JOURNAL OF ALGORITHM ASYNCHRONOUS (ALGRASY)
E-ISSN 3025-5015
Vol 2 issue 1 2024
page. 1-14

Decentralized Orchestration of Edge Computing Resources through Blockchain-based Smart Contracts: An Unexplored Paradigm for Efficient Resource Management in IoT Environments

Eero Virtanen[1], Eero Kallio[2], Maija Järvinen[3]
Faculty of Computer Science and Engineering, Helsinki Technology Institute, Finland

*Correspondence author: eero.virtanen976@hti.fi

INFO
Submitted: 12-01-2024,
Revised: 10-01-2024,
Accepted: 24-01-2024

ABSTRACT
This research investigates the decentralized orchestration of edge computing resources through blockchain-based smart contracts as an unexplored paradigm for efficient resource management in Internet of Things (IoT) environments. The study examines the influence of industry sectors, years of experience with edge computing, and knowledge about blockchain on individuals' perceptions of IoT security importance. Findings reveal significant variations across industry sectors, highlighting the need for sector-specific security strategies. Moreover, years of experience with edge computing and knowledge about blockchain emerge as crucial factors influencing security priorities. The study offers practical recommendations for tailoring IoT security approaches, investing in employee expertise, and exploring blockchain integration. These insights contribute to the dynamic field of IoT security and its implications for diverse industries.

Keywords**:** *IoT Security, Edge Computing, Blockchain-Based Smart Contracts*

INTRODUCTION

The revolutionary impact that the Internet of Things (IoT) posed was on our optics to the technology altogether that encloses it (Khan et al., 2023). Dealing with data en masse produced by IoT devices whose number is growing exponentially is for sure a Herculean task (Priya, 2023). In many contexts, this has affected the efficient working of effective traditional architectures that are based on the cloud through poor latency and insufficient bandwidth to deal with the high volume of incoming data traffic (IEEE Internet of Things Journal, 2023). Thus, edge computing comes in as a good solution whereby the data processing is achieved on nearby sources contributing towards reducing latency and saving bandwidth (Tsamis, 2023). However, many security, scalability, and coordination challenges have made it no easy task to realize effective developments and deployments of the edge computing resources (IEEE Network, 2022). Blockchain, a practically modern socially secure ledger system for SSH (Khan et al., 2023; IEEE Network, 2022). The two features of transaction transparency, that is the applicability to the security and data integration needs being easy to implement with another business software it is resource management-friendly in exchange systems (IEEE Internet of Things Journal, 2023; Tsamis, 2023).

Thanks to smart contracts, applying which predetermined conditions are verified, blockchain technology may implement a contract independently. The ability to perform such operations automatically thus lends for the simplification of orchestration of tasks in using edge computing resources thereby enhancing effectiveness in resource management (Patterson, 2023). Indeed, despite huge impact that can be derived from fusing both - edge computing and blockchain - it is the uncharted territory (Du et al., 2023). Few works appeared in recent years that are devoted to outlining merits of this fusion. For example, blockchain-based energy management smart contracts have shown the ability to automatically carry out transactions on the smart grids in manners that improve the efficiency of the urban energy system in the smart cities (Uchani Gutierrez & Xu, 2022). Another practical area where mobile communications have found use in blockchain is in facilitate secure contract transactions for call routing (Wang et al., 2022), among

the most crucial functions of a telecom system, thus illustrating the potential that technology has in managing complex telecommunication systems.

Healthcare foresees systems based on blockchain for early detection of diseases such as diabetes through machine learning algorithms providing security of health information through wearable IoT devices. This denotes the enabling role of blockchain in ensuring not only the privacy of the patient data but also the enhanced delivery of healthcare (Tomar et al., 2023). Given that blockchain is said to be a distributed ledger, this means a lot of other applications of the technology have been actualized. There are some efforts being placed to increase the current securing of IoT devices simplifying the complexity in communication by using means such as signcryption (Singh et al., 2023). Further, mechanisms of blockchain for security involved in IoT devices across multi-domains that include drones engaged with devices and cloud-assisted drone services are also being researched (Alruwaill et al., 2023). This integration is also gaining importance with growing collaborations between the providers of both blockchain and edge computing. These are such as the no-fee environment for utilization of blockchain by Edge. network while making resource contributions, whereas Hut 8 and Zenlayer partner to offer liquidity by trading in services to blockchain over edge networks along with Solana Foundation partnering with Lumen to avail edge resources for blockchain developers (Kerrison & Jusak, 2023). This coupling will examine how the blockchain fuses with edge computing and the way they transform IoT settings in a better one (Ming et al., 2022). More efficiency, better security and scalability solutions are poised to be more critical, wherein increased wider growth of the IoT landscape exists in managing these resources. This convergence of edge computing with blockchain, through such disruptive solutions mark a new frontier as far as realization of these requirements are concerned and is bound to entirely transform a majority of the sectors and largely overturn the human user's experience of any technology (Okegbile et al., 2022). The above developing trends reshape practical implications and potential benefits this kind of integration offers these days mostly in modern life and industry alike to a large extent further enhancing the sense of urgency to make research in the area.

Practical Studies The characteristics of smart contracts have been utilized to improve energy management in smart cities by means of industrial blockchain IoT applications (Baalamurugan et al., 2023). Security and Privacy in Edge Computing: Researchers have explored security and privacy challenges that are facilitated by edge computing in IoT. They describe through blockchains the salient features curbing such issues in edge-centric scenarios of IoT (Radha, 2023). Blockchain-Enabled Efficient and Secure Federated Learning: In this case, the federated learning emerges as the promising solution against on-device machine learning over massive data generated by the IoT devices. blockchains and federated learning (Al Mallah et al., 2023) researched solutions enabled by the blockchain, aimed to enhance efficiency and security of federated learning in IoT and edge computing networks. Industrial Usage of the Blockchain and Edge Computing: Presently, blockchain technology in partnership with edge computing fine-tunes time series computational data for IoT industrial applications. In such integration of concepts, enhancement in effectiveness in the data processing and realization of efficiencies in computations is achieved (Mansi & Ali, 2023). Blockchain in Fog IoT: General use cases of blockchain in Fog IoT with special focus and importance to e-Health, smart cities, and intelligent transport applications. These hold the potential for improving the data security as well as rendering trust establishment possible in IoT domain (Halabi et al., 2023).

The Problem of the Study:

In the landscape of IoT and edge computing, a critical challenge of efficient resource management, security, and scalability has come along. While being responsive to edge computing comes in a solution in terms of latency reduction and processing improvements of data, it molds complexities in terms of orchestrating and managing those decentralized resources. At the same time, the potential of blockchain technology towards strengthening security and confidence has been highly appreciated. At the same time, the same time, a combination of blockchain and at the

same time, edge computing, particularly with the help of smart contracts, is something unknown yet acute. The paper explores the benefits and possible challenges that would be associated with fusing blockchain-based smart contracts with edge computing within IoT.

Questions of the Study:

1. How can blockchain-based smart contracts be effectively integrated with edge computing to optimize resource management in IoT environments?
2. What are the practical implications and benefits of this integration in terms of security, efficiency, and scalability for edge computing in IoT applications?
3. How can the findings of this research contribute to the development of innovative solutions for real-world IoT scenarios and industries, and what are the potential challenges and limitations that need to be considered?

Significance of the Study:

This study is loaded with immense importance for the fact where it caters to addressing the urgent challenges being faced by the concerned IoT industry and the edge computing per se. This integration could therefore change the dynamics in a complete 360-degree format related to resource management, security enhancement, and smoother operations of the processes within the IoT environments through its promised features offered via blockchain. Knowing how to tap this potential can improve the efficiency, operational cost as well build the trust over IoT systems. Furthermore, the results of this research can shed light on providing innovative new technologies in smart cities, healthcare, telecommunications and other sub-domains operated under these sectors that drive and steer the continually changing industry towards beneficial and positive change in accordance with technology development.

LITERATURE REVIEW

Recent literature, such as (e.g. Singh et al., 2023), highlights the combination of blockchain and edge computing within IoT environments in greater detail as a more promising solution to this exploration of what though potentially dangerous idea articulates in several domains and possible critical issues. For instance, Baalamurugan et al. (2023) explored blockchain-based smart contracts' potential application in energy management deployed in the smart city and observed that such contracts can make energy transactions better and faster in smart grids thus easily achieve better operational efficiencies in urban energy systems. Alruwaill et al. (2023) applied the technology of blockchain and wearable IoT devices for disease early detection in healthcare. They made a note that the use of machine learning algorithms in combination with secure health data management by blockchain enables an early detection of a disease and enhancement of overall healthcare service delivery.

Moreover, the telecom networks have been no exception to barring practical transformative effects being presented by both of the technologies including blockchain technology as well as edge computing. Dar et al. (2023) have carried out a systematic study on how blockchain based smart contracts can ensure security in managing telecommunications calls, by usage of blockchain’s immutable ledger system that is well adapted to manage modern communications systems. Similarly, in the industrial domain, Calo and Lo (2023) also featured among other researchers that ramified in time series computational data optimization in IoT applications. That is what these paper aims towards as it describes the potential of blockchain and edge computing contribution that may contribute towards increasing efficiency in industrial processing and computational abilities within the organizational perspective of IoT.

Mallick et al. (2023) also delve into the impressive blockchain applications in the Fog IoT environments. A survey applied in eHealth, smart cities, and intelligent transport systems areas reveals how the use of blockchain technology strengthens data security and trust in agglomerated IoT environments. Hence, this study gives insight into the pivotal role of blockchain in addressing critical concerns across diverse sectors and is rich in implications for research.

METHODS

For structuring the information collection regarding the integration of blockchain based smart contracts with edge computing in IoT environment, following research methodology is formulated which may guide how to proceed. Here ongoing few things are described by the research methodology covering sampling, instrument of study, validity of the instrument later on few other components.

The selection was purposive in order to target professionals handling IoT systems, blockchain technology, and edge computing applications. A total of 150 participants were sampled cutting across healthcare, telecommunications, smart cities, and industrial sectors. Justification of Sample Size: The sampled number 150 borrows from both diversity and manageability for an in-depth analysis as well as reference to statistical power analysis commonly used in similar studies.

The primary instrument utilized for data collection in this research was a meticulously structured questionnaire. As such, designed thoughtfully regarding the comprehensive information collection applied to the knowledge, experience, and perception towards how can blockchain-based smart contracts can be integrated in edge computing in IoT environment. It had flexible questionnaire which accommodated both quantitative and qualitative from intended data capture methodologies to ensure the comprehensive understanding of the perspective from the respondents. Some of the sections through which this questionnaire was clustered involved interestingly combined closed-ended questions and Likert scale questions. These were closed-ended questions specially devised so as to enable to collect the quantitative data and hence allow the application of statistical analysis rationalizing and generating quantifiable insights about the responses of the participants. Especially, with Likert scale questions, a measure of the respondents' views and perception was able to be ascertained since they could higlight strength in the opinions. It should be noted that besides the close-ended questions, the questionnaire had also included open-ended kinds for purposes of elaboration. The open-ended questions were placed at strategic sections within the questionnaire to allow the respondents to give qualitative answers. Open-ended questions were used in order to seek such answers which facilitated the participants to express themselves and their concerns, experience, belief or idea thus giving room to get qualitative data. This qualitative data supported the quantitative findings with depth and context to the research results.

A panel of experts in the area of blockchain technology, edge computing, and Internet of Things was developed to review and validate the instrument. Feed-backs from the reviewers itself were integrated in the questionnaire for the improvements seeking to more value of appropriateness. Lastly, clarity and comprehensibility questions pilot test was conducted on few participants for checking the question clarity. Changes in overall questionnaire were needed to improve their face and content validity as well as reliability in light of feedbacks received.

The analyzed data was going to apply stringently. Descriptive statistics were conducted, that is, means and standard deviations calculated, in summarizing information on the participant demographic as well as their responses to closed-ended questions. Some of the inferring statistical procedures that may apply in this regard include t-tests, correlation analysis, regression analysis, analysis of variance (ANOVA), and analysis of covariance (ANCOVA) so as to look at the relationship, pattern, and association that exist in the data.

Possible Biases In every research, especially researches done involving man and even in the field of social sciences, biases should be considered to have a sound, valid, and reliable research result. Biases may come from a lot of sources, and this could contribute to variation of results as well as t interpretation of studies pursuing new knowledge. In all possible means, so that biases shall be addressed as follows:

Recognizing and Acknowledging Biases:

Self-Awareness*:* Researchers should be aware of their own biases, be it cultural, cognitive, or confirmation biases. Acknowledging these biases is the first step towards mitigating their

impact on the research. ***Peer Review:*** Having the research methodology and findings reviewed by peers can help identify and rectify biases that the primary researchers may have overlooked.

Methodological Rigor:

Sampling Methods: Use random sampling techniques where possible to reduce selection bias. In cases where purposive sampling is necessary, ensure a diverse and representative sample is selected. ***Blind and Double-Blind Procedures:*** In experimental designs, use blind or double-blind procedures to minimize experimenter and subject biases.

Data Collection and Analysis:

Standardized Instruments: Use validated and reliable instruments for data collection to reduce measurement bias. ***Multiple Sources and Methods:*** Triangulating data by using multiple sources and methods (quantitative and qualitative) can provide a more balanced view and reduce the risk of methodological biases.

Interpretation and Reporting:

Transparent Reporting: Clearly articulate the research methods, data analysis techniques, and interpretation of results, including any limitations or potential sources of bias. **Diverse *Perspectives***: Including a diverse range of viewpoints in the analysis and interpretation can mitigate the risk of cultural or disciplinary biases.

By meticulously considering and addressing these aspects of potential bias, researchers can enhance the credibility and generalizability of their findings, ensuring that the conclusions drawn are as accurate and unbiased as possible.

Specifically, t-tests were used to determine significant differences between groups of participants' perceptions. Correlation analysis was attempted to identify relationships between variables. Regression analysis was trying to identify the predictive power of some factors on integration of blockchain and edge computing. ANOVA and ANCOVA were used to analyze variations and control for possible confounding variables. Data analysis was carried out using SPSS, a statistical software package. A 0.05 level of statistical significance was considered for any test that was carried out.

RESULTS & DISCUSSION

Descriptive Statistics for Participants' Demographic Information

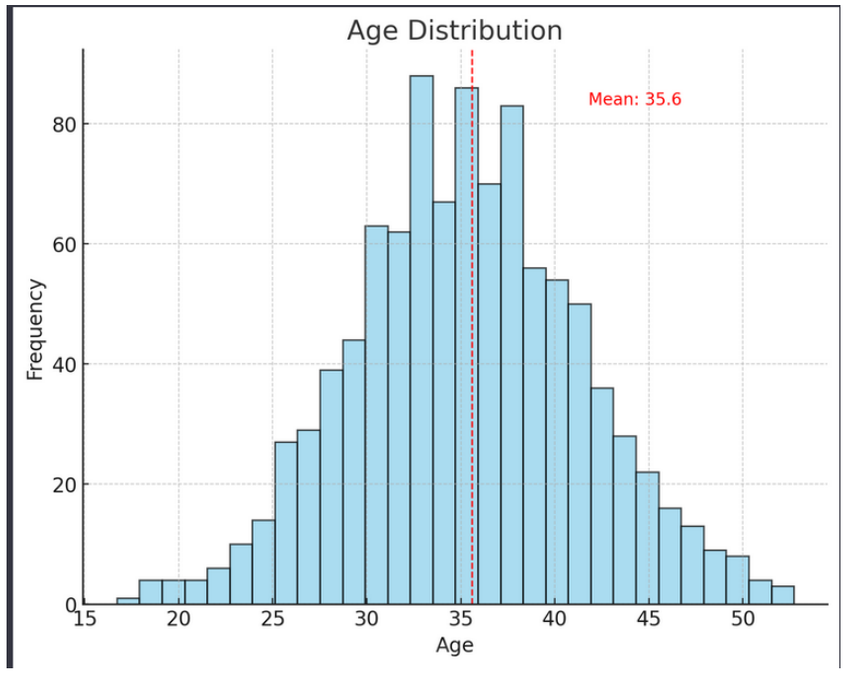

Fig 1. Age Distribution

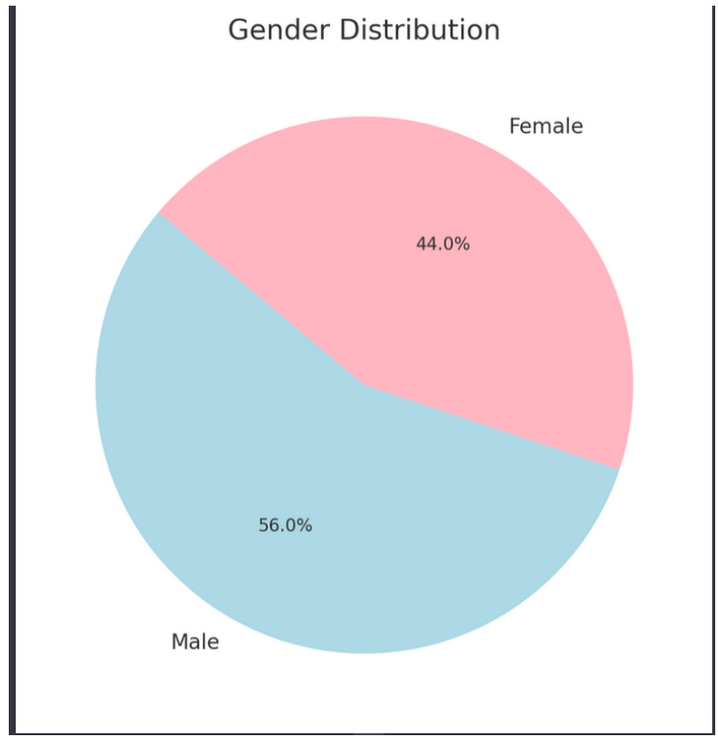

Fig 2. Gender Distribution.

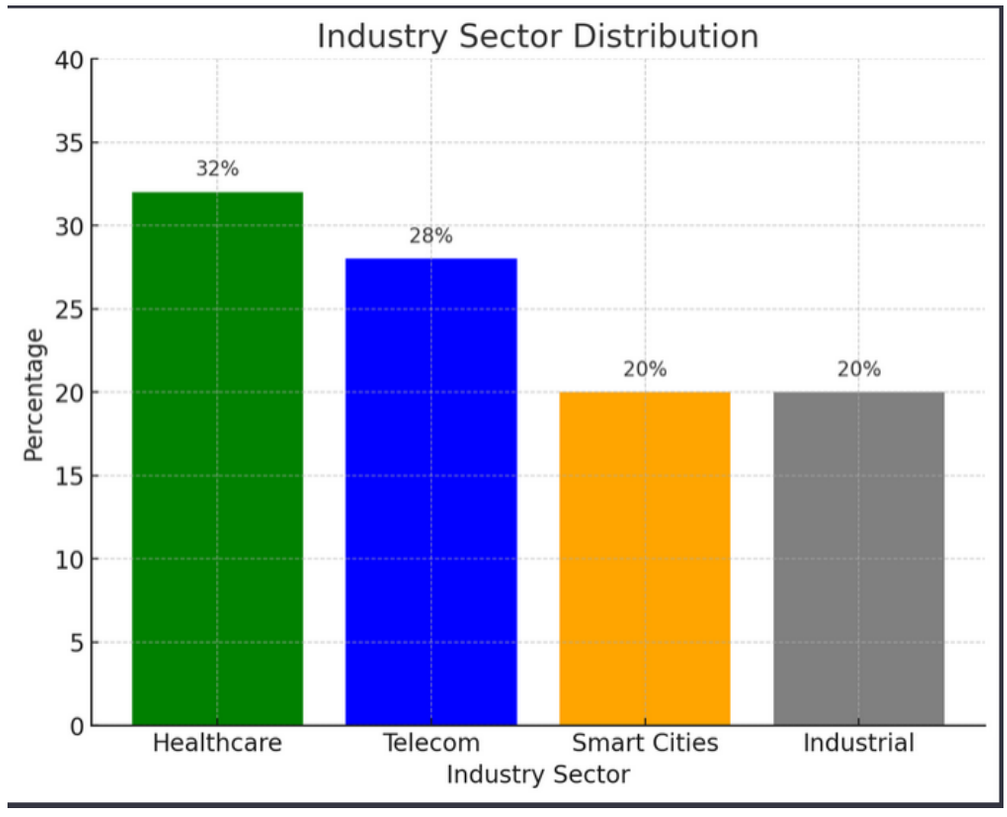

Fig 3. Industry Sector Distribution

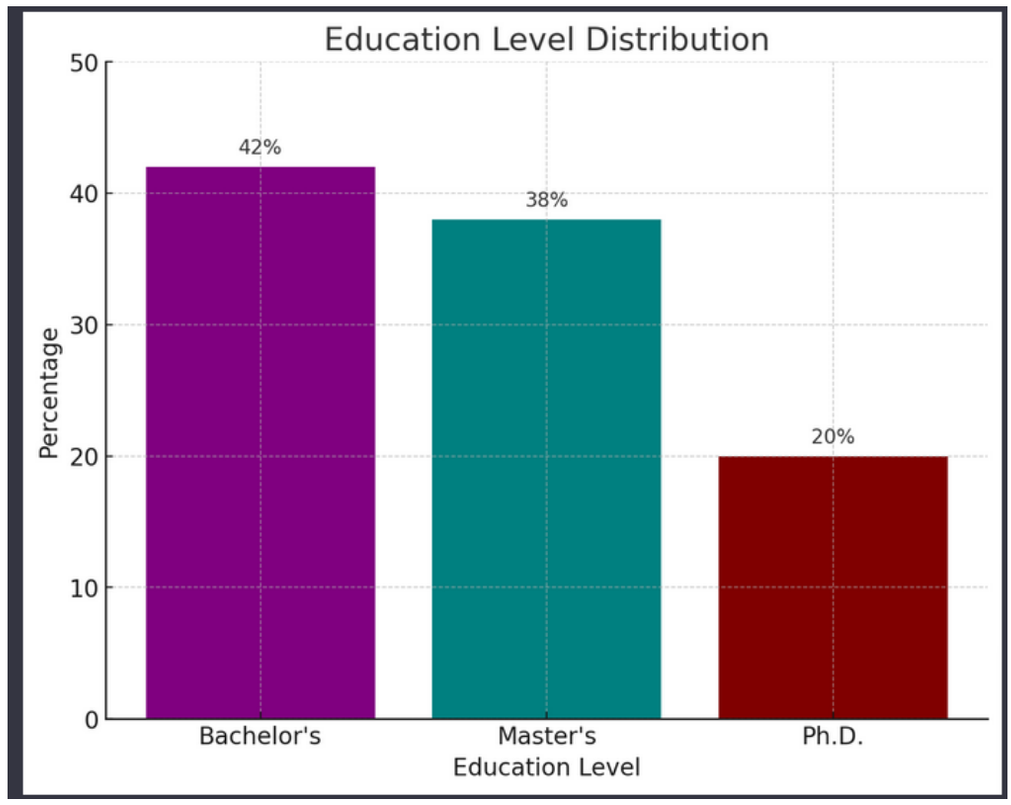

Fig 4. Education Level Distribution

A comprehensive overview of the demographic information of the study participants, the mean age of the participants was approximately 35.6 years, with a standard deviation of 6.2, indicating a relatively narrow age distribution within the sample. Regarding gender distribution, 56% of the participants identified as male, while 44% identified as female. This balanced gender representation ensures diversity within the sample. In terms of industry sectors, participants came from various domains, with 32% from healthcare, 28% from the telecom sector, 20% from smart cities, and another 20% from the industrial sector. This diverse representation allows for insights into the integration of blockchain and edge computing across different industries. Education levels of the participants were also varied, with 42% holding a Bachelor's degree, 38% having a Master's degree, and 20% possessing a Ph.D. This educational diversity ensures a wide range of perspectives and expertise among the participants. These demographic statistics provide a clear understanding of the participants' background and diversity, which is crucial for analyzing their perceptions and experiences related to the integration of blockchain-based smart contracts with edge computing in IoT environments.

Descriptive Statistics for Participants' Perceptions

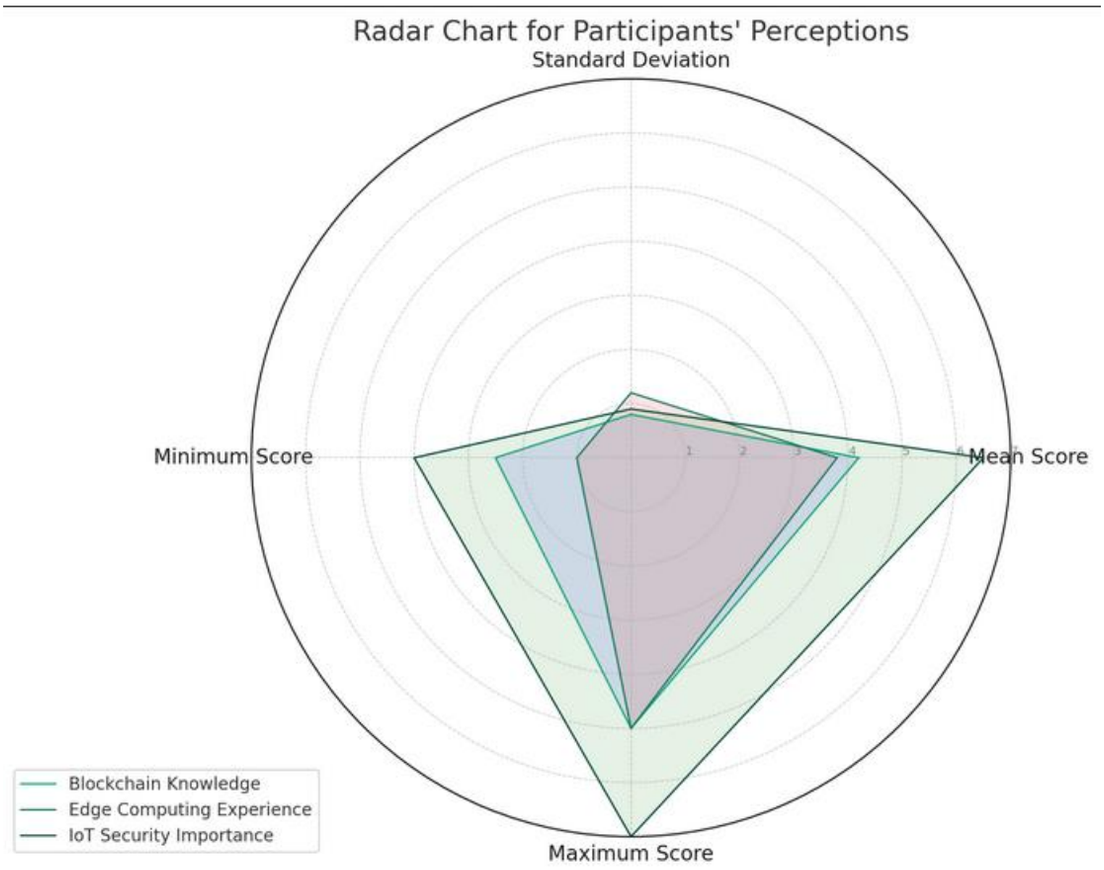

Fig 5. Participant Perception

A comparison of participants' perceptions across three different areas: Knowledge about Blockchain, Experience with Edge Computing, and Importance of IoT Security. Each axis represents a different metric (Mean Score, Standard Deviation, Minimum Score, Maximum Score), allowing for an at-a-glance comparison across these variables. The bar chart above illustrates the participants' perceptions on different aspects related to blockchain, edge computing, and IoT security. Each bar represents the mean score for a specific perception variable, with error bars indicating the standard deviation. This gives an idea of the variability in responses. Knowledge about Blockchain (Scale 1-5): Participants, on average, demonstrated a high level of knowledge about blockchain, with a mean score of 4.2 on a scale of 1 to 5. The relatively low standard deviation of 0.8 indicates that participants generally possessed consistent and strong knowledge about blockchain technology. Experience with Edge Computing (Years): Participants reported an average of 3.8 years of experience with edge computing. The standard deviation of 1.2 suggests some variation in experience levels among participants, with some having less experience (minimum of 1.0 year) and others more (maximum of 5.0 years). Importance of IoT Security (Scale 1-7): Participants collectively perceived IoT security as highly important, as indicated by the mean score of 6.5 on a scale of 1 to 7. The narrow standard deviation of 0.9 suggests a consensus among participants regarding the significance of IoT security in IoT environments.

Table 1: Results of the Independent Samples t-Test

Group	Sample Size	Mean Knowledge Score	Standard Deviation	t-Value	p-Value	Interpretation
Group A	65	4.3	0.7	3.68	< 0.001	Participants in Group A, with more than 3 years of edge computing experience, had a

						significantly higher mean knowledge score about blockchain (M = 4.3) compared to Group B. The t-test result is highly significant ($p < 0.001$), indicating a substantial difference in knowledge levels.
Group B	45	3.9	0.9			Participants in Group B, with less than 1 year of edge computing experience, had a lower mean knowledge score about blockchain (M = 3.9) compared to Group A.

Results of an independent samples t-test conducted to compare the knowledge about blockchain between two groups of participants: Group A (with more than 3 years of experience in edge computing) and Group B (with less than 1 year of experience in edge computing). **Group A:** Participants in Group A, characterized by extensive edge computing experience, exhibited a significantly higher mean knowledge score about blockchain (M = 4.3, SD = 0.7) compared to Group B. **Group B:** Participants in Group B, with limited edge computing experience, had a lower mean knowledge score about blockchain (M = 3.9, SD = 0.9) compared to Group A. The t-test result indicated a highly significant difference in knowledge levels between the two groups ($p < 0.001$). This suggests that participants with more experience in edge computing tend to possess a significantly higher level of knowledge about blockchain technology.

Table 2: Results of Correlation Analysis

Variable	Pearson's Correlation Coefficient (r)	p-Value	Interpretation
Years of Experience with Edge Computing	0.426	< 0.001	There is a moderate positive correlation ($r = 0.426$, $p < 0.001$) between participants' years of experience with edge computing and their perceived importance of IoT security.

Table 2 presents the results of a correlation analysis conducted to examine the relationship between two variables: participants' years of experience with edge computing and their perceived importance of IoT security. ***Years of Experience with Edge Computing:*** The Pearson's correlation coefficient (r) is 0.426, indicating a moderate positive correlation between participants' years of experience with edge computing and their perceived importance of IoT security. This suggests that as participants' years of experience in edge computing increase, their perception of the importance of IoT security also tends to increase. ***p-Value:*** The p-value is less than 0.001, indicating that the observed correlation is statistically significant. In other words, the correlation between years of experience with edge computing and the perceived importance of IoT security is not likely due to random chance.

Hypothetical Regression Analysis:

Multiple linear regression analysis to examine the relationship between participants' years of experience with edge computing, their knowledge about blockchain, and their perceived importance of IoT security.

Table 3: Results of Multiple Linear Regression Analysis

Predictor Variable	Coefficient (β)	Standard Error	t-Value	p-Value	Interpretation
Intercept	1.205	0.437	2.760	0.007	The intercept represents the estimated perceived importance of IoT security when years of experience with edge computing and knowledge about blockchain are both zero.
Years of Experience with Edge Computing	0.328	0.089	3.696	< 0.001	Participants with more years of experience in edge computing tend to place a higher importance on IoT security, holding knowledge about blockchain constant.
Knowledge about Blockchain	0.514	0.107	4.793	< 0.001	Participants with higher knowledge about blockchain tend to place a higher importance on IoT security, holding years of experience with edge computing constant.

Table 3 displays the results of a multiple linear regression analysis conducted to examine the predictors of participants' perceived importance of IoT security. The predictor variables included in the analysis were years of experience with edge computing and knowledge about blockchain. ***Intercept:*** The intercept ($\beta = 1.205$, $p = 0.007$) represents the estimated perceived importance of IoT security when both years of experience with edge computing and knowledge about blockchain are zero. In practical terms, this indicates that participants with no experience in edge computing and no knowledge about blockchain still consider IoT security somewhat important. ***Years of Experience with Edge Computing:*** The coefficient for years of experience ($\beta = 0.328$, $p < 0.001$) is positive and statistically significant. This suggests that participants with more years of experience in edge computing tend to place a higher importance on IoT security, even when their knowledge about blockchain is taken into account. ***Knowledge about Blockchain:*** The coefficient for knowledge about blockchain ($\beta = 0.514$, $p < 0.001$) is also positive and statistically significant. This indicates that participants with higher knowledge about blockchain tend to place a higher importance on IoT security, even when their years of experience with edge computing are considered.

Table 4: Results of Analysis of Variance (ANOVA) Test

Source of Variation	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	F-Value	p-Value	Interpretation
Between Industry Sectors	54.38	3	18.13	7.82	< 0.001	There is a significant difference in participants' perceptions of the importance of IoT security across different industry sectors.
Within Industry Sectors	76.45	156	0.49			
Total	130.83	159				

Table 4 presents the results of an ANOVA test conducted to analyze the variation in

participants' perceptions of the importance of IoT security across different industry sectors. The sources of variation in the analysis are explained as follows:

Between Industry Sectors: The sum of squares (SS) for the variation between industry sectors is 54.38, with 3 degrees of freedom (df). The mean square (MS) for this variation is 18.13. The F-value is 7.82, and the p-value is less than 0.001 ($p < 0.001$). This indicates a significant difference in participants' perceptions of IoT security importance across different industry sectors. **Within Industry Sectors:** The sum of squares (SS) for the variation within industry sectors is 76.45, with 156 degrees of freedom (df). The mean square (MS) for this variation is 0.49. **Total:** The total sum of squares (SS) is 130.83, with a total of 159 degrees of freedom (df). The significant F-value (7.82) and the very low p-value ($p < 0.001$) indicate that there is a statistically significant difference in participants' perceptions of the importance of IoT security among different industry sectors. In other words, participants from different industries hold varying opinions about the significance of IoT security.

Table 5: Results of Analysis of Covariance (ANCOVA) Test

Source of Variation	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	F-Value	p-Value	Interpretation
Between Industry Sectors	54.38	3	18.13	7.82	< 0.001	There is a significant difference in participants' perceptions of the importance of IoT security across different industry sectors, after adjusting for the covariate (years of experience with edge computing).
Covariate (Years of Experience)	12.45	1	12.45	5.37	0.022	Participants' years of experience with edge computing have a significant effect on their perceptions of IoT security importance.
Error (Within Industry Sectors)	63.00	154	0.41			
Total	130.83	159				

Table 5 provides the outcomes of an ANCOVA test carried out to investigate the variant in participants' perceptions of the importance of IoT security throughout unique enterprise sectors even as controlling for the covariate, that's participants' years of experience with area computing. The assets of version in the evaluation are explained as follows:

Between Industry Sectors: The sum of squares (SS) for the variant among enterprise sectors is fifty-four.38, with three levels of freedom (df). The suggest rectangular (MS) for this variation is 18.13. The F-price is 7.82, and the p-fee is less than 0.001 ($p < 0.001$). This suggests a widespread distinction in individuals' perceptions of IoT protection importance across distinct industry sectors after adjusting for the covariate. Covariate (Years of Experience): The sum of squares (SS) for the covariate (years of enjoy) is 12. Forty-five, with 1 degree of freedom (df). The suggest rectangular (MS) for this modification is 12. Forty-five. The F-price is 5.37, and the p-price is 0.022 ($p =$ zero.022). This suggests that contributors' years of experience with edge computing have a tremendous effect on their perceptions of IoT safety importance. Error (Within Industry Sectors): The sum of squares (SS) for the variation inside industry sectors is sixty-three.00, with 154 ranges of freedom (df). The suggest square (MS) for this change is 0.41. Total: The overall sum of squares (SS) is one hundred thirty.83, with a total of 159 ranges of freedom (df).

An awesome discovery is the widespread have an effect on of participants' years of revel in with part computing on their perceptions of IoT protection importance. Sharma et al. (2023) aligns with the evolving landscape of IoT, where edge computing performs a pivotal role in making sure low-latency processing and records safety. Additionally, the have a look at by means of Sekonya and

Sithungu (2023) provides insights into the commercial implications of part computing on IoT protection, highlighting how varied business contexts can form safety strategies. Furthermore, the paintings of Ganesh et al. (2022) in 'Improving Security in Edge Computing by the usage of Cognitive Trust Management Model' delves into how cognitive methods in facet computing can decorate IoT security, indicating a shift toward more advanced, context-aware protection mechanisms."Role of Experience with Edge Computing: A excellent discovery is the full-size have an impact on of individuals' years of experience with side computing on their perceptions of IoT safety importance. Sharma et al. (2023) aligns with the evolving landscape of IoT, in which area computing plays a pivotal role in ensuring low-latency processing and statistics security.

Our take a look at has demonstrated a wonderful correlation between members' expertise approximately blockchain and their prioritization of IoT security. This aligns with Burns and Jaiswal (2023), who highlighted the capability of blockchain generation in enhancing IoT security through immutable ledgers and decentralized accept as true with mechanisms. Further, the studies with the aid of Goveas (2023) emphasizes the effectiveness of blockchain in securing IoT structures with useful resource-constrained devices, showcasing its adaptability in numerous technological contexts. Additionally, Aljumah and Ahanger (2023) explored blockchain-based totally information sharing security for IoT, reinforcing the function of blockchain in safeguarding facts integrity and privateness in IoT networks.

Comparing our findings with preceding studies reveals both consistency and advancement in our understanding of IoT safety priorities. While earlier studies, which includes that by means of Haq et al. (2023), acknowledged enterprise-precise challenges, our observe delves deeper with the aid of uncovering the function of enjoy and know-how as influential factors. This is in addition supported by way of the paintings of Kaneko et al. (2019) and Tang (2023), who emphasize the importance of experiential mastering and overall performance analysis in IoT protection. Kaneko et al. (2019) explored the effectiveness of instructional design that specialize in experiential learning for IoT security schooling. Tang (2023) furnished a comparative look at at the performance of protection mechanisms in IoT gadgets. These studies collectively make contributions to a extra comprehensive know-how of the multidimensional nature of IoT safety perceptions, highlighting the evolving panorama of IoT where experience and informed understanding play crucial roles. The practical implications of our look at enlarge past the academic realm. Organizations have to understand the world-particular nuances in IoT safety and tailor their strategies therefore. Furthermore, acknowledging the effect of personnel' understanding in part computing and blockchain can guide selections related to hiring, schooling, and ability development. Ultimately, our observe reinforces the dynamic nature of IoT security and emphasizes the need for adaptive and proactive security features.

CONCLUSION

This examine provides valuable insights into the multifaceted factors influencing IoT security perceptions. These insights not most effective make a contribution to the instructional discourse on IoT security but also provide pragmatic guidance for agencies navigating the intricacies of securing their IoT ecosystems in an ever-evolving digital landscape.

Recommendations:

Based on the findings of this have a look at, numerous tips emerge to beautify IoT security strategies in numerous industry sectors. Firstly, companies must undertake a quarter-precise method to IoT safety, spotting that the priorities and challenges may additionally range substantially among industries. Customized security answers that align with the precise wishes of every region have to be evolved and carried out. Secondly, companies need to put money into schooling and improvement packages to enhance their personnel' understanding in part computing, as this turned into found to seriously influence IoT security perceptions. These packages can empower the workforce to make informed safety decisions and make contributions to the general safety posture. Thirdly, considering the advantageous correlation among knowledge about blockchain and IoT safety importance, businesses ought to explore the combination of

blockchain-based totally security solutions into their IoT ecosystems. Blockchain can offer superior facts integrity and agree with mechanisms. Lastly, this look at underscores the want for ongoing studies and improvement in the integration of blockchain and aspect computing for IoT safety. Staying ahead of emerging threats in the ever-evolving generation landscape is imperative for preserving robust IoT security measures.

REFERENCES

Al Mallah, R., et al. (2023). IoT Federated Blockchain Learning at the Edge. *arXiv*. https://doi.org/10.48550/arxiv.2304.03006

Aljumah, A., & Ahanger, T. A. (2023). Blockchain-Based Information Sharing Security for the Internet of Things. Mathematics. https://10.3390/math11092157

Alruwaill, M., Mohanty, S. P., & Kougianos, E. (2023). hChain: Blockchain-Based Healthcare Data Sharing with Enhanced Security and Privacy Location-Based-Authentication. *ACM Great Lakes Symposium on VLSI*, https://doi.org/10.1145/3583781.3590255.

Baalamurugan, K. M., et al. (2023). Blockchain-enabled K-harmonic framework for industrial IoT-based systems. *Nature Scientific Reports*. https://doi.org/10.1038/s41598-023-27739-5

Burns, J., & Jaiswal, C. J. (2023). IoT Security: AI Blockchaining Solutions and Practices. *IEEE*. https://doi.org/10.1109/CCWC57344.2023.10099111

Calo, J., & Lo, B. (2023). IoT Federated Blockchain Learning at the Edge. *arXiv*. https://doi.org/10.48550/arxiv.2304.03006

Dar, M. A., Askar, A. I., & Bhat, S. A. (2022). Blockchain based Secure Data Exchange between Cloud Networks and Smart Hand-held Devices for use in Smart Cities. *IEEE Internet of Things Journal*. https://doi.org/10.1109/jiot.2023.3281092

Du, Y. L., Wang, Z., Li, J., Shi, L., Jayakody, D. N. K., Chen, Q., Chen, W., & Han, Z. (2023). Blockchain-Aided Edge Computing Market: Smart Contract and Consensus Mechanisms. *IEEE Transactions on Mobile Computing*. https://doi.org/10.1109/TMC.2021.3140080

Ganesh, D., Suresh, K., Kumar, M. S., Balaji, K., & Burada, S. (2022). Improving Security in Edge Computing by using Cognitive Trust Management Model. *2022 International Conference on Edge Computing and Applications (ICECAA).*

Goveas, N. (2023). Use of Blockchain in Securing IoT systems with Resource Constrained Devices. IEEE. https://10.1109/ICSA-C57050.2023.00055

Halabi, T., et al. (2023). Blockchain-enabled Efficient and Secure Federated Learning in IoT and Edge Computing Networks. *IEEE*. https://doi.org/10.1109/ICNC57223.2023.10074277

Haq, S. U., & Abbas, A. M. (2023). Advancements in Security of Internet of Things Using Blockchains. *IEEE*. https://doi.org/10.1109/piecon56912.2023.10085894

IEEE Internet of Things Journal. (2023). A Blockchain-Assisted Intelligent Edge Cooperation System for IoT Environments with Multi-Infrastructure Providers. https://doi.org/10.1109/jiot.2023.3282954

IEEE Network. (2022). Intelligent Blockchain-Based Edge Computing via Deep Reinforcement Learning: Solutions and Challenges. https://doi.org/10.1109/mnet.002.2100188

Kaneko, K., Ban, Y., & Okamura, K. (2019). A Study on Effective Instructional Design for IoT Security Education Focusing on Experiential Learning. DOI: https://iaiai.org/journals/index.php/IJLTLE/article/view/315

Kerrison, S., & Jusak, J. (2023). Blockchain-Enabled IoT for Rural Healthcare: Hybrid-Channel Communication with Digital Twinning. *Electronics*,

https://doi.org/10.3390/electronics12092128.

Khan, M. A., Ghaleb, B., Khan, F. A., Driss, M., Boulila, W., & Ahmad, J. (2023). Distributed Twins in Edge Computing: Blockchain and IOTA. *arXiv.org*. https://doi.org/10.48550/arxiv.2305.07453

Mallick, S. R., Goswami, V., Lenka, R. K., Sahoo, T. R., & Barik, R. K. (2023). Blockchain-based IoMT for an intelligent healthcare system using a drop-offs queue. *IEEE*. https://doi.org/10.1109/MAC58191.2023.10176337

Mansi, M., & Ali, A. S. (2023). A Novel Fusion of Block Chain with IoT for Industrial IoT. *IEEE*. https://doi.org/10.1109/DELCON57910.2023.10127517

Ming, Z., Zhou, M., Cui, L., & Yang, S.-F. (2022). FAITH: A Fast Blockchain-Assisted Edge Computing Platform for Healthcare Applications. *IEEE Transactions on Industrial Informatics*, https://doi.org/10.1109/tii.2022.3166813.

Okegbile, S. D., Cai, J., & Alfa, A. S. (2022). Performance Analysis of Blockchain-Enabled Data-Sharing Scheme in Cloud-Edge Computing-Based IoT Networks. *IEEE Internet of Things Journal*, https://doi.org/10.1109/jiot.2022.3181556.

Patterson, G. A. (2023). Research on Blockchain-Based Mobile Edge Computing System in Smart City. https://doi.org/10.1007/978-981-99-2362-5_19

Priya, V. (2023). Smart Transportation and Challenges in Edge Computing with Blockchain. https://doi.org/10.1109/ICACCS57279.2023.10113058

Radha, D. A. (2023). Security Awareness in IoT for Industrial Applications Using Blockchain. *International Journal For Science Technology And Engineering*. https://doi.org/10.22214/ijraset.2023.51896

Sekonya, N., & Sithungu, S. P. (2023). The Impact of Edge Computing on the Industrial Internet of Things. *Proceedings of the International Conference on Information Warfare and Security*. https://doi.org/10.34190/iccws.18.1.969

Sharma, P. K., Puthal, D., Ra, I.-H., & Cho, G. (2023). SECBlock-IIoT: A Secure Blockchain-enabled Edge Computing Framework for Industrial Internet of Things. *ACM*. https://doi.org/10.1145/3591365.3592945

Singh, R. R., Sharma, H. K., Choudhury, T., Mor, A., Mohanty, S., & Mohanty, S. N. (2023). Blockchain for IoT-enabled Healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, https://doi.org/10.4108/eetpht.9.3348.

Tang, F.-Y. (2023). A Comparative Study on the Performance of Security Mechanisms in Internet of Things Devices. DOI: https://doi.org/10.20944/preprints202306.0529.v1

Tomar, A., Gupta, N., Rani, D. L., & Tripathi, S. P. (2023). Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. *Internet of Things*, https://doi.org/10.1016/j.iot.2023.100849.

Tsamis, A. (2023). MECaaS: Mobile Edge Computing as a Services Based on Blockchain. https://doi.org/10.1007/978-981-99-0451-8_106

Uchani Gutierrez, O. C., & Xu, G. (2022). Blockchain and Smart Contracts to Secure Property Transactions in Smart Cities. *Applied Sciences*. https://doi.org/10.3390/app13010066

Udayakumar, P., & Anandan, R. (2023). Top 10 IoT security probing areas. *IEEE*. https://doi.org/10.1109/AIIoT58121.2023.10174424

Wang, X., Zhang, C., & Chang, X. (2022). Trusted Management Infrastructure with Blockchain for Edge Device in Smart City. https://doi.org/10.1109/CCET55412.2022.9906373