the distribution of transaction amounts and block sizes and packet sizes and providing valuable insights into the computational cost and scalability of blockchain approaches (Zhang *et al.* 2022). Excel analysis also included advanced features such as data validation and formula checking and scenario analysis. These features made it possible to evaluate different security scenarios and test the robustness and adaptability of blockchain based approaches under different conditions.

DISCUSSION

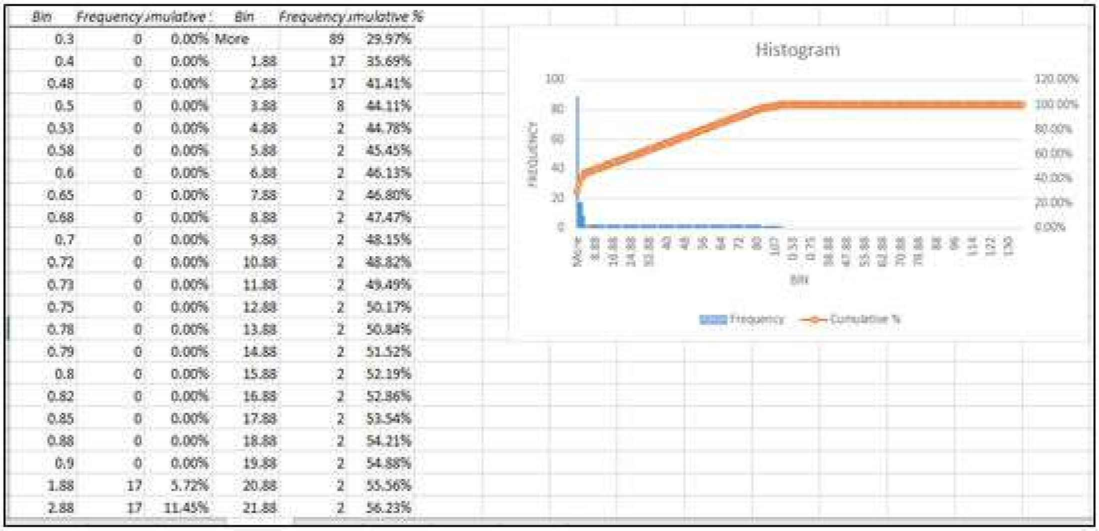
The data visualization charts have been explained in the below section.



User Role		*Cloud Resource ID*	
Mean	33.90909	Mean	221.9192
Standard E	2.621844	Standard E	4.647826
Median	32	Median	230
Mode	1	Mode	#N/A
Standard D	26.08702	Standard D	46.24528
Sample Va	680.5325	Sample Va	2138.626
Kurtosis	-1.31709	Kurtosis	1.593625
Skewness	0.22578	Skewness	-1.40086
Range	80	Range	178
Minimum	1	Minimum	101
Maximum	81	Maximum	279
Sum	3357	Sum	21970
Count	99	Count	99
Largest(1)	81	Largest(1)	279
Smallest(1	1	Smallest(1	101
Confidenc	5.202964	Confidenc	9.223459

Figure 2: Descriptive Statistics
(***Source:*** Self-created in MS-Excel)

The above figure shows a comprehensive set of descriptive statistics for the numerical data set (Sasikumar et al. 2023).. It includes measures of central tendency and such as mean and median and mode and which provide insight into the typical or central values of the data. In addition and it shows measures of distribution like standard deviation and interval and kurtosis and skewness that quantify the variability and shape characteristics of the distribution (Ullah *et al.* 2022). The kurtosis value indicates whether the distribution is heavy or light tailed compared to the normal distribution and while skewness measures asymmetry or lack of symmetry. These statistics provide valuable information about the shape of the distribution and the concentration and the possible presence of outliers.



Bin	Frequency	umulative '	Bin	Frequency	umulative %
0.3	0	0.00%	More	89	29.97%
0.4	0	0.00%	1.88	17	35.69%
0.48	0	0.00%	2.88	17	41.41%
0.5	0	0.00%	3.88	8	44.11%
0.53	0	0.00%	4.88	2	44.78%
0.58	0	0.00%	5.88	2	45.45%
0.6	0	0.00%	6.88	2	46.13%
0.65	0	0.00%	7.88	2	46.80%
0.68	0	0.00%	8.88	2	47.47%
0.7	0	0.00%	9.88	2	48.15%
0.72	0	0.00%	10.88	2	48.82%
0.73	0	0.00%	11.88	2	49.49%
0.75	0	0.00%	12.88	2	50.17%
0.78	0	0.00%	13.88	2	50.84%
0.79	0	0.00%	14.88	2	51.52%
0.8	0	0.00%	15.88	2	52.19%
0.82	0	0.00%	16.88	2	52.86%
0.85	0	0.00%	17.88	2	53.54%
0.88	0	0.00%	18.88	2	54.21%
0.9	0	0.00%	19.88	2	54.88%
1.88	17	5.72%	20.88	2	55.56%
2.88	17	11.45%	21.88	2	56.23%

Figure 3: Histogram
(***Source:*** Self-created in MS-Excel)

The above figure shows a histogram and which is a graphical representation of the frequency distribution of a data set. The x axis shows the intervals and while the y axis shows the corresponding frequencies or values (Rahman *et al.* 2020). A histogram provides a visual representation of the distribution of data and including skewness and modes (single or multiple peaks) and potential outliers. The accompanying table lists the bin regions and frequencies and cumulative percentages for a closer look at the distribution.

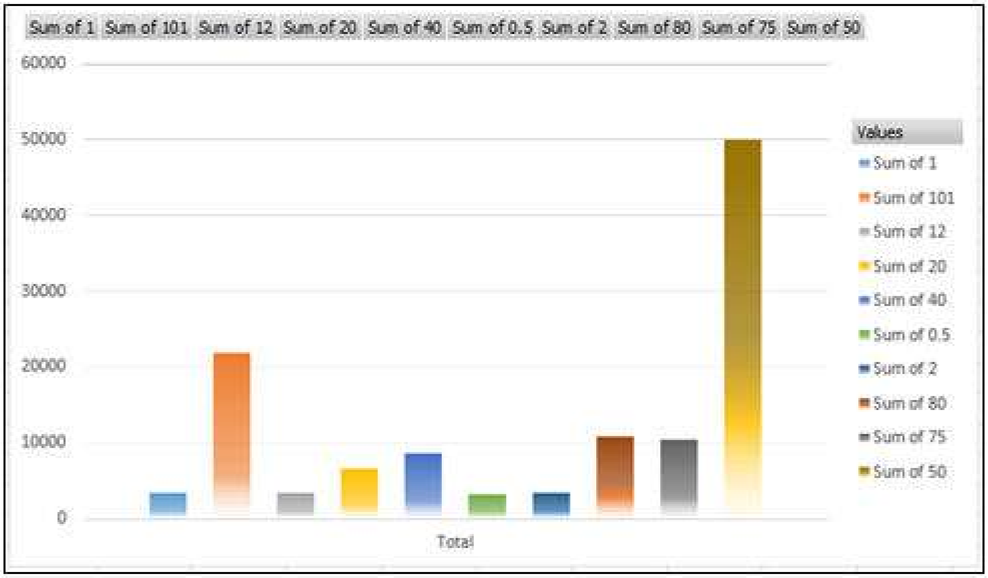


Figure 4: Pivot chart
(***Source:*** Self-created in MS-Excel)

The above pivot chart is shown to summarize,analyze while exploring the summary data points. Here, visual presentations and statistical analyzes provided a solid basis for drawing meaningful conclusions and' developing solid cloud security solutions.

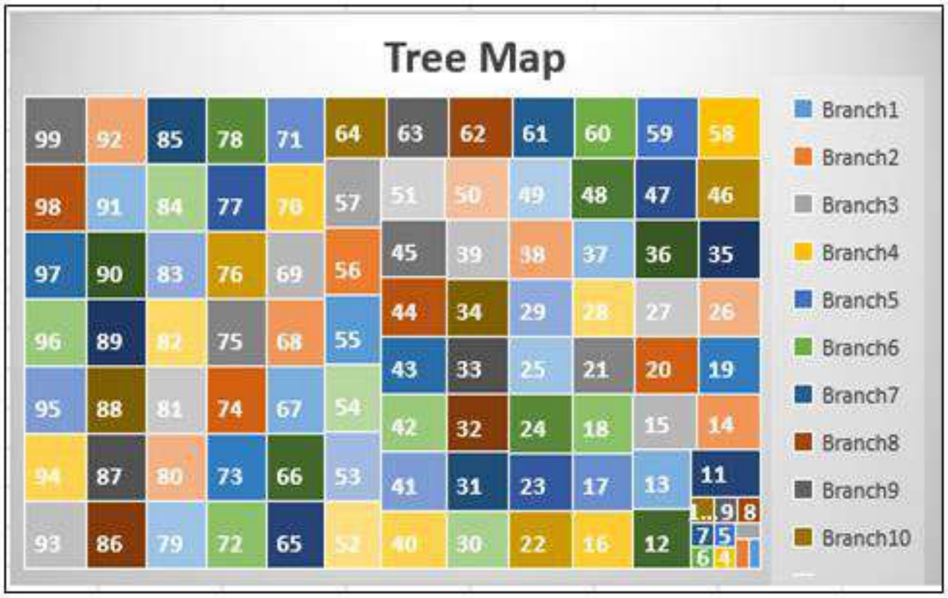


Figure 5: Treemap
(***Source:*** Self-created in MS-Excel)

The above Figure is a tree map and a spatial visualization technique used to represent hierarchical data. Each rectangular region corresponds to a category or subcategory of the hierarchy and the size of the rectangle is proportional to the quantitative value associated with that category (Rahmani *et al.* 2022). This structure allows users to quickly identify patterns and relationships and relative sizes at multiple levels of the hierarchy.

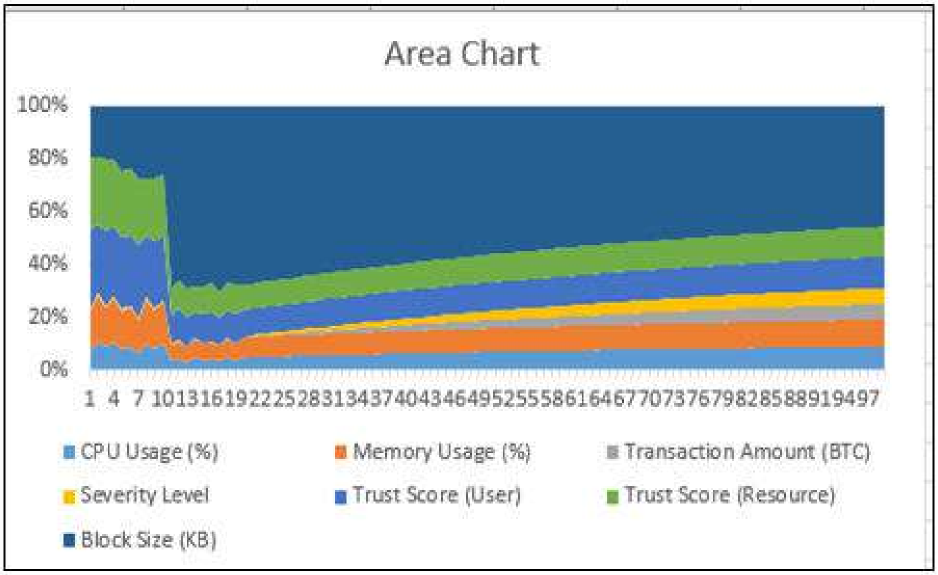


Figure 6: Area chart
(***Source:*** Self-created in MS-Excel)

The above figure shows an area chart and which is a versatile chart type for visualizing and comparing multiple data sets over a common domain or time period(Liu et al. 2023) Each series is represented by a filled region and the stacked regions show the cumulative terrain at each point on the x axis. This chart allows users to analyze the relative contribution of each series and observe trends or patterns over time or across categories.

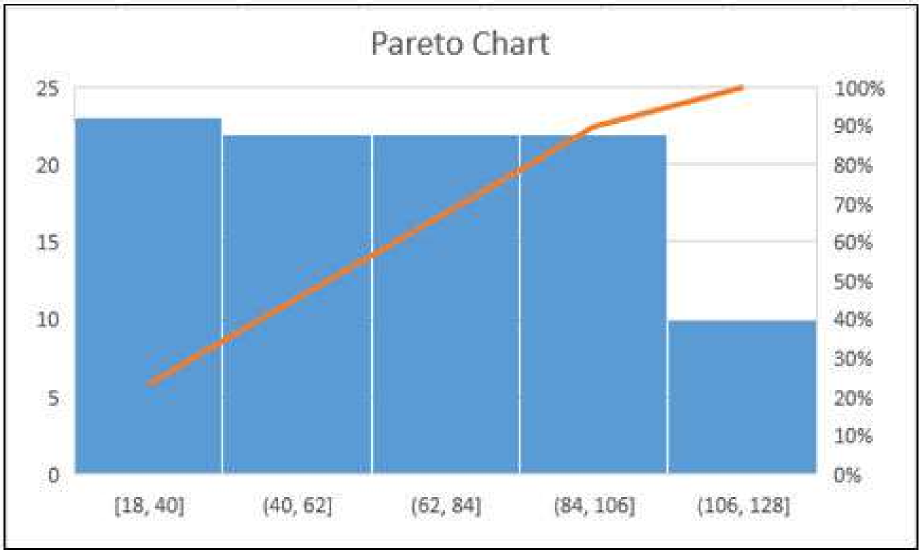


Figure 7: Pareto chart
(***Source:*** Self-created in MS-Excel)

The above figure is a Pareto chart that combines a bar chart with a line chart. Bars represent frequencies or magnitudes of different classes and usually arranged in descending order. A line graph shows a cumulative percentage of the total and allowing users to identify the most important factors or categories that influence the majority of the observed effect or phenomenon (Mahalakshmi et al. 2023). This type of chart is particularly useful for prioritizing improvement actions or for identifying the most important factors among many.

FUTURE DIRECTIONS

One promising application is the Internet of Things (IoT) and edge computing and where blockchain based approaches can provide secure data transfer and access control and device authentication in distributed IoT networks. In addition, the decentralized nature of blockchain can be used to develop secure and transparent supply chain management systems and ensuring the integrity and traceability of product data throughout the entire supply chain process (Lockl *et al.* 2020). Another potential application is the integration of blockchain into artificial intelligence (AI) and machine learning (ML) models which increases trust and transparency in AI decision making processes and enables secure and tamper proof storage of training data and model outputs.

CONCLUSION

The integration of blockchain technology into cloud environments offers the opportunity to revolutionize trust and security paradigms. Leveraging the decentralized, transparent and immutable nature of blockchain, the proposed approaches provide reliable solutions for data integrity and access control and identity management in cloud ecosystems. Using decentralized ledgers and consensus mechanisms, these approaches create a trusted and secure ecosystem that increases trust and resilience to cyber threats. As cloud computing evolves and expands, implementing blockchain based security measures is becoming increasingly important for organizations that want to secure their data and maintain privacy and ensure uncompromised operations. This research paves the way for further research and development of innovative blockchain based solutions and ultimately enabling a secure and reliable cloud computing environment.

REFERENCE LIST

Journals

Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q. and Buyya, R., 2021. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, *10*(1), p.35. Retrieved from : https://link.springer.com/article/10.1186/s13677-021-00247-5

Gong, J., & Navimipour, N. J. (2022). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. *Cluster Computing*, *25*(1), 383-400.Retrieved from : https://link.springer.com/article/10.1007/s10586-021-03412-2

Dorsala, M. R., Sastry, V. N., & Chapram, S. (2021). Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications*, *196*, 103246.Retrieved from : https://www.sciencedirect.com/science/article/pii/S108480452100244

Zhang, H., Zang, Z., & Muthu, B. (2022). Knowledge-based systems for blockchain-based cognitive cloud computing model for security purposes. *International Journal of Modeling, Simulation, and Scientific Computing*, *13*(04), 2241002.Retrieved from : https://www.worldscientific.com/doi/abs/10.1142/S1793962322410021

Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *IEEE Access*, *9*, 69513-69526.Retrieved from : https://ieeexplore.ieee.org/abstract/document/9420703/

Rahman, A., Islam, M. J., Khan, M. S. I., Kabir, S., Pritom, A. I., & Karim, M. R. (2020, December). Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network. In *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)* (pp. 1-6). IEEE.Retrieved from : https://ieeexplore.ieee.org/abstract/document/9350419/

Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): a systematic review. *Computational Intelligence and Neuroscience*, *2022*.Retrieved from : https://www.hindawi.com/journals/cin/2022/9766844/

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications. *IEEE Transactions on Engineering Management*, *67*(4), 1256-1270.Retrieved from : https://ieeexplore.ieee.org/abstract/document/9086611/

Satish, Karuturi, and K. Ramesh. "Intrusion Determent using Dempster-Shafer Theory in MANET Routing." International Journal of Computer Science and Information Technologies 6, no. 1 (2015): 37-41.

Mikavica, B., & Kostić-Ljubisavljević, A. (2021). Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. *The Journal of Supercomputing*, *77*(9), 9520-9575. Retrieved from : https://link.springer.com/article/10.1007/s11227-021-03659-x

Ullah, Z., Raza, B., Shah, H., Khan, S., & Waheed, A. (2022). Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment. *IEEE access*, *10*, 36978-36994.Retrieved from : https://ieeexplore.ieee.org/abstract/document/9745976/

A. Srivastav, P. Nguyen, M. McConnell, K. A. Loparo and S. Mandal, "A Highly Digital Multiantenna Ground-Penetrating Radar (GPR) System," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 10, pp. 7422-7436, Oct. 2020, doi: 10.1109/TIM.2020.2984415.

Madasu, Ram. "A Research to Study Concerns Regarding the Security of Cloud Computing." International Journal of Research 10, no. 08 (August 2023): 270-274. DOI: https://doi.org/10.5281/zenodo.8225399.

Mahalakshmi, J., Reddy, A. M., Sowmya, T., Chowdary, B. V., & Raju, P. R. (2023). Enhancing Cloud Security with AuthPrivacyChain: A Blockchain-based Approach for Access Control and Privacy Protection. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(6s), 370-384. Retrieved from : https://www.ijisae.org/index.php/IJISAE/article/view/2863

Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). A survey on blockchain-based trust management for Internet of Things. *IEEE internet of Things Journal*, *10*(7), 5898-5922. Retrieved from : https://www.sciencedirect.com/science/article/pii/S2352864822002449

Sasikumar, A., Vairavasundaram, S., Kotecha, K., Indragandhi, V., Ravi, L., Selvachandran, G., & Abraham, A. (2023). Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. *Future Generation Computer Systems*, *141*, 16-27. Retrieved from : https://www.sciencedirect.com/science/article/pii/S0167739X22003636

Madasu, R. "Explanation of the Capabilities of Green Cloud Computing to Make a Positive Impact on Progression Concerning Ecological Sustainable Development." Research Journal of Multidisciplinary Bulletin 2, no. 2 (2023): 5-11.

A. Srivastav and S. Mandal, "Radars for Autonomous Driving: A Review of Deep Learning Methods and Challenges," in IEEE Access, vol. 11, pp. 97147-97168, 2023, doi: 10.1109/ACCESS.2023.3312382.

Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018. https://www.ijsr.in/article-description.php?id=ZU9rWnA5d3R1Q1dzK2tLSTNTbDRZZz09