Intrusion Detection System and Security in Cloud Computing

Javiad Ahmad, M.Mazhar Afzal

Abstract: Cloud computing is one of the latest Technologies nowadays used by different organizations. Cloud computing is based on internet and has the most efficient architecture and is totally depend on internet. It begins with the establishment and the compilation of network hardware, software and related infrastructure. This paper is related to the Intrusion detection system in cloud computing by reviewing almost twenty papers on the same topic. Intrusion detection system is very important in cloud computing and it provides the ways to secure our data on cloud. Every industry is at the risk of cyber-attacks, data is very important for industry and providing the security to cloud itself is very important. Intrusion detection system is important because it provides us the real time update in case the data is not secure on cloud or intruder is trying to intrude in our data.

Keywords: Cloud, Sensitive Information, Security, Intrusion Detection, Digitalization, Deployment.

I. INTRODUCTION

The security in cloud computing is critical step which is because the sensitive information is being in service with the different organisations and this also includes the management of sensitive information, so it becomes very important that the measures should be taken to secure this sensitive information. This facility is being provided by intrusion detection system, we can use some techniques to know if the data is on stake or if there is any threat to sensitive data.

Laptop
Network
Smartphone
Cloud Computing
Tablet computer
Server
Mobile
Database

Fig 1 Cloud Computing

Manuscript received on 10 April 2021 | Revised Manuscript received on 18 April 2021 | Manuscript Accepted on 15 May 2021 | Manuscript published on 30 May 2021.
* Correspondence Author

Javiad Ahmad*, Assistant Professor, Department of Computer Science and Engineeering, Savitribai Phule Pune University , Pune Email: javidaltaf@gmail.com

M.Mazhar Afzal, Professor Department of Computer Science and Engineeering, Savitribai Phule Pune University , Pune Email: mazhar@theglocaluniversity.in

The security plays an important role no doubt that cloud computing is one of the growing technologies nowadays but when it comes to security the important question is whether the data is safe when it comes to cloud computing or not, yes there comes the number of techniques that are been used to protect the data that no one would be able to steal the important and sensitive information. So it is very important for the

Cloud service to ensure the privacy, data security and to check whether the data is really protected or not. It is very important to check the same so that the important data will not be compromised in the way either

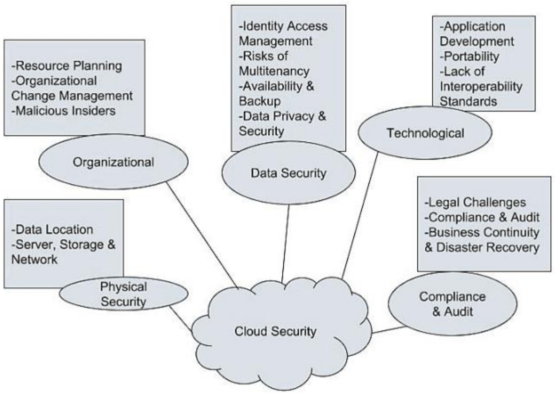

Fig 2 Cloud Provider Risk Categories and sub categories.

Cloud computing not only reduces the overload of infrastructure but it is also best at the efficient and the performance and provides the flexibility and the updated performance to the users. The cloud is being used and there is the major issue of security since the cloud computing is being used by the number of organizations and the end users as well whether the data that is been stored on the cloud is secure or not as the organizations work with the sensitive and the important data , so It is very important to keep the track of the same whether the data is secure or not thus in the same scenario industries use their own cloud to avoid the data lost or any kind of attack on the cloud and on the data. When we store the data on the cloud here comes an advantage out of it that the same data can be shared with the different organizations but with the advantage there is a limitation as well that more the users the more risk it can get. When is data is being shared with the different organizations through the cloud that is not trustworthy weather from the other side the proper security measures are taken or not.

When the data is shared among the different industries it possesses the risk so to overcome on the same risk it is very important to protect the data repositories.

One of the key questions when we use the cloud for the data storage should we use the third party service or the internal cloud services, as we have the sensitive information and exposing the important data in public will be serious issue, so in these cases internal organizational cloud should be preferred. This approach seems the best fit as this can be very helpful when securing the information and data by enforcing the on-premises data usage protocols.

This also does not guarantee for the full security as many organizations are still not qualified and trained enough to use the all layers of protection to the sensitive data and there is always the scope of improvement that is why it does not imply the guarantee that it is properly protected. Data itself is very expensive and number of people are working behind the walls to steal the sensitive information example bank stores the information on the cloud and the important details and the data of the customer is being stored on the cloud like the credit card, debit card and account related details so it is very important to use the optimal techniques to save the important and the sensitive data and to save from the compromising with the hackers as the technologies grow and hackers are working behind and are using the smart ways to steal this critical information since there is a need of an hour that the measures should be taken in order to save the sensitive information.

In past we have seen that the important data has been compromised by the Hackers and the money has been transferred with the number of smart techniques that these hackers use. According to the study these people use the different kind of attacks even on cloud such attacks include covert channel attacks, Denial of service are usually carried out either by co residing the VMs (Virtual Machines), which can be detected easily and a trap can be formed in cloud like the Botnet.

In the environment of cloud computing the already available intrusion detection cannot help to achieve the desired level of security since there has been a rapid change in the architecture of cloud computing. The reputation of cloud computing in terms of use demands the best security measures since intruders can damage the data and cannot be the best choice for the organizations in case this happens. The security and real time alerts will help the organizations to expect the secure deployment and the use of cloud environment

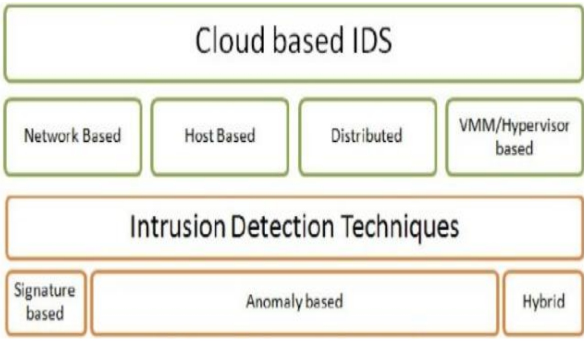

Fig 3 Cloud based IDS

As the Technological innovation and the new way moves and grows there are number of researchers, ethical hackers (white hat hackers) are working on their own system and carrying out different attack to check the loopholes in their own system these people check and think with the perception of the black hat hackers that up to what level they can attack on the cloud, since when these people are able to check and determine the loop holes then they fix it by using the different techniques as it is being checked from the physical to analytical level In order to make sure that the attacks would not affect their system these people are the highly paid engineers in the industry as the data is critical and when it comes on the cloud high level of expertise is required to secure and to protect the whole cloud network, so industries can store the data on the cloud and the right people will access that data as well it is very important .

This paper is the study of the information, data and the different ways or the techniques used in order to make sure that the data is secure and is protected so the users can easily trust and work on the data that is being shared or being used with in the organizations.

II. LITERATURE REVIEW

In order to under the better about the cloud computing and how the data can be stored with the aim that the data will not get compromised, so for that several ways of information has been consulted, in this section I will outline the review of the literature in order to set the basics of discussing the enormous security options of data security in cloud computing.

Srinivas, Venkata and Moiz provide an excellent overview and deemed about that how cloud computing can be much beneficial and grow as a technological innovation, by exploring this paper number of ideas and concepts have been explored thus it provide that outline about the best applications that can be developed used cloud computing.

On the other side, Chen and Zhao have discussed the regarding migrating the data into the cloud the experts say that there remains the threat of compromise of data that is the security issue, so the number of large industries do not prefer to move the data into the cloud. Authors have provided the outstanding explanations on the data security and the protection of data from being getting misused or compromised by the unauthentic users.

However, Lynda Kacha and Abdelhafid Zitouni provided the standard that how the data in transit can be secured, and the encryption is discussed to store the primary data first and this is the most efficient method that is why this method is valuable nowadays as well on the cloud environment, encryption provides the best solution to protect the data but this requires the extra computation. The data encryption is not always possible in data-at-rest.

Tjoa, A.M. and Huemer examine the privacy issue by providing the secure access to the data as the number of cloud attacks have been decoded and studied and thus the cloud attacks have been reviewed and the solution has been proposed to secure the cloud from the cloud attacks. End user's majority of the times trust on the experts but when then experts are not able to propose or implement the proper solution and in that case that case the end user always come under the trap and the important data would get compromised.

Thus, it is very important that the experts should use the proper expertise in order to find the best-fit solution so that the end user will not come into the trap.

Therefore, Abdelkader and Etriby proposed one model in cloud security, which is totally dependent on the cloud security. The software has also been developed by them to enhance the data security in the cloud computing and this will go on until the work is completed.

III. CONCLUSION

As the technology is growing the new technologies are taking place, cloud computing is one of them. There is the rapid growth in this technology and this Technology changed the world in terms of storing the data and to access the data. Cloud is called the best market making technology in twenty first century as this technology is implemented by the number of industries and found the same best fit for their organizations, as we are aware about it that when we migrate on the technology there more beneficial it is there can be threats as well like the attacks on the cloud by the hackers to steal the sensitive information and for that industry based experienced experts are being hired so that they can look over the security of the cloud as the sensitive data is on cloud, the experts check with their system and in case they find any loophole they fix the same .

The aim of this paper is to review some of the techniques that has been used so far and what can be done in the future on order to protect the data and information from being misused by the people who are behind the breaking of privacy and the security.

Anything which is on internet can be compromised if it is not being used in the secure manner and if it is not being used according the security protocols, it is important that before we migrate any data on the cloud or we access the data on the internet we should always take care of the security as this is very important because the number people have lost the information worth millions and billions when we store the data on the cloud it should be encrypted as already mentioned in this paper.

Though in this paper the major concern is the data security for that cloud needs to be secured when the cloud is secured and the proper protocols have been followed then there is no chance that the same data will get compromised in that case the industry based cloud can be trustworthy, nowadays people prefer to use the cloud instead of carrying the physical devices as if the physical device is lost the chances are that the data will be also lost and if the physical device gets destroyed with any natural disaster then there is no chance that the data will be caught back , but in case of cloud certain techniques are used like the alerts when there is an attack on the system there will be the alert in the monitoring team that somebody is trying to intrude into the cloud so the experts can use the techniques where data will be saved . Hence, it is very important that necessary techniques should be used in order to secure and protect the data because everything today is data and when the data is safe we are safe.

ACKNOWLEDGMENT

I would like to thank Dr. M. Mazhar Afzal, my parents and friends for completing this paper.

REFERENCES

1. An, Y.Z., Zaaba, Z.F.,Samsudin, N.F.: Reviews on security issues and challenges in cloud computing. In: IOP Conference Series: Materials Science and Engineering, vol. 160, p. 012106. IOP Publishing (2016).
2. Srivastava et al., International Journal of Advanced Research in Computer Science and Software Engineering 8(6) ISSN (E): 2277-128X, ISSN (P): 2277-6451, pp. 17-20.
3. Cyril, B.R., Kumar, S.B.R.: Cloud computing data security issues,
4. challenges, architecture and methods-a survey. Int. J. Eng. Technol. 2, 848–857 (2015).
5. Arjun, U., Vinay, S.: A short review on data security and privacy issues in cloud computing. In: IEEE International Conference on Current Trends in Advanced Computing, pp. 1–5. IEEE (2016).
6. Venters, W., Whitley, E.A.: A Critical Review of Cloud Computing: Researching Desires and Realities. J. Inf. Technol. 27, 179–197 (2012).
7. Yang, H., Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Commun. Assoc. Inf. Syst. 31 (2012).