Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 7, Issue 01, January -2020

The Future of Cloud Computing

Lokesh Kumar[1]

[1]GSOC, Altran, Gurgaon

Abstract —*This paper is about cloud computing and its future path in the coming decades. Even though it still suffers from its various fundamental issues, such as multi-latency and few security issues, it is clear that cloud computing is the path forward as long as it keeps evolving. This paper will cover everything about the present cloud computing technology and will explore a future where cloud computing evolves after successful integration with artificial intelligence.*

Keywords-*Cloud Computing, Artificial Intelligence, AI, Machine Learning, ML,Multitenancy*

I. INTRODUCTION

Cloud computing can be defined as "a network solution for providing inexpensive, reliable, easy, and simple access to IT resources" [1]. Cloud computing enables its users to access resources online through the Internet, from anywhere at any time, without worrying about technical/physical management and maintenance issues of the original resources. Besides, Resources of cloud computing are both dynamic and scalable. Google Apps such as Gmail is an outstanding example of Cloud computing; it enables one to access services via the browser and services that are deployed on millions of hosts over the Internet. Resources are accessible from the cloud at any time and any place across the globe using the Internet. Cloud computing is more cost-effective than other computing models; there is zero maintenance cost since the cloud technology provider is responsible for the availability of services, and clients are free from maintenance and management problems of the resource machines. Scalability is a crucial attribute of cloud computing and is achieved through server virtualisation. This revolutionary kind of computing uses remote servers placed in extremely safe and secure data centers for storage of data and management, so organisations do not need to pay for and look after their internal IT solutions. After the creation of a cloud, deployment of cloud computing differs according to the requirements and purpose, for which it will be used. The principal service models deployed are:

Software as a Service (SaaS): Cloud server hosts softwares which are provided as a service to the consumers according to their requirement.

Platform as a Service (PaaS): Clients are given access to platforms, which lets them put their customised softwares and other applications on the clouds.

Infrastructure as a Service (IaaS): Rent processing, storage, network capacity, and other essential computing resources are granted, enables users to manage the operating systems, applications, storage, and network connectivity.

A primary concern in the adaptation of cloud for data is security and privacy [2]. The cloud needs to ensure data integrity, privacy, and security. For this, many service providers are using various policies and mechanisms that depend onthe size, nature, and type ofdata.

One of the advantages of Cloud Computing is that data can be shared among various organisations. However, this advantage poses a risk to the data. To prevent potential risk to the data, it is necessary to protect data repositories. One of the critical questions while using the cloud for storing data is whether to use a third-party cloud service or create an internal organisational cloud. Sometimes, the data is sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details. This type of data can be susceptible, and the consequences of exposing this data on a public cloud can be severe. In these cases, it is highly recommended to store data on the internal organisational cloud. This step can help in securing data by applying the on-premises data usage policy. However, it still cannot offer full data security and privacy, as many organisations are not able to add every layer of protection to their sensitive data. This paper is the study of the security issues persisting till date with cloud computing and proposes a future path of cloud computing in which it integrates with artificial intelligence.

II. LITERATURE REVIEW

This section gives a literature review for discussing various fundamental concepts of cloud computing.Srinivas, Venkata, and Moiz provide excellent insight into the basic concepts of cloud computing. Several keyconcepts are probed in this

paper by giving examples of applications that can be developed using cloud computing and how they can help thedeveloping world in getting benefits from this emerging technology [1].

On the other hand, Chen and Zhao have discussed the consumer's concern regarding moving the data to the cloud. According to Chen and Zhao, one of the foremost reasons why large enterprises still would not move their data to the cloud is security issues. Authors have provided outstanding analysis on data security and privacy protection issues related to the cloud. Furthermore, they have also discussed some of the available solutions to these issues [3, 4].

However, Hu and A. Klein have provided a standard to secure data-in-transit in the cloud. For guarding data during transmission, a benchmark for encryption is discussed. For robust security, additional encryption is required, but it involves extra computation. The benchmark considered in their study presents equilibrium for the security and encryption overhead [5].

Tjoa, A.M., and Huemer examine the privacy issue by preserving data control to the end-user to surge confidence. Several Cloud computing attacks have been reviewed, and some solutions are also proposed to overcome these attacks [6].

A paper published by Miranda and Siani states that the most significant obstacle to full acceptance of cloud computing services is the security and privacy issues in cloud computing [7]. Users have grave concerns about confidential data seepage. Privacy is not recognised while critical data is being processed in the public accessible cloud.Some practical scenarios have been discussed in this paper, based on these scenarios, it is strongly recommended that the use of sensitive information must be minimised when data is processed on clouds, and privacy to end-users must be assured. To address this issue, a client-based privacy manager tool has been proposed in this paper. The recommended tool reduces security issues and provides added privacy features. The tool has been tested accordingly in different cloud computing environments.

III. CLOUD COMPUTINGDATA SECURITY

Data security in cloud computing is not merelyjust data encryption. Requirements for the security of data depend on the three service models SaaS, PaaS, and IaaS. Two states of data generally have a threat to its security; Data at Rest, which means the data is stored in the cloudand Data in Transit, which means data that is flowing in and out of the cloud. Confidentiality and integrity of data depend on the nature of data protection processes, mechanisms, and procedures.

3.1. Data at rest

It refers to data that is in a state of rest and is accessible either in the cloud or viathe Internet. This includes live data as well as backup data. As mentioned earlier, it is challenging for organisations to protect data at rest if they are not maintaining a cloud for private use since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

3.2. Data in transit

Data in transit refers typically to data that is moving in and out of the cloud. This data can be a file or database stored on the cloud and can be fetched for use at some other remote global location. When data is uploaded to the cloud, the data at the time of being uploaded is known as data in transit. Data in transit can be sensitive data like passwords, credit card information and can be encrypted at times. However, data in unencrypted form is also data in transit [8].Data in transit is sometimes more susceptible to risks than data at rest because it has to travel from one location to another (Figure 1). There are several ways in which software can eavesdrop the data and sometimes modify the data on its way to the destination affecting its integrity. To protect the data in transit, one of the best methods is encryption.

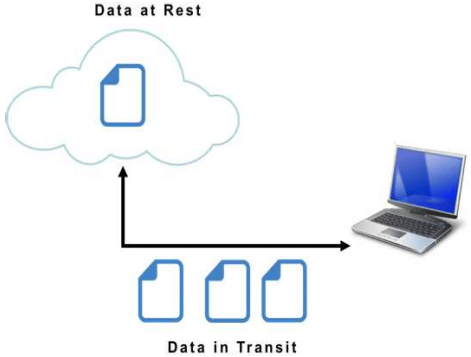

Figure 1. Data at Rest and in Transit

IV. MAJOR SECURITY CONCERNS AND CHALLENGES

The major challenges involved in cloud computing are:

4.1. Lack of appropriate governance

During cloud computing, the service provider has full control. By giving this control to the provider, there is a danger that the loss of control over authority parameters could result in security being compromised, leading to problems in terms of data access and the application of the resources. This compromised security concern comes with another threat of creating a gap in security cover in cases where Service Level Agreements are not in place with the service provider. Further, the terms of use are also open to the liberty of the user, meaning that access to data can be exploited quite easily. For instance, the Google search engine states that the user: "agrees that Google has no responsibility or liability for deletion or failure to store any content and other communication maintained or transmitted through use of the service [9]. Amazon also clearly states that they do not take any responsibility, liability, or authority for unauthorised use, corruption, access, loss or deletion of data, or any other sort of access, including harm to the application [10]. Hence, customers are faced with security concerns regarding their data and application, as hosted by the third party, service provider, or mediator.

4.2. Lock-in

The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities.[27]

4.3. Internal Attacks

Sometimes the architecture of cloud computing environments poses risks to the privacy and security of the customers [11]. When it happens, itis tough to deal with. It can be a malicious cloud provider user, a malicious cloud customer user or a malicious third party user. For example, a cloud administrator can use existing privileges to gain further access or support third parties in executing attacks against the confidentiality, integrity, and availability of information within the cloud service.[28]

4.4. Insecure or incomplete data deletion

In instances where users request their data to be deleted either partially or wholly, a question is raised of whether it will be possible to remove the desired part of their data segment with full accuracy. This makes it difficult for potential users to subscribe to the services of the cloud-computing [12].

4.5. Data interception

Unlike with traditional computing, the data in cloud computing is segmented and distributed in transit. Hence this poses more risk due to the vulnerability and fragility of the technology and, specifically, sniffing and spoofing, third party attacks, and replay attacks [13].

4.6. Compromise of the management interface

Since the services of cloud computing are delivered remotely over the Internet, and the resources are accessible to the service provider, third party access can result in malicious activities [14]. As a result, the vulnerabilities, manipulation of services, and involvement of the service provider are amplified. For instance, the customer may take over the machines, and conversely, the provider can take over the control by setting up no-go zones in the applications of cloud computing.

4.7. Virtualisation

Virtualisation is a technique in which a fully functional operating system image is captured in another operating system to utilise the resources of the real operating system entirely. A particular function called hypervisor is required to run a guest operating system as a virtual machine in a host operating system [3, 15].
Virtualisation is a foundational element of cloud computing that helps in delivering the core values of cloud computing. However, virtualisation poses some risks to data in cloud computing. One possible risk is the compromisation of the hypervisor itself. A hypervisor can become a primary target if it is vulnerable. If a hypervisor is compromised, the whole system can be compromised and hence the data too [16].

Another risk with virtualisation is associated with the allocation and de-allocation of resources. If Virtual machine operation data is written to memory and it is not erased before reallocation of memory to the next virtual machine, then there is a potential for data exposure to the next VM, which might be undesirable [17].
A solution to the issues mentioned above is better planning for the use of virtualisation. Resources should be used carefully, and data must be appropriately authenticated before de-allocating the resources.

4.8. Storage in Public Cloud

Storing data in a public cloud is another security concern in cloud computing. Typically clouds implement centraslised storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are a combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud [18]. It is always recommended to have a private cloud if possible for extremely sensitive data, to avoid the risk.

4.9. Multitenancy

Shared access or multitenancy is also considered as one of the significant risks to data in cloud computing [19]. Since multiple users are using the same shared computing resources like CPU, storage, and memory, it is a threat to not only a single user but numerous users.
In such scenarios, there is always a risk of private data accidentally leaking to other users. Multitenancy exploits can be dangerous because one fault in the system can allow another user or hacker to access all other data [20].
These types of issues can be taken care of by wisely authenticating the users before they can have access to the data. Several authentication techniques are in use to avoid multitenancy issues in cloud computing [21].

Other challenges related to security include the transfer of information within different applications of cloud computing, leakage of information while uploading data to cloud, attacks on privacy and security of user's data, loss or malicious manipulation of encryption keys and conflicts between service providers and customers on procedure and policies on the operation of cloud computing applications. [22].
Some challenges indirectly interact with or influence cloud computing but have no direct impact on the integrity of cloud computing applications. Such scenarios include modification of network traffic, network breaks, and administrative issues, such as non-optimal use of resources, congestion, and miss-connection. There are some other risks associated with the applications of cloud computing, for instance, the risk of social engineering attacks, natural disasters, and theft of equipment [23].

The Treacherous 12: Cloud Computing Top Threats in 2016[26], is a report published by The Cloud Security Alliance (CSA) which shows top 12 security threats for cloud computing and serves as the up-to-date guide to help cloud users and providers make informed decisions about risk mitigation within a cloud strategy. They are as follows-

1. Data Breaches
2. Weak Identity, Credential, and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

V. PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit can be different. For example, encryption keys for data in transit can be short-lived, whereas, for data at rest, keys can be retained for more extended periods.

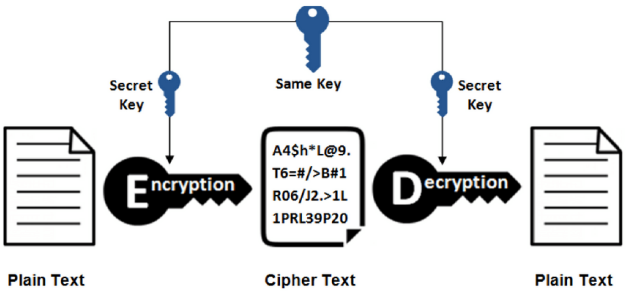

Figure 2. Basic Cryptography Process

Different cryptographic techniques are used for encrypting data these days. The level of data protection for assuring data integrity, authentication, and availability with the help of cryptography has increased. In the basic form of cryptography, the plaintext is encrypted into ciphertext using an encryption key, and the resulting ciphertext is then decrypted using a decryption key, as illustrated in Figure 2. These are the uses of cryptography:

5.1. Block Cipher

A block cipher is an algorithm for encrypting data (to obtainciphertext) in which a cryptographic key and algorithm are applied to a block of data instead of per bit at a time [24]. In this technique, it is made sure that similar blocks of text do not get encrypted the same way in a message. Usually, the ciphertext from the previous encrypted block is applied to the next block in a series. As illustrated in Fig 3, the plain text is divided into blocks of data, often 64 bits. These blocks of data are then encrypted using an encryption key to produce a ciphertext.

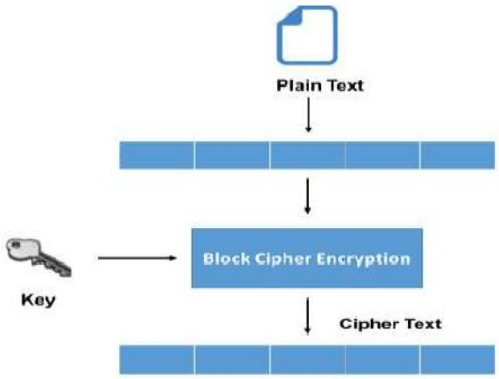

Figure 3. Block Cipher Mechanism

5.2. Stream Cipher

This technique of encrypting data is also called state cipher since it depends upon the current state of cipher. In this technique, each bit is encrypted instead of blocks of data. An encryption key and an algorithm are applied to each and every bit, one at a time [25].

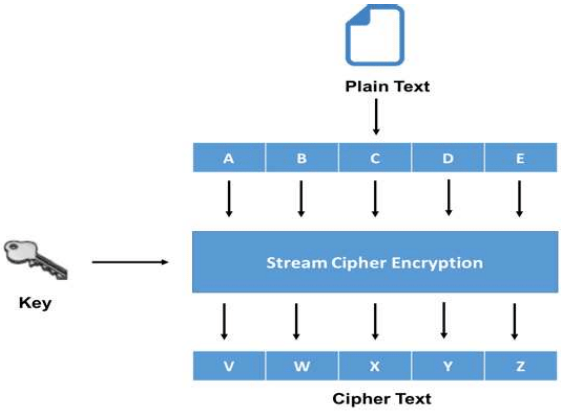

Figure 4. Stream Cipher Mechanism

The performance of stream ciphers usually is faster than block ciphers because of their low hardware complexity. However, this technique can be vulnerable to serious security problems if not used properly. As illustrated in Fig 4, stream cipher uses an encryption key to encrypt each bit instead of a block of text. The resultant ciphertext is a stream of encrypted bits that can be later decrypted using the decryption key to produce original plain text.

5.3. Hash Function

In this technique, a mathematical function called a hash function is used to convert an input text into an alphanumeric string. Typically the produced alphanumeric string is fixed in size. This technique makes sure that no two strings can have the same alphanumeric string as an output. Even if the input strings are slightly different from each other, there is a possibility of vast difference between the outputstrings produced through them.
This hash function can be an elementary mathematical function like the one shown in equation (1) or very complex.
F(x) = x mod 10 (1)
Fig 5, below shows the mechanism of hash function cryptography.

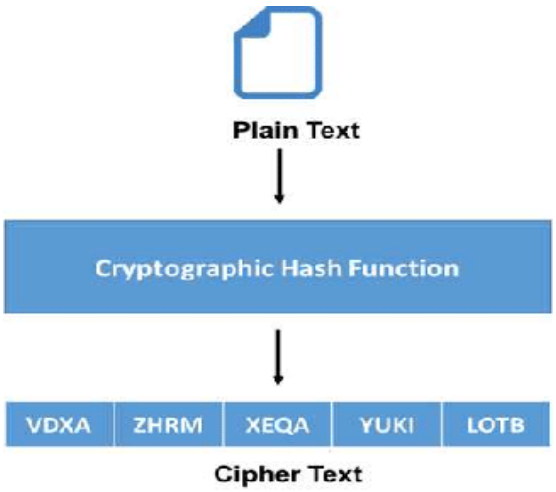

Figure 5. Hash Function Mechanism

All these methods mentioned above and techniques are widely used in encrypting the data in the cloud to ensure data security. Use of these techniques varies from one scenario to another. Whichever technique is used, it is highly recommended to ensure the security of data in both private and public clouds.

VI. FUTURE OF CLOUD COMPUTING

The following are some of the features that will be introduced with integration of AI with cloud computing:

6.1. Seamless data access

It refers to the unlimited data access privilege. Artificial intelligence uses data as input for enhanced performance and smarter decision-making process. In comparison to on-premises data storage, cloud environments can hold a large amount of data.Therefore, AI in the cloud does not needto deal with issues of delay inaccessibility. The cloud environment could learn from the collected data and make calculations as well as solve potential problems early. AI and Machine learning will also facilitate seamless data transfer between the cloud and on-premises infrastructure.

Hybrid cloud environments need smooth movement, connectivity, and accessibility. In the hybrid cloud, AI can help organisations in effective management and control of data. The organisation can gain data insights and scalability according to industry standards for improving resources in their possession.
The use of AI can help in the improved synthesis of continually evolving data systems for identifying useful information. Then, the gathered information can be implemented for practical business use cases. As the amount of data increases each year exponentially, the need for responsive cloud environments is evident.
AI can help in managing the considerably humongous volumes of information for making sense of the data. So, on the one hand, a person will increase the responsiveness of their cloud environment. On the other hand, he can empower the AI component of the combination. The real-time correlation of events can be done by using other industrial applications such as Splunk or a newly developed AI. This will help a dedicated security team to respond to detected suspicious or malicious events faster. On the other hand, AI can itself work singlehandedly, detectingS, and mitigating malicious incidents.

6.2. Analyticaladvantage

Utilisation of AI and cloud computing technology together can ensure assured benefits for analytics. Organisations could obtain an analysis report of relevant data to create promising information. Hence organisations can save the costs for highly trained analysts with the analytics advantage of this technology.

AI could achieve better results and at a lower price than the specialised analysts. Evaluation of statistics for analytics can take the workload from multiple teams outputting the same data which the AI can provide.

AI can help lessen the burden on the analyst teams and give technological support to help obtain accurate predictions from massive datasets.It also provides an advantage in text analytics.Text analytics can utilise AI for reading and analysis of massive volumes of textual content. AI can then identify patterns in text data efficiently and provide recommendations accordingly based on their analysis[29].
AI can go through the logs and analyse the suspicious event patterns quickly and also provide an in-depth analysis of hosts and files in them, which constitute the malicious activities.

6.3. Cloud security automation

Innovations in AI could help it process information and detect inconsistencies on cloud in near real-time. As a result, Ai can notify a human analyst or take alternate actions. These kinds of advancements can help in preventing access to cloud environments.

Furthermore, AI could detect suspicious events and anomalies and block them, restricting the entry of potentially malicious agent into the system. Also, AI can help in reviewing and collecting information from different locations helping organisations engage in security incident response effectively.
Another significant contribution of AI to cloud computing is the possibility of automation of security. It would not be replacing human experts but will be helping security teams work on incidents effectively.

6.4. Event detection and blocking

When AI and machine learning technologies process the data generated by the systems and find anomalies, they can either alert a human or respond by shutting a specific user out, among other options.[31]
Whenever AI and machine learning innovations and integration processes the information produced by the frameworks and discover anomalies, they can either alert a human or take action by blocking a user out among other alternatives.
Hence, events are detected and blocked with hours quickly, stopping the flow of possibly malicious code and agent into the system and preventing potential loss of data. This process of examining and collating data across devices in real-time helps organisation to potentially get enough time to take action ahead of security events.

An AI and ML integrated security platform reducesthe burden on security analyst teams by automating the combing process through telemetry data to find critical insights. A massive amount of data can be analysed with AI to create context and relationships, which is quite impossible for a human analyst.
Besides, ML and AI can also be used to do a risk assessment of an organisation's security posture. By going through vast amounts of disparate data, organisations can identify their most critical areas of risk and prioritise resources accordingly.
ML models learn from the telemetry and correlate different events that are seemingly unrelated, but if put together with enough context, sstheycan identify a critical incident that would likely go unnoticed by an individual.
To get the best out of AI and ML, massive amounts of unbiased data is needed. The recommended way to get this is by working with a partner organisation that has global telemetry monitoring and analytics of cloud security incidents, and proven track record in ML and AI. Doing so ensures that no malicious events or agents evade our monitoring, and the organisation is safeguards against all potential risks.

6.5. Delegating work

With AI and ML technologies handling routine tasks and keeping the basic level of security in check, security teams are free to focus on critical, complex, or prioritised threats. Since cyber threats have both human and machine origin, human analysts cant be replaced by these technologies. Nevertheless, it provides room to prioritise the tasks and completing them more effectively.
The future is all about a symbiotic relationship between humans and machines or applications developed in the future[30]. With the advancement in technology, cloud computing is steadily becoming secure, more comfortable to handle, and scalable.

VII. CONCLUSION

This paper covers the security aspects of cloud computing and explores what the integration of AI and ML with cloud computing will give birth to. Organisations will have to invest in teams who can help build AI and ML operations around the cloud infrastructure from the design to the operation phase. This next generation of cloud computing will come into realisation in the next few decades, as long as cloud computing continues to evolve.

VIII. REFERENCES

[1]J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.
[2] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.
[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.
[4] F. Zhang and H. Chen, "Security-Preserving Live Migration of Virtual Machines in the Cloud," J. Netw. Syst. Manag., pp. 562–587, 2012.
[5] J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.
[6] D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.
[7] Miranda &Siani, ―A Client-Based Privacy Manager for Cloud Computing‖, COMSWARE'09, 2009, Dublin, Ireland
[8] F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.
[9] Ion, I., Sachdeva, N., Kumaraguru, P., &Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM
[10] Lipinski, T. A. (2013, September). Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements. In International Symposium on Information Management in a Changing World (pp. 92-111). Springer Berlin Heidelberg.
[11] Wang, Y., Chandrasekhar, S., Singhal, M., & Ma, J. (2016). A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing. Cluster Computing,19(2), 647-662. doi:10.1007/s10586-016-0560-2
[12] Wang, L., Ranjan, R., Chen, J., &Benatallah, B. 2011.
[13] Shah, H. and Anandane, S.S., 2013. Security Issues on Cloud Computing. arXiv preprint arXiv:1308.5996.
[14] Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L.L., 2009, September. On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
[15] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.
[16] V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.
[17]F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.
[18] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.
[19] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software platforms," Comput. Secur., vol. 31, no. 1, pp. 96–108, 2012
[20]A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.
[21] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.
[22] Winkler, V. (. R.)., & Books24x7, I. (2011). Securing the cloud: Cloud computer security techniques and tactics. NL: Syngress Media Incorporated.
[23] Catteddu, D., &Hogben, G. (2009). Cloud computing risk assessment. European Network and Information Security Agency (ENISA), 583-592.
[24]H. Qian, J. He, Y. Zhou, and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," Math. Probl. Eng., vol. 2010, pp. 7– 9, 2010.
[25] P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348, 2015.
[26] Cloud Security Alliance Releases 'The | Cloud Security https://cloudsecurityalliance.org/press-releases/2016/02/29/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/
[27] Michael A, Armando F, Rean G, Anthony DJ, Randy HK, Andrew K, Gunho L, David AP, Ariel R, Ion S, Matei Z (2010) A view of cloud computing. Commun ACM 53(4):50–58
[28] TayseerTagElsir Ahmed Osman, Dr. Amin babiker A/Nabi Mustafa, "Internal & External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 93-96

[29] Top 7 Benefits of Using AI in Cloud Computing - Whizlabs Blog. https://www.whizlabs.com/blog/benefits-of-ai-in-cloud-computing/

[30] Importance Of AI And ML In Cloud Security | Global Tech ....https://www.globaltechcouncil.org/artificial-intelligence/importance-of-artificial-intelligence-and-machine-learning-in-cloud-security/

[31] Halverson, Grace. "Benefits of AI and Machine Learning for Cloud Security." IT Pro , Dennis Publishing Ltd., Jan. 2019, p. n/a.

