MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Advances in Robotic Technology

Survey on Mobile Cloud Computing

Prajapati DR, Sathwara DD, Suthar RK and Jain R*

Department of Computer Engineering, Ganpat University, Mehsana, India

***Corresponding author:** Rahul Jain, UVPCE, Department of Computer Engineering, Ganpat University, India, Tel: +91-9993671809; Email: rahuljaincse51@gmail.com

Review Article

Volume 2 Issue 1

Received Date: April 01, 2024

Published Date: April 16, 2024

DOI: 10.23880/art-16000111

Abstract

The paper explores how cloud computing offers the capacity to improve computing features and application services while addressing its transformative impact on mobile device systems. It recognizes, yet, the security risks associated with transferring data and computing. Using various cloud types for secure information searches and security-critical activities, the research proposal proposes a secure exporting architecture to basic clouds. It shows the significance of cryptography, confidentiality security measures, and data security methods in solving these security issues with cloud computing and mobile cloud computing (MCC). From the perspective of the specific challenges of mobile environments, that abstract's argument indicates the need for further research to enhance mobile cloud-based applications and improve these security technologies.

Keywords: Mobile Cloud Computing; Cloud Computing; Security; Cryptography; Confidentiality; Data Security

Introduction

At the beginning of the article, Mobile Cloud Computing (MCC) is outlined as a revolutionary combination of cloud and mobile technologies that offers advantages like increased computing power and scalability but also poses security risks. It shows the role that cloud computing serves in providing infrastructure and stresses the importance of the integrity, confidentiality, and availability of data in MCC. To reduce security threats, secrecy techniques, and cryptography are essential security measures. The purpose of the present study is to explore these problems, possible solutions, and the creation of trends in MCC security practices to improve data security and confidentiality in the area of mobile cloud computing.

Mobile Cloud Computing

The aim of Cloud computing for mobile devices (MCC) is to boost processing speed, data storage, and computational capacity by mixing cloud-based computing with mobile devices. It makes use of the cloud's resources to overcome the limitations of handheld devices and provide consumers with greater security and better services. In the present digital world, MCC is vital as it provides flexible options for mobile application development and solves problems like low computation, storage, and power consumption. When everything is looked at, MCC connects mobile phones and tablets with computing resources in the cloud to enhance user experience as well as make it easier to create creative applications for mobile devices (Figure 1).

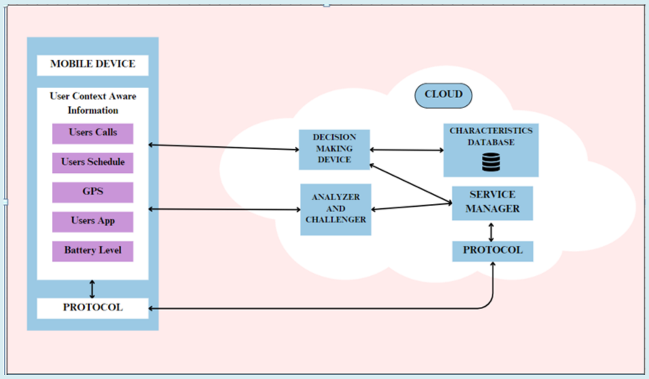

Figure 1: Security Frameworks in Mobile Cloud Computing.

Cloud Computing

A communal repository of hardware and software can be accessible anywhere via the World Wide Web due to the technological model referred to as cloud-based computing. Processing authority, storage spaces. And services represent a few of these resources that may be readily provided and adjusted according to requirements that change. While it is accessible, adaptable, and flexible, the use of cloud computing is becoming ever more popular with customers as well as businesses. It provides advanced computing capabilities accessible to businesses without needing them to make investments in building up infrastructures promotes creativity and boosts cost through an array of sectors [1-3].

Security

A key component of cloud computing security is protecting data, apps, and facilities in cloud locations. This includes procedures like managing identities, security of the network, encryption of information, control of access, and emergency response procedures. Strong safety measures such as firewalls, IDS, encryption, and monitoring are implemented by cloud service providers for protection from attacks and uninvited access. When security protocols for networks ensure safe information movement, control mechanisms such as MFA and RBAC implement safety requirements. In monitoring login information and authorizations, identity management platforms provide restricted access. To appropriately deal with security-related incidents, cloud service providers have incident response processes implemented and respect the requirements that include GDPR, HIPAA, and PCI DSS (Table 1).

Cloud Computing in Security Models		
Security Services/Models	**Description**	**Examples**
Infrastructure as a Service (IaaS) Security	Focuses on protecting the servers, networks, and storage components that make up the underlying infrastructure.	Amazon Web Services (AWS) security groups, Azure Virtual Network security, Google Cloud Platform (GCP) security policies.
Platform as a Service (PaaS) Security	Focuses on securing the cloud provider's platform and development climate.	AWS Elastic Beanstalk security, Azure App Service security, Google App Engine security.
Software as a Service (SaaS) Security	Focuses on managing the information and technology that are accessed online and stored in cloud-based environments.	Office 365 security, Sales force security, Google Workspace security.
Identity and Access Management (IAM) Services	Monitors permissions for access, identities of individuals, and certificates in a cloud system.	AWS Identity and Access Management (IAM), Azure Active Directory, Google Cloud Identity.
Encryption Services	Provides encrypted solutions to protect data while it's undergoing processing, in transportation, as well as at repose.	AWS Key Management Service (KMS), Azure Key Vault, Google Cloud Key Management (GCKM).
Network Security Services	Protect telecommunication and network components, including network firewalls, virtual private networks, and defence against DDoS attacks.	AWS Network Access Control Lists (NACLs), Azure Network Security Groups (NSGs), Google Cloud Firewall Rules.
Security Information and Event Management (SIEM)	Analyses events and security breaches in the cloud environment, finds them, and takes the necessary measures.	AWS Cloud Trail, Azure Sentinel, Google Cloud Security Command Centre (SCC).
Threat Detection and Prevention Services	Identifies and immediately fixes any potential hazards or weaknesses.	AWS Guard Duty, Azure Security Centre, Google Cloud Security Scanner.
Compliance and Governance Services	Provides sure that all management rules, market standard operating procedures, and rules are followed.	AWS Comfit, Azure Policy, Google Cloud Security Command Centre (SCC).

Table 1: Cloud Computing in Security Models.

Cryptography

The studies cover an important aspect of Mobile Cloud Computing (MCC) security: the application of cryptography. Sensitive information that is transferred over the network to cloud servers and tracked on mobile devices is protected using cryptography. Data encryption, secure communication protocols, hash function-based data integrity verification, digital signatures, authentication mechanisms, and reliable key management systems are some of the techniques used in this process. These methods of cryptography are necessary for keeping the information in the MCC environment in opposition to modification, illegal access, and breaches, as well as for maintaining its confidentiality, integrity, and validity.

Confidentiality

These papers explore confidentiality as an important aspect of security in mobile cloud computing (MCC). It deals with avoiding unintentional access to or the publication of confidential data. In MCC contexts, a variety of methods and instruments are implemented for maintaining confidentiality, including data encryption, access control, secure authentication approaches, and secure data storage procedures. By ensuring that only authorized users or entities have the required permissions to access sensitive information saved on mobile devices or in the cloud, those processes attempt to prevent unknown individuals from accessing or viewing private information. All things considered, confidentiality is essential to maintain the security and privacy of data in MCC systems.

Data Security

In the framework of Security in Mobile Cloud Computing (MCC), data security applies to a comprehensive collection of processes and regulations aimed at protecting data from unauthorized communication, changes, or destruction. This includes setting in place accurate information assessment tools, safe authentication operations, control of access structures, and cryptography and data storage strategies. Ensuring the safety, integrity, and accessibility of data at every stage of its lifecycle from processing and storage on mobile devices to sending and storing it on cloud servers is the main objective of data security at MCC. The present study contributes to the improvement of secure data management practices in mobile cloud computing by examining various data security techniques, and difficulties, and creating solutions that are specific to MCC locations (Table 2).

Cryptographic Data Security Scheme Comparisons				
Security Schemes	**Supporting Operations**	**Assumptions**	**Limitations**	**Conclusion**
ENS	The standard method for symmetric cryptography	N/A	Process Overhead	Increase the amount of power usage on mobile devices. Offer extra protection [4,5].
COS	Cells in an array divided by an encoded variable	Developing the Encoding Array	Increased complexity in managing files for mobile devices.	Fewer resources are used than with the ENS System. Intensive on Calculation [4,5].
SHS	X-OR techniques	The method of generating and uploading unexpected files	The processes that support it require a lot of computing power.	Time-consuming. Considerable processing and storage of information requirements [4,5].
BSS	The methods of function for Block-Based Chaining	The file is reasonably structured into chunks.	Dependency executions of blocks. Cryptographic functions are simple XOR procedures.	Energy-Saving. Consume less stuff. Provide rapid implementation [4,5].

Table 2: Cryptographic Data Security Scheme Comparisons.

Literature Survey

A Secure Cloud Computing Model Based on Data Classification

This research provides an original structure for cloud storage with a concentration on processing time efficiency and boosting secrecy [6]. The framework assures data integrity and privacy by using encryption methods such as TLS, AES, and SHA, together with the classification of data [6]. The findings of the simulation show that processing speed was increased without sacrificing security [6]. Further improvements will include the automatic classification of data and the integration of sophisticated cryptographic methods, such as Elliptic curve data encryption and RSA, resulting in greater safety.

A New Secure Model for Data Protection Over Cloud Computing

This research as the use of cloud computing has completely altered how computer services can be delivered, there are dangers related to security [7]. This study presents a methodology that addresses important security issues associated with cloud computing challenges, such as limiting harmful data entry and protecting users from false identities [7]. To ensure security and scalability for data sharing, the paradigm places an extreme value on security without sacrificing usability. Subsequent research endeavors will encompass the application of the model to medical data, strengthening protections against diverse hazards, and maximizing computing setups [7]. The analysis additionally suggests developing a secure service composition for inclusive policy-based cloud computing management.

Application of Cloud Computing Technology in Computer Secure Storage

Computer technology has become indispensable in today's world, supporting social and professional advancement. It does, however, also present threats to information security [8]. With cloud computing, secure network storage and the protection of social and personal data are now guaranteed. Continuous improvements in cloud computing, which provide advantages like consistency and dependability, are essential for improving network drive security [8]. To offer complete security and reduce the hazards associated with data storage, future initiatives should concentrate on combining cloud computing with other technologies.

Survey on Mobile Cloud Computing

The benefits associated with using cloud computing involve additional space, lower costs, and more customization for consumers as well as companies [9]. Enterprises may use resources that are scalable as needed, decrease repair costs, and touch with the requirement for significant servers by utilizing storage and computing services. Subscription-based methods assure the best use of resources and do away with having to buy software upgrades [9]. Chrome books and other cloud-based machines provide mobility, increased life of the battery, and greater safety via cloud storage [9]. When everything is taken into account, cloud-based computing offers consumers increased efficiency and cost savings while carrying regarding an important change in computer models.

A Data Security Framework for Mobile Cloud Computing

The three basic tackles have been included in the projected Security of Data Guidelines: MAC, which is Blow-fish's symmetric method, and CTR mode [10]. The main objective of these techniques is to boost the security of personal data stored on computers in public infrastructures. Developing safe transmission solutions for specified individuals based on the permissions allowed by the data owner is one area of future research opportunity [10]. There's also a chance of lowering the algorithm's cryptographic overhead while maintaining security at the same level.

Mobile Cloud Security Issues and Challenges: A Perspective

The present research examines mobile cloud computing (MCC), highlighting safety problems, frameworks that are already in location, and ways for enhancing security in the MCC system [11]. Data storage, energy-efficient data sharing, and user privacy are major issues [11]. A thorough data security plan is necessary to address these problems, reduce risks, and expedite cloud computing adoption in mobile environments [11]. Performance, enhanced security, and value for money must all be given the greatest importance when developing subsequent designs.

A Survey of Mobile Cloud Computing: Advantages, Challenges and Approaches

The primary goal of this paper is to boost performance on restricted resources mobile devices by providing an in-depth description of mobile cloud computing (MCC) [12]. Ideally suited for handheld devices, MCC combines the advantages of cloud computing and mobile computing [12]. The paper outlines MCC's terms, architecture, goals, advantages and disadvantages, and potential future study areas. To help comprehend MCC better, it additionally offers views on the use of cloud computing.

Security in Mobile Cloud Computing: A Review

The two of us have examined a variety of safety methods, each with advantages and disadvantages specific to mobile cloud computing [13]. Certain models can result in mobile consumers being turned down and their system expenses going up. Others, for example, add additional handling of files overhead while overlooking concerns about cellphone battery life. Disregards the duration and energy constraints faced by the user [13]. The subsequent versions should put safety first without sacrificing system benefits or introducing mobile users to significant resource and time requirements [13]. Designs that decrease expenses while successfully handling safety concerns are additionally necessary.

Mobile Cloud Computing: A Survey on Challenges and Issues

The recently established discipline of smartphone cloud computing (MCC) aims to give mobile customers access to the benefits of cloud computing regardless of the limited capabilities of their devices [14]. This Article offers an overview of MCC. By 2019, cloud-based applications are expected to account for 90% of mobile internet traffic, as reported by Forbes. MCC income is expected to total $5.2 billion, whereas the market is likely to exceed $46.90 billion by the same year. Improvements from MCC include lower costs, more accessibility, and less reliance on hardware and software [14]. The next phase in MCC is likely to include the growing consumerization of IT, the change of work processes, and the integration of IoT (Internet of Things), a collection of multiple technologies that facilitate gathering information and exchange.

A Mobile Cloud-Based Approach for Secure Medical Data Management

To make full use of the large amount of data created by digital medical instruments, healthcare institutions must guarantee data security and integrity [15]. Without sacrificing quality or safety, cloud computing offers a viable way to cut costs, boost performance, and improve patient care [15]. Future studies might concentrate on developing an Android OS and cloud computing-based mobile healthcare information management system. On the other hand, security concerns require consideration, especially about mobile cloud computing. The importance of secrecy and authentication cannot be overstated, and several strategies should be used to guarantee trusted user access [15]. It is essential to put robust confidentiality and safety security in place for medical data stored on cloud servers. Furthermore, imaging methods might be made more mobile-friendly, and medical requirements for data exchange and maintenance need to be established place.

Evaluation Metrics of Cloud Computing Security

Specific the Index Framework

The substantial amount of study on the security of cloud computing shows the importance of regarding security as an independent issue and instead integrating security considerations with various elements of service improvement [16-18]. It supports the point that understanding that security and other system features interact with each other requires a balanced security framework. The connection between security and other reliable characteristics is emphasized, and the objective index technique for analyzing system confidence is offered. The connection between security and reliability features is complex and integrated into the framework of cloud computing [16-18]. For instance, more scalability may result in safety issues even if it improves system features. In the same way, increasing isolation for security reasons may decrease system performance. All things considered, the research shows the importance of a thorough approach to encryption that considers the way it connects to other important system characteristics.

Mathematical Technique or Evaluating Security Parameters

To provide system utility workers with current data on the present state of the system, the following sentence addressed the importance of real-time monitoring services in cloud computing systems [19]. It shows the importance of developing safety parameters that take into account a variety of viewpoints and characteristics and are capable of calculating average and real-time values. It shows that availability is determined by taking availability as an example [19]. The availability is defined as a percentage of the total amount of time that the system can safely operate within a specific time frame and reflects the ability of the system to function securely despite possible flaws or outside challenges. Furthermore stated is the concept of temporary availability, which evaluates a system's simultaneous cyber security condition (Table 3).

$$A_1(t) = P\left\{X(t) \in S_A\right\} \tag{1}$$

The probability of the structure operating in a secure and stable position, or its steady-state accessibility is far more important for the system:

$$A_s = \frac{lim}{t \to \infty} \frac{\int_0^t A_I(u)\,du}{t} \tag{2}$$

It may additionally be calculated by calculating the value of the state's stable state probability matrix in the state diagrams, the structure where steady-state accessibility is illustrated as follows and πi is the system's steady-state accidental of being present from the start of time:

$$A_s = \sum_{t \in S_A} \pi_i \tag{3}$$

Formal Analysis of Variables from an Organizational Approach				
The Mechanism	**Classification**	**The Testing of Authentication**	**The Range of Use Data and knowledge**	**Infrastructure For Programs**
Test	Online examination	√	√	√
Certification	Validation for application portals		√	√
Isolation	The network exclusion	√	√	√
Monitoring	Applications for tracking	√		
Restore	The process of recovery	√	√	√

Table 3: Formal Analysis of Variables from an Organizational Approach**.**

Methodology

The Abstraction in Computing

Techniques and metaphors that reduce complexity while offering location and behavior control are necessary for developing mobile cloud apps. To properly utilize the capabilities of contemporary mobile devices and cloud resources, new programming tools are required. Similar to batch processing frameworks like Map Reduce, these solutions should offer scalability and optimize software modules for different mobile device hardware. Furthermore, programming tools should allow for dynamic computation and storage allocation, enabling holistic application development across cloud platforms, middleware, and mobile clients. For example, Zhang et al. created an SDK that allows developers to use high-level languages like Java or C# to create application interfaces and manage their lifespan. To fully utilize mobile clouds, the emphasis goes beyond developing new apps and also includes transferring current ones to cloud architecture.

Theory of Value

The applications have to be divided into loosely linked modules interacting with each other to dynamically move the computation between mobile devices and the cloud. In a cost model, the modules are dynamically instantiated on mobile devices and switched between the clouds based on many metric criteria. The module execution time, resource usage, battery level, cost, security, and network bandwidth are a few examples of these parameters. User waiting time, or the amount of time a user waits to do certain activities on the device's interface before receiving a desired output or exception, is a crucial component. To choose whether to process data locally or remotely, user wait time is crucial.

The Integration of Clouds

Mobile devices have limited storage, hence cloud storage is a common use case for cloud computing. When it comes to mobile applications, optimizing data transfer size is essential because network bandwidth varies. Data persistence and availability are crucial for continuing operations and saving data till it is required once more. On the other hand, variables like latency, device capacity, bandwidth, and network connectivity must be balanced among them. Although it takes more work, caching benefits distributed databases. The existing lack of cross-platform execution and migration capability underscores a major issue for mobile cloud computing architectures. The problem of movement between cloud structures is still open and needs more work.

Conclusion

The study analyzes how Mobile Cloud Computational (MCC) could improve mobile device application services and computational power while solving security issues. Using a focus on data security and cryptography, it suggests a secure exporting architecture to simple clouds. The summary of the literature provides information on data classification, MCC security, and the integration of technology for improved management of information. To maximize user experience and data transfer, the methodology component of MCC involves value theory, abstraction, and cloud integration. In overall, the study improves MCC's systems and information security, opening up opportunities for additional developments in the area.

References

1. Dixit S, Jain R, Patel HB (2024) Impact of 5G Wireless Technologies on Cloud Computing and Internet of Things (IOT). Advances in Robotic Technology 2(1): 1-7.

2. Jain R, Dixit S (2023) Revolutionizing the Future: Exploring the Multifaceted Advances of Robotic Technologies. Advances of Robotic Technology 1(1)

3. Bhatla AB, Kikani YB, Joshi DG, Jain R, Patel K (2023) Real Time Cattle Health Monitoring Using IoT, ThingSpeak, and a Mobile Application. J Ethol & Animal Sci 5(1).

4. Ren W, Yu L, Gao R, Xiong F (2011) Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing. Tsinghua Science and Technology 16(5): 520-528.

5. Khan AN, Kiah MLM, Ali M, Madani SA, Rehman Khan AU, et al. (2014) BSS: block-based sharing scheme for secure data storage services in the mobile cloud environment. The Journal of Supercomputing 70: 946-976.

6. Tawalbeh L, Darwazeh NS, Al-Qassas RA, AlDosari F (2015) A secure cloud computing model based on data classification. Procedia Computer Science 52: 1153-1158.

7. Sauber AM, El-Kafrawy PM, Shawish AF, Amin MA, Hagag IM (2021) A new secure model for data protection over cloud computing. Computational Intelligence and Neuroscience 8113253.

8. Cao F, Zhang L, Naik DA, Gonzáles JLA, Verma N, et al (2022) Application of cloud computing technology in computer secure storage. Scientific Programming 4767725.

9. Bajad RA, Srivastava M, Sinha A (2012) Survey on mobile cloud computing. International Journal of Engineering Sciences & Emerging Technologies 1(2): 8-19.

10. Patel C, Chauhan SS, Patel B (2015) A data security framework for mobile cloud computing. International Journal of Advanced Research in Computer and Communication Engineering 4(2): 254-257.

11. Donald AC, Oli SA, Arockiam L (2013) Mobile cloud security issues and challenges: A perspective. International Journal of Engineering and Innovative Technology 3(1): 401.

12. Rasoul MM (2015) A survey of mobile cloud computing: Advantages, challenges and approaches. Int J Comput Sci Bus Inform 15: 14-28.

13. Pranav P, Rizvi N. Security in mobile cloud computing: A review. International Journal of Computer Science and Information Technologies 7(1): 34-39.

14. Herbert RP, KumarPR, Jelciana P (2016) Mobile cloud computing: a survey on challenges and issues. International Journal of Computer Science and Information Security (IJCSIS) 14(12).

15. Annapurna P, Ashwini DV, Rashmi RTP, Srinivas T (2015) A mobile cloud-based approach for secure medical data management. International Journal of Computer Applications 119(5).

16. Ghosh N, Chatterjee D, Ghosh SK, Das SK (2014) Securing loosely-coupled collaboration in cloud environment through dynamic detection and removal of access conflicts. IEEE Transactions on Cloud Computing 4(3): 349-362.

17. Namasudra S, Roy P (2017) Time-saving protocol for data accessing in cloud computing. IET Communications 11(10): 1558-1565.

18. Zhang J, Zhang L, Huang H, Jiang ZL, Wang X (2016) Key-based data analytics across data centers considering bi-level resource provision in cloud computing. Future Generation Computer Systems 62: 40-50.

19. Li, Bai J, Luo Y (2016) Efficient resource scaling based on load fluctuation in the edge-cloud computing environment. The Journal of Supercomputing 76: 6994-7025.