RESEARCHERID
THOMSON REUTERS

[Vishistha * *et al.*, 7(6): June, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DATA THEFT DETECTION IN THE CLOUD

Atul Vishistha[*1] & Nidhi Singh[2]

[*1]M. Tech Scholar, Computer Science Engineering (CSE), Vivekanand Institute of Technology and Science, Ghaziabad (VITS)

[2]Assistant Professor, Computer Science Engineering (CSE), Vivekanand Institute of Technology and Science, Ghaziabad (VITS)

DOI: 10.5281/zenodo.1284174

ABSTRACT

Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment.

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 thirdparty 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, IT industry.

I. INTRODUCTION

Businesses, especially startups, small and medium businesses (SMBs), are increasingly opting for outsourcing data and computation to the Cloud. This obviously supports better operational efficiency, but comes with greater risks, perhaps the most serious of which are data theft attacks. Data theft attacks are amplified if the attacker is a malicious insider. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance .While most Cloud computing customers are well-aware of this threat, they are left only with trusting the service provider when it comes to protecting their data. The lack of transparency into, let alone control over, the Cloud provider's authentication, authorization, and audit controls only exacerbates this threat. The Twitter incident is one example of a data theft at-tack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website TechCrunch and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed .The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents, hosted on Google's infrastructure as Google Docs. The damage was significant both for Twitter and for its customers. While this particular attack was launched by an outsider, stealing a customer's admin passwords is much easier if perpetrated by a malicious insider. Rocha and Correia outline how easy passwords may be stolen by a malicious insider of the Cloud service provider The authors also demonstrated how Cloud customers' private keys might be stolen, and how their confidential data might be

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

extracted from a hard disk. After stealing a customer's password and private key, the malicious insider get access to all customer data, while the customer has no means of detecting this unauthorized access. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise. Van Dijk and Juels have shown that fully homomorphic encryption, often acclaimed as the solution to such threats, is not a sufficient data protection mechanism when used alone. We propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. In this paper, we propose two ways of using Fog computing to prevent attacks such as the Twitter attack, by deploying decoy information within the Cloud by the Cloud service customer and within personal online social networking profiles by individual users.

II. CLOUD DATA STORAGE CHALLENGES & ISSUES

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full of control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data leads in greater security issues than the generic cloud computing model as shown in figure 1.

The only encryption doesn't give full control over the stored data but it gives somewhat better than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various possibilities of attacks than in the generic cloud model. The figure 2 has various issues those are discussed below in clearly.

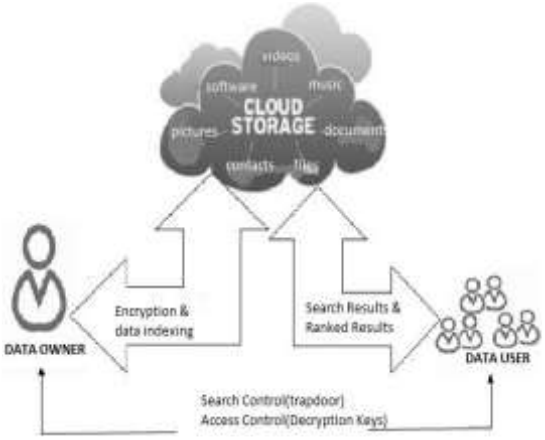

Figure 1: Cloud data storage model

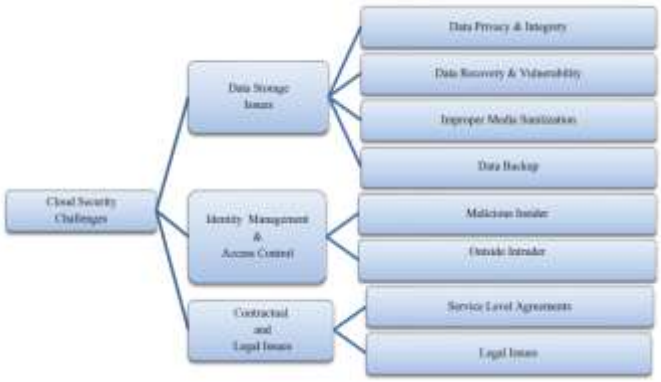

Figure 2. Cloud security Challenges

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

2.1 Cloud Storage issues

2.1.1 Data privacy and Integrity

Even though cloud computing provide less cost and less resource management, it has some security threats. As we discussed earlier cloud computing has to ensure integrity, confidentiality, privacy and availability of data in generic cloud computing model but the cloud computing model is more vulnerable to security threats in terms of above conditions. Because of simplicity cloud users are increasing exponentially and applications are hosted in cloud is very high. These situations lead to greater security threats to cloud clients. If any attack is successful on data entity will leads to data breach and takes an unauthorized access to data of all cloud users. Because of this integrity violation cloud data lost multi-tenant nature. Especially SaaS providers may also lost their technical data and they have great risk over data storage. Apart from these risks, data processing also has great risk while data being transformed among multiple tenants. Because of virtualization multiple physical resources are shared among the users. This leads to launch attacks by malicious insiders of the CSP and/or organization. These situations may allow the malicious user to perform attacks on stored data of other customer while processing their data. Other major risk is when data is outsourced to third party storage by the CSP [5]. The key generation and key management in cryptography for cloud computing is not standardized up to the mark. But without standard and secure key management for the cloud doesn't allow the standard cryptography algorithms to perform well in generic cloud computing model. Such that cryptography may also ensures the potential risks to cloud computing.

2.1.2 Data recoverability and vulnerability

Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on-demand Resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users [13]. The authors in [13] were able to recover Amazon machine images files 98 % of the times. The data recovery vulnerability can pose major threats to the sensitive user data.

2.1.3 Improper media refinement.

The storage medias are sanitize because of following reasons

- the disk may needs to replace with other disk
- No need to maintain the disk or no longer to maintain (iii) massacre of services. Improper refinement ensures great risk to stored data. In multi-tenant cloud it is not possible to refine as it is earlier tenant.

2.1.4 Data backup

The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability. In fact, the backup data should be keeping with security guidelines to prevent malicious activities such as tampering and unauthorized access.

2.2. Identity Management and Access Control

The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. In cloud environment, different organizations use variety of authentication authorization agenda. By using different approaches for authentication and authorization gives a compound situation over a period of time. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quickly updating and managing identity management for joining and leaving users over cloud resources. There are many issues in access control and identity management, for example weak credentials may reset easily, denial of service attack to lock the account for a period of time, Weak logging and monitoring abilities, and XML wrapping attacks on web pages.

2.2.1 Malicious Insiders

An insider threat can be posed by employees, contractors and /or third party business partners of an organization. In cloud environment i.e., at Cloud Service Provider (CSP) side attacks leads to loss of user's information integrity, confidentiality, and security. This leads to information loss or breaches at both

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

environments.. This attack is precious and it is well known to most of the organization [7].There is variety of attack patterns performed by insiders because of sophistication about internal structure of an organization data storage structure. Most organizations ignoring this attack because it is very hard to defend and impossible to find the complete solution for this attack. This attack ensures great risk in terms of data breaches and loss confidentiality at both organization and cloud level [8].

2.2.2 outside Intruder

Attacks that come from external origins are called outsider attacks [30]. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centers. But they must depend on the infrastructure provider to get full data security. In a virtual private cloud environment, the service provider can only specify the security setting remotely, and we don't know exactly those are fully implemented. In this Process, the infrastructure provider must reach the following objectives:

- confidentiality, for secure data transfer and access, and
- audit ability [13]. So that outside intruders can't access sensitive data which is stored in cloud.

2.3 Contractual and Legal issues

After moving to cloud computing environment, there are many issues in geographic jurisdictions, regulatory law, performance assurance, contract enforcements, etc. The above mentioned issues are comes under the legalities, Service Level Agreements and data location in data centers [9].

2.3.1. Service level agreements

The Service Level Agreement (SLA) can be described as a protocol, it specifies set of conditions and terms among user and Cloud service provider. The SLA should specify the following: Actions that CSP will taken when data breach happened, remedial actions and performance level at minimum level [5]. The users should have clear view on security for their resources and all other requirements should be agreed upon the SLA. The contract enforcement becoming issues because statistics provided by CSP are totally unproven. Finally, the contracts are non-negotiable and pre-defined that has to be in friendly manner between CSP and user. The regulatory laws such as Sarbanes- Oxley and HIPAA become an open issue [10].

2.3.2. Legal issues

The legal issues arise because that the presence CSP resources in geographically conflicting various legal jurisdictions [11]. If the user is migrated to one geographical to other, an issue will occur because of different legal jurisdictions. For a movement data is distributed over a various data centers, those are owned by CSP those have different laws and security guidelines. This scenario may takes into the serious issue in cloud computing.

III. EXISTING SYSTEM

In the present system the Cloud computing is new technique to provide service (SaaS, IaaS, PaaS) to the client over the internet, the users can use any type of the cloud service according to his need.

Cloud computing provide storage space service for the users , user can store his data and information in the cloud and he can access to the information and store it from any computer connected to the internet, the important thing that should be known is the user don't know where the information is store? And how it is store? And who can see the data and information?

The problem of the user when he store sensitive data or business information in the cloud , the user need security of the cloud computing to ensure no one can access and view his data and information that is store in the cloud ,the data security is the solution to this problem by doing encryption to the data to convert it to the cipher text by using any of the encryption algorithms and protection mechanisms to prevent any one access this data to understand what it is.

Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Disadvantages:

1. By applying encryption technique to the data we can't achieve total security to confidential data.
2. Anyone can access the data he can decrypt it if he know the algorithm
3. No one is known when the attack is happen.
4. It is difficult detect which client is attack.
5. We cannot detect which file was hacking.

IV. PROPOSED SYSTEM

To solve the problem I propose a different approach for securing data in the cloud using offensive decoy technology. I monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, I launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment. I propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing. I use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.

Advantages:

1. The information stored on the Cloud can be secured commensurable way.
2. The insider attack can be detected. The accuracy of detection of a masquerader a great by combining the technique.
3. The confusion of the attacker through decoy documents safeguards the actual data of the us
4. Using Decoy technology we are protecting our data by eliminating /avoiding the attacker from accessing our data.
5. Low cost and economical as we are not going to encrypt entire data.
6. Using decoy technology we are providing bogus information to confuse the user by confusing the user real user can protect the data.

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

Securing cloud data with fog

Numerous proposals for cloud-based services describe methods to store documents, files, and media in a remote service that may be accessed wherever a user may connect to the Internet. A particularly vexing problem before such services are broadly accepted concerns guarantees for securing a user's data in a manner where that guarantees only the user and no one else can gain access to that data. The problem of providing security of confidential information remains a core security problem that, to data, has not provided the levels of assurance most people desire.

Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls. It is fair to say all of the standard approaches have been demonstrated to fail from time to time for a variety of reasons, including in-sider attacks, misconfigured services, faulty implementations, buggy code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

procedures. Building a trustworthy cloud computing environment is not enough, because accidents continue to happen, and when they do, and information gets lost, there is no way to get it back. One needs to prepare for such accidents.

The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen information to the attacker. We can achieve this through a 'preventive' disinformation attack. We posit that secure Cloud services can be implemented given two additional security features

1) User Behavior Profiling: It is expected that access to a user's information in the Cloud will exhibit a normal means of access. User profiling is a well known Technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. These simple user specific features can serve to detect abnormal Cloud access based partially upon the scale and scope of data transferred
2) Decoys: Decoy information, such as decoy documents, honeyfiles, honeypots, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's ex-filtrated information. Serving decoys will confound and confuse an adversary into believing they have ex-filtrated useful information, when they have not. This technology may be integrated with user behavior profiling technology to secure a user's information in the Cloud. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely legitimate and normal. The true user, who is the owner of the information, would readily identify when decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has inaccurately detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver unbounded amounts of bogus information to the adversary, thus securing the user's true data from unauthorized disclosure. The decoys, then, serve two purposes:

- Validating whether data access is authorized when abnormal information access is detected, and
- Confusing the attacker with bogus information. We posit that the combination of these two security features will provide unprecedented levels of security for the Cloud. No current Cloud security mechanism is available that provides this level of security.

We have applied these concepts to detect illegitimate data access to data stored on a local file system by masqueraders, i.e. attackers who impersonate legitimate users after stealing their credentials. One may consider illegitimate access to Cloud data by a rogue insider as the malicious act of a masquerader. Our experimental results in local file system setting show that combining both techniques can yield better detection results, and our results suggest that this approach may work in a Cloud environment, as the Cloud is intended to be as transparent to the user as a local file system. In the following we review briefly some of the experimental results achieved by using this approach to detect masquerade activity in a local file setting.

Combining User Behavior Profiling and Decoy Technology for Masquerade Detection

User Behavior Profiling: Legitimate users of a computer system are familiar with the files on that system and where they are located. Any search for specific files is likely to be targeted and limited. A masquerader, however, who gets access to the victim's system illegitimately, is unlikely to be familiar with the structure and contents of the file system. Their search is likely to be widespread and untargeted.

Based on this key assumption, we profiled user search behavior and developed user models trained with a one-class modeling technique, namely one-class support vector machines. The importance of using one-class modeling stems from the ability of building a classifier without having to share data from different users. The privacy of the user and their data is therefore preserved.

We monitor for abnormal search behaviors that exhibit de-viations from the user baseline. According to our assumption, such deviations signal a potential masquerade attack. Our pre-vious experiments validated our

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

assumption and demonstrated that we could reliably detect all simulated masquerade attacks using this approach with a very low false positive rate of 1.12%

Decoy Technology: We placed traps within the file system. The traps are decoy files downloaded from a Fog computing site, an automated service that offers several types of decoy documents such as tax return forms, medical records, credit card statements, e-bay receipts, etc. [10]. The decoy files are downloaded by the legitimate user and placed in highly-conspicuous locations that are not likely to cause any interference with the normal user activities on the system. A masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files, if he or she is in search for sensitive information, such as the bait information embedded in these decoy files. Therefore, monitoring access to the decoy files should signal masquerade activity on the system. The decoy documents carry a keyed-Hash Message Authentication Code (HMAC), which is hidden in the header section of the document. The HMAC is computed over the file's contents using a key unique to each user. When a decoy document is loaded into memory, we verify whether the document is a decoy document by computing a HMAC based on all the contents of that document. We compare it with HMAC embedded within the document. If the two HMACs match, the document is deemed a decoy and an alert is issued.

The advantages of placing decoys in a file system are three-fold:

- The detection of masquerade activity
- The confusion of the attacker and the additional costs incurred to distinguish real from bogus information, and
- The deterrence effect which, although hard to measure, plays a significant role in preventing masquerade activity by risk-averse attackers.

Combining the Two Techniques: The correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy. We hypothesize that detecting abnormal search operations performed prior to an unsuspecting user opening a decoy file will corroborate the suspicion that the user is indeed impersonating another victim user. This scenario covers the threat model of illegitimate access to Cloud data. Furthermore, an accidental opening of a decoy file by a legitimate user might be recognized as an accident if the search behavior is not deemed abnormal. In other words, detecting abnormal search and decoy traps together may make a very effective masquerade detection system.

Combining the two techniques improves detection accuracy
We use decoys as an oracle for validating the alerts issued by the sensor monitoring the user's file search and access behavior. In our experiments, we did not generate the decoys on demand at the time of detection when the alert was issued. Instead, we made sure that the decoys were conspicuous enough for the attacker to access them if they were indeed trying to steal information by placing them in highly con-spicuous directories and by giving them enticing names. With this approach, we were able to improve the accuracy of our detector. Crafting the decoys on demand improves the accuracy of the detector even further. Combining the two techniques, and having the decoy documents act as an oracle for our detector when abnormal user behavior is detected may lower the overall false positive rate of detector.

VI. CONCLUSION

In this position paper, we present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access.

Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology, could provide unprecedented levels of security in the Cloud and in social networks.

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

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

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.

VII. REFERENCES

[1] A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a user centered approach, Future Gener. Comput. Syst. (2014)
[2] P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
[3] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.
[4] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30.
[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2)(2012) 220–232.
[6] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
[7] Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
[8] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.
[9] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification.
[10] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing the business perspective, Decis. Support Syst. 51 (1) (2011) 176–189.
[11] B. Hay, K. Nance, M. Bishop, Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1–7.
[12] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) 371–386.
[13] O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J.Comput. Appl. 66 (2013).
[14] M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876.
[15] Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput.9 (6) (2012) 903–916.
[16] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) 355–370.
[17] Z. Tari, Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) (2014) 54–57.
[18] Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, 2011.
[19] Y. Fu, Z. Lin, Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery, in: Proceedings of the 9th ACMSIGPLAN/SIGOPS International Conference on Virtual Execution Environments, 2013, pp. 97–110.
[20] S.M.S. Chow, Y. He, L.C.K. Hui, S.M. Yiu, Spicesimple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 526–543.
[21] S. Yang, P. Lai, J. Lin, Design role-based multi-tenancy access control scheme for cloud services, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), 2013, pp. 273–279.
[22] R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Technology (IIT), 2013, pp. 13–17.
[23] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3 (2003): 586-615.
[24] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[25] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2014) 384–394

CITE AN ARTICLE

Vishistha, A., & Singh, N. (2018). DATA THEFT DETECTION IN THE CLOUD. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 7*(6), 246-254.