A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing

Sanjay Kumar1, Syed Akbar Abbas Jafri2, NishitArun Nigam3, Nakshatra Gupta4, Gagan Gupta5, Dr. S K Singh6
Student2,3, Student4, Asst. Professor1,5, Asst. Professor4, Asst. Professor6, Department of Information Technology, GCET
Email: dhananjay0397@gmail.com, skhakhil@gmail.com

Abstract. The Cloud based Computing is a trending technology in present IT scenario in which data is stocked in a Scattered or distributed manner & resources are shared among people. The data centers are widely distributed across the globe and are accessed by anyone at any time. Data is fetched, uploaded and manipulated by several users simultaneously hence identification and authentication of users who are fetching the data need to be done mandatorily without any error. In this Research Paper we have presented a new advanced security architecture for user identification which includes two factor authentication, AES based file encryption and decryption of data uploaded on cloud, admin verification and locking of users, fetching IP details of users, distributed database storage i.e. data is stored in tiers which means user login details is stored in one database & encryption/decryption details such as (files uploaded, key) is stored on different database. Whole work deals on enhancing security for cloud computing.

Keywords: Cloud Computing, Security architecture, AES, onetime password, Distributed database, Encryption, Description.

1. Introduction
In today’s era of information technology, cloud computing has been one of the major outbreaks for developers and users. Cloud computing works on the concept of distributed computing. Cloud computing has a wide dimension of scope ranging from solving complex problems, huge volume of data storage, lesser storage cost, anywhere and anytime access of user data. In cloud computing a user can store their data and fetch that data, whenever they require, what they need is just to sign up to cloud service. Now, accessing their services require some authentication method, traditionally used method make use of static password mechanism, in which user choose a password while registering and then login using that password. This method of keeping a password that is used for further login is known as one-factor authentication. But guessing these password (one-factor authentication) is easy, as user does not keep strong password, since they are hard to remember and even if they keep strong password then also one
factor authentication is prone to key-logging attack (key logging attack is a attack in which attackers captures the key stokes of the host and gets its details).

One factor authentication is prone to password guessing because people don’t often change their password. Therefore, security of the cloud is essential in today’s world. cloud computing has a very high potential to emerge as a most used technology because of its wide dimensional scope, but still not used due to its security concern like where the data is stocked, its integrity concern etc…. all these concerns steps back users from using cloud services. The things of cloud storage that disturbs clients are decentralized distributed storage and scalability i.e. user do not know where and how its data is stored. User does not have the knowledge from which location and how data is fetched, and where the backup of the data is kept. Therefore, there must be proper cloud awareness among people to believe in service. Now by looking the above belief factor we understood that why cloud computing face challenge in emerging as lead technology, apart from these factors cloud data is also vulnerable to following attacks-

1. Password Guessing Attack- It includes key logging and various other technique to obtain users password. It may be either by hook or crook method.

2. Intermediate Middle Attack- It is an act of hacking server and gaining the password of the user. Here the attackers try to create a breach in the propagation medium and gain access to the secure data.

3. Phishing Attack- This is used to guess the user’s password by creating a fake login page and fetching details.

4. Masquerade Attack- Attackers try to deceive the host by creating fake user identity.

Hence securing the users identity is the only way to gain user belief on cloud computing. Identity and Access Control for the Cloud Services must be provided to the user in cloud storage and computing services, this can be done using Admin Verification/Lock of users by checking the logs and looking for any abnormality in the IP pattern. Identity and access control must provide identity management for the cloud users.In this analysis we have suggested a better way of security mechanism to secure the cloud for identity-based user authentication and a new security architecture is used, here we have used a concept of distributed data storage to safeguard the user details and the stored data from the attacks of intruders and hackers. It also includes two factor authentications,AES based file encryption and description of data uploaded on cloud, admin verify and lock controls for users, fetching IP details of users, distributed database storage i.e. data is stored in tiers, user login details in one database and encryption decryption on different database i.e. the separate data gets stored on distinguished database.

2. RELATEDWORK

The data storage mechanism of the cloud is similar to the data storage mechanism of the storage peripherals like hard disc and pen drive but the only difference is where the data is collected (in cloud data is stored in remote location). Several studies on the security of cloud-based computing has previously been presented and analyzed.

The major four aspect of information security in cloud computing are –

1. Validation
2. Privacy
3. Solidarity
4. Obtain ability

Validation is the throughout process for Verifying the identity of the user/client, now in the previously researched work user authentication is done by password and data confidentiality is maintained using encryption/decryption algorithm. Efficient encryption algorithm must be used in order to ensure good security, to enhance the upload and retrieval of data. Previously the secure login and registration is done using one factor authentication i.e. making use of static password mechanism in which user choose the password while registering and login using that password which is vulnerable to be hacked. One factor authentication is prone to password guessing because it does not have any other security check. Encryption algorithm used in those security architectures was DES (Data Encryption Standard). It is a 64-bit Fiestal block cipher based on the conceptual formulation of Fiestal rounds rule having in total 16 rounds and a massive key size of 56 bit. DES was most widely used encryption scheme adapted in the late 20th Century by N.I.S.T. (National Institute of standard and technology). it follows Fiestal Structure.

![Figure 1: DSS Algorithm Mechanism](image)

Before the development & Implementation of DSS algorithm, the Simple Encipherment and Decipherment Technology was used to encode and decode the data stored in a computer based cloud related services. All the previously used techniques were brutally being cracked and misused as people have understood their loop holes and have identified their weak points which led to the low security in authenticating, validating and protecting user’s data on cloud.

3. MODEL PROPOSED

In our Research Model we have suggested work that deals with a new way of security mechanism including: -
- Admin Verification/Locking of User
- AES for Secured file encryption.
- Distributed data storage for user’s ID details and Files Details
- One-time password for authentication each time user login.

All the algorithms and user authentication mechanism which have been proposed so far have some or more problems. The earliest cipher like (shift cipher etc...) can be broken with ease on modern computation system. The DES (Data Encryption Standard Algorithm) was patched/smashed in 1998 using a computer hardware that cost about $250000/- in 3 days. The triple DES was way too slow for quick and fast retrieval, updating & manipulation. This problem can be solved if we implement AES (Advance Encryption Standards) Algorithm for Encryption/Decryption. NFC is a new yet a very resourceful concept. The concern while developing such system was, would it also have practical application or would it just be limited to a theoretical term. But in recent times there has been an enormous growth in the number of NFC enabled devices.

![Figure 2. AES Algorithm Mechanism](image)

Note that this AES algorithm mechanism wasn’t developed by any organization; it is the work of the people who took part in a large scale competition raised by N.I.S.T. to get an advanced decipherment and decipherment algorithm which follows a standard protocols and are organized in format. N.I.S.T. got several algorithm mechanisms on which several tests were performed in which only 5 algorithms were considered for the final test in which the best algorithm found was AES (Advance Encryption Standard) Algorithm Security Proven architecture. AES is also a block based symmetric cipher system.

With several large companies investing in this technology, this technology looks to completely take over the contactless payment market in future. Google, Apple, Microsoft, Master Card are few of the
many companies venturing and investing in NFC based payment systems. For the Security purposes it has a Registration page where the users first create a Strong Password for login purposes.

After the user is registered, the Admin check for the authenticity of the user and accordingly verify the user or locks the user. User authenticity is checked by looking in the logs and if the user is found genuine then it is verified. After the verification of the user, user can easily access his/her account. To enhance the security TWO STEP VERIFICATION is done at every login i.e. user gets the OTP on their registered email id every time they login to cloud services.

After the correct OTP matching, if the OTP is matched then user gets logged into the cloud service portal. Here the user can look into his/her Profile, Upload/Download Files On cloud using AES encryption/decryption Algorithm. Here the Database is distributed i.e. the database for the User Details, Encryption/Decryption & Key Storage is different so that if by any means hacker/attacker get into the User Detail Database, still he/she will not be able to access to the encryption and decryption algorithm key and therefore not be able to access uploaded data, since he/she will not have key so he will not be able to fetch or download the data.
Figure 5. Key Details

If by any means user gets logged into the system by stealing OTP or By – Passing OTP, then to fetch any details of the user he requires to enter the KEY, on failing which he gets a FAKE DATA of the information downloaded with garbage value.

This fake data will firstly deceive the hacker or the person who has gained unauthorized access to the user’s account and at the same moment of time it will protect the user’s valuable amount of data to be stolen/copied/misused by attacker, hence we can suggest the this garbage data act as the bait to the attacker by which he feels he has succeeded hacking or creating a breach in the cloud architecture but unknowingly he has downloaded garbage content & triggered the alarm to the admin indicating that a malicious activity took place in the user’s account.

Figure 6. Admin lock.
The admin can verify/lock the user by checking for the IPs, if VPN is connected then the IPs change every 5 minutes & hence by observing the malicious intentions of the user admin can lock the users account. After the account gets locked only the Admin is provided the right to Unlock the user using his best knowledge about the user.

![Figure 7.AttackStocked IP Catch Details.](image)

The Module work by grabbing the IP Address of the system through which the user has logged into the account. The IP Address of the system at that time is locked in the database and that IP Address are stored and stocked in the attack and hit database every 5 minutes.

The Admin can keep a check from which IP Address the Particular functionality is been performed like

1. From where the user has Logged In – LOGIN IP Address.
2. Date fetch and Upload Time with IP Address – IP Address recorded at manipulation time.
3. Date and Time the IP Address is being changed.

If the account is reported or any malicious activity is found then the Admin has a right to lock the user and perform necessary action to protect the data from being maliciously used.

A session window of 30 Minutes is kept, i.e. the user’s gets automatically logged out from the account if he is kept inactive for that period/interval of tenure/time. This will help the user from the privileged access of their account from the user who try to take advantage from the user by gaining their faith and using their logged in account for un-ethical use and malicious intensions.

4 CONCLUSION

In this research paper we have suggested a big new/up-to-time security architecture for cloud based computing domain which includes two factor authentication, AES(Advance Encryption Standard) based file encipher and decryption of data uploaded on cloud, admin verification and locking of users.
fetching IP details of users, distributed database storage i.e. data is stored in tiers which means user
login details is stored in one database & encryption/decryption details such as (files uploaded , key) is
stored on different database. Overall work deals on enhancing security for cloud computing,
this work fortfy security for complete cloud-based computing structure.

In our research based suggested working representation, a hacker/attacker cannot easily fetch
information from the cloud databases and load their corrupted files as he require to get access all the
database data centers, which is very tough and hard to breach or crack. All these attacks which could
be performed on the previously implemented system could be reduced to zero enhancing the security
of the cloud and at the same time identifying and servicing only the genuine clients.

References

[1] Yashpa I Kadam, 5 October, 2011 “Security Issues in Cloud Computing A Transparent View”,
International Journal of Computer Science Emerging Technology, Vol-2 No .316-322

[2] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, 2011 “A Survey on Security
Issues in Cloud Computing”.

[3] Mladen A. Vouk, 2008, “Cloud Computing – Issues, Research and Implementations”, Journal
of Computing and Information Technology CIT 16, 4,235–246

[4] Ye Hu, Johnny Wong, Gabriel Iszlai, Marin Litoiu, 2009 “Resource Provisioning for Cloud
Computing”, IBM Canada Ltd.

[5] Daniele Catteddu, Giles Hogben, 2009 “Cloud Computing:- Benefits, risks and
recommendations for information security”, November.

[6] Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang “Recent Advances in Cloud Security”,JOURNALOFCOMPUTERS, VOL.6,

[7] Trusted Computing Group, May2010“Solving the Data Security Dilemma with Self-
Encrypting Drives”.

[8] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, 2009 “Identity- Based
Authentication for Cloud Computing”, CloudCom, LNCS 5931, pp. 157–166,2009

[9] Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, 2011 “Twin
Clouds: Secure Cloud Computing with LowLatency”,CASED, Germany.

[10] Luis M. Vaquero, Luis Rodero-Merino, Daniel Morán, 2011 “Locking the sky: a survey on
IaaS cloud security”, Computing 91:93–118

[11] Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman, 2010“FADE: Secure
Overlay Cloud Storage with File Assured Deletion”.

[12] Thuy D. Nguyen, Mark A. Gondree, David J. Shifflett, Jean Khosalim, Timothy E. Levin,
Cynthia E. Irvine, 2010 “A Cloud-Oriented Cross-Domain Security Architecture”, The
Military Communications Conference, U.S. Govt.
[13] Kumar, Sanjay, Ashish Negi, and J. N. Singh. 2019 "Semantic Segmentation Using Deep Learning for Brain Tumour MRI via Fully Convolution Neural Networks." Information and Communication Technology for Intelligent Systems. Springer, Singapore, 11-19.

[14] Brian, A. Larsan Aro, L. Arockiam, and P. D. S. K. Malarchelvi. 2014. "An IOT based secured smart library system with NFC based book tracking." International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) 11, no. 5.

[15] Kumar, Sanjay, Gagan Gupta, and Kunwar Rajat Singh. 2015 "5G: Revolution of future communication technology." In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 143-147. IEEE.

[16] Monteiro, David M., Joel JPC Rodrigues, and Jaime Lloret. 2012 "A secure NFC application for credit transfer among mobile phones." In 2012 International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1-5. IEEE.

[17] Haselsteiner, Ernst, and Klemens Breitfuß. 2006 "Security in near field communication (NFC)." In Workshop on RFID security, pp. 12-14.

[18] Dutot, Vincent. 2015 "Factors influencing near field communication (NFC) adoption: An extended TAM approach." The Journal of High Technology Management Research 26, no. 1: 45-57.

[19] Sharif, Rabia, Syed Waqas Ahmad, Hirra Anjum, Naveed Ramzan, and Shahid Raza Malik. 2014 "Effect of infusion time and temperature on decaffeination of tea using liquid–liquid extraction technique." Journal of Food Process Engineering 37, no. 1: 46-52.

[20] Van der Aalst, Wil MP, and Akhil Kumar. 2003 "Xml–based schema definition for support of interorganizational workflow." Information Systems Research 14, no. 1: 23-46.

[21] Gavish, B. and Gerdes, J. 1998, "Anonymous Mechanisms in Group Decision Support Systems Communication." Decision Support Systems, 23(4), 297-328.

[22] Von Alan, R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design science in information systems research." MIS quarterly 28, no. 1 (2004): 75-105.

[23] Mulliner, C. 2009 "Vulnerability Analysis and Attacks on NFC-enabled MobilePhones". In Proceedings of. International Conference on Availability, Reliability and Security. 695-700.

[24] Strommer, Esko, Jouni Kaartinen, Juha Parkka, Arto Ylisaukko-oja, and Ilkka Korhonen. 2006 “Application of near field communication for health monitoring in daily life.” In International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 3246-3249. IEEE.

[25] Tiwari, Naveen Kumar, and Sanjay Khakhil. 2015 "Security System for DNS using Cryptography." International Journal of Computer Applications 120, no. 17.

[26] Gupta, Anil Kumar, Shashank Shukla, Sandeep Saxena, and Sanjay Khakhil. 2015. "A Journey towards Workflow Scheduling of Cloud Computing." International Journal of Computer Applications 123, no. 4
[27] Gupta, Anil Kumar, Shashank Shukla, Sandeep Saxena, and Sanjay Khakhil, 2016 "Bloom filter for elasticity in DBaaS." In IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 672-677.

[28] Shukla, Shashank, Anil Kumar Gupta, Sandeep Saxena, and Santosh Kumar, 2016 "An evolutionary study of multi-objective workflow scheduling in cloud computing." International Journal of Computer Applications 133, no. 14 14-18.

[29] Shukla, Shashank, Anil Kumar Gupta, Santosh Kumar Upadhyay, and Ashu Gupta. 2016 "Wireless Sensor Data Collecting to MobileCloud Device." International Journal of Computer Applications 138, no. 11.

[30] AMAZON, MULTI-OBJECTIVE WORKFLOW SCHEDULING IN. "International Journal OF Engineering Sciences & Management Research."