Cyber Security to Cloud Security

1. Nikita Singh
Department of Computer Science and Application,
KL University
Andhra Pradesh, Vijaywada, India
ns4892292@gmail.com

2. Sanyog Bharti
Department of Computer Science and Application,
KL University
Andhra Pradesh, Vijaywada, India
ns489229@gmail.com

Abstract

Cloud Security core are dependent on the cyber security or cloud security; cloud security developed their own domain in the data field.

Cyber security or Cloud security are the term of the Information security. This paper has defines the methodology of these two terms which associate their methods to each other. The concept of these two are same, to provide the security to the data, but their methods are differ to each other. Moreover, this paper posit that Cyber security have some limitation to access, and other hand cloud security will extended their networks and it will work on beyond of the cyber security services. Cyber security used to protect the internet devices which devolve the data from source to destination. Cloud security is the collection of disparate policies and mode which gives the cloud environment with the newly methodology, so in this paper; we discussed that how the cloud security gives the better performance with correlate to the cyber security [1].

I. INTRODUCTION

Cyber security is the huge global interest of the society. The cyber crime likes networking hacks, data-fetching, IP-address spoofing or immeasurably more, who really need of security, but in now days people-to-people are connected so data-by-data also be connected in the long series, where cyber security not been managed to all.

Cyber crime has their cyber-space where unauthorized person can fetch and harmed the data, so we can put on some encryption on that servers; where no one can easily identified the information. So by the cyber security we apply the security and encryption on data, but as it is we know; at today's time huge amount of data will stored, so this is not easy to in-build the cyberspace and provide authentication to the networks or servers, that's why we need a cloud security.

Lot of the literatures and journals are defined the strategy of the security, network security, cyber-security. The international telecommunication union (ITU define

cyber security: [1] [2] Cyber security is the collection of tools, policies, security concept, security safeguards, guidelines, risk management approaches, action, training, best practices,

assurance and technology that can be used to protect the cyber environment and organization and user assets.

Organization

and user assets include connected computing devices, personnel, infrastructure, application, services, telecommunication system and the totality of transmitted and stored in formation in the cyber environment.

This paper will enumerate that; how Cyber Security not provided that kind authentication and security to the networks, or discussed what kind of data security or network security we used to authenticate the cloud data. Mainly cyber security are worked on the CIA triangle (Confidentiality, Integrity and Availability), which are the best taxonomy of the security. CIA triangle is a model of information security, which carry three types of approaches to design and define the compound part of security; it defined the confidentiality, availability, integrity all three are core of information security. Here we discussed the methodology of the cyber security and what kind of the tools are used in it. Some of the aim not worked in the cyber security but held in cloud security. Compare the cloud security to cyber security tools and get in-build in the cloud security to get improved the server security.

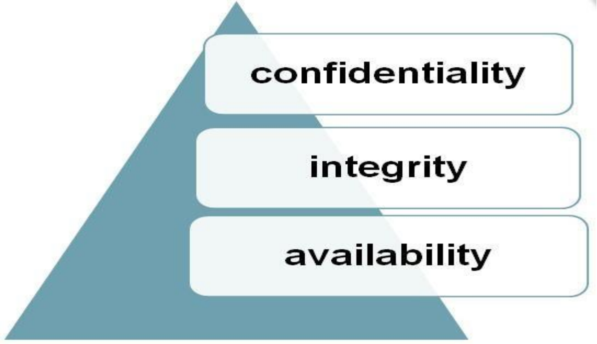
Cloud Security widely adopted by the society very fast, because cloud application needs security and authentications. Cloud has that plat-form where it will face lot of the security challenges, so cloud will prepare their security mechanism and evaluated in the applications or servers.

Cloud security used some frameworks and graphic models which really defined data security. To security of the cloud application is much more challenging, some time it will be complex to solve their complexity, but lot of the tools are available in the network, so with them we solved the problem, whether it is cyber security or cloud security every network security really needs a network tools and

II. CYBER SECURITY

To dealing with the data security and their privacy cyber security is the best term to Identified. Cyber security is interchangeably word of the information security which performed many task of the security.

Here we discussed; [3] CIA triangle and their work, cyber security threats or more. To securing the data are very substantial to shielding the database. Avoid the risk and manage network by the cyber security which gives the better performance in our relevance economy factors. Defense sector are used cyber security mostly; because they really entail authentication and protection to our data, cyberspace are the space; where no one can be allowed to get and access the legal data. When War has been done by cyberspace it's known as cyber-war. The unauthorized user can access the legal data and privacy so it's called cyber-crime, which is the individual part of the cyber-security.

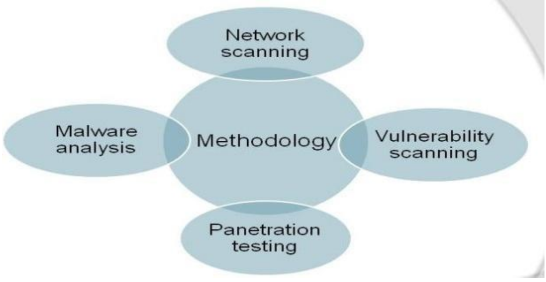


(CIA Triangle of Cyber Security)

Never been stored your data as open source, because it is more easy to access to anyone. [3] [4] The CIA triangle of the cyber security will define that confidentiality gives the protection and security to server or database or integrity define the stats of being complete of the protection and availability compare the resistance of the user that who access or not.

1. *Methodology of the Cyber security*

Here we discussed about the different types of the methodology of the cyber security which really helpful for indentifying the encrypted data or unauthorized user like: network scanning, vulnerability scanning, malware detection, password cracking, penetration testing.



(Methodology of Cyber Security)

A. *Network scanning*

Network scanning are mainly used to gather information from the operating system. It will helpful for find the network error and default performance by the hackers. Network scanning help to recognize the TCP targeted hosts, if any unauthorized user can try to access the network it will determine [5].

In the network security; port scanning is so famous because of the problem solving approaches, by the port numbers we identified user that it will valid to access the network or not. Network scanning refer to the concept of bunch of data which send through the computer network and create the effective troubleshooting problem solving.

B. *Vulnerability scanning*

Vulnerabilities are mainly used to detect and identifies the fragility of the network that any kind of Impact like worm or viruses are occur in the services or not; so it will really easily to get diagnose. IT sectors or department; they have authority to used the vulnerabilities scanning. It is used for the end point or entry point of the attacker surface [5] [6].

Vulnerabilities are working on two approaches: authenticated and unauthenticated. In the unauthenticated vulnerabilities perform a testing method without check the network user or their access, or unauthenticated vulnerabilities firstly scan the network user and gives the authenticity to access.

C. *Malware analysis*

Malware analysis is used for the identification of threat and any malicious files. In the cyber security; word Malware is the key term of the authentication and error detection and reduce the false character from the network system. At today's era; Malware analysis is considerate term in the areas for the error control and cyberspace [7].

Malware contribute the rate in the cyber security for the prevention of network. Malware analysis work on the two detain: static and dynamic. In the static malware analysis it will analysis the network and source without running the code like viruses scanning, fingerprinting, it means it will bounded at some points to access any known and unknown user, but in the dynamic malware analysis, it will analyze the network and source while the time of running code, it will create a control environment where anyone can't easily access.

D. *Penetration testing*

Penetration testing is the way to evaluate the security and network which score the user information. The penetration testing occurs and tested at different area of the system like setting, login method, user access counter.

Penetration doesn't provide to accessing the security service and network services [8] [9]. Sometimes it will test as manual but some time not required to given an access it will automated access and testing.

III. CLOUD SECURITY

Cloud computing invention has done on huge platform, which used by the technologist in advanced level. Cloud computing gives privileges and advantages to data and servers, but we never ignore; that data can occur or access by the user and storage container are become in-large so it's important that we think about the security also. [10] Cloud computing is the strong adoption of potential to stored data, threat scanning or lot more, Increasing the data storage, privacy, protection or Security very important clause in cloud security.

Cloud is the software and hardware storage where data centre to associate all the services. [11] [12] Cloud computing are synchronize by two way:- private cloud and public cloud. Private cloud refers to particular area or institution where only authorized people can access the data centre, where public cloud refers the public services which can accessible by any one. It will never be down; that cloud gives good services to the other data services; like quick to access, storage and provision.

Need of Cloud Services and Security, Lot of the data produced daily in the every sector, it's time to mange and provides security to the data. In every sector whether it is IT, medical, or more; has their own bulk of data which really need of the security [13].

Domain	Services
Computational Resource	IaaS(Infrastructure as a service)
Cloud Software Environment	PaaS (Platform as a Service)
Communication	CaaS (Communication as a Service)
Storage	DaaS (Database/Development/desktop as a service
Hardware	HaaS (Hardware as a Service)
Software Application	SaaS (Software as a Service)
Framework	FaaS(Framework as a Service)

(Services of Cloud Computing)

2. *Services of Cloud Computing*

Cloud computing makes problem easy and less time consuming to data storing their workflow is very efficient to consider. Cloud computing contribute to the services and sources very well, it really helpful for the sharing resources. Cloud security integration in any sector gives a lot of dependability and scalability. Let's discussed abut different sectors why cloud is beneficial for their data storage and security:

A. *IT sectors*

Market of cloud computing and cloud security is the top growth demanding service. We know cloud computing is famous for the data storage or scalability, but in IT sector every tiny things can worked in the bulk of data, which needs organization and security [14]. Cyber attacks are top breaches who really affect the cloud data and data storage container.

B. *Shielding Sector*

Shielding sector or defense sector are authorized compound area where data security are essential. [15] Today's time; when we talking about the defense, the security risk has been occur . there are lot of ethical and legal; data which needs are authentication. Military level security define; companies be sure that they never exchange their data to anyone, prohibited every single information; they must be follow the data protection and security. Each defense sector: Air-force, Military, Navy every operation has been produce the flexible environment to catch their signal are transfer the data. So in between their key inter-connectivity it may e chance to the data leakage and leakage of communication. It is the major sector where mostly data are exchange in real-time which produce more risk. To give a real-time environment and authenticated the defense area by the cloud security; data stored mostly in the cloud storage really impactful for the security purpose.

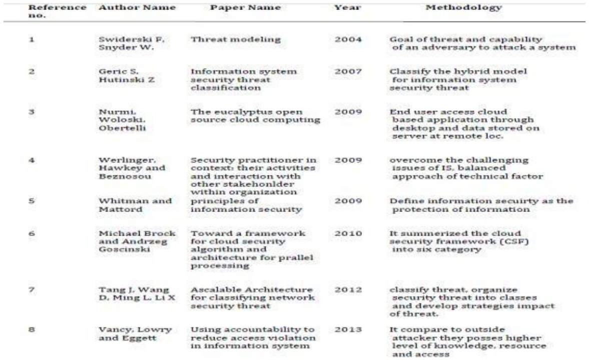
3. *Cloud security risk*

The factor of risk occur in cloud computing, because of their wide range include lot of factor; mostly the cloud security risk are occur in the application level, network level or some time at data storage time.
[16] Application level risk factor across the many sites and servers like: cookies poisoning, Captcha breaking, access the malicious file or lot of programming or recreating services. Network level risk factors occur by DNS attacks, data tapping, any Fiber optic network or IP address. Data storage risk factor occur when any kind of leakage in data container or if fraud user get your user access.

4. *Cloud security risk management*

To manage the cloud security risk we apply treatment on particular risk factors. To do assessment on the risk factors, firstly we identify the specific container area where the clause are been occurred after the Identification, check the potential of the threat that it will harmful for the services or not. To manage the security risk firstly we should do some assessment on particular risk factor so by doing this we can easily found that where and what clauses are been held. Lot of risk assessment methodology gives the IT infrastructure like:- ISO27005, NIST SP800-30, CRAMM, OCTAVE or lot of more.

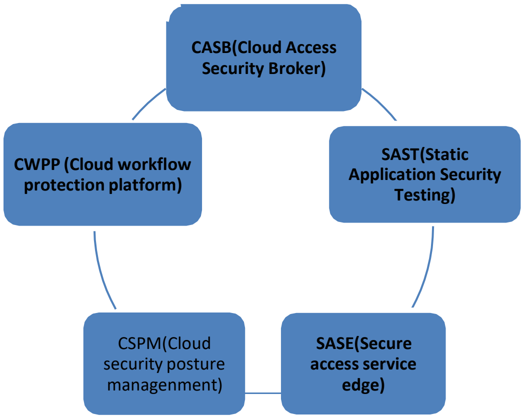
Different journal/papers are work different security method lets discuss:



Reference no.	Author Name	Paper Name	Year	Methodology
1	Swiderski F, Snyder W.	Threat modeling	2004	Goal of threat and capability of an adversary to attack a system
2	Geric S. Hutinski Z	Information system security threat classification	2007	Classify the hybrid model for information system security threat
3	Nurmi, Woloski, Obertelli	The eucalyptus open source cloud computing	2009	End user access cloud based application through desktop and data stored on server at remote loc.
4	Werlinger, Hawkey and Beznosou	Security practitioner in context: their activities and interaction with other stakehonlder within organization	2009	overcome the challenging issues of IS, balanced approach of technical factor
5	Whitman and Mattord	principles of information security	2009	Define information secuirty as the protection of information
6	Michael Brock and Andrzeg Goscinski	Toward a framework for cloud security algorithm and architecture for prallel processing	2010	It summerized the cloud security framework (CSF) into six category
7	Tang J. Wang D. Ming L. Li X	Ascalable Architecture for classifying network security threat	2012	classify threat, organize security threat into classes and develop strategies impact of threat.
8	Vancy, Lowry and Eggett	Using accountability to reduce access violation in information system	2013	It compare to outside attacker they posses higher level of knowledge, resource and access

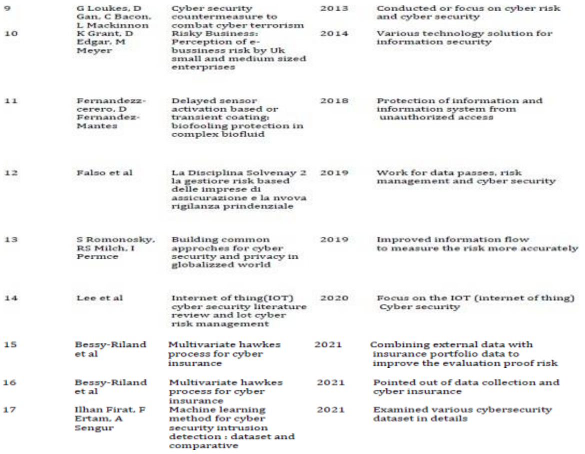
IV. *CLOUD RISK SOLUTION*

Cloud Risk Solution are core domain of the security of cloud data; which efficiently work on the cloud data and define access, testing, management, platform or more regarding to the risk solution. Majorly we have five risk solution cycle which we discussed by in periodic way:


CASB(Cloud Access Security Broker)
SAST(Static Application Security Testing)
SASE(Secure access service edge)
CSPM(Cloud security posture managenment)
CWPP (Cloud workflow protection platform)

(Cloud Security solutions)

A. ***CASB*:** Cloud access security broker is a services or provide software tool which help to reduce the impact of threat through the cloud data. It offers the some security policies like firewall, [16] Authentication, web application firewall, data loss prevention (DLP). T o choosing the right security tools are save-time and money. CASB software tools provide multiple data point authentication and work on the beyond the limitation, like



9	G Loukes, D Gan, C Bacon, L Mackinnon	Cyber security countermeasure to combat cyber terrorism	2013	Conducted or focus on cyber risk and cyber security
10	K Grant, D Edgar, M Meyer	Risky Business: Perception of e-bussiness risk by Uk small and medium sized enterprises	2014	Various technology solution for information security
11	Fernandezz-cerero, D Fernandez-Mantes	Delayed sensor activation based or transient coating: biofooling protection in complex biofluid	2018	Protection of information and information system from unauthorized access
12	Falso et al	La Disciplina Solvenay 2 la gestiore risk based delle imprese di assicurazione e la nvova rigilanza prindenziale	2019	Work for data passes, risk management and cyber security
13	S Romonosky, RS Milch, I Permce	Building common approches for cyber security and privacy in globalizzed world	2019	Improved information flow to measure the risk more accurately
14	Lee et al	Internet of thing(IOT) cyber security literature review and lot cyber risk management	2020	Focus on the IOT (internet of thing) Cyber security
15	Bessy-Riland et al	Multivariate hawkes process for cyber insurance	2021	Combining external data with insurance portfolio data to improve the evaluation proof risk
16	Bessy-Riland et al	Multivariate hawkes process for cyber insurance	2021	Pointed out of data collection and cyber insurance
17	Ilhan Firat, F Ertam, A Sengur	Machine learning method for cyber security intrusion detection : dataset and comparative	2021	Examined various cybersecurity dataset in details

Force-point; it is CASB address product which work on the risk assessment and proved a real time security.

B. SAST: Static application security testing is used for the cloud application security, it provides the software tool which help to reduce the impact of threat but only took the cloud application; it find out the root fault which worked on instantaneously, reduce security risk through the coding which really helpful for the developer. It is essential or initial stop of software development. SAC (Static code Analyzer) tool are exist in the SAST service which analyze the encrypted threat and vulnerabilities in coding.

C. *SASE:* Secure access service edge is mainly network architecture which made up to the combination of VPN and SD-WAN with different types of security. It reduce the complexity and provide real time optimization. Restrict to unauthorized user access and improving lot of security with different policies.

D. *CSPM:* Cloud security posture management, it is market segment of IT sector which reduce the compliance of risk through the cloud. The most attracted things of CSPM is that; it monitor the cloud infrastructure or if any single threat are occur in the compound area it will detected. [17] Mainly CSPM is organized and adopt the hybrid cloud and multi-cloud security, which associated with infrastructure as a service (IaaS)

E. CWPP: Cloud workflow protection platform; it provide the security on the cloud workload or work on the low friction segment neither adopt heavy approaches. Infrastructure clouds are Consider or discovered heavy work load which need a real time service which provide by CWPP. It is more flexible and integrated into development of CI/CD pipelines; it has different stage of CWPP solution stage so that’s why it will save lot of money.

V. Conclusion

In this paper we discussed different approaches of the cyber security and cloud security. Cyber security defines their methodology; how it will perform every single threat through the security task, either Consider the CIA triangle approaches. Different sections analyze the Cyber Security by the network scanning, malware analysis or penetration testing. After defining the cyber security; consider the approaches of cloud security and their methodology. Different sector which really needs of cloud environment; evolving and elaborate the cloud security risk and their management. We also do a research on different journal and articles to resolving different approaches of cyber and cloud security. End; cloud risk solution dines how resolved the threat material with different tools and resources.

References

[1] jhon, van niekerk, "From information security to cyber security,
" *elsevier*, pp. 5-7, 2013.

[2] T. M. N. Q. A. Nassif A, "Machine learning for cloud security,"
IEEE, pp. 1-19, 2021.

[3] A. S. S.-O. F. J, "RSM analysis based cloud access security broker:
a systematic literature review," *CLUSTER COMPUTING*, 2022.

[4] D. L. f. C. S. A. A. C. S. E. t. M. M. T. V. p. A. C. A. o. M. C. U. D.
L. M. i. C.-M. H. L. V. p. D. Learning, "Deep Learning for Cyber
Security Applications: A Comprehensive Survey English to
Malayalam Machine Translation View project A Comparative
Analysis of Machine Comprehension Using Deep Learning Models in
Code-Mixed Hindi Language View project Deep Learning,"
Rsearch gate, 2021.

[5] s. s. k. s. R. c. atul m. tonge, "cyber security: challenges of society,
" *academia*, 2013.

[6] F. C. ·. B. S. ·. M. F. ·. A. N. K. ·. M. M. ·. F. M. ·. S. Materne,
"Cyber risk and cybersecurity: a systematic review of data
availability," *geneva paper*, 2022.

[7] C. B. Temesgen Kitaw Damenu, "Cloud Security Risk Management: A Critical Review," *IEEE*, 2015.

[8] P. K. a. a. M. Singh, "Different Challenges in Energy-Efficient Cloud Security: A Brief Review," *RESEARCH GATE*, 2022.

[9] G. S. Hussain Aldawood, "Educating and Raising Awareness on Cyber Security Social Engineering: ALiterature Review," *Research gate*, 2018.

[10] J. W. A. A. S. B. M. G. Shanks, "A Situation Awareness Model for Information Security Risk Management," *research gate*, 2014.

[11] H. Chen, "Applications of Cyber-Physical System: A Literature Review," *research gate*, 2017.

[12] S. W. a. J. T. M. Cynthia K. Veitch, "Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants," 2012.

[13] . J. H. ,. E. Tatiana Ermakova, "Cloud Computing in Healthcare – a Literature Review on Current State of Research," 2013

[14] R. F. El-Gazzar, "A Literature Review on Cloud Computing
Adoption Issues in Enterprises".

[15] M. B. L. M. G. J. Inger Anne Tøndela, "Information security incident management: Current practice as reported inthe literature," 2014.

[16] M. ZahoorAhmedSoomro∗, "Information security management needs more holi
sticapproach:Aliteraturereview," *elsevier*, 2015.

[17] *. L. B. A. R. A. B. A. Mouna Jouinia, "Classification of security threats in information systems," *elsevier*, 2014.