Journal of Computer Science Engineering and Software Testing
Volume 2 Issue 1

Cloud Security Using AES Algorithm

Akash V. Zawar, Komal Yadav, Swapnali Deshkar, Chaia Mahale, Amol Gaikwad

Department of Information Technology,

YCCE, Nagpur, India

E-mail: azawar123@gmail.com, komalashokyadav@gmail.com, mahalechhaya04@gmail.com, swapnalideshkar95@gmail.com

Abstract

This paper proposes an overview of an android application which uses cloud service and provides a network to user for securing data over cloud by storing it in encrypted format. This data could only be retrieved with the help of key which is provided by the application to the user. The main aspect of cloud computing is how one can Secure, Protect and Process the data Cloud computing is a technology that is recently developed for complex systems with large-scale services sharing among multiple users. Therefore, authentication and integration of both users and services is a significant issue for the trust and security of the cloud computing unique platform has brought new security issues to contemplate. Cloud computing is essentially the management and provision of applications, information and data as a service. Using key based Cryptography technique we propose and implement a new algorithmic approach for cloud security in this paper. The efficiency of the algorithm can be improved by integrating multiple cryptography algorithms. To ensure the data security, we proposed a method by implementing AES algorithm.

Keywords: *Cloud computing, authentication, integration, cryptography, data security, AES algorithm*

INTRODUCTION

Cloud computing is a resource delivery and usage model. It means to obtain resource where by shared software, hardware and other information are provided to computers and other devices as a metered service via network. If your paper is intended for a conference, please contact your conference editor concerning acceptable word processor formats for your particular conference. Cloud computing model is very exciting model especially for business peoples [1, 2]. Many business peoples are getting attracted towards cloud computing model because of the features easy to manage, device independent, location independent. But this cloud models comes with many security issues. A business person keeps crucial information on cloud, so security of data is crucial issue as probability of hacking and unauthorised access is there. Also availability is a major concern on cloud.In order to reduce threats, vulnerability, risk in cloud environment, consumers can use cryptographic methods to protect the data, information and sharing of resources in the cloud computing.

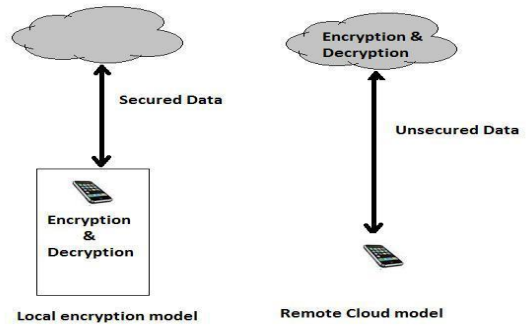
USER INTERFACE

As per the project is for security it will have a very basic GUI. It will only allow the authenticated use to login and for new user there is an available option of registration on the main page. The new user has to register by providing a valid information's about him. The registration will make a new entry in the user detail database and the person will now be an authenticated person to use the software. The GUI is being developed in the JSP. We are being using the SQL database as our background storage of user information [3, 4].

CRYPTOGRAPHIC APPROACH

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. We propose a suitable method that cryptographic algorithms with different key lengths are used in various environments. The number of mobile devices such as smart phones and smart pads grows rapidly recently [5]. End users can access easily to cloud computing environment thought these mobile devices we define that mobile cloud computing is one of specific services of cloud computing and it is a mobile

service which is added a cloud computing service. According to key characteristics, modern cryptosystem can be classified into symmetric cryptosystem, asymmetric cryptosystem and digital signature. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), AES (Advanced Encryption Standard). For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret [6, 7].



OBJECTIVE

Cloud computing is emerging technology that says renting is better than buying as its application need not to be installed on user computer and can be accessed from different places just by paying the rent. Security is also important when you perform any work on cloud server like storage of data, running application etc. for that purpose we have to send the data in cryptographic manner. The general objective of this project is to contribute to the development of these cloud systems as well as to study the technical impacts of a state-of-the-art prototype. More specifically, a secured storage on cloud will be developed, which will take advantage of recent advances in the areas of cloud computing and development, data storage and security, parallel and distributed software engineering and networking techniques. This prototype will be tailored to the specific needs of cloud exploration; furthermore, it will be particularly suitable for areas such as education, training, business, electronic commerce. Thus, the overall objective of this project is to develop a system that stores user data on cloud in a secured manner. In other words, the general aim of the project is to offer a concrete contribution to the creation (and evaluation of its impact) of the Information Society in the Cloud computing region [8, 9].

This general objective can be broken down to three more specific objectives that would together achieve the overall goal of the project as follows:

- Developing Cloud Server.
- Designing User Interface.
- Developing Cryptography Tool.

TECHNOLOGY

JAVA

Java is a Programming language originally developed by James Gosling at Sun Microsystems and released in 1995 as a core component of Sun Microsystems' Java Platform. The language derives much of its Syntax from C and C++ but has a simpler object Model and fewer low-level facilities. Java applications are typically compiled to byte code (class file) that can run on any Java Virtual machine (JVM) regardless of computer architecture [10].

It takes a sophisticated programmer to create Java code and it requires a sophisticated programmer to maintain it. With Java, you can create complete applications. Or you can 20 attach a small group of instructions, a Java "applet" that improves your basic HTML. Java is a powerful programming language with excellent security, but you need to be aware of the tradeoffs. The internet help catapult java to the forefront of programming and java in turn, has had a profound effect. We decided to use java for building this project because it is the best platform for building this project, it is highly secure language and it also includes the following features.

- Simplicity.
- Portability.
- Security.
- Robust.
- Object Oriented.

JDBC (Java Database Connectivity)

JDBC technology is an API (included in both J2SE and J2EE) that provides cross-DBMS connectivity to a wide range of SQL databases and access to other tabular data sources, such as spreadsheets or flat files.

Steps for JDBC Programming:

- Create database.
- Create ODBC DSN by specifying details of database.
- Import java.sql package.
- Create object of JDBC driver like connection, statement, result set.
- Load the suitable JDBC driver to communicate with database through DSN.
- Initialize the connection object with the help of driver manager by specifying the name of DSN.
- Initialize the statement object the help of connection.
- Fire SQL query with the help of statement object.
- Close the object in the reverse order of their creation.

JavaScript

JavaScript is a simple programming language that was developed by Netscape that writes commands to your browser when the HTML page is loaded. JavaScript is the most popular scripting language on the internet and works in all major browsers, such as Internet Explorer, Firefox, Chrome, Opera and Safari. JavaScript adds interactivity to HTML pages JavaScript is a scripting language. Everyone can use JavaScript without purchasing a license. Write software on one platform and run it on virtually any other platform. JavaScript is usually embedded in directly into HTML pages. A Scripting language is a lightweight programming language. JavaScript is an interpreted language (means that scripts execute without preliminary compilation).

Microsoft AZURE

Any developer or IT professional can be productive with Azure. The integrated tools, pre-built templates and managed services make it easier to build and manage enterprise, mobile, Web and Internet of Things (IoT) apps faster, using skills you already have and technologies you already know. Azure supports the broadest selection of operating systems, programming languages, frameworks, tools, databases and devices. Run Linux containers with Docker integration; build apps with JavaScript, Python, .NET, PHP, Java and Node.js; build back-ends for iOS, Android and Windows devices. Azure cloud service supports the same technologies millions of developers and IT professionals already rely on and trust. Some cloud providers make you choose between your datacentre and the cloud. Not Azure, which easily integrates with your existing IT environment through the largest network of secure private connections, hybrid database and storage solutions and data residency and encryption features-so your assets stay right where you need them. And with Azure Stack, you can bring the Azure model of application development and deployment to your datacentre. Azure hybrid cloud solutions give you the best of both worlds: more IT options, less complexity and cost. This is why it is one of the best cloud services available. We know some organisations are still wary of the cloud. That is why Microsoft has made an industry-leading commitment to the protection and privacy of your data. As the best cloud service from Microsoft, Azure runs on a worldwide network of Microsoft-managed data centres across 22 regions-more countries and regions than Amazon Web Services and Google Cloud combined. This fast-growing global

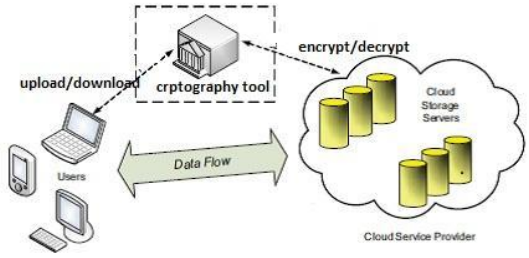
footprint gives you lots of options for running applications and ensuring great customer performance.

Java Cryptography Architecture (JCA)

The Java Cryptography Architecture (JCA) is a framework for working with cryptography using the Java programming language. It forms part of the Java security API and was first introduced in JDK 1.1 in the java. Security package. Java security technology includes a large set of APIs, tools and implementations of commonly-used security algorithms, mechanisms, and protocols. The Java securities APIs spans a wide range of areas, including cryptography, public key infrastructure and secures communication, authentication and access control. Java security technology provides the developer with a comprehensive security framework for writing applications and also provides the user or administrator with a set of tools to securely manage applications. The JCA offers a set of APIs that allow users to query which providers are installed and what services them support. This architecture also makes it easy for end-users to add additional providers. Many third party provider implementations are already available.

SOFTWARE DESIGN

Security is also important when you perform any work on cloud server like storage of data, running application etc. For that purpose we have to send the data in cryptographic manner. The following figure illustrates the flow of project. Data flows from user to the cloud server and vice-versa. User can make use of cryptographic tool if he wishes. Cryptographic tool encrypts data and stores it on server. If the user requests an encrypted file, the cryptographic tool decrypts the file and sends it to the user. This project is designed in 3 main modules:



Cloud Document Server

A Server where a user can store documents. It will be a network application which will use xml based command request to perform operations. It will maintain user registry. It will also maintain storage space of all users Will Store user documents in user space.

Web Application

It will provide an interface between cloud server and end user who wants to store documents. It will provide interface to register new users with cloud server. Will send user registry request to server for registration.Will provide a login interface and will send login information to cloud server. It will provide an interface to upload and download documents.

Cryptography Tool

It is a desktop application which will perform cryptographic operations. This tool can be downloaded from the web application for security. This tool will use AES algorithm for cryptography. It will generate a new AES key whenever requested. This key will be used to encrypt documents. These encrypted documents can be sending to the cloud server by using web interface.

CONCLUSION

In the older techniques these cryptographic algorithms are implemented in the Single system environment. Now due to availability of high performance computing techniques, similar test has been conducted in the single system Environment, i.e., local environment and also in the Cloud environment. From the observed results and based on the considered parameters, storing the mobile data in cloud increases the efficiency. Also, the results reveal that AES algorithm qualifies better than other algorithms in Mean processing time.

FUTURE SCOPE

Cloud computing can play a significant role in a variety of areas including innovations, virtual worlds, e-business, social networks or search engines. But currently, it is still in its early stages, with consistent experimentation to come. Cloud computing solutions are currently used in settings where they have been developed without addressing a common programming model, open standard interfaces, adequate service level agreements or portability of applications. Neglecting these issues current Cloud computing offers force people to be stranded into locked, proprietary systems. Developers making an effort in codifying their applications cannot port them elsewhere. Moreover, users put in the hands of commercial providers applications and data without negotiable quality of service agreements.

REFERENCES

1. Jaber, A.N., Bin Zolkipli M. F. Use of cryptography in cloud computing. *Control System, Computing and*

Engineering (ICCSCE), 2013 IEEE International Conference on Year; 2013.

2. Sabahi F. Cloud computing security threats and responses. *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on 2011*.
3. Okubo T., Wataguchi Y., Kanaya N. Threat and countermeasure patterns for cloud computing. *Requirements Patterns (RePa), 2014 IEEE 4th International Workshop on Year*; 2014.
4. Huifeng Wang, Zhanhuai Li, Xiaonan Zhao et al. A scheme to ensure data security of cloud storage. *Service Operations and Logistics, and Informatics (SOLI), 2013 IEEE International Conference on Year*; 2013.
5. What is Cloud Computing. Retrieved April 6, 2011. Available at: http://www.microsoft.com/business/en gb/solutions/Pages/Cl oud.aspx.
6. Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. White Paper. Information.
7. Z. Zhou, D. Huang. Efficient and secure data storage operations for mobile cloud computing. *IACR Cryptology ePrint Archive*; 2011.
8. Shashi Mehrotra Seth, Rajan Mishra. Comparative analysis of encryption algorithms for data communication. *IJCST*. 2011; 2(2).
9. Pearson S., Y. Shen, M. Mowbray. A privacy manager for cloud computing. *In Proceedings of the 1st International Conference on Cloud Computing*. 2009; 90 –106p.
10. Liu Q, Wang G, Wu J. Efficient sharing of secure cloud storage services. *In: 2010 IEEE 10th International Conference on Computer and Information Technology (CIT10)*. 2010; 922–929p.