May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

Cloud Data Security Management System using Hyperelliptic Curve Cryptography

[1]Devi. T, [2]Ganesan.R

[1]Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai
[2]Professor, Vellore Institute of Technology, Chennai
[1]devi.janu@gmail.com, [2]ganesan.r@vit.ac.in

Article Info
Volume 83
Page Number: 3288-3294
Publication Issue:
May - June 2020

Abstract
Amazon S3 is utilized by different affiliations and it has gotten a gigantic bit of the certifiable market today. The green, or eco-obliging, some part of the cloud is one of the most multifaceted focal reasons for scattered preparing. The typical positive states of cloud S3 associations include: decreasing an association's carbon impression, server farm productivity, dematerialization, sparing green, evoked power use, etc. Certainly, even with its extraordinary new development, the subject of security is comparatively of central worry among the clients of cloud associations. There is a colossal energy for new shows and instruments so as to refresh and audit the security idea of its association. Notwithstanding the current frameworks utilized for scrambling the records in cloud they are not fundamentally useful. Appropriately this refreshed technique is proposed to vanquish these difficulties and improve the ordinary focal points. In this strategy, from the start the certification of the client is checked. Right when the insistence of the client is checked effectively twofold encryption is performed on the cloud put aside records utilizing ElGamal cryptosystem and Hyper Elliptical Curve Cryptography (HECC). The target utilizing the proposed framework is for evaluation of security which can be refreshed through the technique of sharing different keys among the two get-togethers. Number choice is an enormous quality which depicts the best security to the appropriated accumulating. For guaranteeing high security, this whole number confirmation is performed by using BAT figuring. After the encryption, the proposed technique utilizes the HECC calculation. In HECC, key age is finished by point advancement and point copying based elliptic bend cryptography. The twofold encryption in this system gives suitable security to the cloud information. The proposed approach execution is reviewed in reference with ecological security, gathering cost, figuring cost and execution time and is acknowledged in JAVA. The fundamental results show the reasonableness of the structure as it uses just less time for both encryption and unscrambling of delicate information.

Article History
Article Received: *19 August 2019*
Revised: *27 November 2019*
Accepted: *29 January 2020*
Publication: *12 May 2020*

Keywords: *HECC; BAT; S3; point addition; point doubling*

1. Introduction

Flowed figuring advanced through the scattered programming structures versatility and extensibility. As indicated by the National Institute of Standards and Technology (NIST) definition, "the appropriated handling is a model for empowering steady, asset pooling, certain, on-request get to which can be effectively delivered. It is changing approaches to manage equipment and programming plan and acquisitions works out.

May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

Associations without cost, adaptability of advantages, availability through web, and so forth are a portion of the positive conditions that cloud progression offers. With the aggregate of the persistent buzz about flowed figuring, affiliations have discovered that by changing to an open cloud, they can get adaptability and flexibility while simultaneously decreasing expenses. Regardless, what they may not fathom is that the cloud benefits their working environment, yet besides, nature. Controlling and dealing with information on a near to server enormously builds carbon outpourings. In every way that really matters all undertakings (huge or little) are pointing towards refreshing affiliations and tie-ups with different undertakings using cloud headway SaaS, PaaS, Iaas and Private, Public, and Hybrid are the association and sending models autonomously. One of the key reasons why it faces progressively essential security issues is an immediate consequence of high accessibility to end clients. Along these lines, security issues from cloud supplier sendand security issues from Customers end are the two sorts of security related issues. Riddle of information consolidates information security of just critical and embraced access of information that are delicate. Information conventionality contains information content which can be developed especially through consistency and exactness. Imbecile affirmation putting away, kind of cutoff, plans for fiasco recuperation and backing are ensured about under information receptiveness.

As such, affiliations that execute Cloud Computing and Big Data are faced with basic issues of security, trust, confirmation and natural issues. While affiliations are planning to accomplish both expense and operational efficiencies through cloud, it is essential to endorse the structure plan and sending dependent on current security rehearse. Hence the centrality of security weights on the unexpected turn of events and maltreatment of data frameworks has grown persistently. Today, the very truth that data Systems are utilized wherever have made them logically weak against data security assaults. Evidently this sort of trap would accomplish huge loss of cash, time and various significant assets. With an expect to manage such security challenges, the European Network and Information Security Agency made a graph. Additionally, loss of association and consistence dangers was among the two key hazards to such inadequacy. Information security can be guaranteed through clients handle techniques, for example, control of access, the directors of key, encryption, and unscrambling. Before re-appropriating to the cloud, delicate information should be blended for the security of clients.

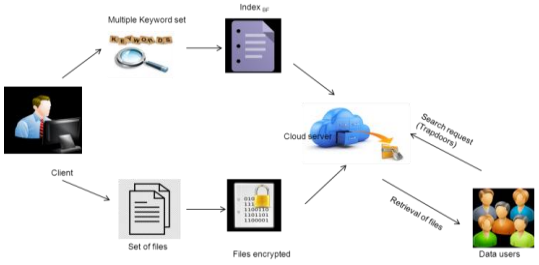

Figure 1: System Architecture

Atmosphere impact is marvelously diminished by the mists improvement in vitality proficiency because of less carbon outpourings. Concurring to AWS, "the common corporate server farm has a dirtier force blend than the typical colossal degree cloud supplier." AWS, in mix in with other cloud suppliers, utilize a 28% less carbon-unbelievable force blend. This in addition impacts atmosphere control costs, since it is astonishingly progressively excessive to run machines at top execution levels in perfect temperature levels. The cloud gets out this inefficient spending because of the use of noteworthiness fruitful hardware and less carbon outpourings. For information activities and transmissions, security attempts must be grown in any case information are viewed as at high hazard. Openness of put aside information is given up for a get-together of clients and along these lines validity of having high information risk is more. Before running Map Reduce tries, the Hadoop security makes it mandatory for a client to sign on to each social event. This system is doubtlessly not obliging for the clients. Along these lines, an ordinary approach is especially basic for disguising the central purposes of the framework's structure and also not to bother the clients with such dull undertakings. Therefore, programming security organizing should be a promising help which with willing satisfy such necessities. It means to give security attempts, for example, procedures and mechanical congregations, structure, evaluation of shortcoming, testing and estimations. Despite the as of late referenced focuses, the cloud star networks (CSP) prosperity attempts are consistently clear to the affiliations. The event of colossal measures of clients that are not identified with the affiliations further decays the worry. At last, a trust model including trust respect is proposed by experts so as to draw in estimation of the idea of cloud association security. A record of parameters covering every single sensible part of security helps in the assessment of trust respect. Hence security is given to the informational index aside in cloud.

2. Related Works

In this past work Numerous investigates have been done in the field of ensuring data security to cloud system. A bit of the consistent looks at in the individual district are sketched out around there which are discussed as follows

May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

ElGamal cryptosystem has monstrous condition in form security and it has wide application. Isolated and RSA computation, elliptic twist encryption figuring has essential inclinations, and it is sensible for application in the earth with obliged resources. Wang and Sun have proposed ElGamal cryptosystem subject to elliptic bend. The two plans are pondered in security and estimation execution. Regardless of to some degree more check, the strategy could improve the security and develop the application field of ElGamal reliant on elliptic breeze cryptosystem. Secure and persuading data putting away was required in the cloud condition in current time of information progression industry. The cloud ensures the authenticity of the cloud relationship without the data on customer's character. The cloud gives titanic data get to really through the web. Joined limit instrument was followed here for sensible getting to of data. Cloud pro centers are generally guarantees about the thing and hardware resources and the cloud buyers are advantage the relationship through the web access in lease premise. Cloud security was improved through cryptography framework applied to the cloud security to keep up a key good ways from vulnerability. The unmanageable calculability was bored in the cloud by using the open key cryptosystem. Selvi and Ganesan [12] have proposed the arrangement of applying hyper elliptic reshape cryptography for data affirmation in the cloud with the little key size. The proposed structure has the further favored condition of taking out intruder in passed on dealing with. Sensibility of the structure was to give the high security of the cloud data.

Flowed enlisting was a latest computational structure which could be used for enormous data masterminding. Goliath degree of unstructured, filtered through and semi made data could be called as huge data. Guide Reduce and the Hadoop urge a sensible instrument to regulate and process data from different sources and store the colossal data in dispersed cloud. Jose and glimmer [13] have explained the ensured about and cost constraining approach to manage supervise move and store amazingly titanic degree of data to cloud. Hyper elliptic cryptography thought about offer encryption to the gigantic degree of data appearing at the cloud. Notwithstanding cryptography, data download module was merged.

Spread planning was a figuring model which gives general, solid, on-demand mastermind access to a shared pool of configurable selecting resources that could be expeditiously provisioned and released with in every way that really matters no prospective IT system encounters costs. Passed on dealing with moves the application and data to the dispersed putting away where the relationship of the data and affiliations clearly won't be completely solid. In this way, there was a requirement for cloud expert concentrations to give a decent level of legitimacy for the client's data. Samson and Kayode [14] have proposed a data security plot using Signcryption and hyper elliptic bends as a singular reasonable new development. Signcryption plans subject to hyperelliptic turns saves effectively computational time and correspondence cost.

Passed on figuring was clearly one of the most essential advances in information improvement (IT) benefits today. A few cloud expert affiliations (CSPs) have offered affiliations that have turned out different transformative enhancements in dealing with rehearses and presented assorted promising creative and budgetary possibilities. In any case, many cloud customers remain reluctant to move their IT needs to the cloud, all around considering their inclinations on cloud security and the danger of the darken. Pichan and Soh [15] have intentionally researched the intelligent troubles in dissipated getting ready and take a gander at their most recent plans and developments. In particular, instead of the present diagrams with respect to the issue, they have delineated the issues in spread enrolling using the long periods of standard modernized awful conduct scene evaluation as the base. For each period of the electronic genuine technique, they experience set an audit of challenges and assessment of their idle limit courses of action.

Dissipated enrolling makes as an arranging perspective that needs to give strong, fix up and nature of affiliation guaranteed count conditions for cloud customers. Applications and databases are moved to the enormous bound together server ranches, called cloud. Wei et al. [16] have proposed an assurance misdirecting disturbing and secure figuring assessing show, or SecCloud, which was a first show crossing secure cutoff and secure estimation looking at in cloud and achieving security misleading crippling by apportioned verifier signature, bundle check and probabilistic inquiring about methods. The point by point evaluation was given to make sure about a perfect studying size to confine the cost. Another essential commitment was that they develop a prudent secure-wary appropriated taking care of exploratory condition, or SecHDFS, as a demonstrating ground to recognize SecCloud. Further crucial outcomes have indicated the credibility and common sense of the proposed SecCloud.

3. Proposed Methodology

Conveyed registering is transforming into the most noteworthy spread handling perspective, a regularly expanding number of examiners and specialists are enthusiastic about it. The full resources of the structure must take an interest to respond to a client request which requires intercommunication between various fragments of the structure to design a section or subset of portions to deal with the sales which can provoke bottlenecks in the framework. With Cloud Computing rapidly getting pervasiveness, it is basic to highlight the consequent perils. As security and insurance issues are commonly huge, they should be would in general before Cloud Computing sets up a noteworthy bit of the general business.

TEST Engineering & Management

May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

A. ElGamal cryptosystem for scrambling messages

ElGamal cryptosystem gives the advantage of scrambling huge messages. This encryption system gives customers the decision of sending any kind of messages with increasingly ensured about access between the customers. The ElGamal cryptosystem fills in as follows,In ElGamal cryptosystem each customer picks their own riddle keys with the ultimate objective that,

$$k_i \in [1, N-2) \quad (1)$$

where,

N - Prime number

The related public key is then given by,

$$p_k = c^{k_i} \bmod N \quad (2)$$

where,

c - Primitive root or generator

For encrypting a large message using ElGamal cryptosystem, the sender computes the cipher text s and t as follows,

$$s = c^j \bmod N \quad (3)$$

$$t = M.p_k{}^j \bmod N \quad (4)$$

where,

$$j \in [1, N-2)$$

Now the receiver can decrypt the cipher s and t by computing,

$$M = t.(s^{k_i})^{-1} \bmod N \quad (5)$$

Based on the above process the ElGamal cryptosystem works and inorder to make the encryption process more secure we have utilized some modification in normal ElGamal process by incorporating optimization process. In our technique for the selection of the integer values in the process of encryption we have used Modified cuckoo search algorithm to optimize the selected values which will help in securing the message more. The process of optimization is explained in the below section

B. Optimization Using cuckoo search estimation

The Cuckoo search estimation addresses a naturally persuaded figuring .Its origin is owed to the duplicating conduct of the cuckoos and it is definitely not hard to execute. Each egg hints an answer and an egg of cuckoo identifies with a novel course of action. The story and dominating course of action is superseded by the most exceedingly terrible plan in the home. A short legitimization of arranged advances that are related with the changed cuckoo search figuring are given underneath

Stage 1: Initialization Phase

People (Pi, where i=1, 2, N) of host home is presented carelessly.

Stage 2: Generating New Cuckoo Phase

With the help of the obligation flights a cuckoo is picked discretionarily which produces novel courses of action. In this manner, the initiated cuckoo is evaluated by using the wellbeing work for discovering the enormity of plans.

Stage 3: Fitness Evaluation Phase

The health work is evaluated according to Equations 6 and 7 demonstrated hereunder, trailed by the assurance of the best one.

$$F_m = \frac{P_C}{p_N} \quad (6)$$

$$fitness = \max imum\ popularity = F_m \quad (7)$$

Where,

P_C - signifies the selected population

P_N - represents the total population

Step 4: Updation Phase

As a matter of first importance, the game plan is improved by the cost trips by using the cosine change. By evaluating the transcendence of the new plan a house is picked erratically among them. If the new game plan in the picked home is preferred and advanced over the past game plan, it is restored by the new game plan (Cuckoo). Something different, the past game plan is considered as the best course of action. The obligation flights used for the general cuckoo search count is imparted by the Equation 8 exhibited as follows

$$Lf_i^* = Lf_i^{(n+1)} = Lf_i^{(n)} + \alpha \oplus Lvy(N) \quad (8)$$

In changed cuckoo search, the above obligation flight condition is modified by joining the Gaussian limit with regards to updation which is given in eqn 9 underneath,

$$Lf_i^* = Lf_i^{(n+1)} = Lf_i^{(n)} + \alpha \oplus \eta_g \quad (9)$$

Where,

$$\eta_g = \eta_0 \exp(-\mu C) \quad (10)$$

η_0, μ - Constants

C - Current generation

Step 5: Reject Worst Nest Phase

Here, the most recognizably awful homes stay indistinctly, considering their opportunity characteristics thusly making new ones. Subsequently, the best courses of action are situated reliant on their wellbeing work. Starting there, the best courses of action are perceived and separate as perfect game plans.

Step 6: Stopping Criterion Phase

Considering the end guidelines, the above method is reiterated until the best course of action is reached. So by utilizing the above streamlining strategy the number for scrambling the messages using ElGamal cryptography is picked which helps in more prominent security of data.

May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

As referenced before we use twofold encryption process for ensuring about the message. Along these lines after the ElGamal encryption of message, we further perform Hyperelliptic twist cryptography for extra security.

C. Hyperelliptic curve cryptography

Before appropriated capacity the customer further encodes the message using the Hyperelliptic twist cryptography. The encoded message from the ElGamal cryptosystem is then presented to Hyperelliptic twist cryptography encryption process. The encryption technique in HECC is as follow,

Select a random prime number for the set N, i.e.)

$$h \in N \tag{11}$$

The coordinate C is given by,

$$C = hD \tag{12}$$

where,

D - Divisor of HEC

Now in our proposed system we have modified the HECC algorithm by including a auxiliary input which is regarded as a key for encrypting the message. The expression is given by,

$$C = \alpha[hD] \tag{13}$$

where,

α - Auxiliary input (additional key)

The key selection is made more effective by utilizing the optimization technique. Here we use GSA for selecting the key which is explained in the below section

A. Bloom Filter and False Random Bit Generator

A Bloom channel is a data structure planned to tell you, rapidly and memory-profitably, whether or not a segment is accessible in a set. In programming, possibly for the duration of regular daily existence, there are certain remarkable trade offs. You can generally trade space for time as the all the more amassing you can hurl at an issue the faster you can make it run. There is moreover a lesser realized trade off which is fundamentally progressively refined. When in doubt, you can trade sureness for time. This the reason of various sporadic computations where the course of action returned isn't sure anyway it is fast appeared differently in relation to a deterministic tally of a comparative sum. These are musings that entrance various designers who become completely devoured by the examination of estimations for the prosperity of their own, anyway they furthermore have practical application. Take for example the at present fervently discussed issue of the Bloom Filter. This may appear as though something an inventive picture taker may put before his point of convergence yet it is in actuality an enamoring figuring that mixes trading both space and sureness for time. A hash work is a limit that will take a thing of data and method it to make a value or key. For example, you could fundamentally incorporate the code regards for each character in a string and return the result mod some given worth. A hash work reliably conveys a comparative hash a motivation from comparable data yet it is possible and in assurance typical for two one of a kind data regards to make a comparative hash regard. That is the hash regard isn't stand-out to a given thing of data and you can't pivot the hashing ability to get the data regards. The hash work is a many-one deterministic limit. A tolerable hash work also has other alluring properties, for instance, spreading the hash regards got as similarly as possible over the yield go anyway for the second permits just spotlight on the key hash work. accept a data thing turns up and you have to know whether you have seen it beforehand. You ought to just apply the k hash limits and investigate the showed display segments. If any of them are zero you can be 100% sure that you have never encountered the thing - in case you had the bit would have been set to 1..

4. Simulation and Result Analysis

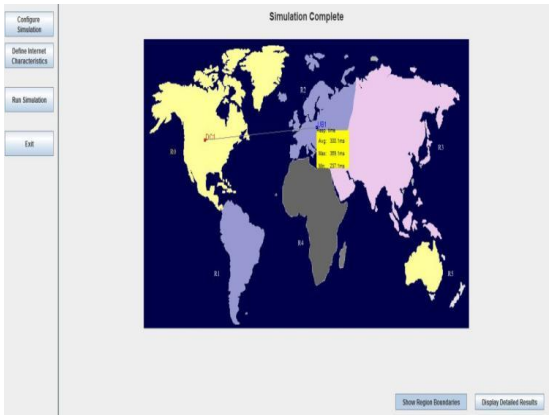

Figure 2: Cloud Simulation

Fig.2 shows the cloud simulation tool to provide Response time in user base and data center hourly base transferring a data from one region to another region.

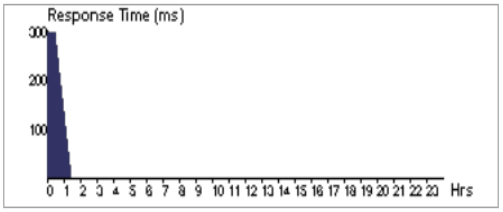

Figure 3: User Base Hourly Response Time

Fig.3 shows the Response time in user base hourly base transferring a data from one region to another region.

May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

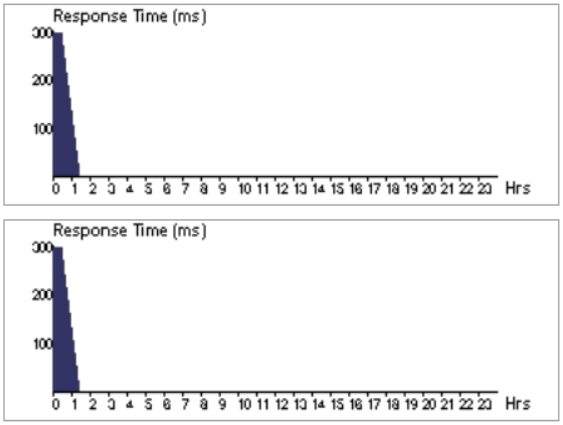

Figure 4: Response Time (ms)

Fig.4 shows the response time for every second in user base hourly base transferring a data from one region to another region.

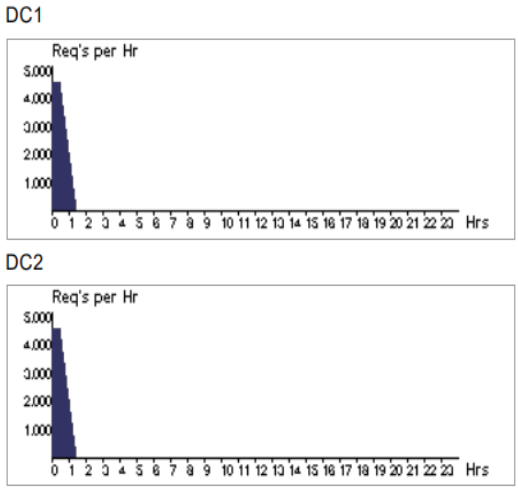

Figure 5: Data Center Hourly Loading

Fig.5 shows the hourly loading response for data center region based request per hour

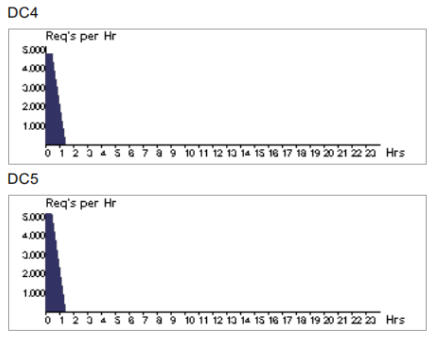

Figure 6: DC Request Per Hour

Fig.6 shows the packet drop ratio is low compared to the existing system thus the delivery rate also increases.

Overall Response Time Summary

	Avg (ms)	Min (ms)	Max (ms)
Overall response time:	300.41	232.64	375.13
Data Center processing time:	0.37	0.02	0.67

Figure 7: Overall Response Time Summary

Userbase	Avg (ms)	Min (ms)	Max (ms)
UB1	300.18	232.64	360.11
UB2	301.05	232.64	375.13
UB3	300.58	237.14	360.14
UB4	299.79	241.61	363.16

Figure 8: Response Time by Region

Data Center	Avg (ms)	Min (ms)	Max (ms)
DC1	0.33	0.02	0.62
DC2	0.38	0.02	0.67
DC3	0.38	0.03	0.66
DC4	0.37	0.02	0.64
DC5	0.36	0.02	0.64

Figure 9: Data Center Request Servicing Times

5. Discussion and Conclusion

The cloud offers huge amount of storage space to place all files both as public cloud and private cloud. When data is exposed to outside world, there are chances of attacking. A strong data security model incorporating effective cryptographic as well as optimization techniques is therefore necessary. Our proposed model also works in such a manner that the data is stored in safe manner. In future, our work can be extended by introducing a cache memory to store the recently used items. The usage of cache memory thus reduces the retrieval time thereby reducing the response time of system. This makes the data retrieval from cloud also easy.

References

[1] Khan, Nabeel and Adil Al-Yasiri "Identifying cloud security threats to strengthen cloud computing adoption framework", Procedia Computer Science, Vol.94, pp.485-490, 2016.

[2] Singh, Saurabh, Young-Sik Jeong and Jong Hyuk Park, "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications, Vol.75, pp.200-222, 2016.

[3] Rao and B. Thirumala, "A study on data storage security issues in cloud computing", Procedia Computer Science, Vol.92, pp.128-135, 2016.

[4] Manogaran, Gunasekaran, Chandu Thota and M. Vijay Kumar, "Meta Cloud Data Storage

May - June 2020
ISSN: 0193-4120 Page No. 3288-3294

architecture for Big Data security in cloud computing", Procedia Computer Science, Vol.87, pp. 128-133, 2016.

[5] Shaikh, Rizwana and M. Sasikumar, "Data classification for achieving security in cloud computing", Procedia computer science, Vol.45, pp.493-498, 2015.

[6] Chang, Victor, Yen-Hung Kuo and Muthu Ramachandran, "Cloud computing adoption framework: A security framework for business clouds", Future Generation Computer Systems, Vol.57, pp. 24-41, 2016.

[7] Jouini, Mouna and Latifa Ben Arfa Rabai, "Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems", Procedia Computer Science, Vol.83, pp. 1084-1089, 2016.

[8] Rasheed and Hassan, "Data and infrastructure security auditing in cloud computing environments", International Journal of Information Management, Vol.34, No.3, pp.364-368, 2014.

[9] Wei, Lifei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing", Information Sciences, Vol.258, pp.371-386, 2014.

[10] Krishna, B. Hari, S. Kiran, G. Murali and R. Pradeep Kumar Reddy, "Security Issues in Service Model of Cloud Computing Environment", Procedia Computer Science, Vol.87, pp. 246-251, 2016.

[11] Rao, R. Velumadhava and K. Selvamani, "Data security challenges and its solutions in cloud computing", Procedia Computer Science, Vol.48, pp.204-209, 2015.

[12] Zhao, Jiaqi, Lizhe Wang, Jie Tao, Jinjun Chen, Weiye Sun, Rajiv Ranjan, Joanna Kołodziej, Achim Streit and Dimitrios Georgakopoulos, "A security framework in GHadoop for big data computing across distributed Cloud data centres", Journal of Computer and System Sciences, Vol.80, No.5, pp.994-1007, 2014.

[13] Ramachandran and Muthu, "Software security requirements management as an emerging cloud computing service", International Journal of Information Management, Vol.36, No.4, pp. 580-590, 2016.

[14] Ali, Mazhar, Samee U. Khan and Athanasios V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Information Sciences, Vol.305, pp.357-383, 2015.

[15] Shaikh, Rizwana and M. Sasikumar, "Trust model for measuring security strength of cloud computing service", Procedia Computer Science, Vol.45, pp.380-389, 2015.

[16] Sookhak, Mehdi, Abdullah Gani, Muhammad Khurram Khan and Rajkumar Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing",

[17] Information Sciences, Vol.380, pp.101-116, 2016.
Li, Yibin, Keke Gai, Longfei Qiu, Meikang Qiu and Hui Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing", Information Sciences, pp.1-13, 2016.

[18] Zhang, Yinghui, Xiaofeng Chen, Jin Li, Duncan S. Wong, Hui Li and Ilsun You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing", Information Sciences, Vol.379, pp.42-61, 2016.

[19] Batista, Bruno Guazzelli, Carlos Henrique Gomes Ferreira, Danilo Costa Marim Segura, Dionisio Machado Leite Filho and Maycon Leone Maciel Peixoto, "A QoSdriven approach for cloud computing addressing attributes of performance and security", Future Generation Computer Systems, Vol.68, pp.260-274, 2016.

[20] Yang, Laurence T., Gaoyuan Huang, Jun Feng and Li Xu, "Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing", Information Sciences, pp.1-27, 2016.

[21] Singh, Anirudha Pratap and Syam Kumar Pasupuleti, "Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing", Procedia Computer Science, Vol.93, pp.751-759, 2016.