www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5 may, 2014 Page No. 6017-6021

Pruning the Cloud Internal Data Stealing By Treachery Attacks

Shobha Agasibagil[1], Mr. G.Lingana Gowda [2]

[1]P.G. Student, Department of Computer Science and Engineering, Channabasaveshwara Institute of Technology, Gubbi, Karnataka

(Shobhama44@gmail.com)

[2]Asst.Professor, Department of Computer Science and Engineering, Channabasaveshwara Institute of Technology,Gubbi, Karnataka

(Glgowdag@gmail.com)

Abstract: Cloud Computing is internet based computing provide computing services those are data, application, software and computing, these computing services are delivered to local devices through internet. To store and share personal and business information and access cloud computing enables multiple users. Insider means, users those who have valid authority on the cloud. Attackers are treated as remote users in the security perspective. If the attacker are not a remote users then that should be checked by the security systems. If a authorized user's access details are stolen by an attacker can enter and access the cloud as a valid user. Distinguishing the real data of user and the attacker data, for this decoy information technology are used in the field of cloud computing. For detection of abnormal access of information and validating whether data access then it confuses the attacker with bogus information.

Keywords :Treachery, Decoy technology and Pilfering

1. Introduction

Everyone's life involved in cloud computing. Data, application, software and computing (Figure.1) provided by cloud .Cloud computing services used on our daily basis. Yahoo and Google are examples for the our daily users and web based email system to exchange messages with others we uses Facebook, it is a social networking sites and Twitter to share information and friends contact, To watch movies and TV shows these are on-demand subscription services. To store music, videos, photos and documents, we use ZumoDrive and Dropboxare used as cloud storages. In the real time Google is online collaboration tool to work documents with people on the same documents and JungleDisk, Carbonite and Mozy are online backup tools to automatically back up our data to cloud services. Businesses, companies rent services involved by cloud computing, these services reduce operational costs and improve cash flow. The social news website, Amazon Elastic Compute Cloud (EC2). Cloud computing works by combining all of a organizations computer operations into a central system that is maintained in off-site by another organization. Public cloud works by purchasing through a contact a cloud services offered by vendors like Microsoft IBM and oracle to name a few.

Figure.1:-**Cloud Computing Services**

The cloud computing really important to the customer because instead of paying for our hard driver space and server space and it support. Data security is very important, because it helps ensure privacy for our data. If our data is not secure then it is easy for others to infringe on our privacy. A new case for trusted third party auditor enables the cloud service providers accountability and protects the cloud users benefits. Trusted cloud computing with secure resources and data.

Computing resources (e.g. servers, storage and applications) delivered by cloud computing providers to users. By web browser user can access on-demand cloud services. Cloud computing service providers offer specific cloud services and ensure the quality services. Cloud computing involved

by three layers: those are 1)Application layer,2)Platform layer and 3)System layer (Figure.2).

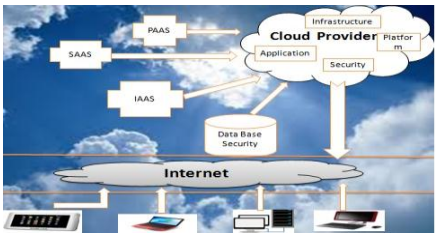

Figure.2:-**Cloud Computing Security**

Businesses, especially start-ups, small and medium businesses (SMBs), are increasingly opting for obviously supports better operational efficiency, but comes with greater attacks, perhaps the most serious of which are data pilfering attacks (Figure.3). Data pilfering attacks are amplified if the attacker is a malicious insider. By the Cloud Security Alliance this is considered as one of the top threats to cloud computing. While customers of cloud computing are threat well awareness, when it comes to protecting their data they are left only with trusting the service.

Figure.3:- **Computing Service Attacks**

Let alone control over lack of transparency the cloud provider's only exacerbates this threats that audit control, authorization and authentication. For fog computing we propose a completely different approach to securing the cloud using decoy information technology. We use this technology to lunch treachery attacks against unauthorized users, preventing them from separates the real sensitive customer data from fake worthless data.

2. Literature survey

When adopting strategies of cloud this research aims at providing the assistance to organizations to educate on attack management decisions. Research and threats were evaluated there were several threats identified. Then threats are discussed in details and with the public examples and offers remediation for these threats along with Impact and CSA guidance reference.

Van Dijk et al in [1] proposed Cloud-Application Class Hierarchy that shift towards thin clients and centralized provision of computing resources in the area of cloud computing. There is data privacy violation, it is also strongly illuminated that due to lack of client resources control, by service provider leakage of sensitive information. The most powerful tool of cryptography that is Fully Homomorphic Encryption (FHE) is one of the data security promising tool to ensure. The privacy demanded by common cloud computing services by defining a hierarchy of natural classes of private cloud applications and no cryptographic protocol can implement those classes where data s shared among clients the cryptography alone can't enforce. The disadvantage is improper usage of data and criminal use of cloud computing.

Iglesi as et al in [2] proposed an adaptive approach is used for recognizing computer users and creating behaviour profiles of users. This method used for updating and evolving user profiles and classifying an observed user it gives. To develop with time user behaviour, the method as described by fuzzy rules to make them dynamic. It makes use of Evolving systems approach. It is a one pass, non-interactive recursive and can be used in interactive mode. It is operating very effective and fast as its structure is interpretable and simple. The disadvantage is Insecure interfaces and APIs.

Rocha F et al in [3] proposed the a malicious insider can steal any confidential data of the cloud user in spite of provider taking precaution steps like.1)Physical access is not allow. 2)For data storage tolerance policy for insiders that access. 3)Later use for internal audits to find the malicious insider and logging all accesses to the services. It proposes to show 3 attacks that malicious insider could do to. i) cryptographiy keys ii)Files and other confidential data iii)compromise passwords. and other confidential data like, on memory snapshots, obtaining private key, clear text password, from hard disk extracting confidential data. The disadvantage is malicious insider.

Salem B et al in [4] proposed an masquerade for the detection trap-based mechanisms and attacks gave security problems and detecting masquerade is very difficult. The means of trap-based mechanisms used for detecting insider attacks is also used for the detection of masquerade attacks. The desirable properties of decoys launch within a user's file space for attacker detection. Two user studies, and proposes recommendations for effective masquerade detection using decoy documents based on findings from the user studies use trade offs for these properties. For effective masquerade detection. The different deployment-related properties of decoy documents and a guide to the deployment of decoy documents. The disadvantage is shared. Data loss or leakage and technology issues.

Godoy et al in [6] for user profiling stated the profiling strategies to help users to cope with the increasing amount of information available on the internet. Here, this user profiling technique stated in detail the success of personal agents in satisfying user information which intensely relies on the learning approach to acquire user profiles as well as the adaptation strategy to cope with changes in user interests. User profiling the authors have surveyed on the main dimensions involved in the construction of user profiles acquisition learning adaptation and evaluation to better understand. This approaches in the user surveyed had only partially addressed the characteristics that distinguish user profiling of related tasks such as text categorization or supervised learning in general. Future focus on user-profiling approaches for successful information agents not only on the above aspects but the next level is also on the assessment of comprehensible semantically enriched user profiles which will take information agents. The disadvantage is Account or service effecting.

Salvatore J.S et al in [5] proposed a fog computing approach for securing data in the cloud. In this we detect illegal data access patterns and information access in the cloud. The decoy information technology used by fog computing to launch treachery attacks against malicious insider and preventing them from distinguish fake worthless data and real sensitive customer data. In this, we can reduce the pilfer of stolen data by reduce the value of stolen information. Two additional security features are used to secure cloud services such that.1)User Behaviour profiling, user profiling is a well known technique that can be applied here to known how much a user accesses their information in the cloud. 2)Decoys are confuses on adversary into believing they have ex-filtrated useful information and validating whether data access is authorized or unauthorized access is detecting then confusing the attacker with bogus information. This technology may be used with user behaviour profiling technology to secure a user's information in the cloud.

3. Problem statement

With Cloud Computing, organizations can use services and data is stored at any physical location outside their own control. Privacy, confidentiality and integrity are security questions and to data confidentiality can be maintained use trusted computing environment. Authentication, verification and encrypted data transfer there is need of a system which performs, hence maintaining data confidentiality to induce trust in the computing.

Attacks	Description
Twitter Attack	Loss or leakage of Data or Information or Documents.
Insider Attack	The User those who have Invalid Authority on the cloud to access data.
Masquerade Attack	The Shared Technology Issues.

Table 1:-**Types of Attacks**

Methodalogy

HMAC Algorithm

Step 1: If the length of K=B ,set Ko=K. Go to Step 4.

Step 2: To obtain an L byte string K=H(K) if the length of K>B hash K.

Step 3: To create a B-byte string Ko if the length of K>B append zeros to the end of K.

Step 4: Exclusive-Or Ko with ipad to produce a B-byte string $\oplus$ ipad.

Step 5: Append the stream of data 'text' to the string resulting from Step 4 (Ko $\oplus$ ipad) || text.

Step 6: To the stream generated H is apply in Step 5: H ((Ko $\oplus$ ipad) || text).

Step 7: Exclusive-Or Ko with opad:Ko $\oplus$ opad.

Step 8: Append the result from Step 7:(Ko $\oplus$ opad) || H (Ko $\oplus$ ipad) || text).

Step 9: Apply H to the result from Step 8: H ((Ko $\oplus$ opad) || ((Ko $\oplus$ ipad) || text).

Step 10: Leftmost t bytes of the result of Step 9 select as the MAC.

HMAC uses the following parameters:

B -Block size (in bytes) of the input to the FIPS-approved hash function.

H -FIPS-approved hash function.

Ipad- Inner pad; the byte x'36' repeated *B* times.

K- Secret key shared between the originator and the intended receiver(s).

*K*0- The key *K* with zeros appended to form a *B* byte key.

L -Block size (in bytes) of the output of the FIPS-approved hash function; for SHA1, *L* = 20.

Opad- Outer pad; the byte x'5c' repeated *B* times.

t -The number of bytes of MAC.

text- The data on which the HMAC is calculated; the length of the data is *n* bits, where the maximum value for *n* depends on the hash algorithm used.

x'*N*-' Hexadecimal notation, where each '*N*' represents 4 binary bits.

||- Concatenation

$\oplus$ Exclusive-Or operation.

4. System design

Data pilfering is a term used to describe other individuals when information is illegally copied or taken from a business. Called as information of user such a because this information is illegally obtained, security questions, other information, or other confidential corporate information. Who stole this information is apprehended when individual, he or she will be prosecuted the fullest extent of the law.

The three core principle of information security are confidentiality, integrity and availability – known as a CIA triad, Figure.4 shows the CIA triad .All information security controls, safe guards, threats, vulnerabilities and security process for every organization are subject to the CIA triad[7].

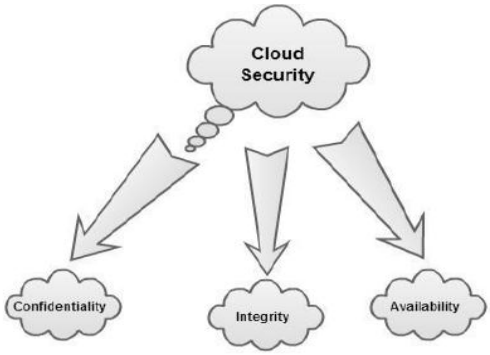

Figure.4:- **CIA Triad**

1)Confidentiality:- Confidentiality is the prevention of unauthorized disclouser information. Confidentiality is ensured by: network security protocols, network authentication service and data encryption services.
2)Integrity:- Integrity is the guarantee that the message that is sent is the same as the message received and that the message is not altered in transit. Integrity is reached if the transmitted data is altered, when it is in transit. Integrity is ensured by: Firewall services, communication security and intrusion detection.

3) Availability:- Availability is the guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of location of the user. The security controls, and the networks connecting clients and the cloud infrastructure should always be functioning correctly means that cloud infrastructure. Availability is ensured by: fault tolerance, authentication and network security.

In our project of system design Administrator and User plays an very important rules.(Figure.5) An administrator is a person or group of people that run either a physical program or are the owner and main operator of a computer system. Planning, supervising, directing, controlling, organizing and budgeting are activities of Administrative.

User is a person who uses a computer or computing services. A user often has a user account and is identified by a username, username include login name. Users are also widely characterized as the class of people that uses a system without complete technical expertise required to understand the system fully. In project, user's also called as software agent, means ultimate operator of a piece of software. A user's account allows a user to authentication to system services and be granted authorization to access them. To log into an account, for the purpose of logging, accounting, resource management and security a user is typically required to authenticate oneself with a password.

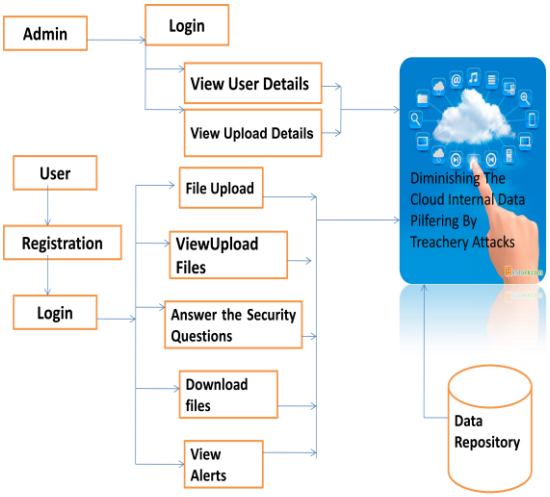

Figure.5:- **System Architecture**

The feasibility of the project is analyzed in this phase and business proposed is put forth with a very general plan for cost measurement and the project the project. The feasibility study of the proposed system is to be carried out during system analysis. Not burden to the company his is to ensure that the proposed system..

Conclusion

This paper presents a survey on various cloud computing attacks that were proposed by earlier researches for the better development in the field of Cloud Computing. For cloud computing various algorithms and methods used will help in developing efficient and effective for finding the fog misuse or attacker detection. We will be presenting a comparative study of various algorithms for Cloud Computing in future scope.

References

[1] M.Van Dijk and A.Jules, "On the impossibility of cryptography alone for privacy-preserving cloud computing ". In Proceeding of the 5th USENIX conference on Hot topics in Security, ser. Hot Sec'10. 'Berkeley, CA, USA":"USENIX Association", 2010.

[2] J.A Igesias, P. Angelov, A. Ledezma, and A. Sanchis, "Creating evolving user behaviour profiles automatically", IEEETrans. On Knowl, and Data Eng, Vol. 24, no. 5, May 2012.

[3] F.Rocha and M. Correia, "Lucky in the sky without diamonds: Stealing confidential data in the cloud", in Proceeding of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops, ser. DSNW' 11. Washington, DC, USA: IEEE Computer Society, 2011.

[4] M.B Salem and S.J.Stolfo, "Decoy document deployment for effective masquerade attack detection", in Proceedings of the 8th international conference on Detection of intrusions and malware,

and Vulnerability assessment, ser. DIMVA' 11.Berlin, Heidelberg: Springer-Verlag ,2011.

[5] S.J Stolfo, M.B. Salem and A.D. Keromytis, "Diminishing The Cloud Internal Data Pilfering By Treachery Attacks"; in Proceeding of the IEEE Sympostum on Security and Privacy Workshop, 2012.

[6] D. Godoy and A. Amandi, "User profiling in personal information agents: a survey", Knowl. Eng. Rev. Vol. 20, no .4. Dec 2005.

[7] R.L.Krutz and R.D.Vines, ―*Cloud Computing Software Security Fundamentals* in Cloud Security: A Comprehensive Guide to Secure Cloud Computing, New York City, NY, Wiley, 2010