



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijirce.com](http://www.ijirce.com)

Vol. 7, Issue 5, May 2019

## Feasibility of Implementing Multi-Factor Authentication Schemes in Mobile Cloud Computing

Miss. Nikita Borade<sup>1</sup>, Prof. Dr. J.R. Prasad<sup>2</sup>

PG Students, Dept. of Computer Engineering, Sinhad College of Engineering, Pune, India

Professor, Dept. of Computer Engineering, Sinhad College of Engineering, Pune, India

**ABSTRACT:** Previous technology is major challenge in cloud and mobile cloud computing is to ensure security and privacy of users personal information (e.g., financial data, health record, location information) from malicious attacks. It is important for a cloud service provider (CSP) to establish trust and gain confidence by providing proper security and privacy to the clients. Authentication is important for establishing accountability and authorization of the users while allocating cloud resources. In this system, we discuss different authentication techniques proposed method is knowledge based and location based. In the knowledge based module the username and password is required for user authentication. In Location based module if user is accessing a file within particular geographical location then only user can access files otherwise not. We categorize the algorithms based on its input, i.e. the credentials required for validating users. However, we emphasize that the classification is not precise, as it is difficult to classify the authentication algorithms relying on more than one user credentials (multi-factor authentication). The proposed authentication process is more efficient, secure and user friendly.

**KEYWORDS:** Cloud Computing, Mobile Cloud Computing, Multi-factor Authentication

### I. INTRODUCTION

Mobile and handheld devices are constrained due to resource limitations primarily caused by limited battery life requiring recharging, constrained size of memory or limited power of the processor especially during roaming and challenge of being seamlessly connected throughout mobility or even limited size of physical persistent storage. Execution of high computational tasks in a mobile device may also drain the battery power very quickly. To address these limitations of mobile devices, cloud computing can be an obvious choice, this means that mobile users offload processing intensive and storage demanding portion of mobile application from resource constraint mobile device to resource enriched cloud. The offloading of the processing intensive and storage demanding portion(s) of mobile application enhances the capabilities of mobile devices in term of processing, storage, and battery.

### II. LITERATURE SURVEY

In this Paper system proposes a location-aware attribute-based access control scheme for cloud storage, in which the location information is flexibly set as trapdoors inside fundamental access policies of CP-ABE, and trapdoors are released with the help of location servers. The trapdoor approach makes that the change of users' locations will not cause revocation of users' attributes. Our analysis shows that the above approach is effective and our proposed LABAC brings little overhead to data consumers, attribute authorities and the cloud. [1]

In this paper, we have covered several novel technologies that use mobile devices to access different services from anywhere and anytime. The definitions, the advantages and the architecture of each technology are explored. The mobile cloud computing technology was taken, recently, more consideration a caused to its importance. Because mobile devices in continuous and quick development, they are taken a care from IT developers. Mobile cloud computing will be the dominate technology and the trend now is to develop new applications and to remodify the old



# International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 7, Issue 5, May 2019

applications to be mobile cloudy. We tried to prove that this technology will conquer the challenges and the problems of preceding technologies. Mobile cloud computing models are presented. These models try to alleviate the problems concerning the limited resources in mobile devices. Despite the enormous development of mobile devices and the support of mobile cloud computing to mobile devices, they still take a lot of attention of researcher because a number of challenges encounter this technology. We are interested to work in this domain and, for future research; we will concentrate on its challenges and explore it deeply. [2]

In this paper, we have undertaken a systematic literature review of mobile cloud computing (MCC), in order to understand the trend of research interests so far in MCC, in terms of the least and most researched issues. We were able to highlight some of the challenges in MCC such as privacy, security and trust, fault tolerance, mobility management, network congestion, heterogeneity and connection protocols, resource constraint and platform heterogeneity, context awareness, presentation and usability issues, battery life and energy awareness, and cloud API Security Management. [3]

In this paper, we tend to propose a unique authentication theme for mobile cloud computing, Data Digest-based Authentication consists of 3 phases: registration, authentication, and update. With these phases, Data Digest Authentication utilizes hashing, additionally to traditional user id and secret primarily based authentication, to make sure confidentiality and integrity throughout the authentication method. It can survive a range of various attacks, like man-in-the-middle, replay attacks, etc. [4]

Cloud computing is the present and futuristic resource pooling paradigm which converges with the Internet of Things (IoT). However, there are authentication and key management issues to be resolved. Identifying users is not an easy task in cloud. As a result in this article we proposed a provably secure multi-factors authentication scheme with trusted third party. In our approach, trustee distributes the authentication tokens on behalf of cloud service providers and allows the cloud servers just to verify the hashed key credential data. This approach also ensures the mutual authentication of the communication entities. We used multi-party station to station Diffie-Hellman key exchange protocol which overcomes many key management problems. Our proposed mechanism preserves the privacy of the remote authentication details in the cloud and significantly helps to protect the stakeholder's sensitive information from the inside and outside malicious attackers. [5]

### III. EXISTING SYSTEM

In the existing system several challenges, including security and privacy are raised from the adoption of this IT paradigm. A major challenge in cloud and mobile cloud computing is to ensure security and privacy of users personal information (e.g., financial data, health record, location information) from malicious attacks. It is important for a cloud service provider (CSP) to establish trust and gain confidence by providing proper security and privacy to the clients.

### IV. PROPOSED SYSTEM

In this paper, system proposed authentication scheme provides a true protection for the user credentials in the cloud. Therefore the problems and risks envisioned in the previous section can be achieved. Advanced Encryption Standard (AES) algorithm is used for symmetric encryption/decryption of communication data between users and servers. A major challenge in cloud and mobile cloud computing is to ensure security and privacy of users personal information (e.g., financial data, health record, location information) from malicious attacks. It is important for a cloud service provider (CSP) to establish trust and gain confidence by providing proper security and privacy to the clients. Authentication is important for establishing accountability and authorization of the users while allocating cloud resources. These days, mobile devices are built with features that allow them to access the clouds resources. The devices are made to easily access the resources due to their portability and ease of use. The mobile devices have two main purposes in MCC. Firstly, the mobile devices serve as the client to retrieve resources out of the cloud since the devices themselves have limited storage and processing capacity thus the use of the cloud. In this case, mobile devices can access to computation and storage resources of cloud service providers. This architecture is the same as the client server architecture. The second purpose of the mobile device is to act the node for the cloud where resources are

# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijirccce.com](http://www.ijirccce.com)

Vol. 7, Issue 5, May 2019

gathered from all the mobile devices that are participating to solve the problem of processing power and limited storage.

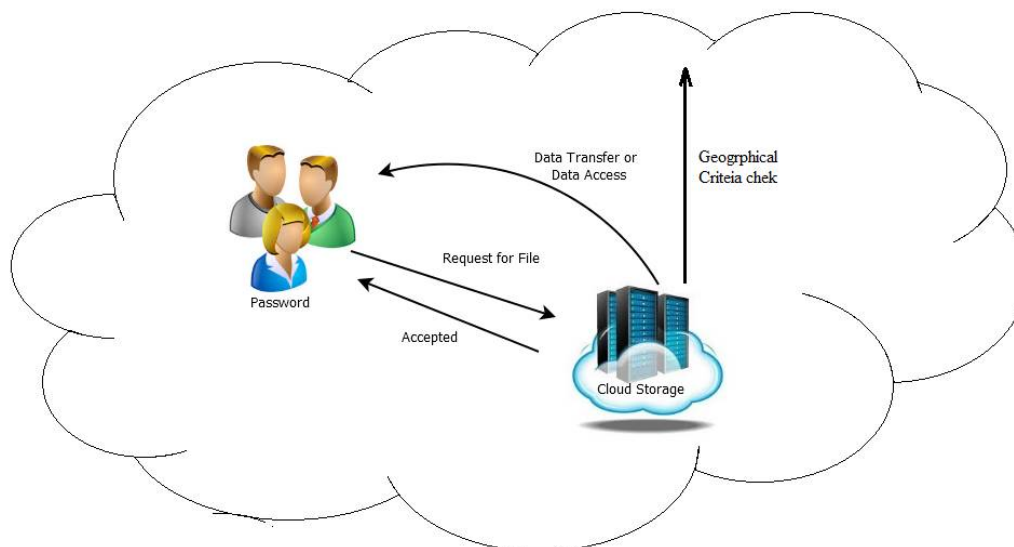


Fig 1: System Architecture

## V. ALGORITHM

### Algorithm 1: AES

#### Key Expansions

For each round AES requires a separate 128-bit round key block plus one more.

#### Initial Round

Add Round Key with a block of the round key, each byte of the state is combined using bitwise XOR.

#### Rounds

Sub Bytes in this step each byte is replaced with another byte.

Shift Rows for a certain number of steps, the last three rows of the state are shifted cyclically.

Mix Columns a mixing operation which operates on the columns of the state, combining the four bytes in each column.

Add Round Key

Final Round (no Mix Columns)

Sub Bytes

Shift Rows

## VI. RESULT

The system has been developed in java. Each entity is tested by deploying them on individual machines. The cloud, Owner, AA, CA and Observer deployed on core I3 processor with 4GB RAM. Client system uses I3 processor with 2GB RAM. JRE-1.8 is installed on each system. The system used jdk 1.7, IDE: Netbeans 8.2 and Adrive cloud for development. Mysql 5.3 database is used for database storage. For implementation of the system users business structure has been followed. The system user's structure along with designation given below:

- Consider a situation, where a user wants to share his/her data with manager and developer of branch 1 and 2 and to generate keys following attributes will be required.
- Branch1-manager branch1-developer
- Branch2-manager branch2-developer

# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijirccce.com](http://www.ijirccce.com)

Vol. 7, Issue 5, May 2019

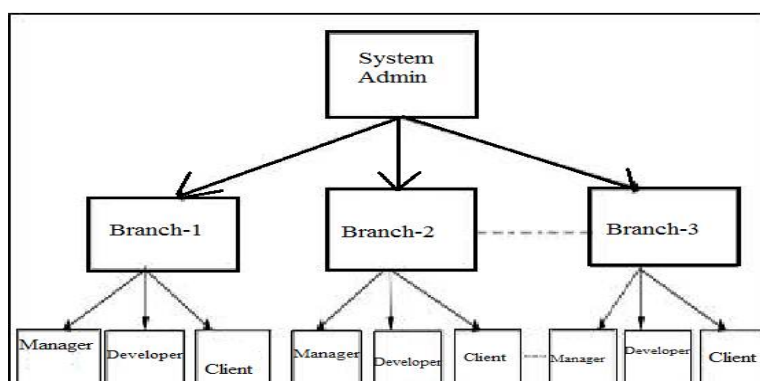


Fig 2: Work Break-Down Structure

Table: Performance Analysis

File size in MB	Key generation Time in milliseconds	Encryption Time in milliseconds	Decryption Time in milliseconds
1	219	5342	7949
2	213	8970	14321
3	214	14307	23579
4	212	17423	27357
5	229	20342	32572

- The system calculated time needed for key generation. For 10 users the average time needed is 30 mili Seconds. The system is working on secret key distribution and its management. Finishing the complete system implementation, the system will evaluate its performance with
- Uploading and downloading time for different sizes of files.
- Key distribution and file sharing times.



Fig 3: Home Page

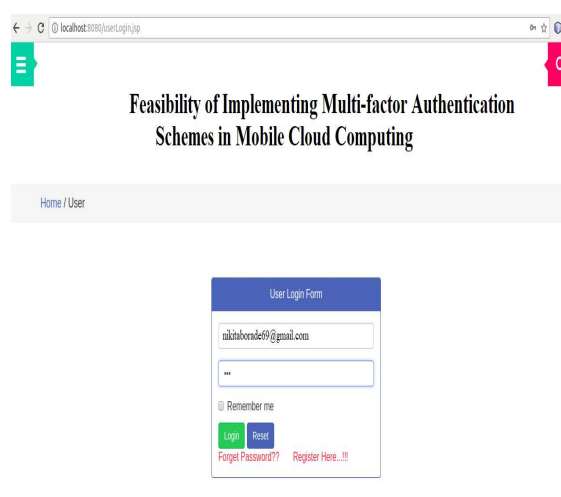


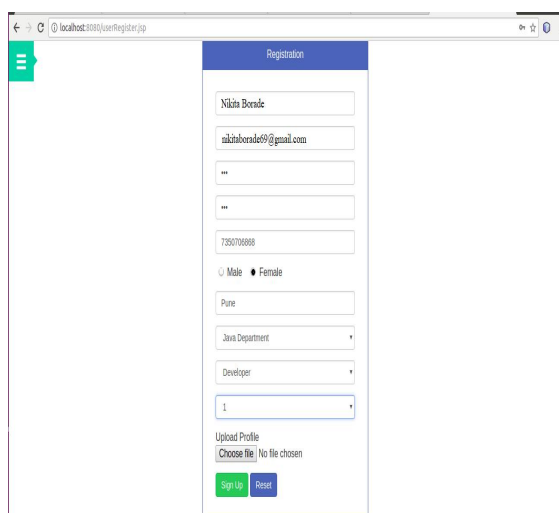
Fig 4: User login

# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijirccce.com](http://www.ijirccce.com)

Vol. 7, Issue 5, May 2019



The screenshot shows a web browser window with the URL localhost:2080/userRegister.jsp. The page title is "Registration". The form contains the following fields: Name (Nikita Borade), Email (nikitaborade69@gmail.com), Password (two fields), Phone (7350706688), Gender (radio buttons for Male and Female), Location (Pune), Department (Java Department), Job Profile (Developer), and Experience (1). There is also an "Upload Profile" section with a "Choose File" button and a "No file chosen" message. At the bottom, there are "Sign Up" and "Reset" buttons.

Fig 5: User Registration



The screenshot shows a web browser window with the URL localhost:2080/userRegister.jsp. The page title is "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing". The page content includes a navigation bar with "Home / User" and "Welcome nikitaborade69@gmail.com". Below the navigation bar, there is a "View Profile" button. The profile information is displayed as follows: Name: Nikita Borade, Email: nikitaborade69@gmail.com, Password: 123, Phone: 9990430022, Gender: Female, Location: Pune, Job Profile: Developer, and Experience: 2. There is also a "Profile Pic" section with a placeholder image.

Fig 6: View Profile

## VII. CONCLUSION

This system proposed an authentication mechanism in mobile cloud computing with combining the two factor authentication and one time dynamic password called OTP token that suitable for mobile device. The generated token is based on geographical location system. To protect user confidential information, data should be accessible to authenticated people. To gain this aim, different authentication methods are proposed. In multi-factor authentication, more than one authentication factor is used. However, this kind of authentication offers better security and privacy. The proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. This scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users requests. It has been proposed an auditing method to trace an attribute authority's potential misbehavior. It has been conducted detailed security and performance analysis to verify that this scheme is secure and efficient.

## REFERENCES

- [1] Yingjie Xue, Jianan Hong, A Location-aware Attribute-based Access Control Scheme for Cloud Storage.
- [2] Erlangung des doktorgrades, Biometric cryptosystems: authentication, encryption and signature for biometric identities.
- [3] Ahmed Dheyaa Basha, Mobile Applications as Cloud Computing: Implementation and Challenge.
- [4] Prof. Mamta sharma, Study on mobile cloud computing, it's architecture, challenges and various trends.
- [5] Zhangjie Fu, Xingming Sun towards Efficient Content-aware Search over Encrypted Outsourced Data in Cloud.