NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 7, ISSUE 2, Feb. -2021

SECURITY DATA MOBILE CLOUD COMPUTING IN THE CLOUD

O'RINOV NODIRBEK TOXIRJONOVICH,
Teacher, Department of Information Technology, Andijan State University +998888388844, nodirbekurinov1@gmail.com

MADOLIMOV FAXRIDDIN ERKINALIYEVICH
Teacher, Department of Information Technology, Andijan State University
+998911745489 f.madolimov_tatu@mail.ru

YUNUSOV ODILJON FOZILOVICH
Teacher, Department of Information Technology, Andijan State University
+998912898903 odiljon.yunusov.71@mail.ru

ABSTARCT:

Mobile cloud computing is a technology for providing services such as software, hardware (including virtual), and bandwidth over the Internet. Mobile devices are included for learning, especially smartphones. Mobile cloud computing technology is growing rapidly among customers and many companies such as Apple, Google, Facebook and Amazon, with rich users. Users can access their data anytime, anywhere, even from any device, including mobile devices, using cloud storage services, although these properties offer flexibility and scalability in data management, but at the same time they remind us of new security threats. These security issues can be addressed through proper data handling. The cloud server provider can protect the data using encryption and decryption methods, keeping the data in the cloud. In this article, we have suggested some encryption and decryption methods to protect data in the cloud so that an unauthorized person or machine cannot access sensitive data due to the encrypted form.

KEYWORDS: Amazon Cloud Server, Cloud Computing, Security, Data Security, AES Encryption, Eclipse IDE, JSON API

SUBJECT AREAS:

Cloud computing, information and communications: security, privacy and trust, mobile computing

INTRODUCTION:

In order to have an in-depth understanding of Mobile Cloud Computing (MCC), it is necessary to gain a better understanding of Cloud Computing [1]. Cloud computing is a new market-oriented business model that delivers high quality and low cost information services [2]. Typically, cloud computing resources that are provided in the form of services such as Infrastructure-as-a-Service (IaaS), Data Storage – Through – Service (DaaS), Communication-as-a-Service (VG), Security as a Service (SecaaS), Hardware as a Service (Haas), Software as a Service (SaaS), Business as a Service (Baas), and Platform as Over Services (PaaS). There are various layered architectures available for cloud computing to provide the above services as a utility [3]. The user can consume these services based on SLAs (Service Level Agreements), which define their QoS (Quality of Service) parameters on a more pay-per-use basis, as well as users can access their data anytime, anywhere, even how - or computing device, including mobile devices.

Cloud computing with resource-constrained mobile devices, ubiquitous wireless infrastructure, mobile Internet and location-based services is creating the foundation for a new computing paradigm called mobile cloud computing (MCC) [4]. The ultimate goal of MCC is to enable rich mobile applications to run on multiple mobile devices with rich user interfaces [5]. According to consumer and enterprise market data, cloud mobile applications are expected to grow to $ 9.5 billion by 2014. Due to the increase in the number of users in the field of MCC, there are numerous problems, including data replication, consistency, and limited capabilities. Scalability, unreliability, unreliable availability of cloud resources, portability (due to lack of a cloud provider standard), trust, security and privacy. In order to attract more potential customers, the cloud service provider must address all security issues to provide a completely secure environment [6]. Many commercial cloud storage services protect user data stored in server storage by implementing client-side or server-side data encryption.

The purpose of this document is to draw attention to many important security and privacy issues and concerns in the development of mobile cloud applications. This document also proposes some encryption and decryption solutions for MCC. The rest of the test is organized as follows. Section 2 presents research background and overview. Section 3 is devoted to the research methodology. Section 4 presents the software and tools, and Section 5 concludes the paper with a summary of our contributions.

BACKGROUND AND OVERVIEW OF THE STUDY:

The term "cloud" is used as a symbol for the Internet and other communication systems, as well as a representation of the underlying infrastructures used.

Cloud computing is commonly referred to as the evolution of the ubiquitous adoption of virtualization, service-oriented architecture, autonomous computing, and service computing. The details of the location of the infrastructure or component devices are unknown to most end users, the user does not need to fully understand or control the technological infrastructure that supports their computing activities, and users do not necessarily have their own resources. Below is a brief history of this evolution.

Mobile devices such as smartphones and tablets are increasingly becoming an integral part of modern life and culture as communication, communication and data exchange between people have become easier and more convenient. Mobile apps (apps) in this regard reduce task performance in minutes and help you get accurate results. Today, mobile applications are created not only for communication, but also for learning, recreation and earning money, in contrast to traditional mobile applications such as ringtone editor, grid-based games, etc. Technology is developing at a rapid pace.

2.1. Cloud computing service:

Cloud service providers offer their services mainly in three different ways, such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Figure 1 describes these three service levels that are provided by cloud providers.

2.2. Infrastructure as a Service:

IaaS mainly offers utility computing, which allows users to receive infrastructure from cloud service providers in the form of virtual resources as needed. Virtual hardware, raw processors, software storage platforms include computers. Despite the fact that in their offices the physical equipment is located in the "cloud", the information is accessed via the Internet. The

basic idea behind IaaS is not new, but this type of cloud computing is getting new life from major providers like Sun , Amazon , Rackspace , according to the architecture shown in Figure 1, IBM and Google . The main advantage is that there is no need to purchase a server or use a physical data center equipment, such as storage, network, and so on. D . [7]. They organized the applications and operating systems that they install on top of rented computing resources [8]. The user cannot manage or manage the underlying cloud infrastructure, but it has power over operating systems, deployed applications, storage, and possibly limited [9]. IaaS company provides offline storage, server and network equipment on a lease basis and can be accessed via the cloud [10]. Customers do not need to purchase the required servers, data center or network resources. The key advantage here is that customers only need to pay for a certain period of time and they can use the cloud service [11].

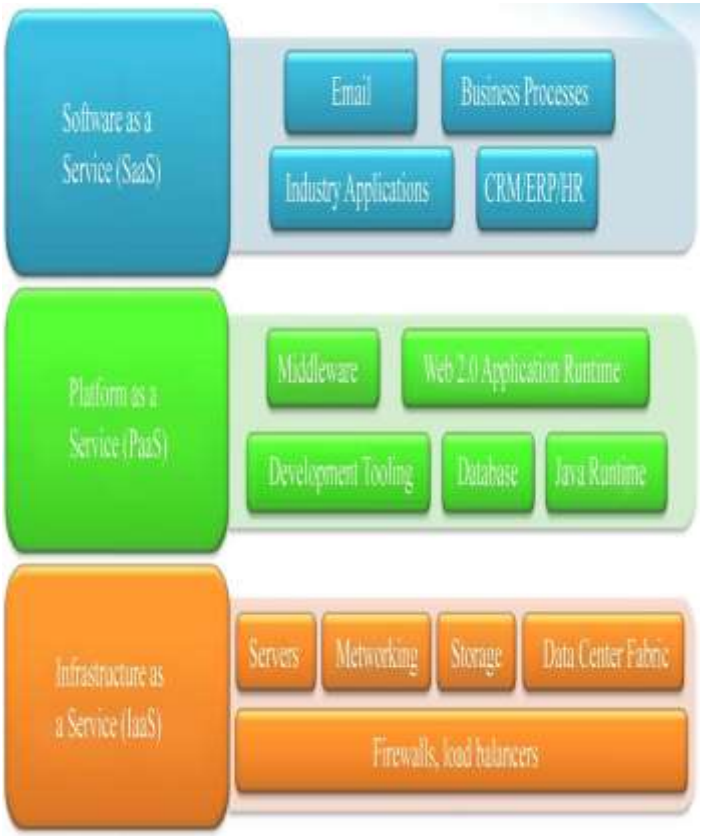


Figure 1. Cloud architecture

2.3. Software as a Service:

SaaS mainly offers on-demand executable applications to users. The software runs in the cloud and serves many end users or customer organizations. This is a software deployment model where the application is hosted on the Internet and served by tenants. This eliminates the need to install and run the application on the client's own computer. These applications are accessible from a variety of client devices through a thin client interface such as a web browser (for example, Internet-enabled email). This type of service provides customers with complete applications that can be customized within certain limits [12]. SaaS service delivery model, customers purchase cloud applications from service providers. The SaaS provider cannot store unencrypted customer data [13]. Network access and management of commercially offered software that is centralized and allows customers to access these applications remotely over the Internet.

RESEARCH METHODOLOGY:

The article uses various research approaches; First, a literature review is conducted to gain a fundamental understanding of cloud computing and the use of its services in software architecture development. It also includes research articles from various researchers who have looked at data storage techniques and applied them in various fields. The secure storage of data by various researchers is also included in this study.

Further, several case studies are also mentioned in this context, in which we will try to find the pros and cons of various options implemented and implemented in various organizations, such as: encryption algorithms like AES, DES, RSA and blowfish for security. data in the cloud. The study will be conducted using the Java runtime the Google the App Engine, it is. JDK

1.6 Eclipse IDE, Google App Engine SDK 1.6.0 or higher. Following are the steps for the proposed work plan.

The mobile cloud ecosystem has many benefits. However, there are some challenges and concerns in mobile cloud computing such as data ownership, data privacy and security, and other security concerns. Some possible solutions for securing access to the cloud are presented. The strong authentication method ensures that only a legitimate user with authorization can access the cloud services built into the device's identity protection. You can embed a personalized configuration profile on each employee's mobile device, thereby embedding credentials or a personal security token on their mobile device. There are some other security features and policies that can be applied to maximize the security of mobile devices, especially in a corporate context.

Security is an important consideration when deploying the cloud, and by leveraging the capabilities described in these six steps, organizations can better manage and protect their customer data in the cloud.

The team will also refer to reports published on IEEE, SEI, AKM and other renowned scientific forums. This method will give us an insight for the implementation of mobile cloud computing as a security point of view.

SOFTWARE AND TOOLS:

Implement secure storage in the cloud.

A. Android
B. Google API
C. Eclipse
D. Json
E. JAVA
F. Amazon AWS Cloud Server
G. Unit testing
H. EC2 Cloud Database

PREVIOUS WORK:

According to an article [14], in mobile cloud computing, there are many problems because - due to limitations of mobile devices. Security is a major concern in mobile cloud computing. In mobile cloud computing, owner data is stored in an unsecured cloud.

According to an article [15], from the - for the particular constraints of resources security of mobile devices can be potential problems in the cloud access, consistent access, data transmission, etc. D. Such problems can be solved by: a special application (service) and middleware (. provide a platform for all mobile cloud computing systems).

According to [15], the security applied on the client side of mobile cloud computing is also inherited in mobile cloud computing with the additional constraints of resource-constrained mobile devices such as time costs.

According to [16], a mobile cloud computing architecture for offloading code in MCC applications solves power and performance problems due to time constraints.

According to article [17], all processing in the MCC is performed on the mobile side. Thus, there are some data movement issues such as throughput, latency, availability, and heterogeneity.

KEY COMPONENTS:

DDOS attack:

Denial of service is a type of attack through the cloud that prevents customers from receiving services from the cloud. The attacker constantly attacks the target server to keep it busy, in order to make the machine or network resource unavailable to intended users, so that clients cannot get service from the server because the server will be busy serving the attack. There are many ways to perform a DOS attack. Like a SYN flood. SYN- flood uses TCP three-way handshake with a query of the compounds to the target server and ignoring the

acknowledgment (ACK) from the server. The attacker applies the attack to the server. This forces the server to wait for an ACK, wasting time and resources. After all, servers don't have the resources to provide services to clients. This type of attack can be prevented by allowing strong access to the cloud and using cryptographic protocols to ensure that the right personnel are gaining access to the cloud [17].

Various technology products were released to prevent and detect DDOS attacks, and security breaches grew at a shocking pace in both cloud computing environments and enterprises.

XML Signature Element Wrapping:

Clients can usually connect to cloud computing through a web browser or web service, attacks on web services also affect cloud computing. Wrapping XML Signature Elements is a familiar attack for web services. Cloud security uses XML signature to protect the name, attributes and value of an element from an unauthorized person, it cannot protect information in a document. An attacker can control a SOAP message by copying the target element and pasting any value that an attacker might insert the source element into elsewhere in the SOAP message. This method can trick the web service to process a malicious message generated by the attack.

As shown in Figure 2, the client is sending data, but this is clear text. If an attacker intercepts and modifies SOAP the message by inserting the same element as the client, but the attackers will send a request 456 instead of 123. After the web service receives the message, the web service will send 456 a parcel back to the client. Another possible attack scenario could be in the form of a web-based email service application. When an attacker intercepts a SOAP message and changes the recipient's email address to the attacker's email address, the web service forwards the email to the attacker.

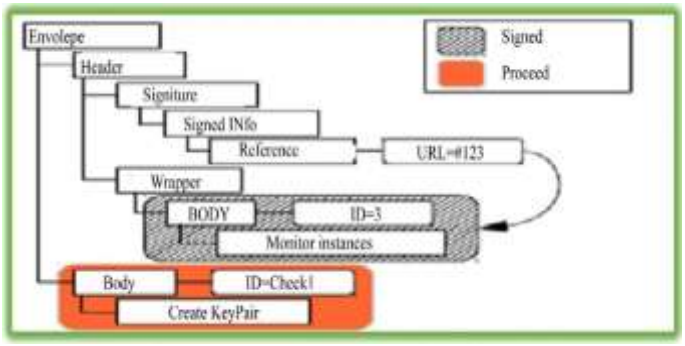


Figure 2. Security of XML data.

XML signature transfer attacks are possible because the signature does not convey any information about where the referenced element is located. This attack was first introduced in 2005 by McIntosh and Austell, specifying different types of this attack, including simple context, optional element, optional element in the security header (sibling), and namespace injection (sibling). This attack occurs in a SOAP message that transmits an XML document over the Internet.

7.1. Malware attack

A malware attack accomplishes this attack, an attacker needs to create his own malicious application, service, or virtual machine instance, and then the attacker has to attach it to the cloud system. When malware is added to the cloud system, an attacker must trick the cloud system into treating the malware as a valid instance. Another scenario is that an attacker might try to upload a virus or Trojan horse to the cloud. Once the cloud system regards it as a valid service, if the virus program runs automatically in the cloud, it infects the virus, which can damage the cloud. Due to this attack, the virus damages the hardware of the cloud system, other instances of the cloud running on the same hardware can affect the virus program because they are using the same hardware. An attacker could plan to use a virus program to attack other users on the cloud system. When a client asks for a case of

malware, the cloud system sends the virus through the cloud to the client and then runs it on the client's machine. The client's computer will be infected with a virus. The type of attack can be possible by performing an integrity check on the service instance for incoming requests. Hash - The value can be used to store the image of the original service instance on top of the file and compare this value with the hash values of all new images of the service instance. The use of hash - values attacker must create a valid comparison of hash - values to deceive cloud system and inject malicious instance of the cloud system.

The term malware refers to any malicious software that can intentionally perform malicious tasks on a computer system or on network systems. Below are some basic definitions of a malware problem.

A virus is a program that is designed to replicate itself and spread from one machine to another using the program of the infected media. This is malware that copies itself into a program. After the infected program is launched, the virus starts its work, infects and damages the machine. Thus, viruses try to spread and infect the infected machine.

7.2. Trojan horse:

Trojan horse - is a program that is considered to be useful, but is malicious intent in relation to the host - machine. Some hidden part of this type of malware containing malicious data that may or may damage the host - system. Trojans can also be spyware due to their malicious activity, such as unauthorized collection of user data.

SECURITY PROBLEMS OF MOBILE TERMINALS:

Mobile terminals security problems - still comes from mobile clients. In - First, mobile clients are not usually aware of the security; and not confidentiality. In - the second, mobile customers can misuse itself. Therefore, it is necessary to identify the abnormality of clients due to the above troubleshooting of attacks on mobile terminals that can cause breach of privacy, leak, irregularity of information and devices damaged by multiple attacks that are harmful to clients due to disclosure of data in the cloud. Can be hacked [17].

RELATED WORK:

Storage problems:

In a previous article [17] in accordance with Figure 3 discussed the security in mobile devices before sending data to the cloud, but we found a problem with the battery consumption, the needs of the time, as well as - for the limited bandwidth some time encryption performance and decryption is reduced ...

According to Table 1, the data stored in the cloud or stored elsewhere are similar, it is necessary to take into account three different aspects of information security: confidentiality, integrity, and availability via the web - services the xml. A possible solution to the data privacy problem is data encryption. To ensure encryption, both the encryption algorithm and the strength of the key must be considered, since the cloud computing environment involves the transfer, storage and processing of large amounts of data. It is also necessary to consider the processing time and the efficiency of encrypting huge amounts of data.

The cloud is extremely powerful for performing computing, while the computing power of mobile devices has its limits, so many challenges arise to show how to balance the differences between the two. Thus, there are some challenges in adopting cloud computing for mobile devices. These issues can be related to limited network resources related to the security of mobile users and the cloud. Some of the problems are explained as follows.

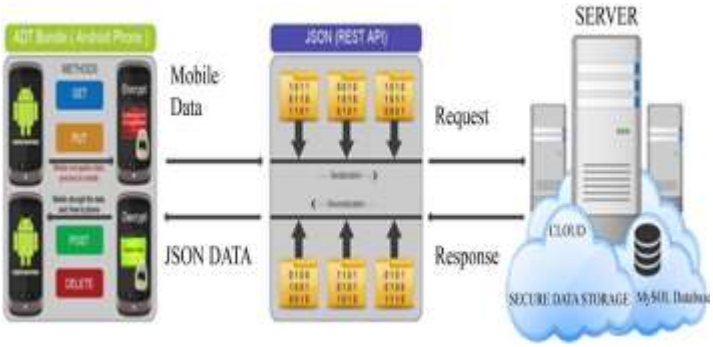


Figure 3. Data security of mobile cloud computing.

Table 1. Security issues in XML.

Issues	Reason
Encryption / decryption	Time consuming
Brute force attack	Because of the open body
Allow external entity	Since XML 1.0 / 1.1 Stand
Implicit trust in the internal DTD	General entity notation declaration
Configuration directories	Entity permission directories
Trust the external schema	Defining an external schema
UTF-8 / UTF-16	Distorted
Of course the trust	Import and include a design

PROPOSED WORK:

Referring to FIG. 4, the data of mobile computing travel to cloud computing through a JSON object, which is trusted, because it has a format for serializing data into a JSON object, then the cloud server will encrypt all data in cryptography, finally, it will store the cloud data in memory.

According to Figure 5, to replace the web - services XML REST API, and decide, first of all, the problem of «XML», and in accordance with Figure 5 Now, data security will be manipulated in a server cloud and offered to work for the safe storage of data in the mobile cloud computing, he wrote encryption and decryption algorithm AES (Advanced Encryption Standards) in Java (JDK and JRE). Now deploy encryption to Amazon Elastic Compute Cloud (EC2). There are three block ciphers, AES, AES-128, AES-192, and AES-256. Each cryptographic key using 128-, 192- and 256-bit is automatically enumerated to encrypt and decrypt data in blocks. The secret key or symmetric key is used for encryption and decryption. Both the sender and the recipient need to know using the same secret key. Please note that all key lengths are sufficient to protect sensitive information up to secret with top secret and must require 192 or 256 bits of key length. Below are the bits for each round:

1.10 rounds for 128-bit keys
2.12 rounds for 192-bit keys
3.14 rounds for 256-bit keys

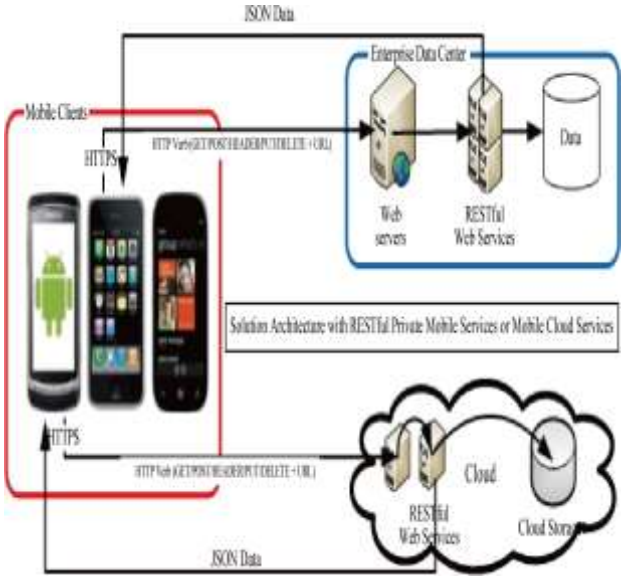


Figure 4. Complete mobile cloud security solution on the server.

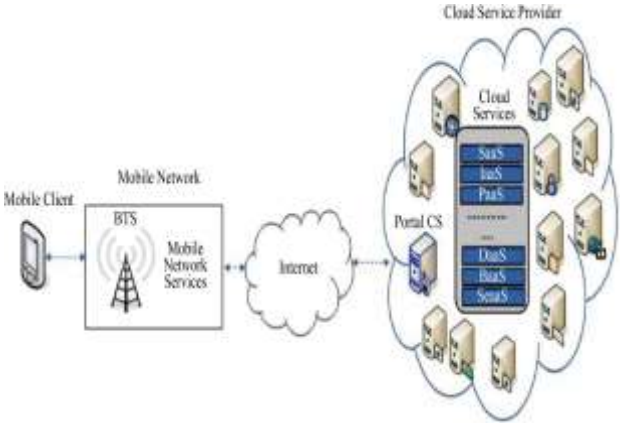


Figure 5. Mobile connection with cloud domain and servers.

Each round consists of many processing steps that include swapping, transposing and mixing the incoming plain text and converting it into the final cipher text result. Cipher text is text that not everyone understands.

10.1. Proposed research methodology:

According to this research methodology, a user can manage Amazon cloud services using the RESTFUL API, integrate the cloud service with complete security, in our previous work [17] we already mentioned how to apply security in mobile computing before moving to cloud computing, but from - the battery is time consuming. This model shows how to overcome problems using the same methodology and without the "QOS" effect.

IMPLEMENTATION:

As shown in Figure 5, the application of the cloud is possible in many areas. One of the areas we're currently interested in is mobile phones. Hence, we will focus on the usefulness of the cloud computing environment for mobile use and how can the cloud improve the overall functionality and performance of mobile devices? According to [9], as shown in Figure 2, MCC is a service that allows mobile users with limited resources to adaptively adjust processing and storage capabilities by transparently sharing and disconnecting resource-intensive computing and data-intensive jobs on traditional cloud resources, providing ubiquitous wireless access.

As shown in Figure 5, this architecture shows that the first step of mobile data is sent to a private cloud server, which is responsible for data encryption and cryptography. The encrypted data then goes to the cloud server, which is publicly available and is responsible for storing the data in the cloud database, which is the storage of the EC2 database.

The communication between mobile cloud computing is now secure, security exists on a cloud server that is in a private and secure location, and the public cloud is only responsible for storing encrypted data in a data warehouse. Thus, the user can safely share their important data on the cloud server without any hindrance. This concept may take a while, but is very secure for mobile cloud computing.

Authentication and authorization are useful for this architecture, now security flows can arise through this architecture.

DEPLOYED APPLICATION:

Build an Android app using the IBM Mobile Data for Blue Mix cloud service Store, delete, update, and query objects stored in the cloud

Step-1 Add a few items to your shopping list

Step - 2 Restart the application.

Please note that your data has been saved. You now have your data in the cloud!

Step - 3 View your data in the cloud

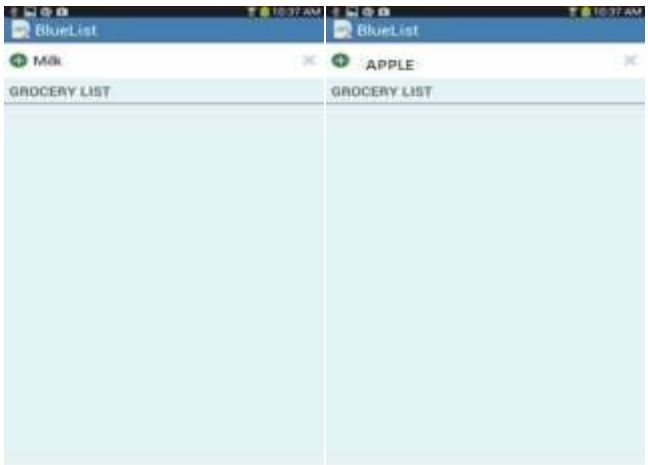
Log into Blue mix .

Click your application in the toolbar.

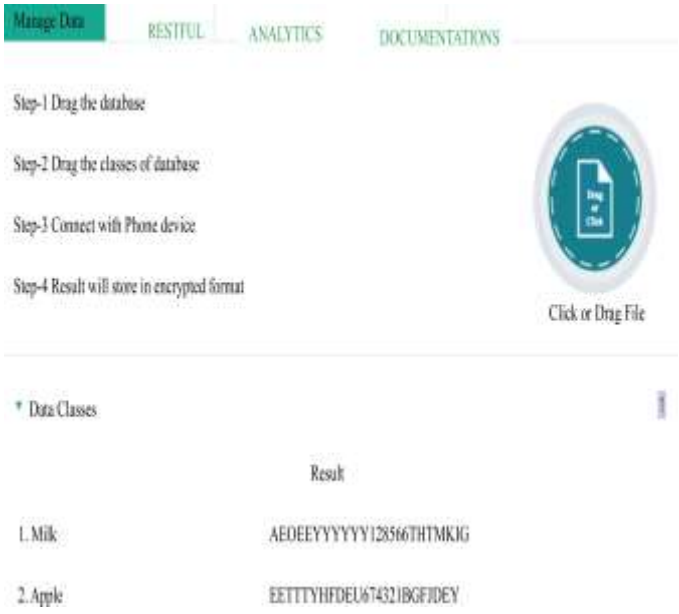
Step - 4 On the Data Management tab, you can see the encrypted data classes stored in the cloud, as well as the instances of each data class being saved.

Step - 5. You can reverse-decrypt your data when you access the data on your mobile device again.

Click Mobile Data Service. Application interface.



Dashboard



CONCLUSIONS:

The concept of cloud computing provides users with an excellent opportunity to use their services on a database on demand. The demand for mobility in cloud computing has spawned mobile cloud computing. MCC provides more options for convenient access to services. A number of mobile users are expected to switch to cloud computing on their mobile devices in a few years.

There are many challenges in mobile cloud computing due to the limitations of mobile devices. Security is a top concern in mobile cloud computing. In mobile cloud computing, the owner's data is stored in the cloud, which is not secure.

This document describes the fundamentals of mobile cloud computing and the challenges associated with it. They mainly talked about the security of data stored in the cloud and the importance of data security. This paper explored a number of data security mechanisms so that mobile cloud computing can be widely adopted by a range of users in the future. He also proposed a mechanism for ensuring privacy, access control, and integrity for mobile users.

References

1) Abrishami S. and Nagibzadeha M. (2012) Time-bound workflow scheduling algorithms for infrastructure as a cloud of services.
2) Armbrast, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konvinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoyka, I. and Zachariya, M. (2013) Above the Clouds: Berkeley's Perspective on Mobile Cloud Computing. Technical Report, EECS Department, University of California, Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html
3) http: // nvlpubs. nist. gov / nistpubs / Legacy / SP / nistspecialpublication 800-145. pdf
4) John R. (2005) Department of Defense Directive 3020.40, Mobile Cloud Critical Infrastructure Protection Program. August 19, p.13.http: //www.dtic.mil/whs/directives/corres/pdf /302040p.pdf
5) Ouyang, XZ (2011) Cloud computing in mobile networks. New technologies for the future of multimedia coding, analysis and transmission, no. http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2011Year/no3/articles/201110/t20111029_260205.html
6) Li, HR, Qian, L.Kh. and Yang, J. (2015) Planning a workflow with deadline and time slots in mobile cloud computing. 19th IEEE International Conference on Collaboration with Computers in Design (CSCWD), Calabria, May 6-8, 2015, 606-613. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7231027
7) (2011) Blog of Adrian Otto. What is a cloud platform? http://adrianotto.com/2011/02/cloud-platform/

8) Pooja, N.D. and Ramteke, P.L. (2013) Mobile Cloud Computing. International Journal of Science and Research.
9) Hampton, TJ. (2011) A quick guide to cloud terminology. 11th August. http://www.thehostingnews.com/a-quick-guide-to-cloud-terminology.html
10) Lahan A. (2015) Data security and privacy through mobile cloud computing.
11) [11] Rahman, M. and Hassan, R. (2015) Adaptive workflow planning for dynamic grid and cloud computing environments.
12) Singh R. (2015) Planning workflows in cloud computing using spot instances.
13) Kaur, N. (2015) Comparison of workflow planning algorithms in cloud computing.
14) Kaur, A. (2015) Review of workflow planning in a cloud computing environment.
15) Singh L. and Singh S. (2015) Review of workflow planning algorithms and research questions.
16) Lakhan A. and Hussein F. (2015) Data security and privacy for crossplatform computing using mobile cloud computing.
17) Lakhan, A.A. (2015) Integration of a double data security algorithm for mobile private cloud computing.