International Journal of Computer Science & Communication (ISSN: 0973-7391)
Special Issue, Page 19-25, December 2020 ------ available at www.csjournals.com

An Insider Threat Identification and Access control in Cloud Environment

Badari Narayan V S[1]
Research Scholar,
Department of Computer Science,
SSIT, SSAHE, Tumakuru,

Dr.Siddappa M[2]
Professor and Head,
Department of Computer Science,
SSIT, SSAHE, Tumakuru

Abstract— Cloud computing is a game changer in the field of data storage service, computer application service, Data provisioning service and many more. More and more organizations are moving towards cloud for different types of services requirement. Cloud computing is an Internet-based computer technology that refers to the use of Computing resources i.e. hardware and software, available on demand as pay and use service over the Internet. Data on the cloud server is the real concern for client as he loses control over the data. Here we highlight the client security concern with respect to data. Overall Cloud functionality has been divided into four layers. Each layer is responsible to carry out specific activity. At each layer data will be handled by different person and at different location. At each layer we propose a four layered security for data. The first layer is cloud user layer, in that a robust and dynamic method has been proposed and implemented for access control. Access control at user layer (client side) to mitigate internal threat is implemented using mathematical model and decision tree.

Keywords: cloud data, Security, Access control, DMAC, ANOVA, Decision tree.

I. INTRODUCTION

Data security on the cloud includes mainly these three functions: Access control, protection of private data and secure communication across public network. The thing that is of concern to client is what will happen to our data when it is placed on the cloud data center with unknown people around, unknown place and hostile environment. Data security and privacy is the major concerns that are in the way of the exponential growth of cloud computing services. Although advanced security algorithms, protocols have been incorporated by cloud service provider to ensure adequate security for client data. cloud user are not fully satisfied to place their confidential , personal , valuable in term of intellectual property and financial information or data on cloud. The main reason for this reluctance is any security mechanisms would not provide the complete data protection because of its vulnerabilities' over the network and cloud service provider has full command on cloud applications, hardware and client's data. Although there is a service level agreement between CSP and CU, Client or cloud user will not get adequate information about how and where data is stored how and when and by whom the auditing is done to check and ensure data integrity and privacy.

In this paper, we try to focus on how data is stored in cloud (cloud data model), various security threats to cloud data, what are the various security measures implemented in cloud server(provided by CSP)and distribution of responsibilities, how to identify threats, what are the client concern regarding data security on cloud , we propose a novel layered security architecture and four level security at each layer, and finally propose and implement client side access control mechanism to mitigate insider threat.

II. CLOUD DATA MODEL

In cloud computing, cloud data service works by connecting servers in network .multiple copies of user data is stored in different servers located in different geographic locations. This is done to protect client data from natural disaster, fire or any other incident which physically damages the data server.

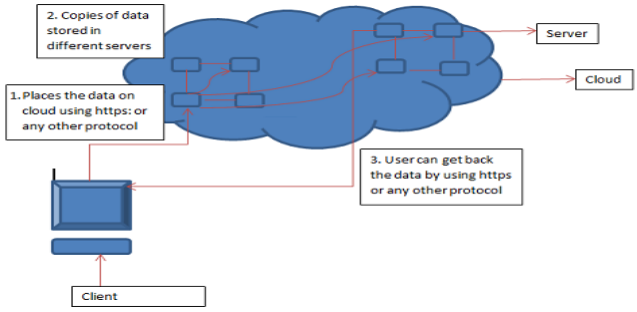


Fig.1. Cloud Data Movement and Storage Model

Client has no way to know where on the cloud your data is stored how many copies of your data is made and where these copies are stored. Data transmission can be done by using http or by using SSL protocol generally data will be encrypted by using public key encryption. Sensitive or secret data will be stored in encrypted form and other data will be stored as plain text i.e. data will be decrypted on receipt and stored in server. When a client wants to access file stored on cloud server, he needs to download the file by going through some authentication procedure, and then decrypt the file to access or update the data in the file. If he again uploads the file to cloud server, consistency should be maintained between all the copies of data stored in different servers and locations. This is most important and time consuming work that should be carried out by CSP. If client want to access the data on cloud server itself, then if it is plain data, direct transaction can be done to access or update the data. If data is sensitive and is encrypted, data should be decrypted at server by using secret key shared between either client or TTP. There is no way that we can run a transaction on encrypted data. Here we are disclosing the sensitive data to unknown person and risking

the privacy and integrity of the data. This type of transactions is most vulnerable and is invitation for data theft.

Cloud computing has been swing in today's technology-driven world for years now and with good reason. Cloud computing offers many supremacy with elasticity, storage, resource sharing, and easy accessibility. Companies of all sizes and capacity are using cloud computing for one or more services. Even an individual at home, use cloud technologies like Google Docs, Skype OneDrive for various daily activities. Virtualization is the back bone of cloud model.

III. CLIENT CONCERN AND ISSUES ON STORING DATA ON CLOUD

The cloud computing does not provide client control over the stored data in cloud servers. The Cloud service providers have full control over the data; they can perform any malicious tasks Such as copy, destroying, modifying data. Most of the operations or functions that happen on the cloud server are transparent to the client. Virtualization, data duplication, data storage location, data segmentation, multitenancy nature of cloud, access control implementation, data availability, data auditing and its reliability, security breaches and its mitigation, disaster and failure management, enforcement of SLA, and handling of sensitive data against modification or theft are the concern that inhibiting the client to fully accept the cloud service model.

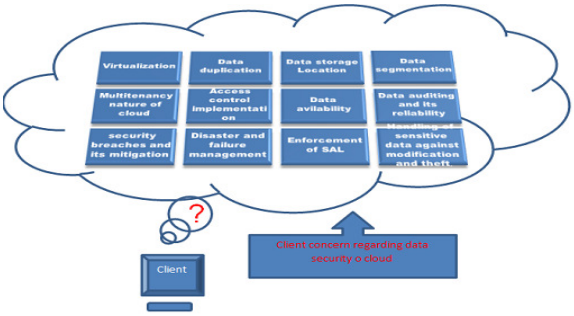


Fig.2. Diagram listing Client's concerns with respect to Data Security on Cloud.

IV. PROPOSED CLOUD SECURITY MODEL

In the proposed model we have divided the cloud architecture into 4 layers. Each layer has different responsibility and different actors are responsible for carrying out these responsibilities. There is a movement of data in both directions between these layers. When we talk about cloud it's a public network there is risk involved in every step, if data or process involved is sensitive and most valuable then we need to be more careful in handling such data. There should no security gap in the entire process of such data handling. It may be any type of cloud service that the client may be receiving form CSP, there is a security risk and it should be handled. We have listed out the security issues or concerns at each layer, to mitigate those concerns we have proposed a four level security check at each layer.

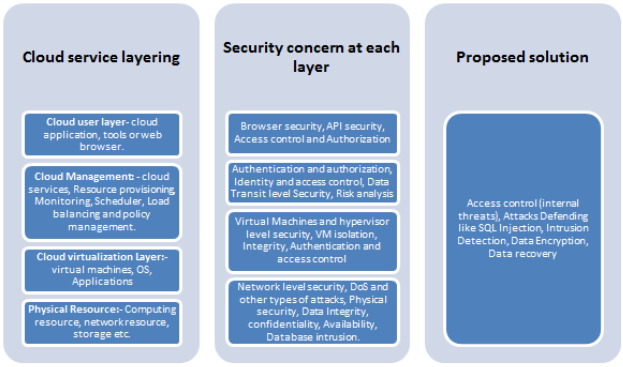


Fig.3. Cloud Security Architecture

Cloud user layer

Cloud user or client is a person or organization who approaches a CSP of one or more services that are on offer that suits his requirement. Generally all the interaction between client and CSP happens on the public network. When you connect to CSP and start interacting and using services from him means you are using public network, all the risk and threat of using or connecting to internet needs to be handled at the client side to protect sensitive data and resources.

Access control and authorization

Access control is the requirement that's specifies how access s managed and who may access the resource under what circumstance. This mechanism controls and authorize individuals to access the information/resource that they are allowed to. Access control rules must change based on the risk factor, which means an organization must use security analytic layer using AI and machine learning that is on top of the existing security layer. They need to identify threats in real time and automate the access control rules accordingly.

Access control based on password is not sufficient in today environment. Password based authentication is vulnerable to an offline password guessing attack and a privileged insider's attack, and is not reparable.[4] If we opt for biometric verification it has its own limitations and drawback. Biometric Recognition: Challenges and Opportunities address the issues surrounding broader implementation of this technology, making two main points: first, biometric recognition systems are incredibly complex, and need to be addressed as such. Second, biometric recognition is an inherently probabilistic endeavor. Consequently, even when the technology and the system in which it is embedded are behaving as designed, there is inevitable uncertainty and risk of error.(Ref- *Biometric Recognition: Challenges and Opportunities, National Academic press).*

Malicious insider is the major threat to any organization. He is the inside person and has access permission to most of the resources inside the organization. If the inside person decides to (cheat) leak the sensitive information, corrupt the high value data there is no one to stop him. As an insider it is very easy to collect some valuable and sensitive information from social engineering Intellectual property theft or fraud can occur in a

couple of ways. The first is when employees are granted more access than necessary to do their jobs. The second arises when someone with valid access uses privileged accounts to purposefully go against policy and abuses their power. There are common behaviors of the human being that suggest an active insider threat – whether digitally or in person. These symptoms are essential for network security team to identify the threat in advance and take essential action to mitigate insider threat.

- Frequent enquire for access to resources not related with their job function
- Frequent usage of secondary memory to copy bulk data. (e.g., USB drives)
- Searches for sensitive data and Network crawling
- Copying files from sensitive directories.
- Sending out the sensitive information through Email.
- Accessing substantial amounts of data.
- Regularly Accessing sensitive data not related to their job function.
- Accessing data that is outside of their unique behavioral profile
- Trying to bypass security mechanism.
- Regularly present in the office during off-hours.
- Behaving differently toward co-workers.
- Not following corporate policies and rules.
- Taking of new opportunities and quitting the present.

Insider Threat Examples

Here are a few recent examples of insider threats from the news.

Tesla reported that a malicious insider was responsible for sending some sensitive information to outsider.

Coca-Cola released a statement that a malicious insider stole a hard drive full of personnel data.

Personal data, including account information, for 1.5 million customers were stolen by fraud insider and provided to a criminal organization as reported by *Suntrust Bank*.

Here we are proposing a **Dynamic and Multilevel Access Control** (**DMAC**), automated and adaptive access control technique, which considers multi-dimensional data over a period of time to come to some conclusion. It is the role and identity based access control mechanism. This DMAC works in two stages .First stage we call it as Identification stage and second stage Authorization stage.

Based on the user identity and his role in the organization, DMAC dynamically will build the profile of that person from the previously stored data. The advancement in the internet technology has brought more and more application. User perform sensitive and critical job using these application. Each user needs to manage more and more passwords for each application. Keeping a strong password for each and remembering it on time is difficult for user and in general, so users may choose name, date of birth, telephone number, hobbies, or a combination of them as passwords. This becomes the most vulnerable part and provides an opportunity for targeted password attacks and password reuse attacks based on personal information. Ip spoofing, social engineering and different types of password attack can be used to obtain or guess passwords. DMAC is going to check the user credentials based on the work history of the user, his performance in the organization, his previous appraisals, user attrition risk, data from his social networking site, his recent and frequent phone calls. Based on these a risk assessment will be done and DMAC will decide to deny or grant permission to access the resource. This is first stage of identification.

In second stage, if the user is accessing any sensitive information or altering or deleting the data or changing the system configuration, then he need to pass through second level of authentication process. It is a continuous process of checking the identity of user by using key stroke dynamic. This program will be run at random interval during session to match the keying dynamics of current user with his stored pattern. If there is a miss match, the session will be closed and will be again asked to login.

V. DMAC STAGE 1 IMPLEMENTATION

It is the first stage of identifying the user based on role he plays in the organization and password associated with role. The unique id and password associated with it and is most simple and primitive authentication which by itself is not enough. User need to identify himself by presenting one of the biometric identities. Most commonly used biometric verification method is by validating either finger print or by iris scanning. Keyboard dynamics is one of the most secure and best suited identification methodology, we are going to use this in later stage. Once user is identified system in the back ground runs a program which take inputs from his personal file regarding his performance in the role, previous appraisal, his attrition risk, unauthorized secondary device access, emailing sensitive information outside organization, previous attempts to by-pass security. The program after getting these inputs validates the data and builds the decision tree to classify the user as authorized or unauthorized for performing the specific task

Class A- Grant Access. (Trustworthy person)

Class B- Grant Access and make him to take an orientation program.

Class C- Deny access.

User: A permanent employee of the organization with valid role and identification. He is the person who is given authorization to access the resources in the organization.

Identification: in this process user will enter his user name (role) and provides his finger or iris impression on the provided hardware devise. The computer system attached to device will collect the biometric information time stamps the data. Biometric data along with time stamp is encrypted using standard encryption algorithm and sent to server for verification. The server process decrypts the data, validates the time stamp. Decrypted data will be matched with the stored credentials of that particular user. Match confirms the person identity and second step of (process) identification is initiated else the user will be denied to enter into system simply saying his login attempt fails.

User verification process (UVP):

This process collects information from three different files which are updated regularly. This program takes input from following three files.

1) Personal file.
2) Data collected from Social Engineering.
3) File recording physical Behavior of the employee.

Based on the information collected each file provides the rating for the user. These rating will be processed by the program and classify the user as class A, B and C.

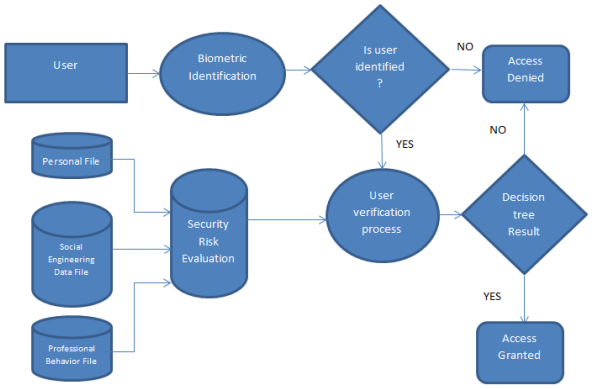


Fig.4. User Access control mechanism in DMAC stage-1(UVP)

Personal file:

The personal file is the Employer file which contains information relevant to individual employees and to their employment. All, important job-related documents should go in the file, including: Job description, work experience, service in the current organization, previous appraisals, Technical expertise, Disciplinary action report if any, Past employment history, background verification report. Organization HR manager is responsible for maintaining and updating the relevant information into the file.

Personal File--xyz	Rating between 0-5		
	Eval-1	Eval-2	Eval-3
Role Description	NA	NA	NA
Total Work Experience	NA	NA	NA
Service in present organisation	NA	NA	NA
Apprisal report rating	0	1	2
Technical expertise rating	1	1	1
Disceplinary Action taken rating	1	1	1
Past employee feed back rating	1	1	1
Company background verification rating	1	1	1

Low value indicates Positivity(Good) Rating.
High value indicates Negativity(Bad)Rating.

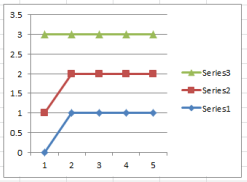


Fig.5. Personal File Data

Social Engineering Data file (SED)

Social engineering is a technique used to deceive and manipulate victims to get some valuable information without the knowledge of the victim. This valuable information may be used to reach a certain goal such as unauthorized access to a computer system, for financial gain or to cause harm or destruction. Social engineering attacks have a significant impact on organizations. A well planned Social engineering enables an attacker to gain some crucial information that helps him to access internal data or information, either physically or virtually. Social engineering may, in some cases, be considered an art of manipulation; it is well planned, researched and executed in order to lure victims into revealing sensitive information. Generally social engineering done to collect information and use it for destructive purpose, but here we are using the information collected for good purpose or in the interest of organization. Some people in the organization may be designated to collect some valuable information about people who are handling sensitive and valuable data/information using social engineering technique. The collected info will be saved in the file called SED file of the particular employee. Information collected using social engineering technique includes:

1) Information about attrition risk
2) Dissatisfaction at work place
3) Discussion of resignation
4) Talking of new opportunities
5) Attitude towards organization on adhering to policies.

Social Engineering Data File--XYZ	Rating between 0-5		
	Eval-1	Eval-2	Eval-3
Attriton Risk Rating	0	0	0
Dissatisfaction at work place Rating	1	1	1
Taking About new opportunity Rating	1	0	0
Attitude towards organization work policies	1	1	1

Low value indicates Positivity(Good) Rating.
High value indicates Negativity(Bad)Rating.

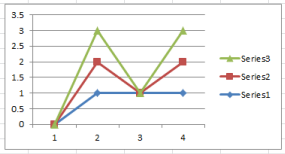


Fig.6. Social Engineering File Data

Professional Behavior Data file (PBD) (Ethical Data)

This is the information maintained by Ethical team, regarding work culture, behavior and other physical activities of the employee. Input regarding following parameters will be updated in the PBD file regularly b Ethical team.

1) Working hours (late night working)
2) Usage of removable storage device
3) Accessing sensitive data not associated with the job.
4) Emailing sensitive information.
5) Attempting to bypass security.

Professional Behavior Data File-XYZ	Rating between 0-5		
	Eval-1	Eval-2	Eval-3
Working hours and timing rating	0	1	1
usage of Secondary storage for bulk copying	1	0	0
Any Recent history of Security Breach	0	0	0
Emailing sensitive information out	1	0	0
Attempts to bypass Security	0	0	0

Low value indicates Positivity(Good) Rating.
High value indicates Negativity(Bad)Rating.

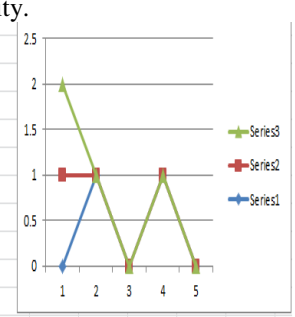


Fig.7. Professional Behavior File Data

Security Risk Evaluation File (SRE)

We select five important security related parameter from the above three files. These five parameters include the following:

Any recent history of security breach

Any attempts to bypass security.

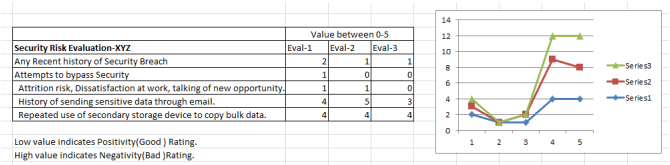
Attrition risk, Dissatisfaction at work, talking of new opportunity.

History of sending sensitive data through email.

Repeated use of secondary storage device to copy bulk data.

Information on these parameters is collected by three independent sources and is stored in a table format. Each parameter is rate in the range 0 to 5 as shown in the table below.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Special Issue, Page 19-25, December 2020 ------ available at www.csjournals.com



Security Risk Evaluation-XYZ	Value between 0-5		
	Eval-1	Eval-2	Eval-3
Any Recent history of Security Breach	2	1	1
Attempts to bypass Security	1	0	0
Attrition risk, Dissatisfaction at work, talking of new opportunity.	1	1	0
History of sending sensitive data through email.	4	5	3
Repeated use of secondary storage device to copy bulk data.	4	4	4

Low value indicates Positivity(Good) Rating.
High value indicates Negativity(Bad)Rating.

Fig.8. Security Risk File Data

Analysis of the Data using one way ANOVA

As can be seen in the above table, Data is collected by three independent persons (Eval1, Eval2 and Eval3) to eliminate any prejudices and bias that may exist between individuals. Because three independent people collect data and rate each parameter, there may be variances in data collected. If the variance is more, then it will be difficult to come to decision. Here we use Analysis of variance (ANOVA) to test the hypothesis that the means of two or more data set are equal. ANOVA is used to determine whether there are any statically differences between the means of three or more independent group of data.

The one way ANOVA compares the mean between two or more groups of independent data and determines whether any of those means are statistically significantly different from each other. It tests the Null hypothesis. This is NULL hypothesis for acceptance of data.

$$H0=\mu A=\mu B=\mu C$$

Where, μ= group mean

K is the no of group.

We need to set alternate hypothesis H_1: At least one of the group means is different from the others.

Steps for calculating One way ANOVA

State your NULL and Alternate Hypothesis.

Calculate the Degree of freedom df.

Calculate the sum of square deviation from the mean (ss).

Calculate the mean square.

Calculate F-statistics.

Compare F value.

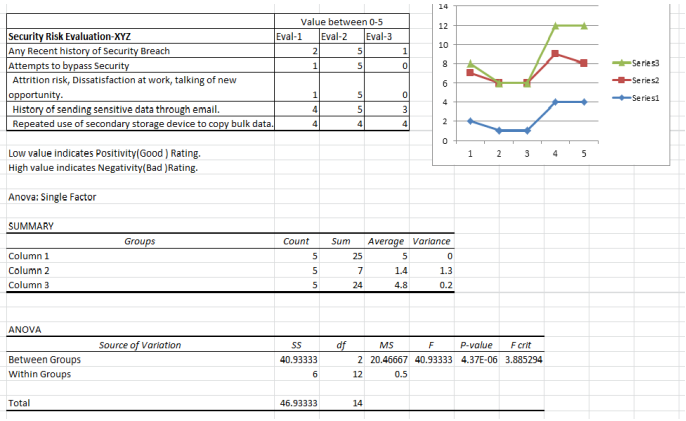
State the conclusion.

Result of the calculation can be judged on the basis of F value. If the calculated F value is less than the tabulated F value, accept the NULL hypothesis (H0).

If the calculated F value is more than the tabulated F value, reject the Null hypothesis and accept the alternate hypothesis.

Table - 1 ANOVA F- Table

Source of variation	Sum of squares (SS)	Degrees of freedom(DF)	Mean Square (MS)	F-statistic
Treatments	$SS_{between}$ (SS_b)	k-1	$MS_b = SS_b/(k-1)$	$F=MS_b/MS_w$
Error (or Residual)	SS_{Within} (SS_W)	N-k	$MSw = SS_W/(N-k)$	
Total	SS_{Total} (SS_T)	N-1		



Security Risk Evaluation-XYZ	Value between 0-5		
	Eval-1	Eval-2	Eval-3
Any Recent history of Security Breach	2	5	1
Attempts to bypass Security	1	5	0
Attrition risk, Dissatisfaction at work, talking of new opportunity.	1	5	0
History of sending sensitive data through email.	4	5	3
Repeated use of secondary storage device to copy bulk data.	4	4	4

Low value indicates Positivity(Good) Rating.
High value indicates Negativity(Bad)Rating.

Anova: Single Factor

SUMMARY

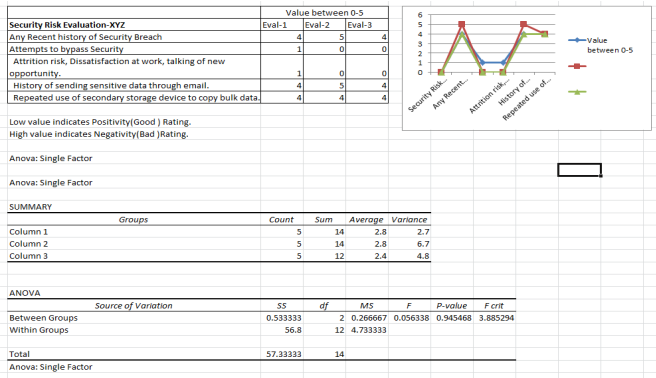
Groups	Count	Sum	Average	Variance
Column 1	5	25	5	0
Column 2	5	7	1.4	1.3
Column 3	5	24	4.8	0.2

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	40.93333	2	20.46667	40.93333	4.37E-06	3.885294
Within Groups	6	12	0.5			
Total	46.93333	14				

Fig.9. Sample variance (ANOVA) Calculation of Rejected Data Set

In the figure above, a sample data from the Security Risk Evaluation File of the particular employee XYZ is evaluated to check variance. As you can observe in the F-Table, calculated F value (40.93333) is far more than tabulated F value (3.885), here we need to reject the NULL Hypothesis (H0) and accept the alternate hypothesis (H1). As you can observe in the table above, there is much variance in the data given by three independent evaluators, we cannot come to the conclusion. In this case, we reject this data set and ask for new evaluation from other group of people.



Security Risk Evaluation-XYZ	Value between 0-5		
	Eval-1	Eval-2	Eval-3
Any Recent history of Security Breach	4	5	4
Attempts to bypass Security	1	0	0
Attrition risk, Dissatisfaction at work, talking of new opportunity.	1	0	0
History of sending sensitive data through email.	4	5	4
Repeated use of secondary storage device to copy bulk data.	4	4	4

Low value indicates Positivity(Good) Rating.
High value indicates Negativity(Bad)Rating.

Anova: Single Factor

Anova: Single Factor

SUMMARY

Groups	Count	Sum	Average	Variance
Column 1	5	14	2.8	2.7
Column 2	5	14	2.8	6.7
Column 3	5	12	2.4	4.8

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.533333	2	0.266667	0.056338	0.945468	3.885294
Within Groups	56.8	12	4.733333			
Total	57.33333	14				

Anova: Single Factor

Fig.10. Sample variance (ANOVA) Calculation of Accepted Data Set

Above table has sample data collected by three independent evaluators. This data set has undergone ANOVA test. AS you can observe Calculated F value (0.0563338) is much lower than the tabulated F value (3.885294), Hence we accept the Null hypothesis (H0) i.e. $H0=\mu A=\mu B=\mu C$

And accept the data set for further processing.

Decision tree for Authorization

Decision tree is a supervised machine learning technique that helps to build a decision

making tree from training data. A decision tree (also referred to as a classification tree or a reduction tree) is a predictive model which is a mapping from observations about an item to conclusions about its target value. Leaves represent classifications (also referred to as labels) in the decision tree. The nonleaf nodes represent features in decision tree and

branches represent joints of features that lead to the classifications.

The algorithm for constructing a decision tree is as follows:

1. Randomly sample *n* training samples with replacement from the training dataset.
2. Create a root node and assign the sampled data to it.
3. Repeat the following steps for each node until all nodes consists of a single sample or samples of the same class.

The training decision tree built for all possible data values. There are five parameters labelled A, B, C, D and E representing non leaf nodes or features. There are three types of leaf nodes representing three type of classification.

A- Any Recent history of Security Breach

B- Attempts to bypass Security

C- Attrition risk, Dissatisfaction at work, talking of new opportunity.

D- History of sending sensitive data through email.

E- Repeated use of secondary storage device to copy bulk data.

These are the features depending the values associated with this feature classification decision is made.

Three types of leaf node indicates three type of classification

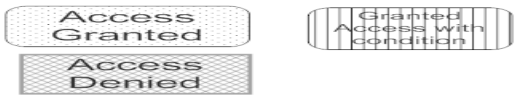


Fig.11. Types of leaf Nodes in Decision Tree.

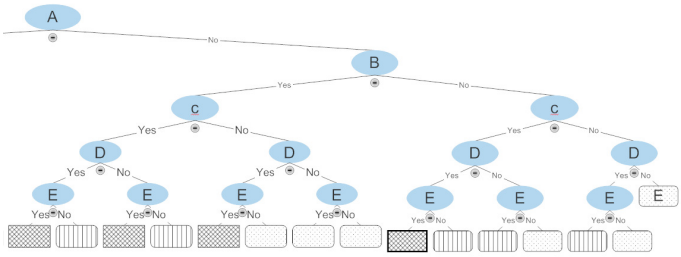


Fig. 12. Decision Tree right branch.

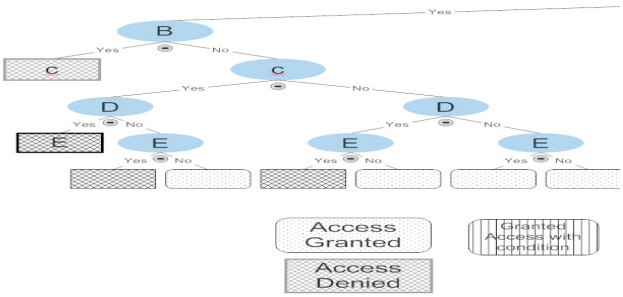


Fig.13. Decision Tree left branch.

VI. TESTING WITH SAMPLE DATA

Data is ready with us, now we need to take a decision whether that person is reliable enough to access the sensitive data. For taking the decision, for each parameter we evaluate we make assignment either 0 or 1. If the value range is between 0 to 2 we consider it as 0 and if in between 3 to 5 we consider it as 1. **0** indicates NO and **1** indicates YES in decision tree. Now the table in the fig.[11] Becomes like this.

Security Risk Evaluation-XYZ	Average
Any Recent history of Security Breach	1
Attempts to bypass Security	0
Attrition risk, Dissatisfaction at work, talking of new opportunity.	0
History of sending sensitive data through email.	1
Repeated use of secondary storage device to copy bulk data.	1

Fig. 14. Sample data from Security Risk Evaluation File

The decision tree for the sample data is as below. As we can observe in the decision the path travelled shown in the shaded box. The sequence followed according to the given table data is Yes, No, No, Yes and Yes. If the tree is traversed till the leaf node with more than two Yes, then the decision is Accessed Denied, as shown in the decision tree diagram.

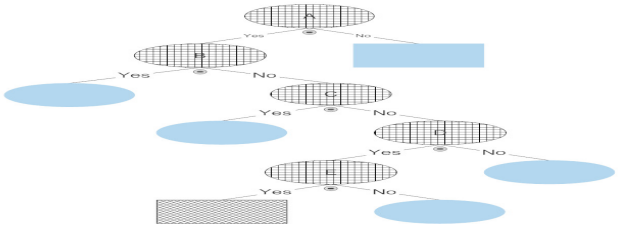


Fig.15. Decision Tree and path traversal for Sample data

VII. CONCLUSION

Securing the data on the cloud is the major concern for most cloud users. Cloud technology and its applications are game changer in the field of information technology. Security risk associated with storing data on cloud and movement of data on public network need to be addressed. Cloud data model and threats associated to storing data on cloud is highlighted. Here we have proposed new cloud data security architecture. Complete cloud data model has been layered and security issues at each layer has been pointed out. A dynamic and multilevel access control mechanism to mitigate internal threat within the organization has been implemented. Data collection and validation process has been done by using ANOVA technique. Finally a decision tree is built to make a decision regarding user authorization. This technique has been tested for different data set and is producing consistent satisfactory result. This method can be implemented on any client machine, where internal users will be using the machine to logon to cloud server to access sensitive information.

REFERENCES

[1] Wei-Chi Ku, "Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture," in IEEE Transactions on Neural Networks, vol. 16, no. 4, pp. 1002-1005, July 2005, doi: 10.1109/TNN.2005.849781.

[2] Wei-Chi Ku and Shuai-Min Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," in IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 204-207, Feb. 2004, doi: 10.1109/TCE.2004.1277863.

[3] Y. Li, H. Wang and K. Sun, "A study of personal information in human-chosen passwords and its security implications", Proc. IEEE 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), pp. 1-9, Apr. 2016.
Show Context View Article Full Text: PDF (264KB) Google Scholar

[4] D. Wang, Z. Zhang, P. Wang, J. Yan and X. Huang, "Targeted online password guessing: An underestimated threat", Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 1242-1254, 2016.
Show Context Access at ACM Google Scholar

[5] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton and R. E. Hohimer, "Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats," 2012 45th Hawaii International Conference on System Sciences, Maui, HI, 2012, pp. 2392-2401, doi: 10.1109/HICSS.2012.309.

[6] Ali I. Siam1, Heba A. El-khobby 2, Hatem S. Abd Elkader3, Mustafa M. AbdelNaby4 "Enhanced Data Security Model for Cloud Computing Platform", 2015 IJSRSET | Volume 1 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099 Themed Section: Engineering and Technology

[7] Mohammed Ahmed "Data Storage and Security Issues in Cloud Computing -An Analysis", Reseach Scholor, Rayalaseema Univ., Kurnool, International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.92.06

[8] Mahesh U. Shankarwar and Ambika V. Pawar" Security and Privacy in Cloud Computing: A Survey", CSE Department, SIT, Symbiosis International University, Pune,India{mahesh.shankarwar,ambikap}@ sitpune.edu.in, Article in Advances in Intelligent Systems and Computing · January 2015
DOI: 10.1007/978-3-319-12012-6_1

[9] Ghada Farouk Elkabbany, Electronics Research Institute, Egypt, Mohamed Rasslan, Electronics Research Institute, Egypt, "Security Issues in Distributed Computing System Models", Copyright c2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

[10] Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, and Mohd Farhan Md. Fudzee, "A survey paper on keystroke dynamics authentication for current applications", AIP Conference Proceedings 2173, 020010 (2019); https://doi.org/10.1063/1.5133925, Published Online: 11 November 2019

[11] Philip A. Legg, Oliver Buckley,Michael Goldsmith, and Sadie Creese, "Automated Insider Threat Detection System Using User and Role-Based Profile Assessment", IEEE SYSTEMS JOURNAL, VOL. 11, NO. 2, JUNE 2017.

[12] Kirichenko Lyudmyla, "Detecting cyber threats through social network analysis: short survey", Doctor, Professor, Department of Applied Mathematics, Kharkiv National University of Radioelectronics, Ukraine.

[13] Anagi Gamachchi, Li Sun and Serdar Boztas, "A Graph Based Framework for Malicious Insider Threat Detection", School of Science, RMIT University, Melbourne, Victoria, Australia, (anagi.gamachchi, li.sun, serdar.boztas)@rmit.edu.au

[14] Soumik Mondal and Patrick Bours, Person Identification by Keystroke Dynamics Using Pairwise User Coupling, vol. 12, no. 6, June 2017.

[15] A. M. Dawn Cappelli Randall Trzeciak,Timothy J. Shimeall, "Common Sense Guide to Prevention and Detection of Insider Threats , 3rd Edition," 2009.

[16] J. R. C. Nurse et al., "Understanding insider threat: A framework for characterising attacks," in Proc. IEEE SPW, 2014, pp. 214–228.