STM JOURNALS

Recent Trends in
Electronics & Communication Systems

ISSN: 2393-8757
Volume 12, Issue 1, 2025
January–April
DOI (Journal): 10.37591/RTECS

https://journals.stmjournals.com/rtecs

Review RTECS

An Overview of Privacy-Preserving Data Encryption Techniques in Mobile Cloud Computing for Big Data

Aakash Dongre[1,*], Shaheen Ayyub[2]

Abstract

With the introduction of mobile cloud computing (MCC), data processing, storage, and sharing have undergone a radical transformation that has greatly improved organizational effectiveness and quality of life. But there are also serious worries about data security and privacy due to the increasing usage of mobile devices and cloud computing, particularly when managing large amounts of data from many sources like sensors and cellphones. The privacy issues surrounding MCC are examined in this study, with a focus on large data applications. It covers several privacy-preserving strategies to protect sensitive data during transmission and storage, such as attribute-based encryption, data sanitization, and cryptographic algorithms. The examination addresses the special limitations of mobile devices and the requirement for safe, effective data handling techniques, emphasizing the tradeoff between security and performance. It also examines the condition of MCC design now, stressing how crucial it is to strike a balance between transmission efficiency and privacy protection. The study's conclusion makes a case for more investigation into scalable, lightweight security solutions to address the changing needs of big data and MCC.

Keywords: Mobile cloud computing, big data, data privacy, cryptography, attribute-based encryption

INTRODUCTION

The mobile cloud computing (MCC) paradigm, brought about by the growing technologies of cloud and mobile computing, produces wonderful applications and services that enhance people's quality of life and organizational effectiveness. The proliferation of products (such as social networks, education, healthcare, and government) that have the potential to produce massive amounts of data, also referred to as big data, was spurred by the continued rise in the use of mobile devices. Although these technological advancements are fantastic, they highlight additional issues that require attention, such as handling and storing large amounts of data, safeguarding user privacy, and securing critical data. Big data are made up of vast amounts of unstructured, semi-structured, and structured data that are typically tagged with implicit information and gathered from many sources, including sensors, smartphones, PCs, and traffic cameras. Here, "big" refers not only to the massive amount of data (often measured in terabytes, petabytes, or zettabytes) but also to the variety of data kinds and data generation velocity (the frequency with which data is created or gathered). Depending on the type of work that must be performed, big data processing might start on demand or in cycles. This processing also referred to as big data analytics, involves looking over and analyzing large datasets to help make better judgments [1].

***Author for Correspondence**
Aakash Dongre
E-mail: aakashdongre2@gmail.com

[1]M.Tech. Scholar, Department of Electronics and Communication Engineering, Technocrats Institute of Technology, Bhopal, Madhya Pradesh, India
[2]Associate Professor, Department of Electronics and Communication Engineering Technocrats Institute of Technology, Bhopal, Madhya Pradesh, India

Received Date: December 02, 2024
Accepted Date: December 08, 2024
Published Date: December 16, 2024

Citation: Aakash Dongre, Shaheen Ayyub. An Overview of Privacy-Preserving Data Encryption Techniques in Mobile Cloud Computing for Big Data. Recent Trends in Electronics & Communication Systems. 2025; 12(1): 1–7p.

© STM Journals 2025. All Rights Reserved

Currently, cloud computing is essential for big data analytics and modeling. It has been effectively implemented in commercial domains and in industrial goods that leverage big data. For instance, Google provides a wide range of real-time services through cloud computing, including voice recognition, real-time translation, and real-time search. We can access enormous amounts of storage space and powerful processing power by using cloud computing [2]. As a result, shifting costly processes to the cloud is a useful way to increase the effectiveness of training deep computation models for big data feature learning. However, because much private data, including demographic and economic data, are gathered from smart cities, privacy issues arising from cloud computing arise. Such data can include private company information or sensitive government data. People's lives and property will be in grave danger if they are revealed. Privacy protection rules such as the Health Insurance Portability and Accountability Act (HIPAA) raise legal and privacy problems when it comes to the sharing of sensitive data, especially in smart cities [3].

Figure 1 depicts the high-level architecture of the mobile cloud along with examples of how privacy measures are addressed [4]. Owing to the workload volume and real-time service considerations, the most important issue is that most modern wireless transfers transmit plain text. Big data technology also prevents the transmission of ciphertexts. The broken-line box in the figure indicates the target protection site and shows the necessity for the security of data flows between mobile computing in the mobile cloud and the physical infrastructure.

Although there are many advantages to adopting MCC, maintaining the privacy of data owners when interacting with social networks or mobile apps is a major challenge. Owing to the massive volume of data, one privacy risk is introduced by unencrypted data transmissions. Many applications give up on using cipher texts in mobile cloud data transmissions because they believe it would still function at a reasonable speed. Because plain text makes it easy for adversaries to obtain information using a variety of techniques, including jamming, monitoring, and spoofing, this phenomenon may give rise to privacy leakage concerns. Owing to the conflict between security levels and performance, which is typically linked to time restrictions, this privacy issue is urgent [5].

PRIVACY CHALLENGES IN MOBILE CLOUD COMPUTING FOR BIG DATA

In the modern world, where information technology and services are ingrained in every part of our lives, cybersecurity and privacy are vital. In particular, a major concern is the security and privacy of large multimedia data in mobile and cloud computing, which is becoming a daily necessity to access various multimedia systems, services, and apps. Furthermore, preserving user privacy and the confidentiality of multimedia data and applications from outside parties is essential for winning over and maintaining customer trust in mobile and cloud platforms. However, this is difficult to accomplish because technology is advancing rapidly, and our systems are becoming more intricate. Furthermore, cyberspace is regarded as the fifth theater of combat after land, air, ocean, and space. Owing to its large volume, unstructured nature, and multiple modalities, the proliferation of multimedia data (images, videos, 3D, etc.) in mobile and cloud computing has brought about both previously unheard-of potential and basic security and privacy issues [6].

Security and privacy are important considerations in the development and application of MCC. These are crucial in mobile commerce and healthcare applications because they include sensitive and urgent information transfers that call for data and user privacy, in addition to guaranteed information transfer security. There are several reasons for this dilemma. The main security and privacy challenges in MCC are shown in Figure 2. First, because mobile devices may be composed of tiny sensors or chips with constrained processing power and bandwidth, they often have significant resource constraints. Consequently, it is impossible to implement complex and advanced encryption methods. Furthermore, owing to the inherent free space, broadcast transmission, and protocol flaws, establishing security on mobile devices has always been more difficult than that on wired systems. Second, communication between mobile devices and the cloud is governed by non-uniform traffic, erratic topology changes,

© STM Journals 2025. All Rights Reserved

varying node densities, high degrees of mobility, and high bit error rates. Third, there is a significant chance that data transferred from the cloud onto a mobile device may be stolen if a client who uses the cloud infrastructure for economical and sensitive data processing misplaces their mobile device [7].

The graphics provided are circular diagrams that highlight different privacy and security issues with mobile cloud computing (MCC). Important topics include data security, location privacy, identity privacy, virtualization security, mobile device security, data privacy, mobile cloud application security, and partitioning and offloading security.

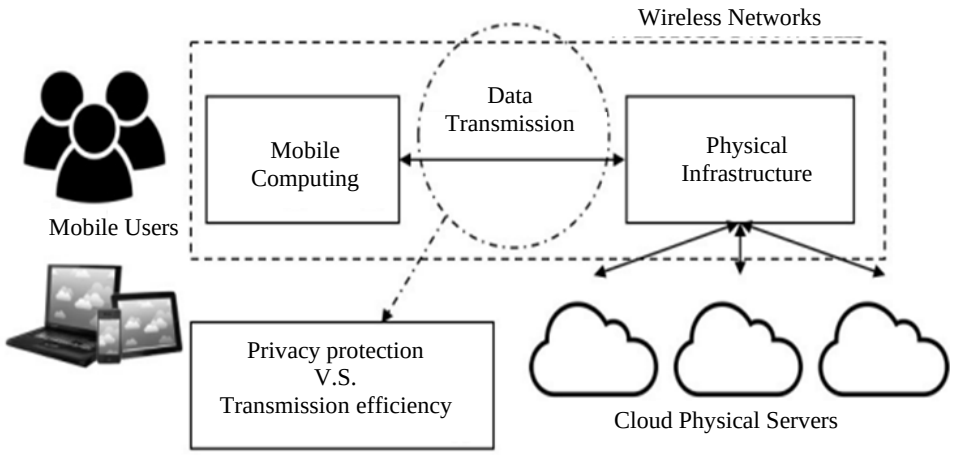

Figure 1. High-level architecture of mobile cloud computing illustrates the balance between privacy protection and transmission efficiency [4].

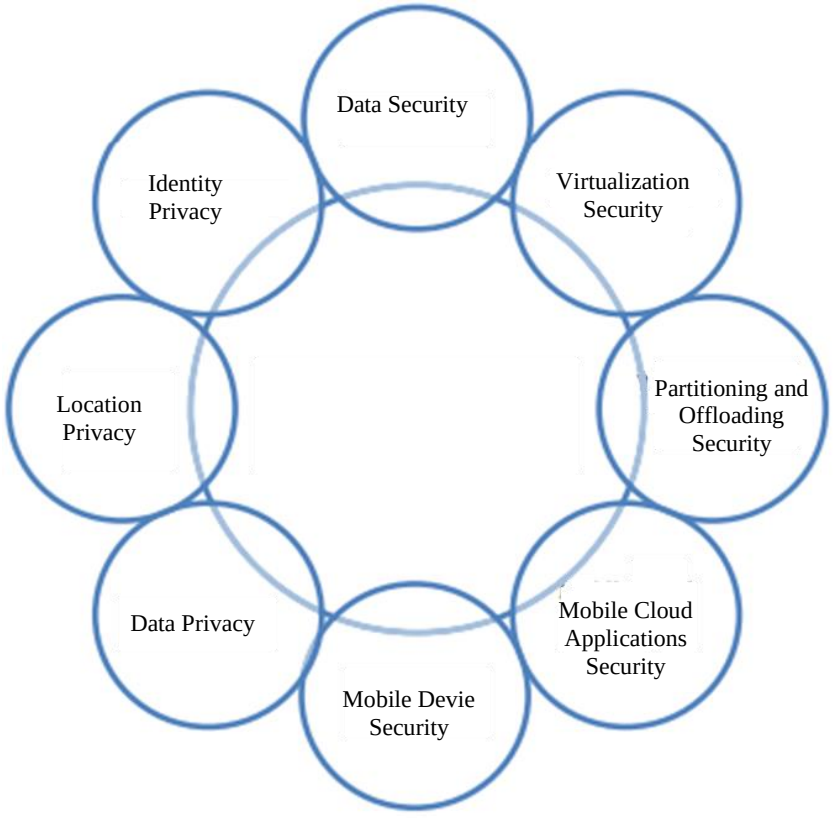

Figure 2. Main security and privacy challenges in MCC [8].

© STM Journals 2025. All Rights Reserved

DATA ENCRYPTION TECHNIQUES FOR PRIVACY PRESERVATION

Owing to a number of factors, including cloud storage and processing in heterogeneous contexts, resource-constrained cellular devices, unsecured open-air transmission media, and privacy in MCC have become more serious issues than once. Numerous outsourcing systems have been proposed in various academic studies. Some of them provide data storage at cloud service provider (CSP) as an outsourcing service and then grant data requesters (DR) access after implementing the necessary access control protocols. Because the DR is unable to access the original data during this process, there is a problem with the submitted data verification. For this reason, certain methods in the literature suggest verifiable outsourcing, in which complex computational tasks are contracted to CSP without revealing more sensitive personal information. A method for cloud-crowded access based on privacy was proposed. Access policies are crucial in these techniques because only authorized users should be able to access a given storage location. Access policies came about because of the solution to this problem. Schemes based on identity are first presented, followed by schemes based on attributes. It was suggested that attribute-based methods be used to grant authorized access. It is possible to verify the access domain by using unique attributes [9].

To ensure secure data sharing over the cloud, desired features such as trust and privacy are necessary. To safeguard data while in transit and prevent the misuse of cloud-stored data, cryptographic activities are required. Security solutions protect against many active and passive threats such as packet sniffing, IP spoofing, identity theft, and man-in-the-middle assaults. An increasing number of mobile devices with extremely accurate sensing features, such as the ability to sense temperature, acceleration, humidity, and images and videos, are becoming available. These features enable them to produce sensing data that can be processed on the cloud to satisfy the DR demand. A DR query in MCC may result in the privacy of several attributes, including identity, location, interests, and habits being exposed. The same is true for mobile crowd contributors (CC), who, in some situations, pose a threat to life. Data sanitization is required to prevent privacy leakage. DRs want to sense the correctness, consistency, and validity of the reports when assessing domain trust. Furthermore, to guarantee safe communication, nonrepudiation, message freshness, and integrity protection are required. Encrypted data are transmitted and stored in the cloud to ensure security from the CSPs.

Application servers guarantee data center connectivity and safe information retrieval during storage. Policies for authorized access are presumed to exist. Programs for managing reputation and trust [10] guarantee the reliability of cloud computing and MCC. A system called attribute-based encryption (ABE) has been suggested to instill confidence and security in MCC. Because mobile devices have limited resources, security and trust can be maintained using services from reliable third parties. Installing and updating a reputation system would require CSPs to have well-managed, effective mechanisms in place, which would also require a lot of storage and processing power. Even if CSPs Ps are expected that CSPs have adequate processing and storage capacity, using them on a wide scale can be costly and difficult. A survey of methods based on reputation and trust has been conducted. Maintaining the privacy of sensitive information can be expensive for CCs and DRs if advanced cryptographic operations are used [11].

The interaction between a data owner, CSP, and cloud consumer in a cloud computing environment is shown in Figure 3 as a flow diagram. This highlights how these entities can securely send data using cryptographic techniques.

SUMMARY OF KEY FINDINGS OF PAST STUDIES

Table 1 provides an overview of six academic publications that address privacy-preserving methods for cloud computing and big data analysis. Each paper's emphasis areas, difficulties addressed, major writers, titles, and techniques and methods are outlined. These strategies cover a wide variety of data privacy, confidentiality, and processing efficiencies in cloud environments, from data splitting and anonymization to encryption approaches, including homomorphic and ABE. With the aid of the table, we can easily comprehend the various strategies for addressing privacy and security issues in cloud-based big data analytics.

© STM Journals 2025. All Rights Reserved

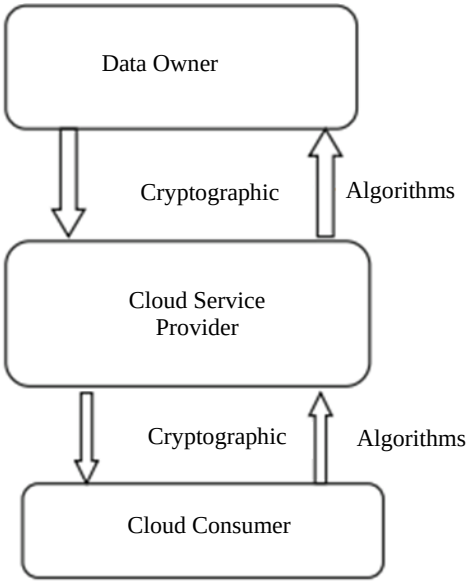

Figure 3. High-level view of cloud security [12].

Table 1. Summary of key findings of past studies.

Authors and year	Title	Key techniques/methods	Focus area	Challenges addressed
Shekhawat, Sharma, and Koli (2019) [13]	Privacy-preserving techniques for big data analysis in the cloud	Homomorphic encryption, order-preserving encryption, attribute-based encryption	Data confidentiality and integrity in cloud computing	Efficient and scalable processing of large datasets; securing user data in untrusted cloud servers
Domingo-Ferrer et al. (2019) [14]	Privacy-preserving cloud computing on sensitive data: a survey	Data splitting, anonymization, cryptographic methods	Privacy-aware outsourcing of storage and processing of sensitive data to public clouds	Security and privacy challenges, compliance with data protection regulations
Li et al. (2019) [15]	Efficient privacy-preserving access control of mobile multimedia data	Ciphertext policy attribute-based encryption (CP-ABE), decryption outsourcing	Privacy-preserving cloud-assisted mobile multimedia data sharing	Secure access control and reduced computational overhead on mobile devices
Lu et al. (2014) [16]	Toward efficient and privacy-preserving computing in the big data era	Privacy-preserving cosine similarity computing protocol	Privacy requirements in big data analytics	Efficient and privacy-preserving data mining
Bahrami and Singhal (2015) [17]	A lightweight permutation-based method for data privacy in mobile cloud	Pseudo-random permutation based on chaos systems	Data privacy in mobile cloud computing	Lightweight and efficient encryption methods for mobile devices
Dong et al. (2014) [18]	Achieving an effective, scalable, and privacy-preserving data sharing service	Ciphertext policy attribute-based encryption (CP-ABE), identity-based encryption (IBE)	Privacy-preserving data sharing in cloud computing	Dynamic access control, scalability, flexibility, and robust security mechanisms

© STM Journals 2025. All Rights Reserved

CONCLUSION

Big data processing and MCC have significantly improved decision-making and data accessibility in a number of industries, including government services, social networks, and healthcare. However, this has also brought significant new difficulties to data security and privacy, particularly considering the sensitive nature of the material at stake and the possibility of exposure through unsealed transfers. The basic problems stem from the dynamic nature of cloud settings, inherent resource limitations of mobile devices, and the complexity of cryptographic solutions. Access control, data sanitization, and encryption work together to effectively preserve privacy in the MCC. For instance, attribute-based encryption (ABE) offers a reliable way to restrict access to private information in accordance with the preset guidelines. Additionally, by ensuring that only pertinent and non-sensitive data are transferred and maintained, data sanitization procedures aid in preventing unauthorized access to personal information. However, these approaches are expensive, particularly in terms of resource usage and computational overhead, which are important factors to consider for mobile devices. This study highlights a number of topics that require further investigation. Creating mobile-friendly cryptographic protocols and lightweight encryption techniques may contribute to improving the tradeoff between performance and data privacy. Furthermore, improvements in CSP reputation and trust management systems may boost user confidence in MCC environments. Ensuring strong privacy and security protection while preserving efficiency is a significant focus area for researchers and practitioners alike, as the cloud and mobile computing ecosystems continue to grow. To promote trust in MCC and facilitate the expansion and uptake of big data solutions in cloud environments, it is imperative to resolve these issues.

REFERENCES

1. Tawalbeh LA, Saldamli G. Reconsidering big data security and privacy in cloud and mobile cloud systems. J King Saud Univ Comput Inf Sci. 2021;33:810–9. DOI: 10.1016/j.jksuci.2019.05.007.
2. Zhu X, Chen C, Yang LT, Xiang Y. Angel: Agent-based scheduling for real-time tasks in virtualized clouds. IEEE Trans Comput. 2015;64:3389–403. DOI: 10.1109/TC.2015.2409864.
3. Zhang Q, Yang LT, Chen Z. Privacy-preserving deep computation model on cloud for big data feature learning. IEEE Trans Comput. 2015;65:1351–63.
4. Gai K, Qiu M, Zhao H. Privacy-preserving data encryption strategy for big data in mobile cloud computing. IEEE Trans Big Data. 2017;7:1–1. DOI: 10.1109/TBDATA.2017.2705807.
5. Weng L, Amsaleg L, Morton A, Marchand-Maillet S. A privacy-preserving framework for large-scale content-based information retrieval. IEEE Trans Inf Forensics Secur. 2014;10:152–67.
6. Gupta BB, Yamaguchi S, Agrawal DP. Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimed Tools Appl. 2018;77:9203–8.
7. Mollah MB, Azad MAK, Vasilakos A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. J Netw Comput Appl. 2017;84:38–54. DOI: 10.1016/j.jnca.2017.02.001.
8. Yang K, Zhang K, Ren J, Shen X. Security and privacy in mobile crowdsourcing networks: challenges and opportunities. IEEE Commun Mag. 2015;53:75–81. doi: 10.1109/MCOM.2015. 7180511.
9. Wang H, He D, Shen J, Zheng Z, Zhao C, Zhao M. Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing. Soft Comput. 2017;21:7325–35.
10. Shen J, Liu D, Shen J, Liu Q, Sun X. A secure cloud-assisted urban data sharing framework for ubiquitous-cities. Pervasive Mob Comput. 2017;41:219–30.
11. Ahmad W, Wang S, Ullah A, Mahmood Z. Reputation-aware trust and privacy-preservation for mobile cloud computing. IEEE Access. 2018;6:46363–81.
12. Shivanna K, Deva SP, Santoshkumar M. Privacy preservation in cloud computing with double encryption method. In: Computer Communication, Networking and Internet Security: Proceedings of IC, Vol. 3t 2016. Springer; 2017. p. 125–33.
13. Shekhawat H, Sharma S, Koli R. Privacy-preserving techniques for big data analysis in cloud. In: 2019 second international conference on advanced computational and communication paradigms (ICACCP). IEEE; 2019. p. 1–6.

© STM Journals 2025. All Rights Reserved

14. Domingo-Ferrer J, Farràs O, Ribes-González J, Sánchez D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Comput Commun. 2019;140–141:38–60. DOI: 10.1016/j.comcom.2019.04.011.
15. Li Q, Tian Y, Zhang Y, Shen L, Guo J. Efficient privacy-preserving access control of mobile multimedia data in cloud computing. IEEE Access. 2019;7:131534–42. DOI: 10.1109/ACCESS.2019.2939299.
16. Lu R, Zhu H, Liu X, Liu JK, Shao J. Toward efficient and privacy-preserving computing in big data era. IEEE Netw. 2014;28:46–50.
17. Bahrami M, Singhal M. A light-weight permutation based method for data privacy in mobile cloud computing. In: 3rd IEEE international conference on mobile cloud computing, services, and engineering. IEEE; 2015. p. 189–98. DOI: 10.1109/MobileCloud.2015.36.
18. Dong X, Yu J, Luo Y, Chen Y, Xue G, Li M. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Comput Secur. 2014;42:151–64. DOI: 10.1016/j.cose.2013.12.002.

© STM Journals 2025. All Rights Reserved