"Security And Privacy Enhancement In Mobile-Cloud Computing Through Cloud Broker Trust Management Implementation Using CITE Frame Work"

Prof. Parthasarathi Murugesan[1*], Dr. Koppula Srinivas Rao[2]

[1*]Research Scholar, Himalayan University, Itanagar, AP, India. Parthasarathi.murugesan@gmail.com
[2]Professor, Himalayan University, Itanagar, AP, India. Ksreenu2k@gmail.com

Abstract
This study proposes a holistic cloud broker trust management system for mobile-cloud that addresses many significant issues in privacy and security. The research adopts the CITE (Context, Integration, Trust and Evaluation) framework in designing secure protocols for cloud brokers with special reference to encryption, authentication, and privacy preservation. The strategy incorporates CBC mode of Advanced Encryption Standard for encryption and Composite Trust Scores (CTS) in determining the broker's trustworthiness. The results indicate the efficacy of the system in retaining management of trust relationships through active score adjustments, enhanced encryption protocols and frequency analysis of the risk factors. The framework seamlessly connects multiple layers of security, including trust computation and data encryption, providing a comprehensive security framework. The science and engineering of trust is used soundly in the study and its appropriate components are robustly integrated to enhance the security of mobile-cloud computing. This research lays the groundwork for security systems in cloud brokers, while showing how all-inclusive trust management systems can be applied in the real world of cloud computing.

INTRODUCTION

Over the last few decades, technological advancements play a crucial role in every aspect of the business operations. Data becomes transferred through the Internet with the development of different technologies like mobile, web, Internet of Things (IoT), cloud computing, etc., Remote services and servers are mostly employed by these businesses to perform various services like hybrid model, public model, private model, SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). The digital transformation, technological advancements, and the need to satisfy users' and markets' dynamic needs have pushed the modern-day businesses to rely increasingly on cloud-based services. However, implementing cloud environment in the conventional business arena comes with its own challenges like security- and privacy-related concerns, processing speed, accessibility issues, and storage capacity. Assuring data security and privacy before outsourcing the data to the cloud through adopting strong encryption mechanisms is one of the popular solutions followed worldwide (Tabrizchi & Kuchaki Rafsanjani, 2020; Ofuokwu, 2024). Mobile cloud computing (MCC) is the method that offers combined benefits of cloud computing, mobile computing, and wireless networks to the users. Local private cloud providers, network providers, service providers, public cloud providers are the major components of MCC. The efficiency of MCC is improved and privacy and integrity of users' data are assured through different policies employed by cloud service providers (CSPs). This MCC method utilizes sophisticated technologies and integrates network and shared cloud resources for offering the seamless mobility and functionality for mobile devices. In recent times, a greater number of studies have been conducted on MCC due to its capability of providing users the portable and effective communication anywhere and anytime. On the other hand, the primary role of cloud broker is to reserve resources for different CSPs. The cloud broker offers other benefits such as analyzing requirements of cloud users, handling medium-term workloads through IaaS services, increasing profits, offering cost-effective solutions towards satisfying the dynamic demands of cloud users.

Despite the benefits MCC offers, there are still concerns over the trust management and data privacy in the system. Thus, the current study attempts to solve these challenges by focusing on creating robust security protocols for cloud brokers to adhere to encryption, authentication, and privacy-preserving requirements during cloud interactions to prevent vulnerable mobile data from being inserted into cloud interactions.

2. LITERATURE REVIEW

2.1. Cloud Service Model

Cloud model implementation provides on demand networking access from a shared pool of computing resources (Shah et al., 2021). Data stored in the cloud can be accessed by users based on the use of the mobile devices at any location and at any time. Examples of such mobile cloud interaction include checking mail, viewing saved photos and documents, and reading the online chat history. Data security remains the major challenge for interacting with mobile cloud service. As a means of solving the problem of security in MCC, adequate encryption mechanisms must be adopted. Although data may be encrypted before it is outsourced to the cloud, there must be some need to control protection and data privacy. Encryption

however has had an effect in the utilization of the data in the cloud. When data is stored encrypted in cloud environments, the process of searching and indexing has become more complex, as argued by Seth et al. (2022).

Sen et al. (2024) argued that there are various factors that can be used to assess cloud computing such as cloud application type, mobile device limitations, wireless communication quality, and the cloud computing environment itself. Organizations should define clear roles and responsibilities for services while integrating cloud systems into their business environment. Cost control must be the primary focus behind this integration. To assure cloud services' integrity and protection, information should be accessible only to authorized individuals. Both CSPs and customers must have unique roles and responsibilities and access to these cloud services.

Despite the benefits cloud services offer, ensuring security and privacy in the data transmission should be the key focus of businesses. Since cloud environment holds sensitive information of individuals, they should be protected with strong encryption protocols. These protocols are adopted with an aim to not only address these challenges but also meeting regulatory standards, and ensuring compliance with the laws (Subramanian & Tamilselvan, 2019; Soms et al., 2022). Moreover, an increasing number of stakeholders, complex network dependencies, and extensive security controls have all made cloud computing management a challenging task. Organizations should develop cloud-based framework with well-defined security policies towards assuring security and integrity for user data. They also need to conduct periodic risk analysis in order to identify any possible vulnerabilities and threats and act accordingly.

Mandal and Khan (2021) argued that different security-related risks are emerging everyday as businesses move towards adopting cloud infrastructures. In particular, cyber security risks are most evidential in these environments. Since cloud data contains sensitive information, attackers get unauthorized access to these data and use them. There are also other challenges to cloud environments, including man-made errors, misconfigurations, etc., According to Sun (2018), different techniques are used by modern-day attackers towards accessing the cloud environment. While comparing the threats posed by traditional networks, cloud-based threats are high.

2.2. MCC Method

The cloud environment is used in various domains such as banking, healthcare, education, etc., Hence, ensuring data security and privacy remains the crucial concern for them to deal with (AlAhmad et al., 2021). According to De et al. (2020), MCC method helps users to use both mobile services and cloud services from anywhere and at any time. It provides great encryption technique available to store sensitive and confidential information in the cloud for ensuring privacy and security. In order to crypt securely sensitive data in the cloud, various methods are used such as symmetric, disparate attribute-based cryptography and asymmetric methods.

2.2.1. Security Issues in MCC

The inability or lack of security and protectivity are the major challenges in these methods. Security and privacy challenges were caused by the transfer of data between different program. Security and privacy challenges posed by mobile and cloud were addressed by the integration of security and privacy requirements in a flexible framework (Masthan et al., 2019). Hence, high-level security protocols should be implemented within MCC models for improving its efficiency as well as ensuring data integrity and privacy (Wu et al., 2020). Verma et al. (2020) argued that MCC applications enhance the cloud services to operate on portable devices. These applications employ offloading to indicate the status of cloud server towards using it. Adding an encryption data layer can worsen the challenge of heavier communication overhead in the cloud environment (Derhab et al., 2020). More research should be carried out towards ensuring security and integrity to MCC environment. They should mainly focus on different security-based implementation challenges of MCC associated with multifactor authentication issues, cloud-to-client, and client-to-cloud services.

The integration of biometric remote authentication and cryptographic techniques have been recommended while implementing secured data accessibility scheme and offering enhanced MCC reliability. Various past scholars have only focused on identifying the challenges associated with implementing MCC; thus, left the gap in the literatures on focusing secure data and resources. Client-to-cloud authentication does not solely improve the MCC security and requires security establishment while implementing cloud computing systems. Adopting and deploying MCC presents various challenges such as privacy, trust, synchronization, data management, energy efficiency, and heterogeneity. Hence, different strategies are needed in mitigating the risks associated with MCC security and ensuring privacy and security to both CSPs and the users (AlAhmad et al., 2021).

2.3. Review of Encryption Methods

In this section, various studies that have been conducted on different encryption methods to manage security and privacy in the cloud environment are discussed.

A study conducted by Thakor et al. (2021) investigated the lightweight cryptography algorithms and its role on resource-constrained IoT devices. Existing algorithms on this subject matter were compared in this study with regards to attack resistance properties, software and hardware performances, and implementation cost. The authors also suggested future researchers to extend this study towards achieving optimized balance among security, performance, and cost. Another study conducted by Thabit et al. (2021) identified the issues associated with cryptographic algorithms. According to initial findings, cost was not the actual issue; rather, it is the closure time of the entire guidelines. Power-ingestion methods was suggested by this study within the IoT environments to deal with the observed guidelines closure time issue. The study concluded that a large power quantity has been needed within cryptographic methods for resource-constrained IoT devices. A power consumption encryption algorithm is needed in the implementation of IoT device into the cloud environments, as suggested by the authors of this study. Hybrid cryptographic solutions are proposed in another study by Anjana (2022) that used MD5, Blowfish, and RSA algorithms and implemented various security measures in cloud computing. A recent study conducted by Krishnamoorthy and Umarani (2024) used elliptical curve cryptography to implement and manage security related concerns for cloud data. A random evaluation method has been recommended to use by this study towards implementing IoT resources since cryptographic models and security techniques were not adequately demonstrated. The cryptographic security systems have two major demands such as power and time. This study introduced four different novel algorithms and found that the durations for encryption and decryption mechanisms are reduced; and hence, the time taken to control uploading and downloading durations are also controlled.

2.4. Existing Solutions Provided for Security Issues

A secure framework is used by MCC model to protect the privacy of users where mobile applications integrated with different CSPs. According to Rahman et al. (2024), this secured framework also holds the responsibility of secure storage and processing of data on mobile devices. Asghari and Sohrabi (2024) discussed that the integrity of mobile users is assured through trusted computing and incremental cryptography techniques. Furthermore, it became evident that addressing security challenges of MCC entailed the inclusion of some advanced cryptographic algorithms for data security. The transmission and storage of sensitive information involved advanced cryptographic techniques to keep the information secure. Moreover, through the use of AI techniques and machine learning algorithms, the security challenges of MCC can be identified and resolved in terms of threat detection in network community, as argued by Lakhan et al. (2024). The issues in trust management in MCC implementation were solved by integrating the blockchain technology that made a decentralized problem solution. It was blockchain implementation which made an immutable, transparent, and secure system. Moreover, the distribution of data complexity and volume driven by IoT applications demanded some specialized security measures (Zangana & Zeebaree, 2024). To follow ethical and legal standards, it is important to have adequate privacy protocols and regulatory frameworks. However, DNA-based encryption data analysis required more secure methods. Adaptive, multifaceted security strategies implied the evaluation of such highly scalable, resilient security infrastructures in cloud computing, with technological advancements encouraging innovation as well as collaboration (Sami et al., 2024).

Searchable encryption remains a solution for searching data in the cloud (Andola et al., 2022) and save encrypted data in the cloud. Keyword search encryption provides effective solution to query data in cloud. However, with the currently available technique of searchable encryption, this outsourced data was not adequately protected in the cloud. Most data searching methods upon the cloud require users to employ searchable encryption schemes for ensuring security along with protected search upon encrypted data. While traditional searchable mechanisms used to identify keywords are inadequate and supporting only exact keyword matching, it is not suited in new generation mobile devices. Fuzzy keyword method offers the fuzzy keyword search option that replaces the traditional searchable encryption method in a cloud environment and offered increased usability. This option uses keyword simplicity techniques to look at files based on initially the nearest matching files based on keyword, and then based on the keyword in question itself. The fuzzy searchable encryption method integrated with ranked search capabilities make that possible. Ranked search finds files according to appropriate relevance criteria in ranked order (Chen et al., 2024).

In summary, the study recommends employing trustworthy providers and safeguarding sensitive information to provide adequate support to both CSPs and users, as well as ensure trust, security and privacy in mobile-cloud environments. The findings of this study also help to inform technological innovations in the future and guide industry stakeholders and policymakers towards strengthening the cloud security practices.

Methodology

The study method applies the CITE Framework (Context, Integration, Trust, and Evaluation) to create a full trust management system for mobile-cloud computing environments. It begins with Context analysis where it looks at user preferences and device capabilities in order to identify operational environments as well as trust requirements. As Integration stage aggregates data from different sources like performance metrics, security logs and SLA compliance data, normalizing them for consistent analysis. Trust part of it utilizes Advanced Encryption Standard (AES) in CBC mode for data protection by implementing a sophisticated trust score computation mechanism. Through dynamic weighting based on contextual conditions such as latency and security events it calculates Composite Trust Scores (CTS) which is performed by evaluating multiple metrics including SLA compliance, bandwidth. The Evaluation implements continuous monitoring and refinement of trust scores through real-time validation and feedback loops. This methodology includes novel features involving combining multi-attribute trust evaluation with secure encryption protocols. Python libraries are used in the implementation which include pandas for data manipulation, cryptography for secure encryption along with custom algorithms for calculating trust scores hence guaranteeing scalability and adaptability in large-scale mobile-cloud environments.

Result and Discussion

The deployment of cloud broker trust management system produced fruitful results let us consider it in terms of three principal aspects, trust score modification, security protocols, and periodic evaluation of cipher technique analysis. The system accomplished its goal of forming Composite Trust Scores (CTS) by using variety of measures that included security incidents, latency, bandwidth used and so on SLA compliance (Al-Qerem *et al*. 2023).

1. **Adjusted Trust Scores**
    1. **Purpose**: Represents normalized reliability/trust scores (CTS column).
    2. **Key Metrics**: Trust Score, Security Events, Latency, Bandwidth, SLA Compliance.
    3. **Outcome**: A normalized score (0.0 to 1.0) reflecting reliability and risk level

2. **Encrypted Trust Scores**
    1. **Purpose**: Stores encrypted versions of trust scores (Enc_CTS column).
    2. **Implementation**: Combines random initialization vectors (IV) with secure padding and encoding.
    3. **Outcome**: Confidentiality ensured for storage and data transmission.

3. **Frequency Analysis**
    1. **Purpose** : Summarizes occurrences of each trust score (Freq column).
    2. **Implementation**: Counts occurrences of each score in the dataset.
    3. **Outcome**: Identifies trust trends and highlights high-risk or high-performing entities.

Figure 1: Output Summary

Those normalized scores of trusts varying between 0.0 and 1.0 are useful in indicating the trustworthiness of the cloud brokers and devices during a mobile-cloud interaction environment. The proposed scoring scheme was shown to be very adaptable and exhibited one more strong point of being able to modify weights as parameters during the operation change and this ensured correctness of trust representation. The integration of encryption proved to be quite successful in safeguarding sensitive trust data with its use of Advanced Encryption Standard CBC mode.

```
d['Encrypted Trust Score'] = encrypted_scores

d = pd.merge(d, f_df, on="Adjusted Trust Score", how='left')
output = f"processed_{datetime.now().strftime('%d-%m-%Y_%H-%M-%S')}.csv"
d[['ID', 'Adjusted Trust Score', 'Encrypted Trust Score', 'Frequency']].to_csv(output, index=False)
files.download(output)

ttl = d['Encrypted Trust Score'].str.len().sum()
print(f"Total characters in encrypted file: {ttl}")
```

Figure 2: Enhanced Trust Score Framework

Each trust score was obscured with secure algorithms using random vectors as IVs in combination with PKCS7 padding protected Enc_CTS field. This cryptographic strategy helped to solve the problems of confidentiality for both the storage of data and the transmission of information between the main components of the system. The introduction of Base64 encoding also facilitated the system to pass encrypted trust scores over different components without loss of information while the system was able to maintain the integrity of the data.

```
cts_scores = []
for i, row in data.iterrows():
    ctx = {
        'rt': row['Latency (ms)'] < 50,
        'hs': row['Security Events'] > 30,
        'hb': row['Bandwidth (Mbps)'] > 80
    }

    norm_factors = {
        'Trust Score': row['Trust Score'],
        'Security Events': 1 - (row['Security Events'] / 100),
        'Latency (ms)': 1 - (row['Latency (ms)'] / 200),
        'Bandwidth (Mbps)': row['Bandwidth (Mbps)'] / 200,
        'SLA Compliance': row['SLA Compliance']
    }

    dyn_weights = {
        'Trust Score': 0.3 if not ctx['hs'] else 0.2,
        'Security Events': 0.3 if ctx['hs'] else 0.1,
        'Latency (ms)': 0.3 if ctx['rt'] else 0.1,
        'Bandwidth (Mbps)': 0.1 if ctx['hb'] else 0.2,
        'SLA Compliance': 0.2
    }

    cts_score = sum(
        norm_factors[f] * dyn_weights[f] for f in norm_factors
    )
    cts_scores.append(round(max(min(cts_score, 1.0), 0.0), 2))
data['CTS'] = cts_scores
```

Figure: Frequency Analysis for Decision Support

The frequency analysis component proved to be a powerful risk assessment tool as well as a strategic decision-making tool. The patterns of the trust score occurrences were used by the system to diagnose the trends and abnormalities of the brokers and devices involved in the operations of the system. This analysis helped understand how trust scores were distributed over the network and allowed quick detection of the high-risk members and the good brokers. The frequency metrics were found to be very helpful for measuring the trust patterns at all levels of the system and making the desirable changes to the development process.

The integrated data structure that included ID's, CTS's, Enc_CTS and frequency metrics became the basis of a reliable trust management system. Such organization enabled the cost-effective reporting and analysis of data while still respecting the security requirements. Through these relationships matrix and mobile-cloud environments the system demonstrated the ability to manage and maintain several data fields at once proving its scalability and strength. The findings endorse performance of the CITE framework in achieving its primary goals of enhancing security and protecting privacy (Noor *et al*. 2018). The nature of trust score computation as well as the implementation of encryption protocols and the use of frequency analysis complements to a strong system which can effectively address changing security needs. The ability of the framework to keep the user data private while at the same time providing reasonable trust metrics is a great improvement in the field of strategic management of security in mobile-cloud computing. The results indicate that the implemented system enables to meet the security needs while maintaining operational effectiveness in trust management of a cloud broker.

Conclusion

The study managed to design an actionable application that enables a trustworthy mobile-cloud environment. It was shown through the work that through the deployment of the Composite Trust Score, the system as a whole is able to achieve a far more secure and sophisticated level of multi-broker activity through the integration of various trust parameters and even eludes some of the most pertinent issues in regards to privacy and security of the mobile brokers by employing Highest Level Encryption Standards. The application of AES encryption in CBC mode has been employed and highlights the importance of managing trust scores through encryption and confident data whereas the frequency analysis with its multi-layered strategy helps in real time assessment of the risks and actionable strategies that need to be executed. Through its modular structure, CITE offers great promise in the management of trust relationships and conflicts in mobile-cloud environments. Furthermore, the fact that trust values are not static and can vary according to the prevailing conditions, in combination with secure data management techniques, is an improvement in the management of security within the cloud. In the context of the research, a number of security layers were integrated into a complete security solution from the trust computation level to encryption, which proved to be effective. This research will greatly assist the area of cloud-computing security by shedding light on the framework for trust management that is effective, scalable, and secure. The results are promising for further advances in security systems for cloud brokers while proving the practicality of integrated cloud computing environment solutions employing trust management.

REFERENCES

1. AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications*, *190*, 103152.
2. Al-Qerem, A., Ali, A. M., Nashwan, S., Alauthman, M., Hamarsheh, A., Nabot, A., & Jibreen, I. (2023). Transactional Services for Concurrent Mobile Agents over Edge/Cloud Computing-Assisted Social Internet of Things. *ACM Journal of Data and Information Quality*, *15*(3), 1-20.
3. Andola, N., Gahlot, R., Yadav, V. K., Venkatesan, S., & Verma, S. (2022). Searchable encryption on the cloud: a survey. *The Journal of Supercomputing*, *78*(7), 9952-9984.
4. Anjana, D. A. S. (2022). Hybrid Cryptographic solution using RSA, Blowfish and MD5 for Information Security in Cloud Computing. *Mathematical Statistician and Engineering Applications*, *71*(3s), 1250-1268.
5. Asghari, A., & Sohrabi, M. K. (2024). Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. *Computer Science Review*, *51*, 100616.
6. Chen, D., Liao, Z., Xie, Z., Chen, R., Qin, Z., Cao, M., ... & Zhang, K. (2024). MFSSE: multi-keyword fuzzy ranked symmetric searchable encryption with pattern hidden in mobile cloud computing. *IEEE Transactions on Cloud Computing*.
7. De, D., Mukherjee, A., & Guha Roy, D. (2020). Power and delay efficient multilevel offloading strategies for mobile cloud computing. *Wireless Personal Communications*, *112*, 2159-2186.
8. Derhab, A., Belaoued, M., Guerroumi, M., & Khan, F. A. (2020). Two-factor mutual authentication offloading for mobile cloud computing. *IEEE Access*, *8*, 28956-28969.
9. KRISHNAMOORTHY, N., & UMARANI, S. (2024). IMPLEMENTATION AND MANAGEMENT OF SECURITY FOR SENSITIVE DATA IN CLOUD COMPUTING ENVIRONMENT USING ELLIPTICAL CURVE CRYPTOGRAPHY. *Journal of Theoretical and Applied Information Technology*, *102*(15).
10. Lakhan, A., Mohammed, M. A., Zebari, D. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., ... & Martinek, R. (2024). Augmented iot cooperative vehicular framework based on distributed deep blockchain networks. *IEEE Internet of Things Journal*.
11. Mandal, S., & Khan, D. A. (2021). Comprehensive Survey of Security Issues & Framework in Data-Centric Cloud Applications. *Journal of Engineering Science & Technology Review*, *14*(1).
12. Masthan, K., Sharma, K. V., & Peddi, P. (2019). USER REVOCATION AND FINE GRAINED ACCESS CONTROL OF PHR IN CLOUD USING HASBE.
13. Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Mobile cloud computing: Challenges and future research directions. *Journal of Network and Computer Applications*, *115*, 70-85.
14. Ofuokwu, I. K. (2024). *Strategies for Securing Users' Personal Data against Security Threats in MCC Networks* (Doctoral dissertation, Walden University).
15. Rahman, A., Ashrafuzzaman, M., Jim, M. M. I., & Sultana, R. (2024). Cloud Security Posture Management Automating Risk Identification and Response in Cloud Infrastructures. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 151-162.
16. Sami, T. M. G., Zeebaree, S. R., & Ahmed, S. H. (2024). Designing a New Hashing Algorithm for Enhancing IoT Devices Security and Energy Management. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(4s), 202-215.

17. Sen, P., Islam, T., Pandit, R., & Sarddar, D. (2024). A Comparative Review on Different Techniques of Computation Offloading in Mobile Cloud Computing. *Fog Computing for Intelligent Cloud IoT Systems*, 33-44.
18. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*, *33*(4), e4108.
19. Shah, S. D. A., Gregory, M. A., & Li, S. (2021). Cloud-native network slicing using software defined networking based multi-access edge computing: A survey. *IEEE Access*, *9*, 10903-10924.
20. Soms, N., Oswalt, M. S., & Santhosh, K. P. (2022). A case study on cloud security controls. controls. *International Journal of Health Sciences, 6*(S1), 11374-11380.
21. Subramanian, E. K., & Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security. *Service Oriented Computing and Applications*, *13*(3), 237-249.
22. Sun, X. (2018). Critical security issues in cloud computing: a survey. In *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 216-221). IEEE.
23. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.
24. Thabit, F., Alhomdy, S., & Jagtap, S. (2021). Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing. *Global Transitions Proceedings*, *2*(1), 100-110.
25. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access*, *9*, 28177-28193.
26. Verma, R. K., Panigrahi, C. R., Pati, B., & Sarkar, J. L. (2020). An efficient approach for running multimedia applications using mobile cloud computing. In *Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2018, Volume 2* (pp. 315-324). Springer Singapore.
27. Wu, Y., Wang, X., Susilo, W., Yang, G., Jiang, Z. L., Chen, Q., & Xu, P. (2020). Efficient server-aided secure two-party computation in heterogeneous mobile cloud computing. *IEEE Transactions on Dependable and Secure Computing*, *18*(6), 2820-2834.
28. Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, *5*(1), 11-30.