Review of an Enhanced Authentication Strategy for Multiservice Authorization over Mobile Cloud

Mr. Falesh M. Shelke
M.E. 3rd Sem Computer Science and Engineering
P.R.Patil College of Engineering
Amravati, India
falesh123@gmail.com

Prof. Pravin D. Soni
Prof. Department of Computer Science and Engineering
P.R.Patil College of Engineering
Amravati, India
pravindsoni@gmail.com

***Abstract*—** Cloud computing has changed the corporate as well as educational industry since it was introduced. The cloud computing is basically cost effective, convenient and on demand service offered to the end users. For instance it lead to cost reserve funds as well as better resource usage and removing the need of specialized technical skill for the users. There exists a huge security concern when utilizing cloud services. The security is extremely vital in cloud computing since individuals and organizations store private information in the cloud and it should likewise be not difficult to utilize the services provided to users. Since the control of services and information required for the regular run of a organization is handled by third party service providers, End user needs to believe the third party cloud service providers and trust that they handle their information in a right way and resources are available as and when needed. There are many approaches proposed for authentication in cloud services. They are intricate, insecure or highly exclusive. In this Paper we have carried of the comparative study of different authentication schemes in cloud computing finally summarize on the basis of different evaluation criteria.

Keywords- *cloud computing, authentication, security*

*****

I. INTRODUCTION

In today's decade cloud computing has gained a considerable acceptance as a promising model from both business and academic society. It is a model for enabling ubiquitous, handy, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. It has been provides resources as a part of service using internet technology. The cloud computing allows tenants to store programs or documents stored individually in large-scale computer to which can be accessed anytime and anywhere and to perform necessary works through various terminal units including PCs or Smartphone. In cloud computing environment tenants borrows and uses cloud resources as required and pays the expenses as uses. Most large-sized organizations have enough investment strength and high technical skills to build private cloud for the reason of security. In small and medium-sized organizations lack capital compared with large-sized organizations and so they tend to use public cloud with lower initial capital and operation costs compared with private cloud. In addition, the cloud computing technology comes with several problems and various security issues [2,3].

There are several schemes have been proposed to provide adequate security to cloud computing [4]. But, these existing security schemes measures lack security. The major issue consists of packet transmission multi-tenancy and storing, also encrypting user's data, cloud integrity, application security and security related to third-party [3,6]. In addition the openness nature of internet has many security flaws. so, attackers can misuse these flaws [5] to disturb various services using various kinds of threats and attacks.

1.1. Evaluation Criteria

In general authentication is the act of validating someone as authentic and claims they are legimistic users. In cloud computing validation is generally done using the login username and password. The knowledge of the password is adopted to ensure that the tenant is true. Each tenant registers first or gets registered by someone else on cloud server and using an assigned or self-stated secret word. During each successive use the tenant must know and use the password which is already declared. The weakness of this system is that passwords can often be stolen, unintentionally revealed or forgotten. Following table I describes possible authentication attacks.

TABLE I. Authentication attacks

Attacks	**Details**
Password guessing attack	This includes multiple attacks, including brute force, common passwords and dictionary attacks, which aim to obtain password of the user. The attacker can try to guess a specific user's password, try common passwords to all users or use an already made list of passwords to match against the password file, in their attempt to find a valid password.
Replay attack	The attacker tracks the authentication packet and replays this information to get an unauthorized access to the server.
Man-in-the-middle attack	The attacker passively puts himself in between the user and the verifier in an authentication process. The attacker then attempts to authenticate by pretending to be as the user to the verifier and the verifier to the user

Masquerade attack	The attacker pretends to be the verifier to the user to obtain authentication keys or data that may be used to authenticate fallaciously to the verifier.
Insider assisted attack	Systems managers intentionally compromise the authentication system or thieve authentication keys or relevant data of users.
Phishing attack	Social engineering attacks that use fake emails, web pages and other electronic communication to encourage the user to disclose their password and other susceptible information to the attacker.
Shoulder-surfing attack	Social engineering attacks definite to password systems where the attacker secretly directs observing the password when the user enters it.

A number of the security frameworks presented in the survey deal with security flaws or high computational cost. following evaluation parameters have been selected for comparing the presented security framework on the basis of what we have reviewed from different papers:

1) Identity management
2) User Privacy
3) Mutual Authentication
4) Replay attack
5) Man in middle attack
6) Denial of Service
7) Masquerade attack
8) Password guessing attack
9) Insider attack
10) Anonymity
11) Computational cost
12) Shoulder surfing attack
13)Phishing attack

II. SURVEY OF EXISTING SCHEMES IN CLOUD COMPUTING

One of the most popular and elderly remote user schemes was suggested by Lamport [7] in 1981, in which, the server stores the hashed value of a user's password. In Lamport's scheme, password table utilized to confirm the authenticity of users, but if this password table is compromised, stolen, or altered by an adversary, then the system could be in part or totally compromised.

Choudhury, A.; Kumar, P.; Sain, M.; Lim, H. and Hoon Jae-Lee proposed a method which uses Two Factor Authentication (2FA) where first the tenant gets verified by a password and smart card and then is authenticated by Out Of Band (OOB) authentication. Drawback of this work is smart card as login is prone to get stolen. For the messages sent from A to S are only related with secret data stored in the smartcard, the attacker can impersonate as a legal tenant. The attacker can compute intermediate values. Therefore, the messages in login phase authentication phase can be generated by the attacker so that the attacker can successfully create a valid login request as a legal tenant. Moreover, this method uses One Time Passwords (OTP)/OOB that is prone to phishing attacks [9] and clock has to be synchronized from time to time with the server.

The stolen-verifier attack works by stealing the password file. People fight this attack by saving hashed or encrypted password in the server. However, this solution is vulnerable to other attacks, as the tenant is still required to enter a password. The plain-text password traveling through the network can be intercepted by a third party [10], which called the man-in-the-middle attack. A countermeasure against the man-in-the-middle attack is to hash or encrypt the password before it is sent to network. However, this does not prevent the replay attack, which captures the encrypted password and uses it to intrude into the system.

Tenants are also authenticated using graphical passwords. The algorithm works as the tenant is made to select one image from multiple images and then tenant draws a correct pattern to get authenticated [11]. This algorithm is prone to shoulder surfing attacks. Another problem is the images are stored locally so if the device crashes, authentication would not be possible.

Some algorithms use biometric values as input to authenticate a tenant but despite all the benefits as a password technology, there are still some challenges. This technology cannot guarantee 100% correct identification [12]. Additionally, the implementation cost also increases as it needs hardware for taking biometric input. Another method proposed in [15] verifies a tenant is using Elliptic Curve Cryptography (ECC) where an elliptical curve equation with order n and selects a base point and generates pair of private public keys. The size of the curve ascertains the complexity of the problem. One of the fundamental demerits of ECC is that it expands the size of the encrypted message significantly more than RSA encryption. Moreover, the ECC algorithm is more complex and more difficult to implement than RSA, which expands the probability of implementation errors, thereby decreasing the security of the algorithm.

One time passwords are generated from algorithms. They are different from typical algorithms as they generate random passwords and do not repeat themselves. Every new password generated is unique from the previously generated ones. The main element of this algorithm is the seed value that is shared between the user and the server. During the authentication process, both user and server both individually generate OTPs and the user OTP is sent to server for verification. Server then verifies its own OTP with the user OTP. If both OTPs match, the tenant is authenticated. A software developer can use algorithms to generate one time passwords. The password generating software can be embedded in hardware or Java Smart cards, USB dongles, and mobile phones can run the password generating software to generate one-time passwords.

One time password can be generated in any of the two ways, HMAC based One Time Passwords (HOTP) [13] and Time based One Time Passwords (TOTP) [8, 14]. In HOTP, both the user and server will typically have an identical

initial seed (counter value). User generates a one-time password from the initial seed and any other input (PIN) and updates the seed (increment/ decrement the counter). Tenant submits the generated one-time password to server. Server likewise generates the password for that instance utilizing the seed and different inputs. If both passwords match, the server authenticates the tenant and updates the seed (increment/ decrement the counter). In TOTP, both the user and server will have synchronous time clocks and use an algorithm that generates one-time password from the synchronous time and any other inputs (PIN). User generates a one-time password and submits it to server. Server also generates a one-time password for that tenant for that instance of time and verifies it with the password received from user. As the clocks on user and server tend to drift over a period of time, maintaining time synchronization is a major challenge in this method. The main problem with the OTPs is the phishing attack. Common phishing attacks always lead the tenant to a fake web site whose look-and-feel is identical to legitimate one. The tenant generates the OTP and sends it to the fake website controlled by the attacker, which can now use this password to login to the real web site. Another problem with OTPs is if the seed value is compromised, the passwords can be generated by attacker and can impersonate the tenant to gain access to cloud resources.

Another 2FA method proposed in [16] authenticates the tenant using zero knowledge proof. First the tenant is verified using the username and password and the second factor is the credential file which is stored on tenant's USB or phone. The benefit of this scheme is the password need not be stored on the cloud server. This assures tenant from third party cloud service providers. However, this scheme would not allow the tenants to access the cloud resources if the credential file is lost or stolen.

In [17], author has proposed a scheme where tenant inserts smart card into the card reader and enters password as well as identifier. Tenant side generates a random value is generated using which is nonce and few variables are computed and sent to server. Upon receiving response from tenant, server checks upon the values to authenticate tenant. But this scheme is vulnerable to phishing attack and if the smart card is stolen, it would be impossible for tenant to get the access of cloud's resources.

Mohammad [18] highlighted the significant key drivers and constraints for secure cloud computing from a societal and technical perspective. The trust, privacy and user approach towards cloud computing are the social issues while on the other side encryption, scalability, reliability, data rights and transparency are the stern technological issues in cloud computing. Mostly cloud users are unaware of the risk of storing and transmitting private information in a shared environment. Therefore, key technological constraints like encryption, compliance, transparency, multi-tenancy and integrity should be addressed suspiciously. The transparency is the biggest challenge for the enterprises at current, and due to that, they are reluctant to switch to cloud computing surroundings. Once the cloud becomes transparent and the users have full control to admission, manage and report pertaining to the state of data and services only then it will help increase the trust and minimize the social and technological constraints.

Mirashe et *al.* [19] discuss the cloud computing service and deployment models and highlight their advantages. Authors further define the classes of cloud users e.g. families, corporations and community. According to the author's data protection is the major issue in cloud computing. Customer's data could be prone to serious threats if it is kept unencrypted on disk or memory or over the network in the cloud. Second major concern is related to the auditing of public cloud. The last but not least issue is legal jurisdiction over the cloud. Kandukuri et al. [20] discussed importance of the legal agreements between the service provider and client. Cloud service provider can secure trust of a client through SLAs and service quality. The SLA normally consists of eight main contents including Definition of Service, Problem Management, Customer Duties , Performance Management, and Responsibilities, Disaster, Recovery Security and Business Continuity and Termination. Moreover, the SLA should also describe how the security in the cloud is maintained and what are the methods and procedures used in maintaining security to make it client acquiescent.

Khan et al., [21, 22] proposed a machine learning approaches for post-event timeline reconstruction. They proposes techniques however are based on static analysis of the data enclosures. Iqbal et al., [23, 24] proposed performance metrics for software design and software project management. The Process improvement methodologies are elaborated in [25, 26] and Khan et al., [27] carried out quality assurance assessment. Amir et al., [28] discussed agile software development processes. Khan et al., [29] analyzed issues pertaining to requirement engineering processes. Khan and Umar [30, 31] analyzed non-functional requirements for software maintainability. Khan [32] suggests that Bayesian techniques are more promising than other conventional machine learning techniques for timeline reconstruction. Rafique and Khan [33] explored various methods, practices and tools being used for static and live digital forensics. In [34], Bashir and Khan discuss triaging methodologies being used for live di gital forensic analysis. Shahzad et al., [35] proposed a novel technique to protect systems form malware attacks. Zia et al., [36, 37] proposed a technique to reduce response time in cloud environment.

Table-II. Critical Evaluation of Security and Privacy Issues in Cloud Computing

Ref	Research	Theme	Issues Discussed Proposed Solution	Strength/Benefis	Scope
Jansen [38]	Security and Privacy issues in Cloud Computing	Trusted and reliable computing	Service Level Agreements, Policies and Procedures,Risk Management.	Data Security and Privacy will be Ensured	Limited to addressing technical issues
Julisch [39]	Security and Control in Cloud Computing	Security and controls concerns	Service Level Agreements, Virtual Information, Security Management System (ISMS).	Standard compliant management process and assets protection will be ensured	Limited to addressing the management and controls issues
Mohammed [40]	Secure Cloud Computing	Social and Technological Constraints	Proposeda solution to address Compliance, Transparency, Encryption and Multi-tenancy.	Data privacy will be ensured	Limited to addressing social and technical issues
Mehmood [41]	Security and Data Storage Location in Cloud Computing	Data issues of storage location, cost, availability and security	Appropriate use of cloud technologies	Data storage location and availability will be ensured	Limited to addressing data storage location issues
Svantesson [42]	Risk in Cloud Computing	Legal Regulatory Aspects and Consumer Rights	Improvement in consumer rights and privacy laws.	Consumer rights protection will be ensured	-
Almulla [43]	Security Management in Cloud Computing	Data Security and Identity and Access Management (IAM)	A solution to address Identity Management-as-a-Service (IDaaS).	Authentication, Authorization and auditing will be ensured	Limited to discussing the identity and access management
Relly [44]	Forensic Investigation for Cloud Computing	Computer Forensic from Law Enforcement prospective Pros and Cons of Forensic	-	Law Enforcement	Scope to improve and develop forensic procedures and tools
Patil [45]	Data Security in Cloud Computing	Data Access Control	A solution to address Authenticati-on mechanism.	Security, privacy and compliance will be ensured	Limited to addressing access control issues
Chen [46]	Security Controls in Cloud Computing	Life Cycle Data on Cloud	Data Security and Privacy.	Data Identification, Isolation and Privacy protection will be ensured	-
Kandukuri [47]	Service Level Agreements for Secure Cloud	Client Compliance and Trust	Compliance, Trust,Data Segregation and Recovery	Data security policies and procedures will be ensured	Scope to design standard SLAs

III. PROPOSED WORK

I have proposed a system which will covers the security issues related to Cloud authentication and identity management over the cloud.

Steps of working**:**

1. User Signs up with Log In Id and Password
2. User Logs In on Cloud
3. Token is given via Multichannel to the user (this is done using Kerberos Authentication)
4. If user wants to access a service then that token and service id is passed from mobile to server
5. The Server matches the token and finds out if the user is allowed to access the particular service. If service access is not allowed then server logs the user out else provides service.

Diagrammatic Representation of a system:

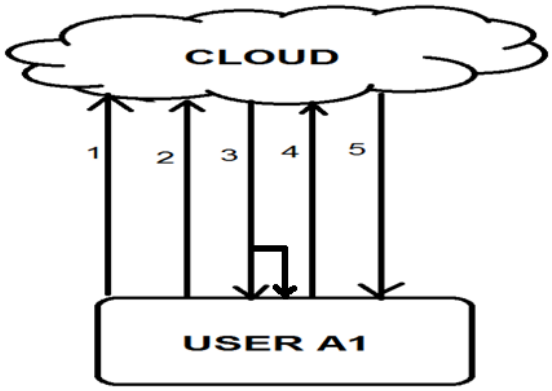

Fig.1. Diagrammatic view of proposed System

IV. CONCLUSION

We have discussed various authentication schemes for cloud computing. With wide variety of applications of cloud computing, security is one of the major issues. Authenticating cloud users is gaining more attention. Diverse schemes have been proposed in literature, some of which we have stated in our survey. From our observations, we conclude that the reviewed cloud authentication schemes lack resistance to some or the other attacks. However none of the scheme fulfills all the criteria of the evaluation. So using this work one can get encouragement to develop new scheme that may satisfy the all criteria of the evaluation.

REFERENCE:

[1] "The NIST Definition of Cloud Computing", NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Ronald. and Russell, D.,Cloud Security: A comprehensive Guide to Secure Cloud Computing, Wiley 2012, ISBN 978-0470589878.

[3] Mutum, M. and Goel, A., "Security issues in cloud computing", Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on, pp.1321-1325, 16-18 Oct. 2012.

[4] S. Lee lim, lee "Two factor authentication in cloud computing" – downloads/cloud/security

[5] Jaatun M., Zhao G. and Rong C., "Access Control of Cloud Service Based on UCON", CloudCom 2009, LNCS 5931,pp. 559–564, 2009.

[6] [6] Tianfield, H., "Security issues in cloud computing", Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on, pp.1082-1089, 14-17 Oct. 2012.

[7] Lamport, L., "Password Authentication with Insecure Communication", Communications of the ACM 24.11 , pp.770-772, Nov. 1981.

[8] Choudhury, A.; Kumar, P.; Sain, M.; Lim, H. and Hoon Jae-Lee, "A Strong User AuthenticationFramework for Cloud Computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, pp.110-115, 12-15 Dec. 2011.

[9] Xuguang, R. and Xin-Wen, W., "A novel dynamic user authentication", Communications and Information Technologies (ISCIT), 2012 International Symposium on, pp.713-717, 2-5 Oct. 2012.

[10] Forouzan, B., Cryptography and Network Security (Sie), Tata McGraw-Hill Education, 2011, pp.416-421, ISBN 9780 070660465.

[11] Guo, M.; Liaw, H.; Hsiao, L.; Huang, C.; and Yen, C., "Authentication using graphical password in cloud", Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on , pp.177-181, 24-27 Sept. 2012.

[12] Khitrov M., "Talking passwords: voice biometrics for data access and security", Biometric TechnologyToday, Volume2013, Issue2, February2013, Pages9-11,ISSN 0969-4765, http ://dx .doi .org /10. 1016/S0969-4765(13)70036-5.

[13] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, December 2005.

[14] D., M'Raihi, S., Machani, M., Pei and J., Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, May 2011.

[15] Chen, T.; Yeh, H. and Shih, W., "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing", Multimedia & Ubiquitous Engineering(MUE),2011 5th FTRA International Conference on, pp.155-159, 28-30 June 2011.

[16] Yassin, A.A.; Hai J.; Ibrahim, A.; Weizhong Q. and Deqing Z., "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing", Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, pp.1210-1217, 21-25 May 2012.

[17] Jaidhar, C.D.,"Enhanced Mutual Authentication Scheme for Cloud Architecture", Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp.70-75, 22-23 Feb. 2013 doi: 10.1109/IAdCC.2013.

[18] D. Mohammed, "Security and Cloud Computing: An Analysis of Key Drivers and constraints", Information Security Journal: A Global Perspective, vol. 20, (2011), pp. 123-127.

[19] S. P. Mirashe and Dr. N. V. Kalyankr, "Cloud Computing", Journal of Computing, vol. 2, issue 3, (2010)March.

[20] B. R. Kandukuri, R. Paturi V and Dr. A. Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, IEEE.

[21] M. N. A. Khan, C. R. Chatwin and R .C. Young, "A framework for post-event timeline reconstruction using neural networks. digital investigation, vol. 4, no. 3, (2007), pp. 146-157.

[22] M. N. A. Khan, C. R. Chatwin and R .C. Young, "Extracting Evidence from Filesystem Activity using Bayesian Networks", International journal of Forensic computer science, vol. 1, (2007), pp. 50-63.

[23] S. Iqbal, M. Khalid and M. N. A. Khan, "A Distinctive Suite of Performance Metrics for Software Design", International Journal of Software Engineering & Its Applications, vol. 7, no. 5, (2013).

[24] S. Iqbal and M. N. A. Khan, "Yet another Set of Requirement Metrics for Software Projects", International Journal of Software Engineering & Its Applications, vol. 6, no. 1, (2012).

[25] M. Faizan, S. Ulhaq and M. N. A. Khan, "Defect Prevention and Process Improvement Methodology for Outsourced Software Projects", Middle-East Journal of Scientific Research, vol. 19, no. 5, (2014), pp. 674-682.

[26] M. Faizan, M. N. Ahmed and S. Ulhaq, "Contemporary Trends in Defect Prevention: A Survey Report", International Journal of Modern Education & Computer Science, vol. 4, no. 3, (2012).

[27] K. Khan, A. Khan, M. Aamir and M. N. A. Khan, "Quality Assurance Assessment in Global Software Development", World Applied Sciences Journal, vol. 24, no. 11, (2013).

[28] M. Amir, K. Khan, A. Khan and M. N. A. Khan, "An Appraisal of Agile Software Development Process", International Journal of Advanced Science & Technology, vol. 58, (2013).

[29] A. Khan, M. Naeem, M. Khalid and S. ul Haq, "Review of Requirements Management Issues in Software Development", International Journal of Modern Education & Computer Science, vol. 5, no. 1, (2013).

[30] M. Umar and M. N. A. Khan, "A Framework to Separate Non-Functional Requirements for System Maintainability", Kuwait Journal Of Science & Engineering, vol. 39, no. 1 B, (2012), pp. 211-231.

[31] M. Umar and M. N. A. Khan, "Analyzing Non-Functional Requirements (NFRs) for software development", In Software Engineering and Service Science (ICSESS), 2011 IEEE 2nd

International Conference, IEEE,(2011) July, pp. 675-678.

[32] M. N. A. Khan, "Performance analysis of Bayesian networks and neural networks in classification of file system activities", Computers & Security, vol. 31, no. 4, pp. 391-401.

[33] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools".

[34] M. S. Bashir and M. N. A. Khan, "Triage in Live Digital Forensic Analysis", International journal of Forensic Computer Science, vol. 1, (2013), pp. 35-44.

[35] A. Shahzad, M. Hussain and M. N. A. Khan, "Protecting from Zero-Day Malware Attacks", Middle-East Journal of Scientific Research, vol. 17, no. 4, (2013), pp. 455-464.

[36] A. Zia, A. Khan and M. Naeem, "Identifying Key Challenges in Performance Issues in Cloud Computing",International Journal of Modern Education & Computer Science, vol. 4, no. 10, (2012).

[37] A. Zia and M. N. A. Khan, "A Scheme to Reduce Response Time in Cloud Computing Environment", International Journal of Modern Education & Computer Science, vol. 5, no. 6, (2013).

[38] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences - 2011, IEEE.

[39] K. Julisch and M. Hall, "Security and Control in the Cloud", Information Security Journal: A Global Perspective, vol. 19, (2010), pp. 2099-309.

[40] D. Mohammed, "Security and Cloud Computing: An Analysis of Key Drivers and constraints", Information Security Journal: A Global Perspective, vol. 20, (2011), pp. 123-127.

[41] Z. Mehmood, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web technologies, IEEE, (2011).

[42] D. Svantesson and R. Clarke, "Privacy and Consumer Risks in Cloud Computing", Computer Law and Security Review, vol. 26, (2010), pp. 391-397

[43] S. A. Almulla and C. Y. Yeun, "Cloud Computing Security Management".

[44] D. Relly, C. Wren and T. Berry, "Cloud Computing: Pros and Cons for Computer Forensic Investigations", International Journal Multimedia and image Processing (IJMIP), vol. 1, issue 1, (2011) March, pp. 26-34.

[45] D. H. Patil, R. R. Bhavsar and A. S. Thorve, "Data Security over Cloud", International Journal of Computer Applications® (IJCA), (2012).

[46] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering, IEEE.

[47] B. R. Kandukuri, R. Paturi V and Dr. A. Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, IEEE.