# Dynamic Key Generation Algorithm for User Authentication at Mobile Cloud Enviroinment

**Deepak G[1], Dr. Pradeep. B. S[2], Shreyas Srinath[3]**

[1] Department of Computer Science & Engineering, Dayananda sagar college of Engineering, Bangalore, India

[2]Director, International R&D department, Linyi Top Company Ltd., Linyi, Shandong Province, China-276023

[3]Department of Information Science & Engineering, Dayanada sagar college of Engineering, Bangalore, India

**Abstract:** ***Cloud computing is an emerging concept combining many fields of computing. The motive of mobile cloud computing is to deliver the services, software and processing capacity over the Internet so far to reduce the computation cost and increase the storage capacity. The goal of this paper is to implement a user authentication algorithm, which can be used in cloud storage to verify the authenticity of the user. In this paper we build a secure mobile cloud-based algorithm, where the user's mobile phone is used as an authentication device, presenting a onetime encrypted password for the user and password is decrypted using proposed algorithm in user's mobile application.***

**Keywords:** virtual machine, thin client, fat client, OTP component, cloud, IaaS, PaaS, SaaS.

## 1. Introduction

Cloud computing is a distributed computing over a network, where the application may run on many connected computers at the same time. Emerge of cloud computing has empower the possibility of doing complex calculations, mass storage and device operations to the cloud in a powerful way. The most common login form used today, is the use static passwords. Cracking of Static passwords is achieved without much great effort, since users prefer un-complicated passwords. The users also rarely change their passwords or use the same password to access multiple services [8]. The major challenge we face is securing the information on the cloud when many users are accessing the cloud services.

In this paper we propose the user's mobile phone as an authenticating device presenting a onetime password for the user, and assuming most people always carry their phone with them, the problem with a separate authentication device for two-factor authentication is solved. As the mobile gives the user a encrypted one time password, the problem with static passwords for logins is also solved. The aim of this paper is to implement a authentication solution, which can be used in cloud services. The authentication method will be two-point authentication with a mobile phone as an authentication device, that decrypts the key (sent to client mobile) which is generated by key generator as shown in figure 1 which is valid one time for a certain amount of time. The decrypting key mobile application will only be given to the user after a successful login with username/unique number with password, which is discussed in pre-phase and phase 2 in section 4.

## 2. Issues relating to Mobile Applications

Several researchers have identified the fundamental challenges in mobile computing. Since mobile devices have constraints on resources (clock speed, ram, cache memory) and also on continuously changing of operation environment, Mobile devices intrinsically have and will continue to have limited resources as processing power, memory capacity, display size, and input forms. These have been the forming factors of existing mobile application approaches [11].

### A. Offline Applications

Most of the applications available for modern mobile devices fall into this category. They act as fat client that processes the presentation and business logic layer locally on mobile devices with data downloaded periodically from backend systems. There is regular intervals synchronization between the client and backend system [12]. A fat client is a networked application with most resources available locally, rather than distributed over a network as is the case with a thin client. Offline applications, also often called native applications, offers: 1. Good integration with device functionality and access to its features 2. Performance optimized for specific hardware and multi- tasking 3. Always available capabilities, even without network connectivity. On the other hand, the native applications have many disadvantages: 1. No portability to other platforms 2. Complex code 3. Time needed to come to market is more 4. A requirement for developers to learn new programming languages [2].

### B. Online Applications

An online application assumes that the connection between mobile devices and backend systems is available most of the time, but there are problems related to it such as cross-platform issues. Adoption of Web technologies in online application can overcome them; applications based on Web technology are an effective alternative to native applications [10]. Mobile has the capacity to overcome some of the dis-advantages of offline applications like 1. They work on multi-platform 2. Directly accessible from anywhere as it runs on GSM (Global System for Mobile Communications) network 3. Knowledge of Web technologies is extensively used among developers, greatly minimizing the learning curve required to start creating mobile applications, as the single application developed for one platform generates code automatically for other platforms ex: IBM's open source worklight software. However, mobile Web applications have disadvantages too: 1. As there is latency in processing session may terminate because of delay in accepting/receiving the information 2. Sensor's, camera and other features are not accessible 3 Complex situations where it requires session over long period cannot be handled.

### C. Issues with Offline and Online Mobile Applications

All most all the ongoing application's execution happens on the device or on backend systems so they are statically partitioned. However, mobile clients can face broad variations and abrupt changes in network conditions and local resource availability when accessing remote data and services. As a result, all application types and devices do not satisfy one partitioning model. In order to setup applications and systems to continue to operate in such dynamic environments, mobile cloud applications must react with dynamical adjusting of the computing functionality without compromising computational power between the mobile device and cloud depending on circumstances. Cloud has to be flexible and robust in response for the computation of clients and also to the changes in mobile computation environments [1].

## 3. Related Work

Paper titled “Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities” by Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal [4]. presents a 21st century vision of computing; identifies various computing paradigms promising to deliver the vision of computing utilities; defines Cloud computing and provides the architecture for creating market-oriented Clouds by leveraging technologies such as VMs; provides thoughts on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA(Service Level Agreement) oriented resource allocation; presents some representative Cloud platforms especially those developed in industries along with our current work towards realizing market-oriented resource allocation of Clouds and concludes with the need for convergence of competing IT paradigms for delivering our 21st century vision.

Christina Hoffa, Gaurang Mehta, Timothy Freeman, Ewa Deelman, Kate Keahey, Bruce Berriman, John Good. Their paper explores the use of cloud computing for scientific workflows, focusing on a widely used astronomy application-Montage. The approach is to evaluate from the point of view of a scientific workflow the tradeoffs between running in a local environment, if such is available, and running in a virtual environment via remote, wide-area network resource access. Their results show that for Montage, a workflow with short job runtimes, the virtual environment can provide good compute time performance but it can suffer from resource scheduling delays and wide area communications [14].

Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues. To address the problem of confidentiality and integrity of data and computation they propose a design of trusted cloud computing platform (TCCP). TCCP enables Infrastructure as a Service (IaaS) providers such as Amazon EC2 to provide a closed box execution environment that guarantees confidential execution of guest virtual machines[15][1]. Moreover, it allows users to attest to the IaaS(Infrastructure as a Service) provider and determine whether or not the service is secure before they launch their virtual machines.

Ari Juels and Burton S. Kaliski Jr. In this they defined and explored Proof of Retrievability which enables an archive service (prover) to produce a concise proof that a user (verifier) can retrieve a target file F. They explored POR(Partial Order Reduction) protocols here in which the communication costs, number of memory accesses for the prover, and storage requirements of the user are small parameters essentially independent of the length of F.A successfully executed POR assures a verifier that the prover presents a protocol interface through which the verifier can retrieve F [10].

Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik. In their paper, they construct a highly efficient and provably secure Provable Data Possession technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. PDP technique efficiently supports operations, such as block modification, deletion and append.

Mark Lillibridge Sameh Elnikety Andrew Birrell Mike Burrows. They present a novel peer-to-peer backup technique that allows computers connected to the Internet to back up their data cooperatively: Each computer has a set of partner computers, which collectively hold its backup data. By adding redundancy and distributing the backup data across many partners, a highly-reliable backup can be obtained in spite of the low reliability of the average Internet machine [9]. Because their scheme requires cooperation, it is potentially vulnerable to several novel attacks involving free riding (*e.g.*, holding a partner’s data is costly, which tempts cheating) or disruption. They defend against these attacks using a number of new methods, including the use of periodic random challenges to ensure partners continue to hold data and the use of disk-space wasting to make cheating unprofitable [3].

Jinyuan Li and David Mazi`eres. Their paper argues that wecan and should bind the system behavior beyond failures. They present BFT2F, an extension to the well-known Castro-Liskov PBFT algorithm, to explore the design space beyond failures. Specifically, BFT2F has the same interactions and consistency guarantees as PBFT when no more than f replicas fail as, with more than f but no more than 2f failures, BFT2F prohibits malicious servers from making up operations that clients have never issued and restricts malicious servers to only certain kinds of consistency violations[6].

## 4. Proposed Work

Our proposed method dynamic key generation for mobile cloud security includes six phases, where each phase has its own process involved in authentication.

**Pre-Phase:** The client should register with a unique number /user id and password by accepting all the regulations to use the cloud services. During this phase mobile client details are stored in the database of Authenticated server [5].

**Phase 1:** The mobile devices are connected to the mobile networks through base stations that establish and control the connections (air interface) and functional interfaces between the networks and mobile devices. Mobile users request and information are transmitted to the central processors that are connected to the servers providing mobile network services. Here, services like AAA (Authentication, Authorization and Accounting) can be provided to the users based on Home Agent (HA) and subscriber's data stored in databases. The subscriber's requests are then delivered to a cloud through the Internet. During requesting phase the client has to provide his unique number/user id and password which was given in pre-phase.

**Phase 2:** The authentication server receives the user id and password provided by client and searches of the perfect match. If the id and password both the entities matches then a confirmation notification message is sent along with dynamically generated key. The dynamic key is generated from the proposed encryption algorithm 1.If the user id and password did not match the message "accesses denied" is sent to the user.

**Phase 3:** In this phase of action, dynamic key is sent to the client on successful authentication during second phase. Dynamic key is a unique encrypted key which is generated and sent to user during each login session. It offers much higher security than static passwords, in expense of user friendliness and configuration issues [7]. This method is immune against password sniffing attacks, if an attacker use software to collect your data traffic, video records when you type on your keyboard, it doesn't matter since the password that the attacker gets hold on will not be valid to use as it keeps on changing during each session.

**Phase 4:** Data transfer between client and cloud are taking place in an unreliable medium, so unique encryption and decryption method of key plays a important role in secure data transmission. The user receives the unique encrypted key which is generated by Key generator (using the proposed algorithm 1), on successful login in the previous phases. The decrypting application is given to the user only on successful registering and by accepting all the terms and conditions, regulations of the company; the decryption method is the reverse process of encryption. Client decrypts the key by using decryption application which uses the algorithm 2, there by client obtains the original key, this key is sent to the authentication server to get access to the cloud storage.

**Phase 5:** In this phase the original key which is sent to the user after encryption and the key sent by user both are compared, if both the keys are matched then user is allowed to access the cloud storage. If the key does not match with that of the generated key for that client, then the access is denied as shown in Phase 6 of figure 1. During this phase the control terminates if the key did not match, then the user has to go through all the phases once again to get access to the cloud .This happens only when the decrypted key is wrong or an unauthorized user tries to access the cloud storage.

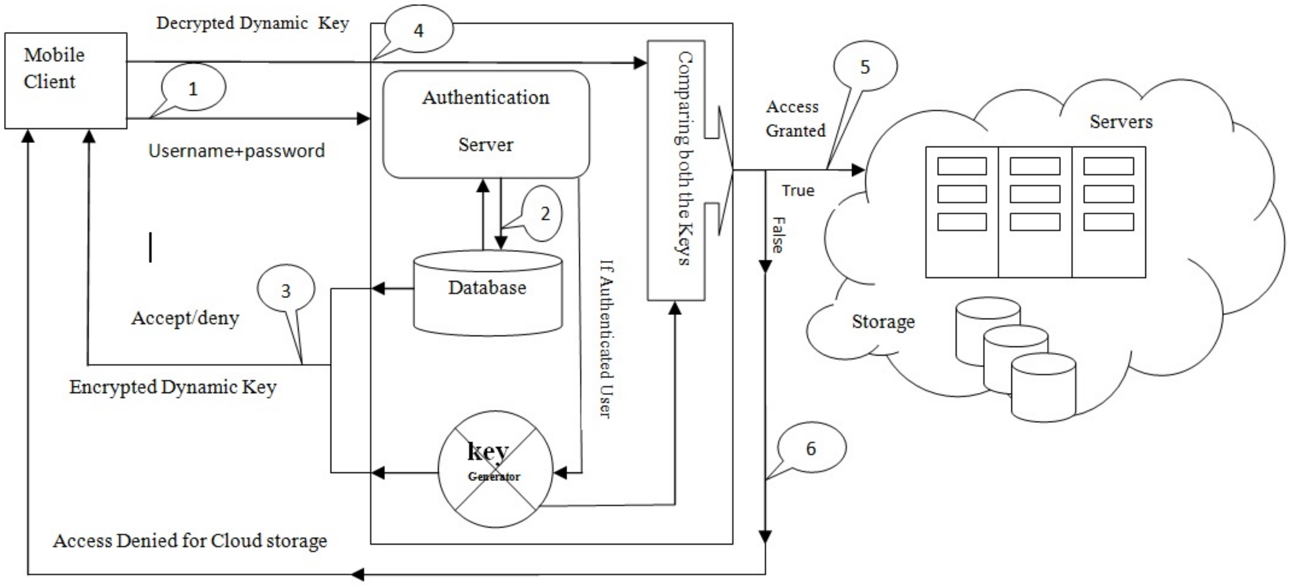

**Figure 1:** Proposed Security Architecture for mobile cloud environment

## 5. Algorithm

### Encryption Algorithm

**Step 1:** Generate Random String using random number Generator.
/*Generated random string includes [A-Za-z0-9] */
**Step 2:** Each character is converted to its equivalent ASCII Number [16].
**Step 3:** Apply log to the result obtained in step 2.
**Step 4:** Applying trigonometric function on the result obtained in the step 3 (like sine, cos...) and round/approximate the value to four decimal places.
**Step 5:** Transmit this generated key (result of step4) to mobile client.

### Decryption Algorithm

**Step1:** Receive the code sent by key generator from authentication server
**Step 2:** Shifting the number of decimal places indicated by the last bit of the encrypted key. /* if the key is 452322 the number of places shifted should be 2 so the value obtained is 45.232*/
**Step 3:** Applying inverse of sine function to the key/*this helps in the reverse process of getting the original key*/
**Step 4:** Applying antilog function to the result obtained.
**Step 5:** The result of step 4 will give the key in numerical format
**Step 6:** The result obtained in the step 5 is converted to ASCII to get the original key as string
**Step 7:** This key is sent to the authentication server for getting access to cloud storage

## 6. Results and Discussions

The Encryption method is implemented and tested in Matlab2012a version. Generating a random string of 20 characters using the equation 1.

str = char(33 + floor(94 .* rand(length,1)))';.....................(1)

In equation number 1 the variable length is set to fix length of 20 characters .The more number of characters in key ensures more secure. For testing reason the password is set to constant of 20 characters. The Matlab generated random strings and corresponding encrypted key generated for five test cases are shown below

**Table1:** Encrypted key for five random string

| Test case # | Random String Generated | Encrypted Key |
|---|---|---|
| 1 | $px`hfE^1c#;%*nb>z$J | 726061 |
| 2 | Dhk2OJ]cg:`^0,O{@X6g | 705041 |
| 3 | 8Pbt{T./9p8m7xA38ZMB | 704061 |
| 4 | {!imr(F9lIv29.-rWT.q | 732421 |
| 5 | [AQF(7,27H%uyON@uC+j | 694181 |

The last bit indicates the decimal point to be shifted during decryption, since the sine value gives the output in floating point for better transmission purpose that floating point value is converted to a integer and is appended with a number that indicates the number of times the decimal point to be shifted to get the original string.

For example: In test case 1 the random string generated is $px`hfE^1c#;%*nb>z$J corresponding ASCII value[16] is 36112120391041026994124993559374211098621223674 .

After applying logarithmic operation on this ASCII value it gives the output 46.5576 by applying sine value to the above generated result the obtained result is 0.72606. The last value appended in this case is 1 as the mantissa part starts after one decimal point .If the result obtained after sine operation is 76.522 then the last value appended will be 2 as the as there should be two place decimal value shift to 76522 to 76.522.The encrypted key is sent to the mobile client over a unreliable network.

The Decryption algorithm is implemented in android platform for decrypting the key sent received over unreliable network .After decryption the original key is obtained is sent to the authentication server for getting access to the cloud storage as shown in the architecture in figure 1.
The string matching is done by using equation 2

STR_MAT= strcmp(s1,s2)................................................(2)

Function Strcmp returns logical 1 if both the strings are true else it returns logical 0, based on this comparison the access to the cloud storage is provided.

Encryption is done character wise on random string which consists of A-Z, a-z,0-9,special characters as shown in table 1, generated by key generator , based on proposed algorithm. Therefore this proposed method of an encryption cannot be broken by brute force attack, timing attack and meet in middle attack, so the data is protected and improved the privacy of data.

## 7. Conclusion

In this paper, we first discussed current issue of mobile application in cloud environment. These issues include storage security, middleware security, data security, network security and application security. The biggest challenge in implementing successful Cloud computing technologies is managing the security. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted [13]. Cloud computing has the potential to become a leader in promoting a secure, virtual and economically feasible IT solution and future work and progress lies in standardising Cloud computing security protocols. In this paper we have developed an user authentication algorithm which provides a onetime password, for an user to get access to the cloud server.

## 8. Future Work

The paper mainly discusses about user authentication, for getting an access to the cloud storage. The paper can be further extended to data authentication along with user authentication, so for to provide more security. In the future work this method can be merged with data authentication mechanism, where once the user gets an access he can claim that the data belongs to him by using mechanisms such as encryption and decryption methods.

## 9. Acknowledgment

The authors are thankful to the management of Rajarajeshwari College of engineering, Bangalore, India for allowing to pursue research at their research center and providing the necessary facilities and guidance to carry out the research work. The authors are also thankful to the management of Dayananda Sagar Institutions, Bangalore, India for providing necessary facilities to carry out the research work.

## References

[1] Cloud Computing: saas, paas, iaas, virtualization, business models, mobile, security and more by Dr.Kris Jamsa.
[2] Cloud Computing Bible by Barrie Sosinsky ”www. cs.ecust.edu.cn/~yhq/course.../cloud/Cloud%20Computing%20Bible.pdf”.
[3] Mobile Cloud Computing: A Comparison of Application Models by Dejan Kovachev, Yiwei Cao and Ralf Klamma ” www.arxiv.org/pdf/1107.4940”.
[4] Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing by ” by Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal“www.buyya.com/papers/CloudFGCS2009.pdf”
[5] A Novel Approach for Improving Privacy of Data Using Dynamic Key Generation by Rajesh Kumar J N “www.ijritcc.org/vol_2_issue_3.h”ml"
[6] Cloud Based Security by Nikita M. Ikhar, Shivani S. Meghal and Prof. Kaustubh Satpute in International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 3.
[7] Technical report on Mobile One Time Passwords and RC4 Encryption for Cloud Computing by Markus Johnsson & A.S.M Faruque Azam.
[8] Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues by Qureshi, S.S. ; Beijing Key Lab. of Network Syst. & Network Culture, Beijing, China Ahmad, T,Rafique, K and Shuja-ul-islam published in IEEE International Conference Cloud Computing and Intelligence Systems (CCIS), 2011
[9] Towards Trusted Cloud Computing by Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues.
[10] A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environments by Abdul Nasir Khan, M.L. Mat Kiah,Sajjad A. Madani,Atta ur Rehman Khan, Samee U. Khan
[11] File Transfer Protocol in Cloud Computing by Ch.Madhu Babu, O.Lakshmi Chandana published in International Journal on recent and innovation trends in Computing and Communication Volume 2,Issue 3.
[12] search on mobile cloud computing: Review, trend and perspectives by Han Qi ; Fac. of Comput. Sci. & Inf. Technol., Univ. of Malaya, Kuala Lumpur, Malaysia ; Gani, A. published in second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), 2012.
[13] Mobile Cloud Computing the Necessity of Future with its Architecture, Advantages and Applications by Anup Arvind Lahoti ME (Student) and Prof. Prabhaker L. Ramteke (Associate Professor) International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 3.
[14] A Secure Cloud Storage System with Secure Data Forwarding by Aarti P Pimpalkar, Prof. H.A. Hingoliwala International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.
[15] A Novel Approach to Data Integrity Proofs in Cloud Storage by Neha T P.S Murthy published in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2,Issue 10,October 2012.
[16] www.asciitable.com/

## Author Profile

**Deepak. G** has received B.E degree in 2007 from VTU University, Belgaum and M.Tech degree in 2010 from VTU University, Belgaum, Karnataka, India. Currently he is working as Assistant Professor at Dayananda Sagar College of Engineering, Bangalore, India and His experience in teaching started from the year 2010. His areas of interests include Security issues of Cloud Computing & mobile cloud computing.

**Dr. Pradeep B.S** has received B.E degree in 2001 from Mangalore University, M.Tech degree in 2005 from VTU University, Belgaum, Karnataka, India and Ph.D from Magadh University in 2008. He has worked as Prof & Head, Dept. of CS&E, RRCE and Currently working as Director, International R&D division, China at Linyi Top Network Company Ltd.

**S. Shreyas** presently pursuing B.E degree in Department of ISE under VTU at Dayananda sagar College of engineering, Bangalore, India. His areas of interest include wireless Communication, artificial intelligence and substitutions to bio-fuels.