IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Data Security of Mobile Cloud Computing on Cloud Server

Simran Sanjay Bhalerao
Student, Master of Computer Application
Late Bhausaheb Hiray S.S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Mobile cloud computing refers to the technology that allows services, such as software, virtual hardware, and bandwidth, to be delivered over the Internet. This technology primarily benefits mobile devices, particularly smartphones. The popularity of mobile cloud computing is rapidly increasing among consumers, and major companies like Apple, Google, Facebook, and Amazon have a large user base in this field. With the help of cloud storage services, users can conveniently access their data anytime, anywhere, and from any device, including mobile devices. While this provides flexibility and scalability in data management, it also introduces new security risks that need to be addressed. However, these security concerns can be mitigated by implementing appropriate data handling practices. Cloud server providers can enhance data security by employing encryption and decryption techniques when storing data in the cloud. In this study, we propose various encryption and decryption methods to safeguard data in the cloud, ensuring that confidential information remains inaccessible to unauthorized individuals or machines due to its encrypted form.*

Keywords: Mobile cloud computing

I. INTRODUCTION

In order to gain a comprehensive understanding of Mobile Cloud Computing (MCC), it's important to first grasp the conception of pall computing [1]. pall computing is a ultramodern business model that offers cost-effective information services of high quality (2). generally, pall computing coffers are handed as services, similar as structure as a Service (IaaS), Data storehouse as a Service (DaaS), Communication as a Service(CaaS), Security as a Service (SecaaS), Hardware as a Service (HaaS), Software as a Service(SaaS), Business as a Service(BaaS), and Platform as a Service(PaaS). Colorfull layered infrastructures live in pall computing to offer these services as serviceability (3). druggies can pierce and use these services grounded on Service position Agreements (SLAs) that define the quality parameters of the service on a pay- per- use base. also, druggies can pierce their data from anywhere, at any time, and using any computing device, including mobile bias. The confluence of pall computing with mobile bias that have limited coffers, wide wireless structure, mobile web capabilities, and position-grounded services has given rise to a new computing paradigm known as Mobile Cloud Computing (MCC) (4). The primary thing of MCC is to enable the prosecution of point-rich mobile operations on a wide range of mobile bias, furnishing druggies with a rich stoner experience (5). The consumer and enterprise requests prognosticate that pall- grounded mobile operations will reach a value of$9.5 billion by 2014. still, the adding number of druggies presents several challenges in the field of MCC, including data replication, thickness, limited scalability, unreliability, uncertain vacuity of pall coffers, lack of portability (due to the absence of pall provider norms), trust, security, and sequestration. To attract further implicit consumers, pall service providers must address these security enterprises to give a fully secure terrain (6). numerous marketable pall storehouse services insure the protection of stoner data stored in garçon warehouses through the perpetration of customer- grounded or garçon- grounded data encryption. This paper aims to punctuate the significant issues and challenges related to security and sequestration in the development of mobile pall operations. also, the paper proposes colorful results for data encryption and decryption in the environment of MCC. The remaining sections of the paper are organized as follows Section 2 provides an preface to the exploration background and an overview of the content. Section 3 discusses the exploration methodology employed. Section 4 presents the software and tools used in the study. Eventually, Section 5 concludes the paper by recapitulating the benefactions made.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

II. RESEARCH BACKGROUND AND OVERVIEW

The term" pall/Cloud" is used as a representation of the Internet and other communication systems, as well as the conception of the underpinning architectures involved. pall computing is the result of the elaboration and wide relinquishment of virtualization, service- acquainted armature, autonomic computing, and mileage computing. utmost end- druggies are ignorant of the specific locales of the structure or element bias involved in pall computing. They don't need to have a deep understanding or control over the technology structure that supports their computing conditioning, and they may not have their own coffers. Then's a brief overview of the elaboration of pall computing. Mobile bias, similar as smartphones and tablets, have come decreasingly essential in ultramodern life and culture. They enable easier and more accessible connectivity, communication, and sharing among people. Mobile operations, generally appertained to as apps, have significantly bettered task performance and delicacy, frequently delivering results within twinkles. moment, mobile apps aren't limited to communication purposes but also serve colorful functions similar as literacy, recreation, and indeed income generation, unlike traditional mobile apps like ringtone editors or grid- grounded games. Technological advancements continue at a rapid-fire pace.

2.1 Cloud Computing Service

Cloud service providers primarily provide their services through three distinct models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).Figure 1 describes these three layers of services which are provided by cloud service providers.

2.2 Infrastructure as a Service

(1)IaaS primarily focuses on Utility computing, enabling users to obtain virtual infrastructure from cloud service providers on an as-needed basis. (2)This includes virtual hardware, processors, storage, and software platforms.(3) Instead of having physical hardware within their own offices, users access information through the internet, utilizing the resources available in the "cloud."(4) While the concept behind IaaS is not new, it has gained renewed momentum with the involvement of major providers like Sun, Amazon, Rackspace, IBM, and Google, as depicted in Figure 1.

(5)The main advantage of IaaS is that there is no need for users to acquire their own servers or invest in physical data center equipment such as storage and networking (6) The providers manage the applications and operating systems installed on the rented computing resources (7). Although users have control over operating systems, deployed applications, and storage to some extent, they cannot manage the underlying cloud infrastructure entirely

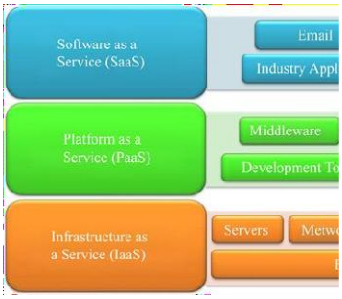


Figure 1. Cloud architecture.

IaaS companies offer offline storage, servers, and networking hardware on a rental basis, accessible through the cloud (8). Customers are relieved of the burden of procuring servers, data centers, or network resources. One significant advantage is that clients only pay for the duration of their usage, making cloud services cost-effective

2.3 Software as a Service

SaaS primarily focuses on delivering on-demand applications to users. The software is executed over the cloud and serves multiple end-users or client organizations. This deployment model involves hosting an application on the Internet, eliminating the need for installation and execution on the customer's own computer. These applications can be accessed from various customer devices through a thin client interface, such as a web browser (e.g., web-enabled email). SaaS offers complete applications to clients that can be customized within certain limitations . In the SaaS model, clients acquire cloud-based applications from service providers. However, it is important to note that a SaaS provider cannot store unencrypted client data . This service model enables network-based access and management of commercially offered software, which is operated from centralized locations and allows clients to remotely access these applications via the Internet.

III. RESEARCH METHODOLOGY

The paper utilizes colorful exploration approaches to explore different aspects of pall computing and the application of its services in software architectural development. The original approach involves conducting a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

literature review to establish a foundational understanding of pall computing and the operation of its services in software armature. This review encompasses exploration papers from different scholars who have studied data storehouse ways and their perpetration in colorful disciplines. It also includes an examination of secure data storehouse styles proposed by different experimenters. also, several case studies are substantiated to dissect the advantages and disadvantages of different approaches enforced in colorful associations. For illustration, encryption algorithms similar as AES, DES, RSA, and Blowfish are estimated for their effectiveness in icing data security in the pall. The exploration will be conducted using Java runtime of Google App Engine, specifically JDK1.6 Eclipse IDE and Google App Engine SDK1.6.0 or advanced. The proposed work plan outlines the way to be taken. Within the mobile pall ecosystem, multitudinous advantages live. still, there are also challenges and issues, similar as data power, sequestration enterprises, data security, and other security- related matters. The paper presents implicit results for addressing these challenges, including strong authentication styles for pall access protection and bedded device identity protection to insure that only authorized druggies can pierce pall- grounded services. fresh security features and programs can be executed to enhance security on mobile bias, particularly in commercial settings. Security is a pivotal factor in pall deployment, and by enforcing the six way outlined in the paper, associations can effectively manage and guard client data in the pall. The exploration platoon will also source reports published by estimable exploration forums similar as IEEE, SEI, ACM, among others, to gain perceptivity into the perpetration of mobile pall calculating from a security perspective.

IV. SOFTWARE AND TOOLS

To ensure secure data storage in the cloud, the following components and tools can be utilized:

- Android platform
- Google API
- Eclipse development environment
- JSON data interchange format
- JAVA programming language
- Amazon AWS Cloud server
- Unit testing framework
- EC2 cloud database provided by Amazon AWS
- By implementing these components and utilizing the specified tools, secure data storage can be achieved in the cloud environment.

4.1 Key components

DDOS Attack

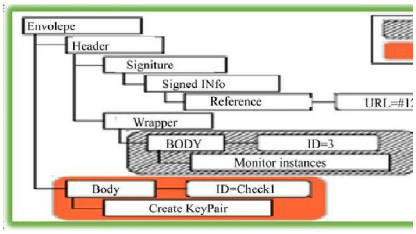
A Denial of Service (DDoS) attack is a type of attack on cloud systems that aims to disrupt the service and prevent clients from accessing resources. The attacker continuously targets the server, overwhelming it and rendering it unavailable to its intended users. This results in clients being unable to receive services from the server as it becomes occupied with servicing the attack. Various techniques can be employed to execute a DDoS attack, such as SYN flood, which exploits the TCP 3-way handshake by sending connection requests to the server and disregarding the acknowledgement (ACK) from the server. The attacker's goal is to make the server wait for the ACK, consuming its time and resources. Consequently, the server becomes unable to allocate resources to provide services to clients.

Preventing such attacks involves implementing strict access controls for the cloud and employing cryptographic protocols to ensure that only authorized personnel can access the cloud . Additionally, various technology products have been developed to detect and mitigate DDoS attacks. The frequency of security breaches in both cloud computing environments and enterprise systems has been increasing rapidly.

XML Signature Element Wrapping

Guests can generally pierce pall calculating through web cyber surfers or web services, but it's important to note that web service attacks can also have an impact on pall computing. One generally known attack in web services is XML hand element wrapping. pall security employs XML autographs to guard the name, attributes, and value of an element from unauthorized individualities. still, it doesn't give protection for the information within the document itself. In an XML hand element wrapping attack, an bushwhacker earnings control over a Cleaner communication by duplicating the target element and fitting any asked value. By doing so, the bushwhacker can manipulate the original element within the Cleaner communication, leading to the prosecution of vicious conduct by the web service.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023



In Figure 2, the client sends data with an open body, leaving room for implicit attacks. For illustration, an bushwhacker can block the Cleaner communication and modify it by replacing the client's requested value of 123 with 456. Upon entering the manipulated communication, the web service will inaptly reuse it as a valid request and respond with the value of 456, which the bushwhacker can also exploit. Another possible attack script involvese-mail web service operations, where the bushwhacker intercepts the Cleaner communication and alters the philanthropist's dispatch address to their own. Accordingly, the web service intentionally on the dispatch to the bushwhacker. XML hand wrapping attacks exploit the fact that the hand itself doesn't give information about the placement of the substantiated element. These types of attacks were first introduced by McIntosh and Austel in 2005, who linked colorful variations, including Simple environment, voluntary Element, voluntary Element in security title (stock value), and Namespace injection (Stock order). These attacks specifically target Cleaner dispatches, which are used to transfer XML documents over the Internet.

Malware Attack

Malware attacks involve the prosecution of vicious software or operations within a pall system. In order to carry out this attack, an meddler must produce their own vicious operation, service, or virtual machine case and also attach it to the pall system. The bushwhacker's thing is to deceive the pall system into treating the vicious software as a licit case. Another script involves trying to upload a contagion or Trojan program to the pall. Once the pall system accepts it as a valid service, the contagion program can automatically execute within the pall, potentially causing damage. This type of attack can harm the tackle of the pall system, and other pall cases running on the same tackle may also be affected due to their participated coffers. also, an bushwhacker might plan to use a contagion program to target other druggies on the pall system. When a client requests the vicious program, the pall system intentionally sends the contagion to the client's machine, performing in the customer's computer being infected. To alleviate these attacks, one possible approach is to perform integrity verification on service cases for incoming requests. By storing a hash value of the original service case's image train and comparing it with the hash values of all new service case images, the pall system can descry any vicious cases. This verification process makes it more delicate for an bushwhacker to produce a valid hash value comparison and fit a vicious case into the pall system. The term" malware" refers to any vicious software designed to perform dangerous tasks on computer systems or networks. One common type of malware is a contagion, which replicates itself and spreads from one machine to another by infecting host programs. Once an infected program is executed, the contagion activates and can beget damage to the machine. Contagions aim to spread and infect other corridor of the compromised system.

Trojan Horse

A Trojan horse is a program that appears to be helpful or beneficial, but in reality, it has harmful intentions towards the host machine. These types of malware often have hidden components that contain a malicious payload, which can exploit or cause damage to the host system. Additionally, Trojan horses can act as spyware by engaging in unauthorized activities, such as secretly collecting a user's data without their knowledge or consent.

Mobile Terminal Security Issues

Security concerns related to mobile devices primarily stem from the behavior and actions of mobile users. Firstly, mobile users often lack security awareness and may not prioritize confidentiality measures. Secondly, users may not properly utilize security features and protocols available on their mobile devices. It is essential to identify and address any abnormal behaviors exhibited by users in order to mitigate potential security threats. Mobile terminal attacks can result in privacy breaches, data leakage, and damage to devices. These consequences are detrimental to clients as they can lead to the unauthorized access and compromise of data stored in the cloud

V. RELATED WORK

Data Storage Issues

In the previous study, the authors discussed the security aspects within the mobile device before transmitting data to the cloud, as illustrated in Figure 3. However, several challenges were identified, including battery consumption, time delays, and decreased encryption and decryption performance due to limited bandwidth.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Table 1 emphasizes the importance of information security, particularly confidentiality, integrity, and availability when storing data in the cloud or other locations. Data encryption is a potential solution to ensure confidentiality. To achieve effective encryption in the cloud computing environment, factors such as encryption algorithm selection and key strength need to be carefully considered. Additionally, the processing time and efficiency of encrypting large volumes of data should be taken into account.

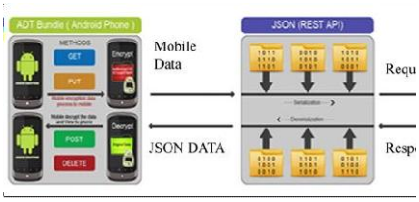


Figure 3. Mobile cloud computing data security

While cloud computing offers substantial computational power, mobile devices have inherent limitations, resulting in challenges in balancing the differences between the two. Implementing cloud computing for mobile devices raises various issues, including resource limitations, network-related concerns, and the security of both mobile users and cloud systems. The following paragraphs elaborate on these issues.

s	Reason
ption/Decryption	Time Consuming
Force Attack	Because of open body
ve the external entity	Because XML 1.0/1.1 Stand
cit trust of internal DTD	Declaring the general entity notation
guration catalogs	Entity resolve catalogs
the external schema	External schema definition
8/UTF-16	Malformed
the trust entity	Import and include construct

Table 1. Security Issues in XML

VI. PROPOSED WORK

According to the depicted diagram in Figure 4, mobile computing data is transmitted to cloud computing in the form of a JSON object, which is trusted due to its serialized data format. Once received, the cloud server encrypts the data using cryptographic methods and securely stores it in the cloud data storage.

In Figure 5, the XML web services REST API is replaced with a solution that addresses the aforementioned issues associated with XML. The data security is now managed at the cloud server. The proposed approach for secure data storage in mobile cloud computing involves implementing the AES (Advanced Encryption Standard) Encryption and Decryption algorithm in Java (JDK and JRE). This encryption is deployed on the Amazon Elastic Compute Cloud (EC2) platform.

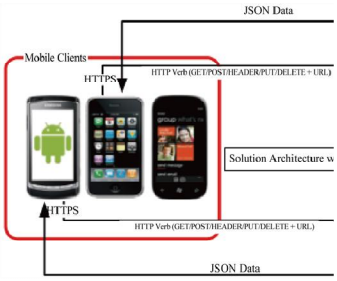


Figure 4. Complete solution mobile cloud computing security on server

The AES algorithm consists of three block ciphers: AES-128, AES-192, and AES-256. Each cipher utilizes a cryptographic key of 128, 192, or 256 bits to automatically encrypt and decrypt data in blocks. For secure communication, both the sender and receiver must possess and use the same secret key. It is important to note that all key lengths are deemed sufficient to protect classified information up to the "Secret" Level, and key lengths of 192 or 256 bits are necessary for "Top Secret" information. The number of rounds for encryption and decryption are as follows:

10 rounds for 128-bit keys
12 rounds for 192-bit keys
14 rounds for 256-bit keys

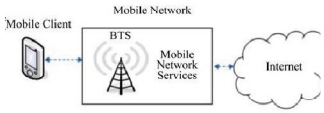


Figure 5 Mobile communication with the cloud domain and servers involves multiple processing steps in each round. These steps encompass various operations such as interchange, transposition, and mixing of the input plain text to ultimately generate the resulting cipher text. Cipher text refers to a form of text that is not easily understandable to anyone without the proper decryption process.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

VII. IMPLEMENTATION

In agreement with the depicted Figure 5, pall computing has set up operations in colorful disciplines, one of which is the mobile sphere. thus, our focus lies on exploring the mileage of pall computing in enhancing the functionality and performance of mobile bias. As bandied in and shown in Figure 2, Mobile Cloud Computing(MCC) is a service that enables mobile druggies with limited coffers to stoutly acclimate their processing and storehouse capabilities. This is achieved by partitioning and unpacking computationally ferocious and storehouse- demanding tasks to traditional pall coffers, eased by ubiquitous wireless access. In Figure 5, the armature illustrates the inflow of mobile data. originally, the data is transmitted to a private pall garçon responsible for data encryption and cryptography. The translated data is also encouraged to a public pall garçon, which is responsible for storing the data in the pall database, specifically the EC2 database storehouse. With this armature, the relationship between mobile pall computing becomes more secure. The security measures are enforced on the private pall garçon, icing its safety, while the public pall garçon solely handles the storehouse of translated data in the pall. This enables druggies to securely partake their important data on the pall garçon without encountering any obstacles. Although this conception may introduce some fresh processing time, it provides a largely secure terrain for mobile pall computing. Authentication and authorization mechanisms are pivotal factors within this armature, icing the secure inflow of data throughout the system

VIII. CONCLUSION

The concept of cloud computing offers users the flexibility to access services on- demand. As the need for mobility in computing arises, Mobile Cloud Computing (MCC) has emerged, providing users with convenient access to services. It is predicted that in the coming years, an increasing number of mobile users will adopt cloud computing on their devices.

However, mobile cloud computing faces several challenges, primarily related to the limitations of mobile devices. Among these challenges, security stands out as a major concern. In the context of Mobile Cloud Computing, the data belonging to the owner is stored on the cloud, which raises concerns about its security.

This paper provides an overview of the fundamentals of Mobile Cloud Computing and delves into the associated issues, with a particular emphasis on data security. Various mechanisms for ensuring data security are explored, aiming to foster widespread adoption of Mobile Cloud Computing among users in the future. Additionally, a proposed mechanism is presented to address confidentiality, access control, and integrity, thereby enhancing the overall security for mobile users.sss

IX. ACKNOWLEDGEMENTS

The successful completion of this research was made possible through the collaborative efforts of a dedicated team. The team members actively contributed their expertise, insights, experience, and support, which played a vital role in achieving the final results. Their collective efforts were focused on addressing the challenges pertaining to client and server-side security. The team worked diligently to mitigate these issues, aiming to enhance the overall security measures. The collaboration and contributions of each team member were instrumental in reaching the research objectives and obtaining valuable outcomes.

X. FUTURE WORK

This paper introduces a prototype of a secure data processing model specifically designed for mobile cloud computing. Moving forward, our research will primarily concentrate on the following areas: 1) exploring additional application scenarios that involve data sharing between the private and public domains of the cloud; 2) assessing the resilience of the Tri-rooted ESSI solution; and 3) examining the implementation of security monitoring, auditing, and misuse detection mechanisms within the mobile cloud system. These research directions will contribute to further advancements in the field of mobile cloud computing security.

The authors declare no conflicts of interest.

REFERENCES

[1]. Data Security in Mobile Cloud Computing: A State of the Art Review Rida Qayyum, Hina Ejaz, " Data Security in Mobile Cloud Computing: A State of the Art Review", International Journal of Modern Education and Computer Science (IJMECS), Vol. 12, No. 2, pp. 30-35, April 2020. DOI: 10.5815/ijmecs.2020.02.04

[2]. Privacy and data protection in mobile cloud computing: A systematic mapping study.Hussain Mutlaq Alnajrani, Azah Anir Norman , Babiker Hussien Ahmed, Published: June 11, 2020

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

[3]. Carchiolo V., Longheu A., Malgeri M., Ianniello S., Marroccia M., & Randazzo A. (2019). Authentication and authorization issues in mobile cloud computing: A case study. In CLOSER 2019—Proceedings of the 9th International Conference on Cloud Computing and Services Science (pp. 249– 256). SciTePress.

[4]. Nasiraee H., & Ashouri-Talouki M. (2018). Dependable and Robust Attribute- Based Encryption in Mobile Cloud Computing. In Electrical Engineering (ICEE), Iranian Conference on (pp. 1536–1541). IEEE.

[5]. Fatima A., & Colomo-Palacios R. (2018). Security aspects in healthcare information systems: A systematic mapping. Procedia computer science, 138, 12–19.

[6]. WITTI M., & KONSTANTAS D. (2018). IOT and Security-Privacy Concerns: A Systematic Mapping Study. International Journal of Network Security & Its Applications, 10(6), 25–33.

[7]. Kumar P. R., Raj P. H., & Jelciana P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691–697.

[8]. Rayapuri, Bhuvaneswari, "A Survey of Security and Privacy in Mobile Cloud Computing" (2018). Master's Theses. 3406.

[9]. Waseem, M. , Lakhan, A. and Jamali, I. (2016) Data Security of Mobile Cloud Computing on Cloud Server. Open Access Library Journal, 3, 1-11.

[10]. Kaur, A. (2015) A Review of Workflow Scheduling in Cloud Computing Environment.

[11]. Lakhan, A.A. (2015) Integration of Dual Data Security Algorithm for Mobile Private Cloud Computing.

[12]. Lakhan, A. and Hussain, F. (2015) Data Security and Privacy for Cross Platform Using Mobile Cloud Computing.

[13]. Lakhan, A. (2015) Security and Data Privacy Using Mobile Cloud Computing