

# An Analysis of Cloud Security

Tushar Parmanand Budhwani<sup>1</sup>, Potlapally Tejaswini<sup>2</sup>, Ayanesh Chowdhury<sup>3</sup>, Durga Bhagavan Bolli<sup>4</sup>, Mohammed Khaja Fahad Uddin<sup>5</sup>, Hari Hara Chaitanya Kurapati<sup>6</sup>

\*\*\*

**Abstract** - Cloud computing is used by a number of organizations for storing a large quantity of records on the clouds. Therefore, there can be need to protect the data which may additionally furthermore in the shape of text, audio, video, and lots of others. There are several algorithms designed with the aid of using the way of the researchers for securing the facts on the cloud. The present paper via using is a try to point out some of the crucial algorithms for the safety of statistics for this cause, exhaustive literature has been executed.

**Key Words:** Cloud Security, Genetic Algorithm, Data Encryption, Intrusion Detection System, Security Techniques.

## 1. Introduction

The term "Cloud computing" has defined through National Institute of Standards and Technology (NIST) is complete and developing era inside the everyday existence for each one that gives call for internet offerings like networks, storage, servers and programs with flexibility and cost efficient performance for customers. Cloud computing is a generation that boom or lessen the storage functionality as peruse without funding in new infrastructure. The method of cloud storage includes 4 layers newly storage layer that save facts on cloud records middle, control layer which ensures privateness and safety of cloud storage, application interface layer that provide cloud application provider platform, and in the end cloud get right of entry to layer which offer accessibility to the cloud man or woman. The cloud fashions are classified with distinct offerings like Infrastructure as a Service (IaaS): is most usual and advanced marketplace segments of cloud that deliver customized infrastructure on name for, Platform as a Service (PaaS): that gives platform and surroundings to the developers that construct cloud offerings and application on the web and that services are saved inside the cloud and accessed by using cloud customers the use of web browser, Software as a Service (SaaS): that gives its own software program going for walks on a cloud infrastructure. The cloud patron need no longer manage or manipulate the cloud infrastructure along with storage, working system, services, network and application. It moreover reduces the want of pc systems, server, storage and control and run all application. In cloud computing facts are growing exponentially but safety of statistics is still questionable. Due to the transfer of statistics to the cloud facts center, the safety trouble takes place and information proprietor loss their manipulate on information. Security and privacy for cloud records is a first rate element of cloud computing this is though now not solved. These cloud safety

worrying conditions consist of unauthorized access, records leakage and person's sensitive facts leaks.

## 2. Literature Review

Firstly considering the In the twelve months 2011, authors provided a bit related to cloud computing offerings like networks, storage, servers, services and applications with out physically receipt them. As in line with observation in the paper it's far observed that overhead of the large machine has been decreased of danger, statistics leakage and so on [1]. Cloud computing provide on- call for internet offerings. If a corporation supplying internet offerings need to make investments massive capital cash for infrastructure and issues like system failure, disk failure and software bugs and many others. Because of this cloud is great solution for folks that does no longer want to setup infrastructure in personal device. [2] According to this paper cloud person no want to make investments cash on infrastructure and pay as in keeping with offerings use.

In the one year 2012, authors discussed approximately cloud security that facts developing exponentially however safety of an open- ended and rather easily on hand property continues to be questionable and investigates risks of safety from cloud computing surroundings, traits, cloud transport version and the cloud stakeholder [4]. The authors short discussed about cloud protection. In in recent times increasingly more human beings are the use of clouds which have sensitive information and ship, reap and save in community in order that cloud community protection has end up most important troubles [5] in above artwork creator communicate some Violation of private facts, man-in-middle assault, information corruption are risk problems that impact cloud protection. Cloud is one of the most technological research location because of its flexibility and price performance and transformation of data among patron and server. [6] this paper elaborates to make certain the strong statistics safety is managed with the assist of recognition control gadget additionally hold the transaction desk that contains the facts. In cloud, virtualization is important for cloud computing however the safety for virtualization isn't properly studied [7]. This paper assessment of cloud protection makes a speciality of how virtualization assaults influences excellent cloud computing issuer model. The cloud computing offers platform for sharing of property that contains software program and infrastructure with the help of virtualization [8]. Which discuss cloud surroundings makes try to be flexible and dependable to offer offerings. Cloud protection provides a few sort of protection pattern which cloud provider company cloud comply and uses RSA set of regulations with Digital

Signature is used to encrypt cloud information While records are transferred in network [9] is defined the safety control fashions and protection necessities and RSA set of regulations with Digital Signature to boom cloud facts safety in cloud.

Firstly considering In the twelve months 2011, authors provided a bit related to cloud computing offerings like networks, storage, servers, services, and applications without physically receipt them. As in line with observation in the paper, it's far observed that overhead of the large machine has been decreased of danger, statistics leakage and so on [1]. Cloud computing provides on-call internet offerings. If a corporation supplying internet offerings need to make investments massive capital cash for infrastructure and issues like system failure, disk failure and software bugs and many others. Because of this cloud is great solution for folks that does no longer want to setup infrastructure in personal device. [2] According to this paper cloud person no want to make investments cash on infrastructure and pay as in keeping with offerings use.

In the one year 2012, authors discussed approximately cloud security that facts developing exponentially however safety of an open- ended and rather easily on hand property continues to be questionable and investigates risks of safety from cloud computing surroundings, traits, cloud transport version and the cloud stakeholder [4]. The authors short discussed about cloud protection. In in recent times increasingly more human beings are the use of clouds which have sensitive information and ship, reap and save in community in order that cloud community protection has end up most important troubles [5] in above art work creator communicate some Violation of private facts, man-in-middle assault, information corruption are risk problems that impact cloud protection. Cloud is one of the most technological research location because of its flexibility and price performance and transformation of data among patron and server. [6] this paper elaborates to make certain the strong statistics safety is managed with the assist of recognition control gadget additionally hold the transaction desk that contains the facts. In cloud, virtualization is important for cloud computing however the safety for virtualization isn't properly studied [7]. This paper assessment of cloud protection makes a speciality of how virtualization assaults influences excellent cloud computing issuer model. The cloud computing offers platform for sharing of property that contains software program and infrastructure with the help of virtualization [8]. Which discuss cloud surroundings makes try to be flexible and dependable to offer offerings. Cloud protection provides a few sort of protection pattern which cloud provider company cloud comply and uses RSA set of regulations with Digital Signature is used to encrypt cloud information While records are transferred in network [9] is defined the safety control fashions and protection necessities and RSA set of regulations with Digital Signature to boom cloud facts safety in cloud.

In the 12 months 2013, it is determined that multi-clouds providers to govern safety has secured an awful lot less attention from the studies network than the use of unmarried cloud provider [10] the principle interest of this paper is locate of multi-clouds, lessen safety dangers and facts safety. Cloud consumer"s motives loss of control from the proprietor"s aspect due to moving data outward from organizational obstacles and get admission to them via internet. [11] provides quick description approximately records securing and preserve a degree of consider amongst information proprietors is become an essential issues for cloud carriers. The nasty human beings have 2nd option to purpose harm to human beings"s touchy facts by means of doing cyber attacks in desire to bodily attacks and to save you the cyber attacks wishes time and sake of securing business, non-public records and nation [12]. In this paper noted assuring cloud records protection, data mining and algorithms contribute specially.

In the year 2014, the maximum critical strategies in our existence is Internet of Things (IoT) and cloud computing. Their leased and use is expected to increase further, because of this cause will become maximum required component on net

[13] offer interest on integration of IoT and cloud computing, which is added as CloudIoT. Cloud offers virtual pool of sources to the cloud customers as carrier thru an internet interface and Cloud sources include infrastructure, community, platform, software program software, storage and most of the corporation are migrating their facts over the cloud, it's far important to ensure safety and integrity of cloud person"s statistics [14] has speak the safety dangers posed to statistics at the cloud computing. The rapid increment within the vicinity of cloud computing also will increase server security problems and it's far difficult to song the security threats and one of the most right threats comes in the Diversity of a Denial-of- Service(DOS) and its larger element is Distributed Denial-of- Service(DDOS) assault those are the splendid sorts of network intrusion in cloud computing surroundings [15] are presenting a manner which might be able to clean out and hit upon essentially attacked web page traffic inside a very a lot less term.

In the 12 months 2015, determined that Distributed Denial of Service Attack is one of the important troubles, it's miles a sort of assault where a group of intruder start attacking in a single goal that allow to keep away from from services for the consumer of the focused device [16] defined the various Distributed Denial of offerings assault detection and prevention strategies. Investigation of cloud safety is more tough instead of investigating virtual forensic, many demanding conditions are confronted by way of using investigator in forensic research, to extract evidences from the cloud forensic investigations may additionally end up complex [17] creator provided the complexity of cloud and a manner to impacts digital investigations. Cloud is a shape of

dispensed computing wherein assets and application are shared over the internet and cloud client can pay on utilization basis [18] the purpose of this paper is to speak about several unsolved safety risks that affecting the cloud computing and moreover speak the benefits and downsides of present cloud security plans and additionally introduced cloud safety issues which includes records segregation, safety and records integrity.

In the 12 months 2016, determined that Internet of things (IoT) defines the entirety, which are connected to Internet with functionality to exchange information over community however the layout and configuration of technology improperly will brought about to safety threats [19] defined the security threats of Internet of things (IoT) after which proposed the protection framework to lessen the safety threats. Cloud computing is dynamic generation, that offers the transformation of information and avoid the weight of nearby storage of cloud users [20] proposed a manner to enhance the safety elements by way of the use of stenography and cryptographic strategies. Security-as-a-Service(SaaS) model affords protection in cloud environment and client can without issues use those services using net browser and set of rules is canny in a way the Encryption into multiple encryption [21] In this paper author worked in encryption and decryption in cloud issuer in highbrow and transpicuous manner.

In the year 2017, authors mentioned about cloud computing platform is implemented and designed to use net applications and proportion by means of net such sort of technology built using OpenStack framework, open to multimodal enhancements and exploiting fingerprints is an precise biometric technique for user authentication, the platform offer comfy get right of entry to for more than one customers ensures and offer complete logical dissociation of information resources and computation related to particular enterprise [25] defined topics related to cloud protection, the safety of data storage on public cloud servers and authentication of logical user having access to the cloud. In cloud, multi-cloud storage is one of the important problem. This is used to save and get entry to cloud statistics remotely, and storage are capable of encrypting and hold records in awesome cloud drives [26] proposed model, that offer answer for one-of-a-type insider's assault, privateness for one-of-a-kind documents uploaded through brilliant customers, and decentralized distribution of statistics storage the use of an index based cryptographic information.

In the year 2018, the cloud safety grow to be largest concern for cloud researchers because of unauthorized sports are growing on in keeping with cloud customers [27] proposed new safety architecture for cloud framework that offer greater facts transformation and defends information from data leakage. Data owners and cloud servers have different identities, this framework offer records storage and feature

unique safety troubles, an unbiased technique required to make sure that cloud information is hosted efficiently within the cloud server [28] mentioned one-of-a-kind safety strategies for secure information stored on the cloud. Cloud computing makes use of "Utility Computing" and "Software-as-a-Service" to provide the required provider with the resource of cloud character, cloud protection is a notable and important fact, has several problems and trouble associated it [29] Described the list of parameters which is probably affected the protection and discover protection troubles and troubles are faced via the usage of cloud service provider and purchasers like records privacy, protection issues and infected application.

### 3. METHODS FOR SECURING ROUGH DATA SET

#### A. Genetic Algorithm

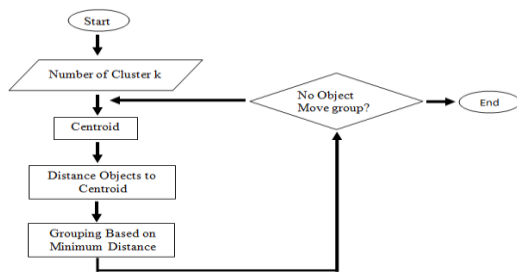
Genetic Algorithm (GA) is a looking method this is used to discover approximate or specific solution to optimization and seek problem [30] GA convert great domain hassle to a model through the use of chromosome and the set of rules manner begins off evolved with a random choice of the populace of chromosomes. Chromosomes are converted into bits or numbers consistent with the hassle [23]. Natural and successive guidelines are advanced thru Genetic Algorithm that suggestions are used for community site visitors that differentiate amongst everyday or splendid web site visitors.

Pseudo code of Genetic Algorithm

- Select initial populations
- Repeat
  - Find out the person health of a tremendous percent consistent with the population
  - Choose the excellent rating human beings pair to reproduce
  - Use crossover and mutation operator
  - Repeat the device until the termination condition came about

#### 4. K-Mean Algorithm

K-propose is an appropriate set of guidelines of partitioning approach for clustering evaluation. The purpose of this set of rules is to reduce an goal function referred to as square mistakes feature.



Where  $k_i$  shows the number of data points in  $i$ th cluster

- Find new cluster center by using re-computation of distance between all data points

Bayes' Theorem

$$P(m/n) = \frac{P(m)P(n/m)}{\sum_{n=1}^m P(m/n)}$$

$$P(\bar{m}) = \prod_{i=1}^m P(M_i/n) | P(n)$$

$P(\frac{m}{n})$  is the posterior probability

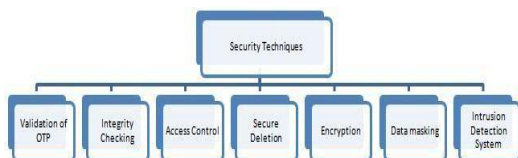
$P(n)$  is prior probability

$P(\frac{m}{n})$  is likelihood which is probability of predictor

$P(m)$  is the prior probability of predictor

### 5. Security Techniques for Securing Cloud

Cloud records encryption is not the solution for statistics that would keep religion over cloud safety. It may be made thru utilizing gift security strategies like Authentication and identification, encryption, integrity checking, get entry to manipulate, cozy detection, and facts covering are all of the protection strategies are applicable to cloud facts. Figure 2 explains safety strategies.



### A. Validation of OTP

In the cutting-edge scenario, a lot of banks are providing authentication via One Time Password (OTP) approach that is generated thru random beneath technology and used to verify the cloud person someday it is used for one time authentication called as device aspect authentication that is verified in figure three. While sometime it's miles used for 2 time authentication referred to as as Multiple Authentication Factor.

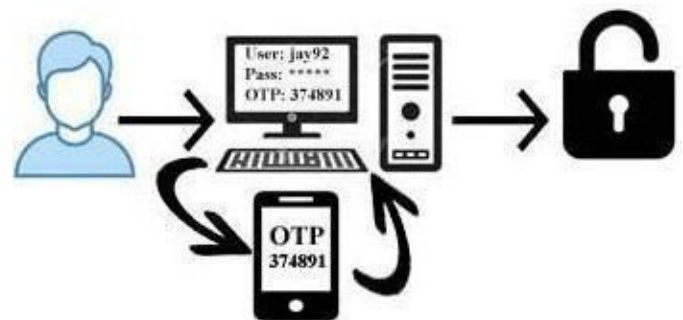


Figure 3 OTP Authentication

### B. Integrity Checking

The integrity of cloud information is a guarantee that cloud records can only be modified or accessed by way of an authorized user. In easy phrases, it is a cloud-primarily based absolutely facts verification device guarantees that the information is unmodified, correct and the fundamental techniques of data integrity are Provable Data Possession (PDP) is a way to make sure the integrity of cloud information on a miles off server and the approach Proof Of Retrievability (POR) to attain and affirm the proof that cloud statistics is stored thru the individual on the server is not changed [24].

### C. Access Control

Access manipulate manner cloud facts owner can execute some restrictive permission to get proper of access to their facts outsource to cloud and records proprietor's felony patron can get admission to cloud facts at the equal time as unauthorized customer can't due to access manipulate cloud statistics are included from amendment or unauthorized disclosure of records.

### D. Secure Deletion

It is crucial to apprehend how the information is deleted from the server. Deletion uses outstanding techniques like Clearing, on this approach we delete the media before the reuse of those media and on the identical time offer safety for accepting the statistics that contained in the media earlier than deleted. Sanitization, proper here the safety for accepting preceding statistics isn't always furnished and this shape of records is often circulated for lower degree of kind [32].

### E. Encryption

Cloud safety presents statistics encryption provider to encrypt cloud records earlier than switch from nearby storage to cloud storage and it's miles no longer viable to recognize from any machine, database or report to decrypt records with out decryption key and encrypted statistics is high-quality possible to access with a certified purchaser with the decryption key and separation of encrypted records and encryption key's crucial for maintaining cloud records at ease. Figure 4 explains encryption and decryption system given below.

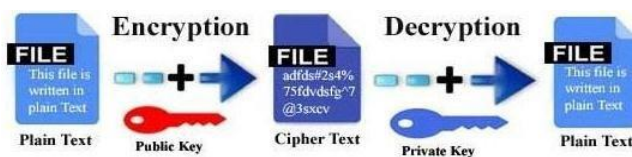


Figure 4 Data Encryption and Decryption

### F. Data Masking

Data protecting is a way of securing and hiding cloud facts from attackers and robbery and it moreover insure that the records is changed with realistic but no longer real records. While people interchangeably use phrases together with records de-popularity, statistics cleansing and statistics the time period defining the hard machine. Data overlaying is not most effective set of rules however moreover a public information set. There are superb methods or strategies are used to mask cloud facts, Static Data Masking (SDM) is used by most organizations when growing checks and this is definitely the only method of protecting viable even as the usage of outsourced builders in a separate site or enterprise. In those cases, it is critical to duplicate the database. Dynamic Data Masking (DDM) provide get right of entry to primarily based on their role within the corporation [3].

### G. Intrusion Detection System

Intrusion Detection System (IDS) defines as a software program program applications or gadgets that hold eyes on device sports or community site visitors and locate if any illegal sports befall. In the modern-day technology, maximum of the hackers use distinct attacking strategies for locating customers touchy records. An intrusion suggests any unlawful get admission to or evil sports for IT resources. The intruders try to find unauthorized get admission to in touchy facts, reasons harmful sports activities. The forms of Intrusion Detection System are defined, Network- Based Intrusion Detection System (NIDS) that observed in a devices or computer connected section of an corporation's community and monitor network website site visitors and hold eyes on ongoing assaults, Host-Based Intrusion

Detection System (HIDS) is hooked up on unique system or server and display unlawful activities on that device.

### 6. CONCLUSION

In the above presentation, it's far positioned that there is a large scope for the technology of new safety algorithms for securing the statistics set. The importance of every method has been provided in quick however, the ones can be implemented for securing the cloud records within the above in which exhaustive literature has been consulted and explained in quick.

### REFERENCES

1. R. Choubey, R. Dubey, and J. Bhattacharjee, "A survey on cloud computing security, challenges and threats," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 3, pp. 1227-1231, 2011.
2. R. P. Padhy, M. R. Patra, and S. C. Satapathy, "X-as-a-Service: Cloud Computing with Google App Engine, Amazon Web Services, Microsoft Azure and Force.com," *Int. J. Comput. Sci. Telecommun.*, vol. 2, no. 9, pp. 8-16, 2011.
3. G.K. Ravikumar "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", *International journal of engineering science and Technology*, vol. 3, no. 6, pp. 5150-5159, 2011.
4. A. Behl, K. Behl, "An Analysis of Cloud Computing security issues," *2012 World Congr. Inf. Commun. Technol.*, pp. 109- 114, 2012.
5. D Chopra, D Khurana, K Govinda, "CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTION," *International Journal of Advances in Engineering Research*, vol. 3, no. 2, 2012.
6. G. R. Vijay, "An Efficient Security Model in Cloud Computing based on Soft computing Techniques," vol. 60, no. 14, pp. 18-23, 2012.
7. H. Tsai, N. Chiao, R. Steinmetz, and T. U. Darmstadt, "Threat as a Service?: Virtualization's Impact on Cloud Security," no. February, pp. 32-37, 2012.
8. K. Kumar, V. Rao, S. Rao, and G.S. Rao, "Cloud Computing : An Analysis of Its Challenges & Security Issues," *IJCSN*, vol. 1, no. 5, 2012.
9. K. D. Kadam, S. K. Gajre, and R. L. Paikrao, "Security Issues in Cloud Computing," *Proceedings published by International Journal of Computer Applications*, pp. 22-26, 2012.

10. M. Shrawankar, A. Kr. Shrivastava "Comparative Study of Security Mechanisms in Multi- cloud Environment," vol. 77, no. 6, pp. 9-13, 2013.
11. N. Aggarwal, P. Tyagi, B. P. Dubey, and E. S. Pilli, "Cloud Computing: Data Storage Security Analysis and its Challenges," vol. 70, no. 24, pp. 33-37, 2013.
12. P. Aggarwal, M. M. Chaturvedi, "Application of Data Mining Techniques for Information Security in a Cloud: A Survey," Int. J. Comput. Appl., vol. 80, no. 13, pp. 11-17, 2013.
13. A. Botta, W. De Donato, V. Persico, and A. Pescapé, "On the integration of cloud computing and internet of things," Proc. - 2014 Int. Conf. Futur. Internet Things Cloud, FiCloud 2014, pp. 23-30, 2014.
14. D. Panth, D. Mehta, R. Shelgaonkar "A Survey on Security Mechanisms of Leading Cloud Service Providers," Int. J. Comput. Appl. , vol. 98, no. 1, pp. 24-34, 2014.
15. D. Porwal, P. Mohmood Khan and D. Shankar Ray, "Cloud Computing Security Threats and Countermeasures", International journal for innovations in Engineering Science and Management, vol. 2, no. 4, pp. 1-4, 2014.
16. D. Parwani, A. Dutta, P. Kumar Shulka, and M. Tahilyani, "Various Techniques of DDoS Attacks Detection and Prevention at Cloud: A Survey," Orient. J. Comput. Sci. Technol., vol. 8, no. 2, pp. 110-120, 2015.
17. G. Al, "Cloud Computing Architecture and Forensic Investigation Challenges," Int. J. Comput. Appl., vol. 124, no. 7, pp. 20-25, 2015.
18. M. U. Shankarwar and A. V. Pawar, "Security and Privacy in Cloud Computing: A Survey," Adv. Intell. Syst. Comput., vol. 328, pp. 1-11, 2015.
19. A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework," Proc. Int. Conf. Internet things Cloud Comput. - ICC '16, pp. 1-5, 2016.
20. B. Pathankot, "Review Paper on Enhancing Data Security for Cloud Environment Cryptography and Steganography," International Journal of Engineering Applied Sciences and Technology, vol. 2, no. 1, pp. 44-48, 2016.
21. D. H. Sharma, C. A. Dhote, and M. M. Potey, "Intelligent Transparent Encryption-Decryption as Security-as-a-Service from clouds," 2016 Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut. CSITSS 2016, pp. 359-362, 2016.
22. B. Mahesh, "Data Security and security controls in cloud computing", International journal of advances in Electronics and Computer Sciecnce, pp. 11-13, 2016.
23. T. Singh, S. Verma, V. Kulshrestha and S. Katiyar, "intrusion Detection System Using Genetic Algorithm for Cloud", International journal of Advances in Electronics and Computer Science, pp. 1-6, 2016
24. S. Sharma, "Data Integrity Challenges in Cloud Computing", 4th international conference on recent innovations in science engineering and management, pp. 736-7436, 2016.
25. G. L. Masala, P. Ruiu, E. Grosso, "Biometric Authentication and Data Security in Cloud Computing," Comput. Netw. Secur. Essentials, pp. 337-353, 2017.
26. K. Subramanian and F. L. John, "Secure and Reliable Unstructured Data Sharing in Multi-Cloud Storage using the Hybrid Crypto System," IJCSNS, vol. 17, no. 6, pp. 196-206, 2017.
27. A. Hussain, C. Xu, and M. Ali, "Security of Cloud Storage System using Various Cryptographic Techniques," International Journal of Mathematics Trends and Technology ( IJMTT ), vol. 60, no. 1, pp. 45-51, 2018.
28. A. Venkatesh and M. S. Eastaff, "A Study of Data Storage Security Issues in Cloud Computing," IJSRCSEIT, vol. 3, no. 1, pp. 1741-1745, 2018.
29. G. Jain and A. Jaiswal, "Security Issues and their Solution in Cloud Computing", Concepts journal of applied research(CJAR), vol. 02,no. 03, pp. 1-6, 2018.
30. Y. Guo and B.Wang et.al., "Feature Selection Based on Rough Set and Modified Genetic Algorithm for intrusion Detection" , The 5th International conference on Computer science & Education Hefei, China, pp. 1441-1446, 2018.
31. Data clustering algorithms[online] <https://sites.google.com/site/dataclusteringalgorithms/k-means-clustering-algorithm> (Accessed 08 March 2019).

32. CloudCodes[online]  
<https://www.cloudcodes.com/blog/data-protection-controls-techniques.html> (Accessed 20 December 2019).
33. DIGITAL GUARDIAN [online]  
<https://digitalguardian.com/blog/what-cloud-encryption> (Accessed 25 December 2019).