ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

Fog Computing: Data Theft Detection in Cloud with Behaviour Pattern & Decoy Stuff

Saniket M. Kudoo, Prof. Dilip Motwani

M.E Student, Dept. of Computer Engineering, Vidyalankar Institute of Technology, Wadala,Mumbai, India.

Assistant Professor, Dept. of Computer Engineering, Vidyalankar Institute of Technology, Wadala, Mumbai, India.

ABSTRACT: Day to day era of Cloud Computing growing as an emerging technology and its critical role in the IT industry upgrade and economic development in the future. Cloud computing is becoming the next revolution in the IT industry, providing centralize storage for internet data and network services that have the potential to bring data transmission performance, security and privacy and inefficient architecture to the next level. With these new computing paradigms arise new data security challenges. Data security is the biggest challenge faced by cloud storage. Existing mechanism in cloud storage have failed time to time for variety of reasons to maintain security. Cloud computing and storage solutions provide users and various enterprises with various capabilities to store and process their data in third-party data centers. We propose different technique for securing data in cloud storage with fog computing. We monitor data access in cloud environment and depends on user behavior technique, detects abnormal behavior of user data access patterns. When abnormal pattern is suspected and then verified using challenge question then we launch disinformation to the user with fog computing to the attacker this will protects against companies real data to be hacked.

KEYWORDS: cloud computing, fog computing, data theft attack, cloud security

Cloud computing allows kinds of organizations to have the opportunity to use Internet-based services (SAAS, IAAS, PAAS) so that they can reduce start-up costs, lower capital expenditures, use services on a pay-as-you-use basis, access applications only as needed, and quickly reduce or increase capacities.

The existing mechanisms only facilitate security features to data and thereby don't allow for detection of invalid access and thereby its prevention to enable valid distribution of data. The proposed mechanism facilitates security features to data and thereby allows for detection of invalid access and thereby its prevention to enable valid distribution of data.[1]

In today's generation of cloud computing most of the small and medium scale business are increasingly outsourcing data and computation to the cloud.[3] This obviously reduces their cost and infrastructure but at the high risk of data theft attacks. This is considered as one of the top thread to the cloud computing by cloud security alliance.(CSA)[4]

The data breach at Target, resulting in the loss of personal and credit card information of up to 110 million individuals, was one of a series of startling thefts that took place during the normal processing and storage of data.[9] "Cloud computing introduces significant new avenues of attack," said the CSA report authors. The absolute security of hypervisor operation and virtual machine operations is still to be proved. Indeed, critics question whether such absolute security can exist. The report's writers said there's lab evidence -- though none known in the wild -- that breaches via hypervisors and virtual machines may occur eventually.[9]

"Unfortunately, while data loss and data leakage are both serious issues [1] to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other," the report said. Encryption protects data at rest, but lose the encryption key and you've lost the data, so sometimes encryption also fails. The cloud routinely makes copies of data to prevent its loss due to an unexpected die off of a server. The more copies, the more exposure you have to breaches. [8]

Several twitter corporate accounts and personal documents of U.S.President Barack Obama [7] were illegally accessed, the attacker used a twitter admin password to gain access to twitter corporate documents.[3] The authors also demonstrated how cloud customers private keys might be stolen and how their confidential data might be extracted from hard drive. After stealing the customer password and private key the intruder get access to all customer data while the customer has no means of detecting this unauthorized access.[1]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

Much research and study in cloud computing security domain has demanded for preventing unauthorized access to data by implementing access control and encryption technique. However these mechanism have not been able to meet customer's data protection. Van dijk and Juels have shown that fully homomorphic encryption [3] often acclaimed as solution to such threads is also not sufficient data protection mechanism when used alone.

I. ACCESS CONTROL AT CLOUD

Numerous technique are present to cloud based services to store digital stuff, documents in a remote service that may anywhere anytime. Particularly many proposal have been made yet to secure remote data to cloud using encryption techniques and access controls. [1] Building the trust cloud is not enough but also you have to give assured authentication for data protection to the user because accidents of intruders and attacker continues happens and once we lost our confidential data we cannot get it back.

The basic idea of this paper will recognized user behavior into the cloud environment for daily routine work. That daily routine employee contains limited search of their work. User pattern search algorithm will continually monitor every moment performing into cloud to check whether it is normal access or abnormal access. This method of behavior based profiling is commonly used in theft detection application. Such mechanism would naturally include huge information in environment that which documents are typically accessed by whom and how it is accessed often. These simple user specific features can apply to detect abnormal access into cloud environment for trusted user or un-trusted user.

II. USER BEHAVIOR PATTERN RECOGNITION

Behaviouralanalytics [2] like utilizes user data captured while using the web application, game, or website or any cloud environment is in use by analytic platforms like Google Analytics. Users Platform traffic data like navigation paths, users clicks, users social media interactions is all recorded.[6] Also, other more specific advertising metrics like users click-to-conversion time, and comparisons between other metrics like the monetary value of an order and the amount of time spent on the site These all data points are then compiled and analyzed, Behavioral analysis allows future actions and trends to be predicted based on all the data collected.[6] Like this it also works for cloud security environment users or intruders behavior search, users clicks, users password insertion, users file searching criteria depend on this pattern of every user recorded.

III. PATTERN BASED DECOY STUFF

Decoy documents contain honey files, honeypots and other various bogus information will be generated on demand and provide as a means of detecting unauthorized access to information and "POISON" to thief's ex-filtered information. Providing this type of decoy fake information to the attacker or intruder confound and confuse them into believing that they have downloaded or accessing useful information when they have not actually.

This decoy technology [8] may be integrated with user behaviour pattern technology for securing user confidential data in cloud. Whenever there is abnormal access in cloud service is tracked decoy information may be provide by the cloud and deliver to the attacker or user in such a way that as appear in normal and legitimate.

IV. FOG COMPUTING

We placed traps within the cloud real data storage. The traps are decoy documents downloaded or prepared from fog computing site, an automated service that offers several types of decoy files such as employee's medical records, bank account statements, credit card statements, tax returns documents, and online purchase receipts. The decoy documents are downloaded from legitimate user and stored in location of highly accessible module that are not likely to cause any interference with daily normal user activities on the system.

An intruder or attacker who is not familiar with our file system and its content is same as accessing the decoy files if she or he is in search for sensitive information. On the basis of behaviour testing he or she will get redirect to decoy module of fake information which is not useful for the any user weather he is normal or abnormal. We implement different mechanism to securing the cloud using decoy information technology that we have come to call Fog Computing. We used this technology to launch fog information attacks like disinformation attack against malicious

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

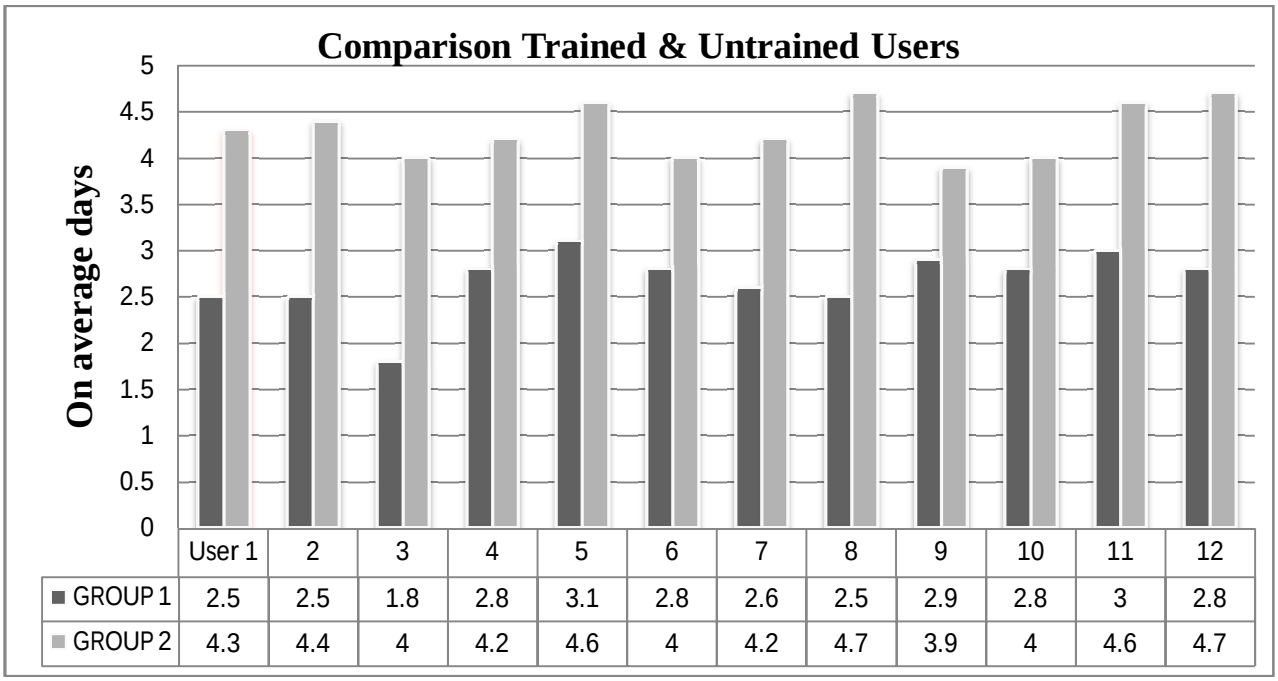
intruders,insider's theft preventing them for distinguishing the real sensitive customer data from fake Cloud fog computing data.

HMAC Authentication Key

A key hash message authentication code (HMAC) is a specific construction mechanism for calculating message authentication code containing cryptographic hash function in combination of secret cryptographic key. [5] As with any message authentication code it may be used to simultaneously verify both the authentication of a message and data integrity. An iterative hash function breaks up a message into blocks of fixed size and iterate over them with a compression function like MD-5 and SHA-1 operates on 512 beats blocks. The size of the output is same as that of the underlying hash function that is 128 or 160 bits in the case of MD-5 or SHA-1 although it can be truncated if desired.

$$HMAC(K,m) = H\Big((K \oplus opad) \mid\mid H\big((K \oplus ipad) \mid\mid m\big)\Big)$$

Where H is a cryptographic hash function, K is a secret key padded to the right with extra zeroes to the input block size of the hash function and if it is longer than the block size, m is the message to be authenticated. || denotes concatenation, K EXOR outer padding & K EXOR inner padding. [5]
The decoy documents carry HMAC authentication code for every file user download or access. The HMAC is computed over the file's content unique to each user. When decoy documents loaded into memory we verify that weather document is decoy documents by computing HMAC based on all the contents of that documents. For accessing or downloading any documents from environment our system will ask every time for user to insert passkey which they already got from system at the time of registration into cloud environment. So every trusted or registered user have their respective passkey generated by the hash message access control for every time.
When unauthorized or abnormal user accessing the decoy documents or any other documents into the system it will ask for passkey which every trusted user have which can be on the basis of recovery with the use of one challenge question for register user.



	User 1	2	3	4	5	6	7	8	9	10	11	12
GROUP 1	2.5	2.5	1.8	2.8	3.1	2.8	2.6	2.5	2.9	2.8	3	2.8
GROUP 2	4.3	4.4	4	4.2	4.6	4	4.2	4.7	3.9	4	4.6	4.7

We studied 12 cloud users on our system, collected over a period of 5 days on average. The 12 users (GROUP 1) were trained about the system and we also trained other 12 (GROUP 2) cloud users for without any knowledge of system like intruders or attackers. We tested these users using simulated data into the cloud and our result states that user's profiles are accurate enough to identify normal or abnormal user. When such unauthorized or abnormal access is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

detected system can respond by presenting the user by challenge question or decoy fog computing data. First trained group of series (GROUP 1)those who are having complete knowledge of system machine does not recognized any abnormal pattern for them where as another group of 12 members (GROUP 2)those who are not familiar with cloud system machine detect various enough abnormal access for them which are redirected to fog decoy data.

V. CONCLUSION

In this paper we present novel approach to securing personal and business data in the cloud environment. We implement monitoring data access pattern into the cloud with the help of user'sbehaviour pattern search to determine if and when malicious insiders or intruders accesses someone's documents into cloud storage. Decoy documents of our fog computing are in the cloud alongside the users real data. Once unauthorized data access or exposure is suspected in system and later verified with the passkey or challenge question and system can redirect him or her to fog data. Based on this we also can distinguish real users and data theft attacker and system can block his access or declared as an invalid user. Such preventive attacks with fog computing we can really protect our personal confidential as well as cloud information.

ACKNOWLEDGEMENT

This material is based on work supported by Defence Advanced Research Project Agency (DARPA) under the Anomaly detection at multiple scales (ADAMS) program. As I wish to express my sincere gratitude to PROF. DILIP MOTWANI (Vidyalankar Institute technology , Wadala) for providing me opportunity to do my project work in cloud – fog computing. I also wish to express my sincere thanks to all other staff members of Vidyalankar Institute of Technology, Wadala.

REFERENCES

[1]Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2]M. Ben-Salem and S. J. Stolon, "Combining a baiting and a user search profiling techniques for masquerade detection," in Columbia University Computer Science Department, Technical Report # cucs-018-11, 2011.
Available: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1468

[3] Fog Computing: Mitigating Insider Data Theft Attacks.PDF http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6227695

[4] The permanent and official location for the Cloud Security Alliance Top Threats research is: http://www.cloudsecurityalliance.org/topthreats

[5] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION:The Keyed-Hash Message Authentication Code (HMAC).pdf

[6] International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013 DOI: 10.5121/ijcnc.2013.5112 171: A USER PROFILE BASED ACCESS CONTROL MODEL

[7] P. Allen, "Obama's Twitter password revealed after French hacker arrested for breaking into U.S. president's account," March 2010.[Online]. Available:http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas- Twitter-password-revealed-French-hacker-arrested.html

[8] Protecting cloud through decoy technology: international journal of technology and Engineering science (IJTES) volume 1(9) Dec2013

[9] Data breach attack:https://en.wikipedia.org/wiki/Data_breach