# Research About Attacks Over Cloud Environment

Li Jie, Fatma Fawzi

**Abstract**: Cloud computing is expected to continue expanding in the next few years and people will start to see some of the following benefits in their real lives. Security of cloud computing environments is the set of control-based technologies and policies absolute to adhere regulatory compliance rules and protect information, data applications and infrastructure related with cloud use. In this paper we suggest a model to estimating the cloud computing security and test the services provided to users. The simulator NG-Cloud (Next Generation Secure Cloud Storage) is used and modified to administer the proposed model. This implementation achieved security functions, potential attacks as defined in the proposed model. Finally, we also solve some attacks over cloud computing to provide the security and safety of the cloud.

**Index Terms**: cloud computing, attacks, countermeasures.

## 1 Introduction

A model for enabling ubiquitous, suitable, on-demand network access to a shared pool of computing resources (e.g., servers, storage, networks, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. Security is associated to the important aspects of confidentiality, authentication, identification, authorization, integrity and availability; they thus become building blocks to be used in designing secure systems. Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. Security refers to a wide set of policies, technologies, and controls deployed to protect files, data, applications, and the related infrastructure of cloud computing [2]. Key security considerations and issues which are currently faced in the Cloud computing are very important. The existing adoption of cloud is associated with plentiful challenges because users are still skeptic about its authenticity. Security and privacy are the challenges associated with cloud computing, which relates to storing and securing information, oversight the use of the cloud by the service provider (SP) [3]. There are many attacks which affect the security of cloud computing and on its ability to provide an efficient security system. Hence, we will introduce some potential attacks in cloud computing. Also, we will introduce solutions for these problems and concerns that should be avoided in order to ensure high security over cloud computing.

## 2 REVIEW OF CONCERNS AND ATTACK OVER CLOUD

### 2.1 Cloud Computing Concerns

Some concerns have to be provided in a cloud system to ensure the security of the cloud service. These concerns are enforced through regulations, contracts, or framework. These concerns are:

1. **Multitenancy:** multitenancy is a key security concern in Cloud. For example, Cloud Clients (Co-location of multiple (Virtual Machines) VMs in a single server and sharing the same resources increases the attack surface). CSPs, Enforcing uniform security controls and measures is difficult. Mutual client isolation is a key measure against multitenancy-related concerns: Isolation of VMs, Isolation of Data and Isolation of network communication.
2. **Velocity of attack:** Security threats amplify and spread quickly in a Cloud – known As “Velocity-of-Attack” (VOA) factor: Cloud infrastructure is comparatively larger and Similarity in the platforms/components employed by a CSP increases the speed at which an attack can spread. Effects of high VOA are Potential loss due to an attack is comparatively higher and it is comparatively difficult to mitigate the spread of the attack. To overcome the issue of VOA, CSPs need to adopt more robust security enforcement mechanisms such as for defense-in-depth.
3. **Information Assurance and Data Ownership:** Information assurance concerns for Cloud users embrace CIA, Authenticity and Authorized use. Data ownership concerns for Cloud clients. In Cloud, data belonging to a client is maintained by cloud service provider (CSP), who has access to the data and important information, but is not the legitimate owner of it and Data should be protected using encryption and access control mechanisms.
4. **Data Privacy:** Potential for unauthorized detection of private data of a Cloud client. Private data may include individual identity of the client, Details of the services requested by the client and regal data of the client. Should overcome the issue of privacy to provide the safety of cloud computing.

### 2.2 Attacks over cloud

There are various issues in cloud that need to be resolved respect to security and privacy. The serious issues that need to be addressed are secure delivery of data to and from the cloud and security attacks [4].. There are different types of attacks:

1. **Flooding Attack:** attackers can send very large amounts of packets from exploited information resources, and they are called zombie [5].
2. **Denial of Service Attacks:** A DOSA is an attempt to make the services assigned to the authorized users unavailable. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error [3].
3. **Man in the Middle attacks (MITM):** in this type of attacks,


- *Li Jie: Department of Computer science and technology, Harbin Institute of Technology, Harbin, China. E-mail: jieli@hit.edu.cn*
- *Fatma Fawzi: Department of Computer science and technology, Harbin Institute of Technology, Harbin, China. E-mail: love-stories20@yahoo.com*

an entity tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them. So should avoid MITM attack to protect data transferred between user and cloud.

4. **Sniffer Attacks:** These types of attacks are initiated by applications that can capture data packets flowing in a network especially if the data is not encrypted.
5. **CAPTCHA Breaking Attacks:** the spammers are able to break the CAPTCHA [8], provided by the Hotmail and Gmail service providers. They make use of the audio system able to read the CAPTCHA characters for the visually impaired users.
6. **Authentication attacks:** Authentication is a weak point in hosted and virtual services and is frequently targeted. Most user-facing services today still use simple username and password type of knowledge-based authentication, with the exception of some financial institutions which have deployed various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc.) to make it a part more difficult for attackers.

## 3 PROBLEM FORMULATION

Cloud data security models should be able to solve all the possible issues and challenges of cloud computing, so as to provide the benefits and efficiency of cloud computing and protecting the owner's data from all the risks associated. There are different issues in cloud that need to determine for security and protection. The major issue that should be addressed is secure delivery of data to and from the cloud, concerns and security attacks. So we should take into consideration the concerns and the information security policies to avoid issues of security. Find more effective solutions to these problems. It became the challenges and motivation to propose a secure data model to achieve high level of the security for cloud computing users. Xin Dong's scheme [10]focuses on providing a dependable and secure cloud data sharing service that allows users dynamic access to their data. A privacy-preserving data policy with semantic security is proposed in the scheme; by utilizing cipher text policy attribute-based encryption (CP-ABE) combined with identity-based encryption (IBE) techniques. Although, Dong's scheme enables only the authorized users to access and restore files correctly, the scheme doesn't solve the problem of fake identity, the system cannot know whether he/she is an authorized user or not. This issue is a very important requirement for security over cloud because in case of unauthorized user access to the system security violation can’t be accepted We overcome these issues using one time password (OTP) technique in the process of user login and the process of uploading file on the cloud by data owner. In our proposed model, OTP is defined as a random code which is generated by the cloud server, and sent to the user's or data owner's email address and mobile in the process of logging and uploading, respectively. OTP was prior to that stated in 2014, by [11], however, both didn’t clarify the concept nor how to use it and the possibility of its application in practice. We integrated the idea of OTP with the functions of Dong's scheme model to get a new proposed model to solve the fake identity problem.

## 4 PROPOSED MODEL

The main goal of any cloud data-sharing model is accessing data in an easy way without reducing the security of the model. The proposed model presents a solution to some security issues of cloud such as, data protection from any violations, and protection from a fake authorized identity user. Our proposed model provides benefits and effectiveness of security in cloud computing, as well as, security and scalable data sharing for users on it. Also, this model protects the system from any fake data owner who can enter malicious information that may destroy the main goal of cloud services. So we propose the one time password (OTP) as a logging technique to protect users from any fake unauthorized access to the cloud. The OTP code is used when uploading data by data-owners to cloud server or when the user logs in. Also, when the OTP code is accessed through the user's or data owner's communication setting, we send OTP code for data owners by mobile data owners and their email address in the process of uploading their files on cloud server. The one time password (OTP) is a logging technique to protect users from a fake authorized access to the cloud. When any user registers to the cloud, the cloud will request to send an OTP code text to his private email and/or his private phone number. Each user must enter the received OTP code correctly to the cloud to verify his identity as an authorized user. In our model we added the OTP login between the users and the cloud to prevent any unauthorized user to access the system illegally. The OTP, in our model, makes the login process securely to protect users and their private data We also proposed the PKG in our model, Trusted Third Party (TTP) is a structure, which facilitates interactions between users and data owners who both trust the third party. Data owners may be a person or an organization. PKG checks all critical procedure communications between user and data owner. In this model, the relying parties (user and data owner) use this trust to secure their own interactions. And finally we use the RSA Algorithms to encryption and decryption data,RAS was developed by Rivest, Shamir and Adleman at MIT in 1977 Tom (Davis, 2003) [12]. RAS is best known and widely used for public-key generation. RSA use large integers (eg. 1024 bits) and the cost of their security depend on the factorization of large numbers. RSA is an algorithm for public key cryptography. It involves the use of two keys:

- A public key, which can be common, and used to encrypt messages.
- A private key, known only by the recipient, and used to decrypt messages.

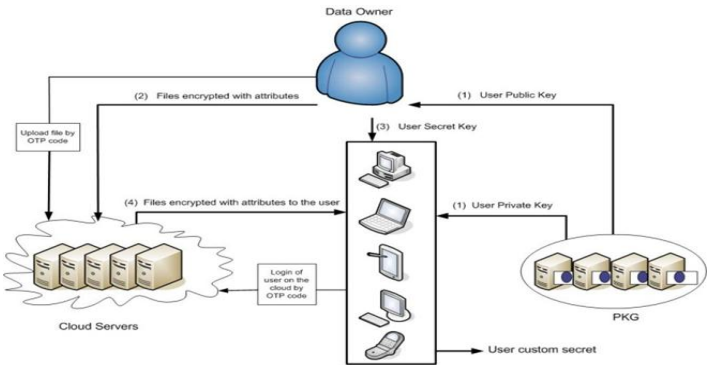



***Fig. 1.*** *The proposed*

### 4.1 Roles of our proposed model

There are important roles in our proposed model that control execution of all process in the system. Every role affects the efficiency of the proposed model to provide best services for cloud users. These roles are listed as follows:

1. PKG gives data owner user public key (user ID) for every user in the system.
2. The Data Owner stores encrypted files on the cloud server with attributes.
3. When a user requests access, he would obtain the file`s secret key from the Data Owner.
4. Cloud Server gives every user in the system the encrypted files with attributes assigned to each user.

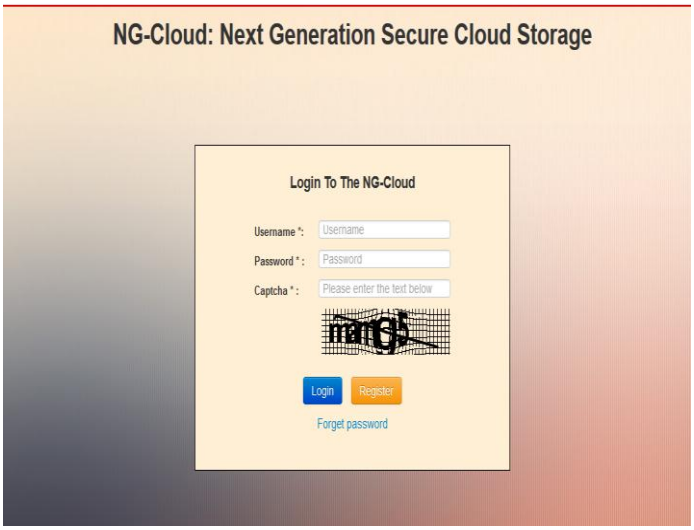
A system administrator is a cloud administrator (cloud A) that maintains the cloud system, and is responsible for the integrity of the data, as well as, the efficiency and performance of the system

### 4.2 Analysis of The proposed Model

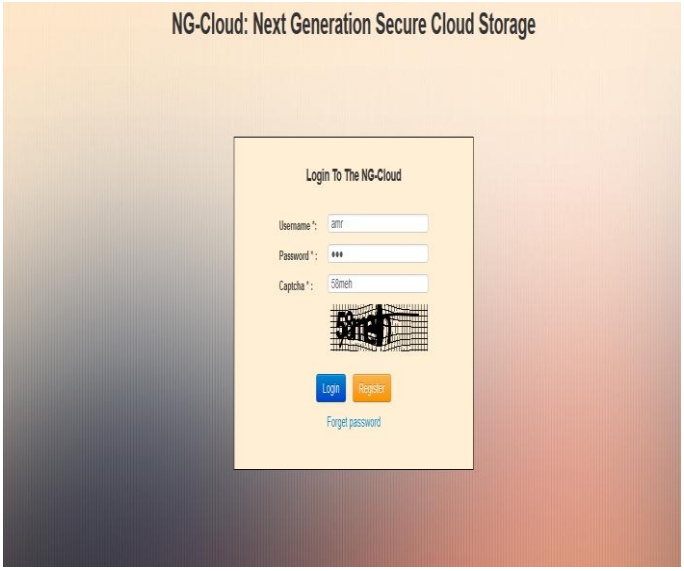
The solutions of some potential attacks over our proposed model

1. **Flooding attack:** In this model we overcome the flooding attack by limiting file upload process from data owner to cloud server to be every 5 minutes. We will limit the time of file upload process according to the number of data owner to avoid the flooding attack. For example, when we have 5 data owners or less in the system will limit file upload process to be every one minute or less. System to become smooth and supple. We will make our system available to users when they send their requests. We will limit the number of request for each user in the same time to make the system available to another user all time. When user sends many requests to the server exceeding the allowable limit by the system, then the server will not respond to these excessed requests.
2. **Man-In-The-Middle:** Any person tries to spy in a current conversation between a cloud server and a user to insert false information and to have knowledge of the important data transferred between them. We secure the system against man in the middle attack (MITM), by securing the channel between Data Owner & Cloud storage, and Data User & Cloud storage. The secure channel is https over Transport Layer Security TLS. To reduce threat of Man in the Middle we use strong encryption and origin authentication techniques. Strong encryption is implemented through symmetric encryption (secret cryptographic) and asymmetric encryption (public cryptographic). We use RSA and AES algorithms as asymmetric and symmetric cryptographic to provide higher security of the system. We use origin authentication techniques such as One-Time Password (OTP) in the login process and CAPATCHA technique to provide the authentication of the system; and so we protect our system from Man in the Middle attack.
3. **Sniffer Attacks:** We proposed a solution for the attack of sniffer to provide the safety of our system. We provide the process of encryption management to secure the data. Data should be encrypted efficiently to secure the transferred data or information between users and cloud servers. The data is encrypted from data owner to cloud server, then these files are sent encrypted from cloud server to users as it has been explained previously. Accordingly, applications that capture packets flowing in a network are not readable.
4. **Authentication Attacks:** In the model, we overcome the attack of authentication by some techniques of strong authentication. Any user or data owner will login in the system by a secure way to protect user or data owner from any attacker in the registration process. By CAPATCH technique each user cannot log in the system without being verified. CAPATCH helps user or data owner providing strong authentication, One time numeric password (OTP) technique which provides the level of security for cloud computing. In this model, One-Time Password (OTP) in the login process, via email and SMS is found. So that the user or data owner can use it for only 10 minutes and then must send it back in order to increase the authentication of the system.

## 5 Simulation Results

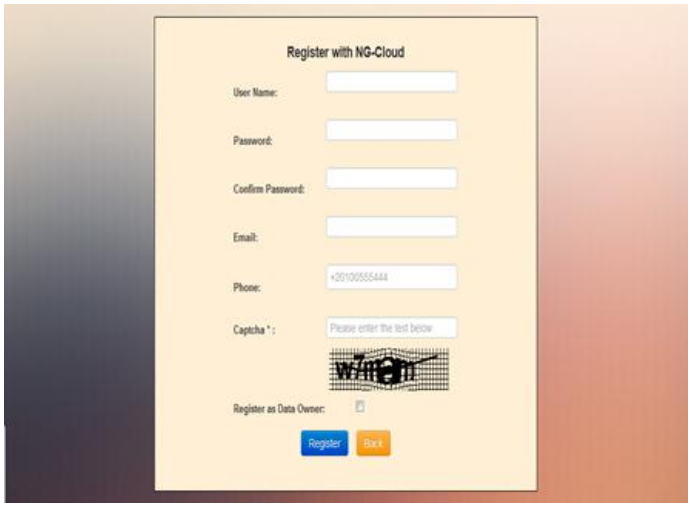



***(a)*** *Login in the system*

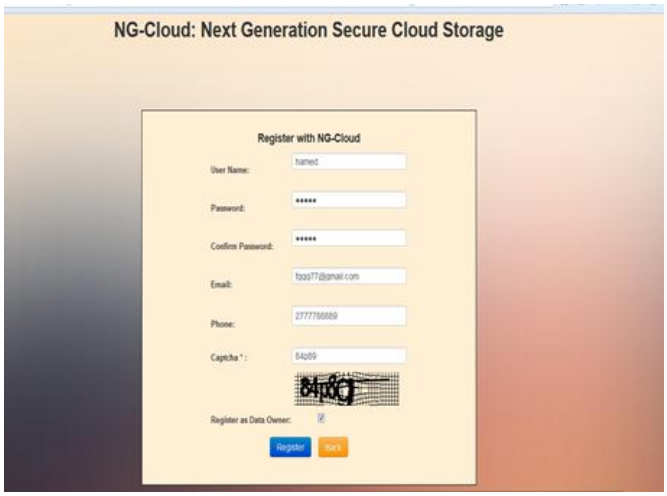



***(b)*** *Example of login*

***Fig. 2.*** *The process of login*




***(a)*** *Register in the system*




***(b)****Example of register*

***Fig. 3.*** *The Registration process*

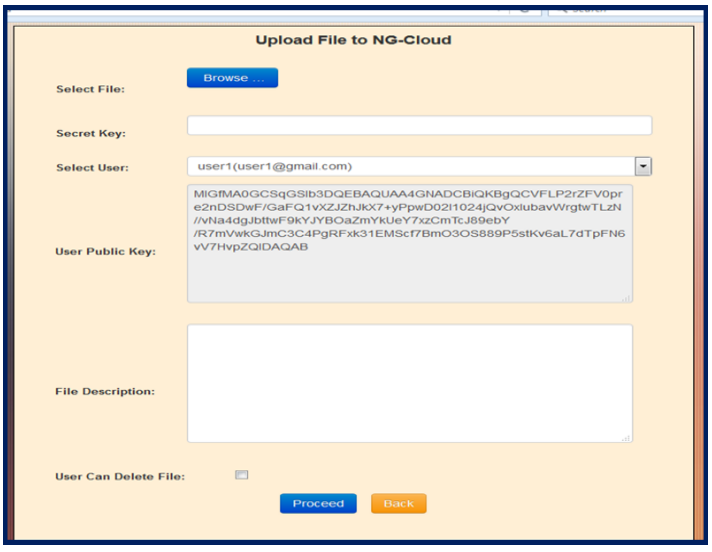



***Fig. 4.*** *File upload process*

In the end of the process of registration, each user or data owner will be able to login the NG-Cloud. We will explain the file upload process in our application as follows:

1. The data owner selects the file which he wants to upload as described in the button Browse.
2. He should type secret key to encrypt your file.
3. Select user from the group of users existing in the system.
4. A user public key is associated with selected user.
5. File description helps the user to see this special file and the quality of it's content.
6. The user can delete this uploaded file; the data owner is the one who determines whether or not this privilege is available. When the owner checks box "User Can Delete File", the user has this privilege. On the other hand, when this box is not checked, data owner doesn't grant this privilege to the user.
7. When the data owner uploads his file on the cloud server; the cloud sends an OTP code on his email and mobile. Then, the data owner should type the correct OTP code to be able to upload his file successfully.
8. Then, clicking the button "Proceed" to end the process of file uploading.

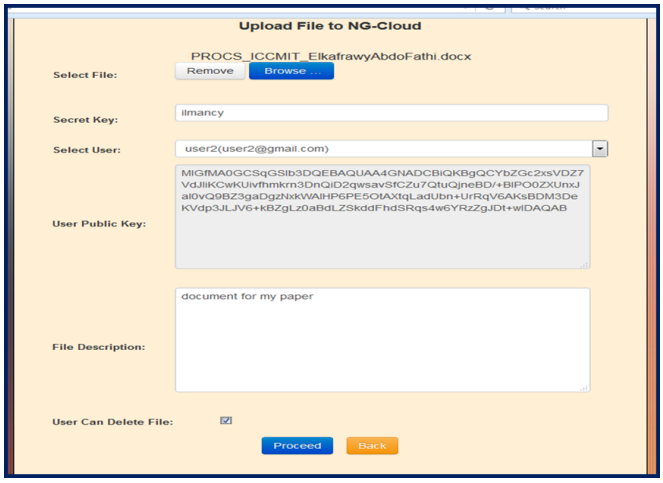



***Fig. 5.*** *example of file upload*

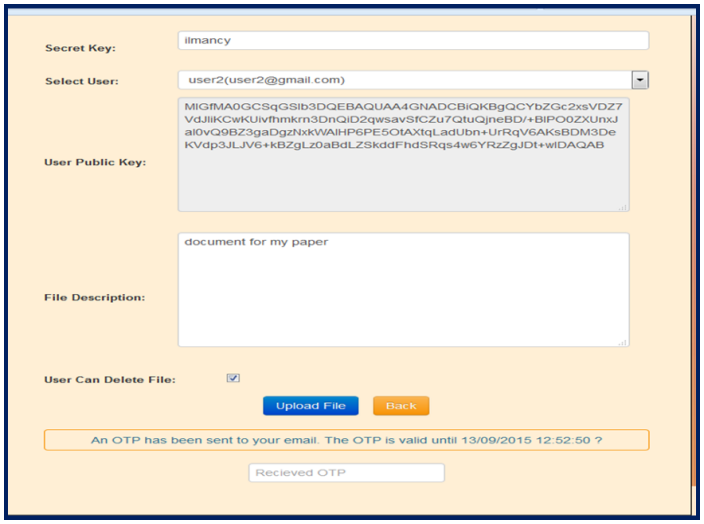



***Fig. 6.*** *request OTP code*

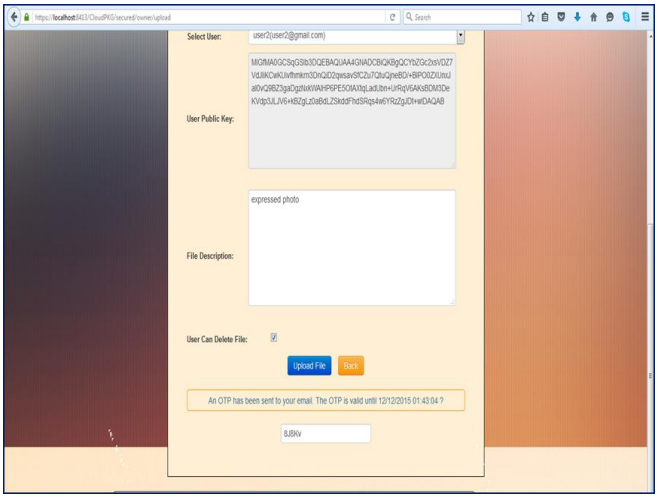



***Fig. 7.*** *correct OTP code*

One time password technique is used to verify any user login in the system. OTP code will be sent to email address and phone number of every user in the system.

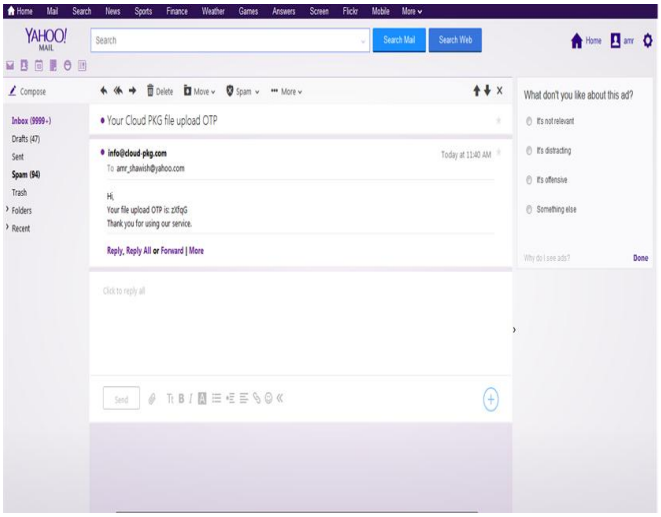



***Fig. 8.*** *OTP code in the email address*

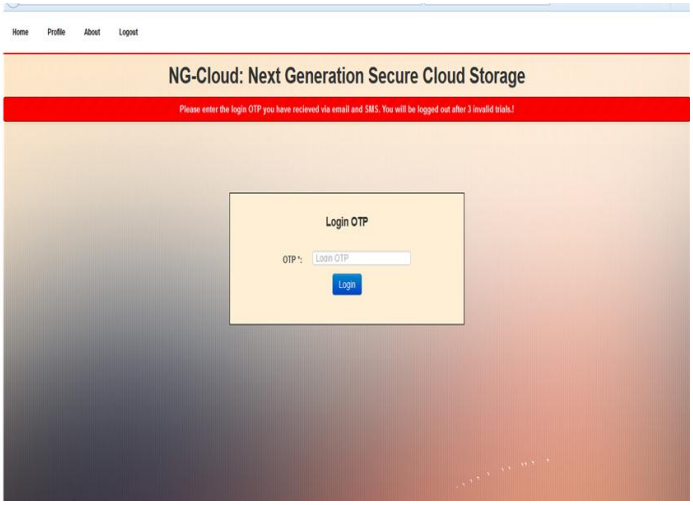



***Fig. 9.*** *OTP code in the phone number*

## 6 CONCLUSION

Cloud computing is one of the rapidly growing field of IT among the many business activities of large organization. It provides resources in the form of services as per usage base model. The proposed model presents a solution to some security issues of cloud computing. Protection of authorized user from any fake identity is one of the most important contributions to this model. Our proposed model provides the benefits and effectiveness of security in cloud computing.

## 7 REFERENCES

[1] G. P. Pragnesh, and M. S. Sanjay," Survey On Data Security In Cloud Computing, " International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 9, pp. 1-8, 2012.

[2] Z. Dimitrios, and L. Dimitrios," Addressing cloud computing security issues," FutureGenerationComputerSystems, vol. 28, pp. 583–592, 2012.

[3] S. O. Kuyoro, F. Ibikunle, and O. Awodele," Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), vol. 3, no. 5, pp. 247-255, 2011.

[4] R. Ajay, L. Sharma, and R. Bhardwaj "Possible Attacks in Cloud Computing," National Conference on Advanced Computing Technologies (NCACT) at Maharshi Dayanand University, Rohtak, 2013

[5] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013.

[6] E. Ogren, "Whitelists SaaS modify traditional security, tackle flaws," Sep. 17, 2009. http://searchsecurity. techtarget. com/news/column/0, 29 4698, sid14_gci1368647, 00. html. 2009.

[7] Z. Trabelsi, H. Rahmani, K. Kaouech, and M. Frikha, "Malicious Sniffing System Detection Platform," Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004.

[8] E. D. John, "Spammers break Hotmail's CAPTCHA yet again," Tech- world, Feb. 16, 2009.

[9] M. Gregg "10 Security Concerns for Cloud Computing," Expert Reference Series of White Papers, www.globalknowledge.com.

[10] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, amd M. Li,"Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," journal of computer & security, vol. 42, pp. 151-164, 2014.

[11] P. Lavanya, S. Komala, and N. Vikram," Anonymous Data Sharing Scheme for Dynamic Groups in an Untrusted Cloud," International Journal of Computer Science (IIJCS), vol. 2, no. 8, pp. 39-45, 2014.

[12] T. Davis, "RSA encryption." Chapter one (2003): 1-4.