Secured data storage with users validation in cloud environment

Naveen Kumar Chunganahalli Gangadharaiah[1,*], Chandrasekar Chinnasamy[2]

1. Bharathiar University, Coimbatore, India

2. Govt. Arts College, Udumalpet, Tamilnadu, India

cgnaveenkumar11@gmail.com

ABSTRACT. *Cloud computing is the idea actualized to break up the Daily Computing Problems. Cloud computing is essentially virtual pool of resources and it gives these resources to clients through web interface. Cloud computing is the web based improvement and utilized as a part of PC innovation. The common issue related with Cloud computing is information protection, security, obscurity and unwavering quality and so forth. The paper proposed a new authentication method for validating cloud users. The Paper proposed a new technique for energy consumption reduction in cloud centers so that efficient computing can be done An improved validation component for distinguishing client in cloud condition is likewise proposed. There are three fundamental parts engaged with this structure in particular Cloud User (CU), Trusted Authenticator (TA) and Cloud Service Providers (CSPs). The TA gives secure access to the client by creating the computerized mark. In this paper, the means for confirming the clients are additionally depicted and the power consumption is also reduced.s.*

RÉSUMÉ. *Le cloud computing, en français l'informatique en nuage, est l'idée concrétisé afin de résoudre les problèmes informatiques quotidiens. Il est essentiellement un pool de ressources virtuel et le fournit aux clients via une interface internet. Le cloud computing est une amélioration basée sur l'internet et utilisé dans le cadre de l'innovation de l'ordinateur personnel (PC en anglais). Le problème commun lié au cloud computing est la protection des informations, la sécurité, l'obscurité et une qualité constante, et ainsi de suite. Cet article a proposé une nouvelle méthode d'authentification pour valider les utilisateurs de nuage ainsi qu'une nouvelle technique de réduction de la consommation d'énergie dans les centres de nuage afin de permettre une efficacité informatique. Un composant de validation amélioré pour distinguer le client dans des conditions de nuage est également proposé. Il y a trois parties fondamentales qui sont impliqués dans cet article, en particulier les utilisateurs de nuage (CU, le sigle de « Cloud User » en anglais), l'authentifiant de confiance (TA, le sigle de « Trusted Authenticator » en anglais) et les fournisseurs de services de nuage (CSP, le sigle de « Cloud Service Providers » en anglais). Le TA donne un accès sécurisé au client en créant la marque informatisée. Dans cet article, les moyens permettant de confirmer les clients sont également décrits et la consommation d'énergie est également réduite.*

KEYWORDS: *privacy, encryption, decryption, cloud registering, security, trusted authenticator (TA), energy consumption, energy reduction.*

MOTS-CLÉS: confidentialité, cryptage, décryptage, enregistrement en nuage, sécurité, authentificateur de confiance, consommation d'énergie, réduction d'énergie.

DOI:10.3166/ISI.23.6.61-72 © 2018 Lavoisier

1. Introduction

Cloud computing is an adaptable, practical and demonstrated conveyance stage for giving business or customer IT benefits over the Internet. Cloud computing bolsters appropriated benefit arranged design, multi-clients and multi-area regulatory framework, it is more inclined to security dangers and vulnerabilities. A noteworthy worry in cloud appropriation is its security and Privacy. Interruption prospects inside cloud condition are numerous and with high picks up. Security and Privacy issues are of more worry to cloud specialist organizations who are really facilitating the administrations (Abdul, 2009). Much of the time, the provider must ensure that their foundation is secure and customers' information and applications are protected by executing security strategies and instruments.

The cloud can likewise be utilized to store archives either as a huge pool of reinforcement drive or as essential store of record storage. The servers utilized for Cloud storage are facilitated by third get-together organizations who work substantial server farms. When we buy in to Cloud storage we rent storage limit from the Cloud storage (Arora, 2012). The information might be put away over different servers and at various areas. The "cloud" is made out of equipment, storage, systems, interfaces and administrations (Jadeja and Modi, 2012). Clients can get to the registering power, framework, programming applications and administrations on request and they are free of areas. Cloud computing is a compensation for every utilization display that empowers constant conveyance of exceedingly versatile resources to various organizations utilizing the web.

Cloud computing gives customers a virtual registering framework which empowers them to store information and run applications. Cloud computing presents new security challenges as customer can't completely trust cloud providers. Cryptography in Cloud computing relies upon a protected Cloud computing engineering. Cloud computing is a processing model that is driven by economies of scale and is disseminated on huge scale. Cloud designs are created by most recent and dire requests. That is, the resources are progressively given to a client according to his demand, and reclaimed after the activity is finished.

Security assumes an essential part in cloud, looked by the clients and additionally CSPs. The engineering of the Cloud computing includes various cloud parts collaborating with each other. In this way, it causes the client to get to the required administrations at a quicker rate.

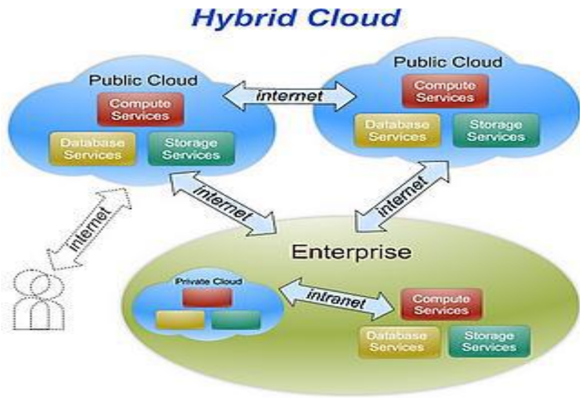

Figure 1. Cloud deployment models

This paper proposes an upgraded verification instrument for validating the clients in cloud condition. In this structure, an idea of giving Digital Signature (DS) at the client level and furthermore in the Trusted Authenticator (TA) for high security is presented. Thusly, this model illuminates primary security issues like DOS Attack, DDoS Attack, Google hacking, listening stealthily, and so forth in a cloud domain. This model enables the client to get to the administrations from the cloud specialist organization side by confirming the entrance (Chandramohan, 2013).

The target of this examination is to pick the best physical machine to reallocate cloud environment and to diminish of relocation of cloud memory keeping in mind the end goal to decrease energy utilization. To accomplish this objective, the Power Reduction Algorithm (PRA) will be adjusted to choose the fitting physical machine for reallocation and the calculation utilized as a part of (Jadeja and Modi, 2012) will be utilized to diminish the quantity of relocations.

1.1. Security issues in cloud data storage

•The physical security with the information is lost when we transfer the information in the cloud. The resources are additionally shared among various organizations (Fanfara, 2012). Clients don't have any learning or control of where the resources are running and where the information's are being put away.

•Though the information exchange, storage and recovery are done in light of approved exchange. Basic standard for information honesty not yet exists.

•The client's information individual information and data can be utilized or gone to different gatherings (Gampala, 2012).

•The encryption and decoding is being finished by the cloud specialist co-op and even the keys are with them. Clients don't have any control on their information once the information are being submitted to the cloud specialist organization. Legitimately the keys ought to be available with the clients.

The above security issues talked about above demonstrates that there are different strategies issues and dangers exhibit in Cloud computing innovation. These issues incorporate protection, information isolation, unwavering quality, storage, security, get to control and some more (Gupta, 2012). Investigating the distinctive issues we understood that security is one of the principle issues. It might be any venture information, a scholastics information or any basic clients information, security is the fundamental issue is security (Kumar, 2012). So we can propose some encryption calculation utilizing some learning of existing calculation.

2. Literature survey

These days, a few number of investigates on security issues in Cloud computing are being done. Different security systems are proposed by various analysts. By breaking down those works, some security issues are distinguished and few works are considered for proposing another system to verify the client for getting to secure administrations from the cloud specialist co-op.

Jadeja and Modi, (2012) proposed Agent Based approach for Authentication in the Cloud (ABAC) to validate the clients for getting to the cloud administrations and furthermore to lessen the inward and outside assaults. In cloud condition, the VMware parts included are VMware ESX, VCenter Server, and Active Directory Server. The stages engaged with the ABAC design are Registration Phase, Key Generation and Distribution Phase and Authentication and Verification stage. The benefit of the ABAC is; it given an additional layer of security for the whole cloud. The significant disservice is; it doesn't give versatile validation foundation.

Kaur and Kaushal (2011) proposed a confide in demonstrate for cloud engineering. It utilizes the portable operator which is utilized as a security specialist and it screens the respectability and genuineness. This framework remotely screens and authenticates the trustworthiness of vital framework records, therefore filling a hole in the Xen Cloud Platform (Harjani, 2013). This was its significant favorable position. Additionally specialist co-op can guarantee satisfaction of security strategies by staying away from assaults on VMs. The disadvantage of the proposed show is; it gives secure and dependable correspondence just through a portable specialist not through operators introduce in the cloud condition.

Nirmala *et al*. (2013) proposed a model for trusted registering and illuminate the data fraud in the cloud and it was mimicked in the .Net condition. The assessment of the proposed display happens in three ways: security breaking down, reproducing, and BLP private. The model includes six stages on the Open ID trade of information stream. The quality of the proposed show is assessed against phishing assaults and it brings about an ideal arrangement (Hirani, 2003). The constraint of the proposed demonstrate is it was assessed just in united condition and it was its downside.

Bhisikar *et al*. (2013) proposed a power-mindful system for a heterogeneous virtual condition. They utilized equipment systems, for example, dynamic voltage and recurrence scaling and virtualization to oversee energy. A worldwide chief is characterized to assign new Virtual Machine (VM) and reallocate relocated VM. The relocation cost is ascertained utilizing the extent of VMs (Kaur, 2011). The creators likewise analyzed a few calculations for tackling the power enhancement issue.

Gupta *et al*. (2012) proposed a model consolidating powerful cud click focuses, alphanumerical validation, sound mark and attract a-mystery request to conquer the ease of use and security. This framework is the blend of graphical watchword, content, draw-a-mystery strategy and telephone message, which increment the certainty and unwavering quality (Jadeja, Y 2012). This was the upside of the proposed framework. The detriment was that there is precariousness happens in information storage for cloud.

Fanfara *et al*. (2012) coordinated the hubs utilizing the VM movement calculation in green cloud figuring. Since movement costs a great deal for the cloud provider, the second objective of the creators was to limit the quantity of relocations. Their approach outflanks the container pressing heuristic calculations, for example, the principal fit diminishing calculation.

3. Crypto cloud computing

Crypto Cloud computing is another system for digital asset sharing. It ensures information security and protection. All things considered, in cloud condition, crypto Cloud computing ensures the data security and trustworthiness amid entire strategy (Jansma, 2004). Security administration of Cloud computing can likewise be performed by approving the marks of each component included. What’s more, a client can recover every single related asset utilizing his QDK key. There is no individual security under the present cloud structure, as pointed out by Mark Zuckerberg, 'the Age of Privacy Is Over' (Chandramohan *et al*., 2013). However, with the advancement of crypto Cloud computing, we can resolve the contention between administrations information sharing and protection security. It opens up new prospects for the improvement of data sharing innovation.

4. Proposed framework

The proposed system for validating the client in cloud stage. In this model, an idea of giving a Digital Signature (DS) at the client side and service provider side and a Trusted Authenticator (TA) for giving high security is displayed. This model enables the cloud client to get to the administrations from the cloud specialist organization's by verifying the entrance demands. The correspondence between the client and the CSPs are validated by the Trusted Authenticator (TA). The trusted authenticator confirms the client and enables the client and CSP to convey in getting to the administrations.

The TA has two stages, one was the Registration stage and another was the confirmation stage. The TA has a database server which checks for enlisted client and approves the client to get to administrations from CSP and it also maintains backups. On the off chance that the client isn't an enrolled customer, it makes an impression on the invalid customer. The TA likewise gives an advanced mark, which gives higher security level of getting to administrations.

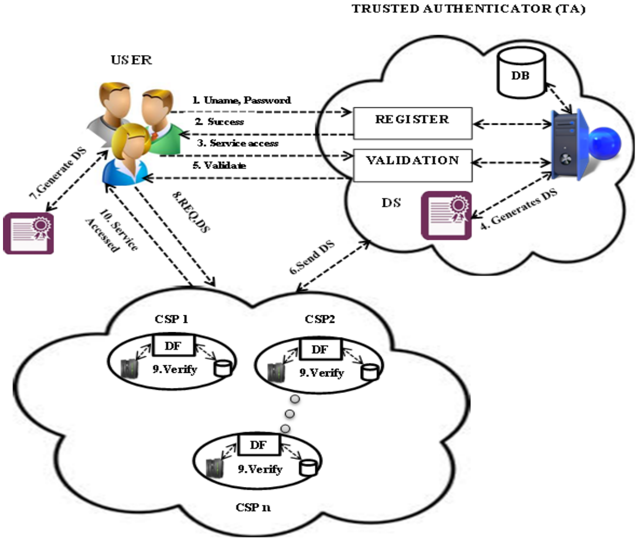

Figure 2. Proposed authentication mechanism

At the point when the client gets approved, he is allowed to approach the CSP for requesting the administrations alongside the Digital Signature. The program on the client side has an extra which creates the Digital Signature of similar qualifications in which the TA produces, and the Digital Signature wraps the client ask. The client demands for getting to administrations alongside Digital Signature will be sent to the CSP.

The billows of CSP have the demand from the client side and the DS from the TA and apportion the regarded CSP which has the asked for administrations. The regarded CSP has an operator who checks the DS from both client and CSP. In the event that they are equivalent, at that point the client is permitted to get to the administration effectively.

4.1. Proposed algorithm

The proposed algorithm provides high security to the data in cloud by performing cryptographic mechanisms. The proposed algorithm provides security to the data. When a cloud environment is established then there is a need to select the

Trust Authenticator (TA) which is a third party in the organization which has its task and it is independent authority in the organization. When a user wants to make use of cloud space then initially they need to register with the cloud service provider. When a user gets successfully registered then the Trusted Authority will generate a Secret ID(SID) for that registered user.

SID=TA(evaluate(uid, pwd, secret Key))

Here a secret Id is generated with the use of user id,password provided at the time of registration and the key provided by Trusted authority)

$$SID=\frac{Uid * pwd}{Secret\ Key} * Hash\left(Secret\ Key\right)$$

The registered users when in need to make use of cloud space then they have to provide all the login credentials along with the SID. Then the TA will check the identity of the user.

The algorithm for validating cloud users is given below.

```
Algorithm CloudUserValidation
{
STEP-1: Input UID,PWD,SID to TA
Step-2: The details are listed in TA Backup for present validation and for future use also.
Step-3: If the details are found in the TA backup then the user is validated and a Digital
signature is sent to the Cloud service provider(CSP) and to cloud user(CU).
If(CU(uid,pwd,SID)==TA(Backuplist())
Generate Digital signature(DS).
Send DS→CSP,CU;
Update Backup;
else
Unauthorized access.
Terminate Process.
Step-4: If user wants to use cloud space then they need to provide DS.
Step-5: To upload any data into cloud space every time CU has to provide a new DS.
Step-6: Stop
}
```

The working of the algorithm is explained below

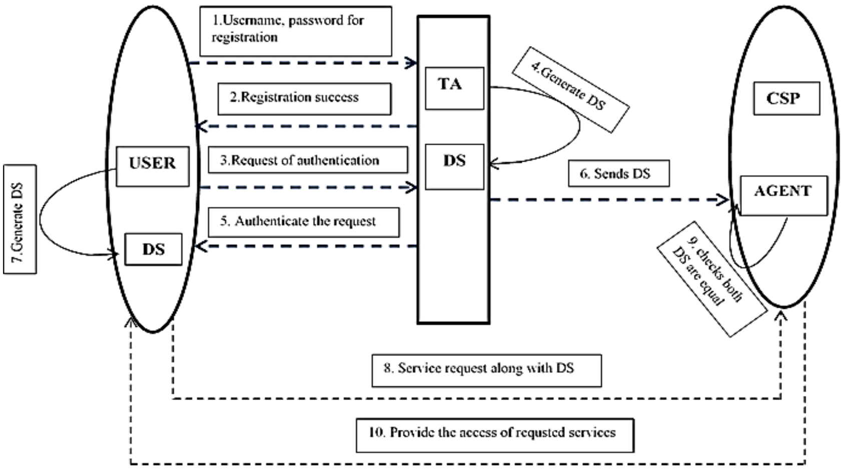
1.Username, password for registration
2.Registration success
3.Request of authentication
4.Generate DS
5. Authenticate the request
6. Sends DS
7.Generate DS
8. Service request along with DS
9. checks both DS are equal
10. Provide the access of requsted services
USER
DS
TA
DS
CSP
AGENT

Figure 3. Workflow of authentication mechanism

4.2. Proposed method for power reduction

This paper goes for energy effectiveness in the foundation as an administration level. The principle strategy utilized for enhancing the effectiveness of assets in the server farms is virtualization. When a Cloud user want to upload any sensitive data into cloud space, then it needs to submit the Digital Signature (DS) to the CSP. Now the cloud administrator (CA) will check for the available space in the cloud, if there is enough space then the data can be uploaded. Otherwise a reminder is sent to CSP to extend memory levels. The proposed approach decreases the cloud memory movement and energy utilization, utilizing dynamic arrangement of relocated CUs. The proposed power reduction algorithm is.

Step-1: Input the Total No.of CU and CP.

Step-2: Calculate the workload of each CU.

Load=(Data sent rate*Total Available space in cloud)/Data Stored in Cloud

Step-3: Arrange all the CU as per their loads such that high load CUs are given priority.

Step-4: CA will check Cloud memory for availability of space to store the data.

Step-5: All the CU are arranged in sorted order based on load.

Step-6: Based on sorted order the available data of High Load CU is stored in CP memory.

Step-7: Only CUs data whose power remaining is below 30% can be stored in CP space.

$$Power\ Consumed\left(PC\right)=\frac{N*T}{1000\ Joules}$$

N is Power Given initially to CU in Joules, T is Number of hours CU is in active Mode.

Power Remaining= TP-PC

TP is total power initially allotted to CSP.

Step-8: Low load CUs are stored only after the high load CUs data is stored.

Step-9: All CUs who have not provided DS to CSP is removed as they are treated as unauthorized users.

Here N is No.of Hours Used

The proposed Power reduction algorithm can be applied in any central organization where the CUs load is calculated initially. Then based on the load of each CU they are arranged in sorted order with Higher Load CU occupying first precedence to store its data in cloud. Then the CUs whose remaining power is less than 30% will get the next precedence to store their data. After all these CUs data is stored then remaining CUs are permitted to complete their task.CA will continuously monitor the memory levels for avoiding any delay during storage of data.

5. Results

The proposed algorithm which performs authentication mechanisms performs better when compared to traditional methods and the results show that the proposed better and provides high level of security in validating cloud users in . The performance levels of validating cloud users is illustrated as below.

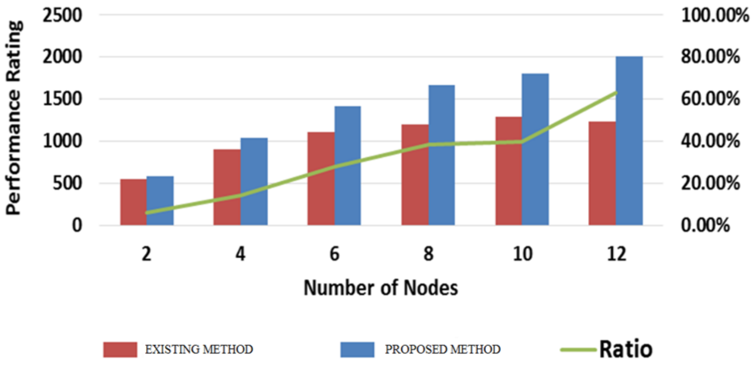

Figure 4. Performance comparison

The energy comparison of cloud users based on no.of joules is calculated and depicted in below figure

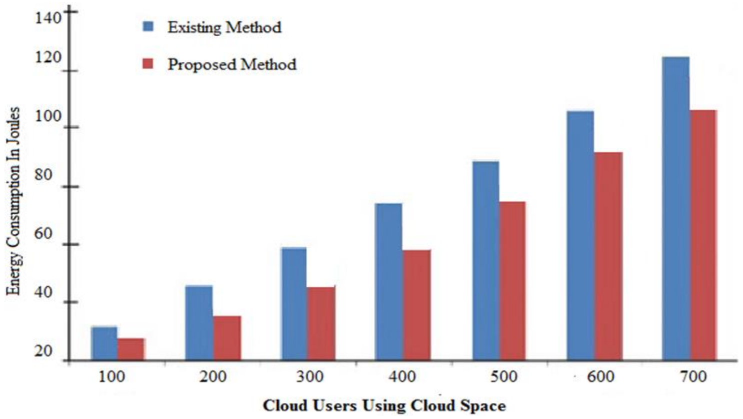

Figure 5. Energy consumption levels

The energy level consumption is reduced when power reduction algorithm is applied on cloud data providers and service providers. The rate of processor load due to power reduction is illustrated as.

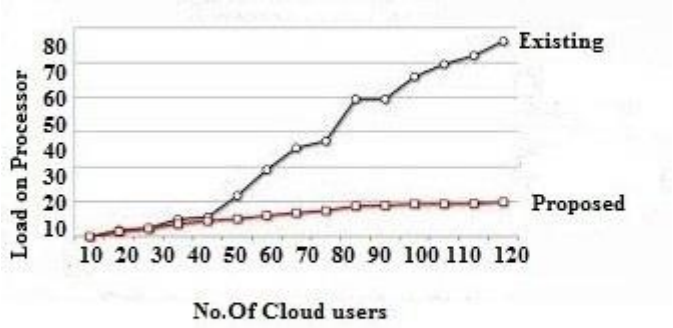

Figure 6. Processor load

6. Conclusions

The Cloud processing as an innovation would be embraced if the zones of concerns like security of the information will be secured with full evidence component. The quality of Cloud computing is the capacity to oversee hazards specifically to security issues. The proposed system represents the means for getting to the administrations. Along these lines, the client is in charge of verify himself with the TA and allowed to get to the administrations as per his demand.

Computerized Signatures brings the largest amount of security. With a specific end goal to keep the interloper demonstration amid the travel Digital Signature from TA to client, the idea of making the DS on the client side is connected. Accordingly, the DS is recently made at the client agree with a similar qualification made by TA. The proposed power reduction algorithm is applied on cloud users for power reduction so that cloud users can effectively make use of cloud services. Our recommended model will introduce a diagram portray of engineering to be received by planners engaged with actualizing the Cloud computing. Security calculations said for encryption and unscrambling and routes proposed to get to the media substance can be executed in future to improve security system over the system. Later on, we will endeavor to investigate our exploration by giving calculation usage and creating results to legitimize our ideas of security for Cloud computing. All together for this way to deal with fill in as expected, the cloud specialist organization must co-work with the client in executing arrangement. Some cloud specialist co-ops construct their plans of action with respect to the offer of client information to sponsors. These providers presumably would not enable the client to utilize their applications in a way that jelly client security.

References

Abdul D. S., Elminaam H. M., Kader A., Hadhoud M. M. (2009). Performance evaluation of symmetric encryption algorithms. *International Conference on Parallel, Distributed and Grid Computing*, Vol. 8, pp. 58-64. https://doi.org/10.1109/PDGC.2014.7030724

Arora P., Singh A., Tyagi H. (2012). Evaluation and comparison of security issues on cloud computing environment. *World of Computer Science and Information Technology Journal*, Vol. 2, No. 5, pp. 179-183

Bhisikar P., Sahu A. (2013). Security in data storage and transmission in cloud compituing. *International Journal of Advanced Research in Cloud Science and Software Engineering*, Vol. 3, No. 3, pp. 410-415.

Chandramohan D, Vengattaraman T, Rajaguru D, Ramachandran B., Dhavachelvan P. (2013). A privacy breach preventing and mitigation methodology for cloud serv ice data storage. *IEEE International Advanced Computing Conference*. https://doi.org/10.1109/IAdCC.2013.6514199

Fanfara P., Dankova E., Dufala M. (2012). Usage of asymmetric encryption algorithms to enhance the security of sensitive data in secure communication. *IEEE 10th Jubilee International Symposium on Applied Machine Intelligence and Informatics*, pp. 213-217. https://doi.org/10.1109/SAMI.2012.6208959

Gampala V., Inuganti S., Muppidi S. (2012). Data security in cloud computing with elliptic curve cryptography. *International Journal of Soft Computing and Engineering*, Vol. 2, pp. 138-141.

Gupta S., Satapathy S. R., Mehta P., Tripathy A. (2012). A secure and searchable data storage in cloud computing. *IEEE International Advance Computing Conference*, pp. 106-109. https://doi.org/10.1109/IAdCC.2013.6514203

Harjani D., Jethwani M., Keswaney N., Jacob S. (2013). Automated parking management system using license plate recognition. *Int. J. Computer Technology & Applications*, Vol.

4, No. 5, pp. 741-745.

Hirani S. (2003). Energy consumption of encryption schemes in wireless devices thesis. Master's Thesis, University of Pittsburgh.

Jadeja Y., Modi K. (2012). Cloud co mputing - concepts, architecture and challenges. *012 International Conference on Computing, Electronics and Electrical Technologies*, pp. 877-879. https://doi.org/10.1109/ICCEET.2012.6203873

Jansma N., Arrendond B. (2004). Performance comparison of elliptic curve and RSA digital signatures. *International Conference on Information and Network Technology*, pp. 58-62.

Kaur H., Kaushal K. (2011). Security concerns in cloud computing. *High Performance Architecture and Grid Computing: International Conference*, pp. 103-112. https://doi.org/10.1007/978-3-642-22577-2_14

Kumar A., Lee B. G., Lee H., Kumari A. (2012). Secure storage and access of data in cloud computing. *International Conference on ICT Convergence*, pp. 336-339. https://doi.org/10.1109/ICTC.2012.6386854

Leistikow R., Tavangarian D. (2013). Secure picture data partitioning for cloud computing services. *International Conference on Advanced Information Networking and Applications Workshops*, pp. 668-671. https://doi.org/10.1109/WAINA.2013.157

Nadeem A., Javed M. Y. (2005). A performance comparison of data encryption algorithms. *IEEE Information and Communication Technologies,* pp. 84-89. https://doi.org/10.1109/ICICT.2005.1598556

Nirmala V., Sivanandhan R. K., Lakshmi R. S. (2013). Data confidentiality and integrity verification using user authenticator scheme in cloud. *International Conference on Green High Performance Computing*. https://doi.org/10.1109/ICGHPC.2013.6533902

Srikanth B., Kumar H., Rao K. U. M. (2018). A robust approach for WSN localization for underground coal mine monitoring using improved RSSI technique. *Mathematical Modelling of Engineering Problems,* Vol. 5, No. 3, pp. 225-231. https://doi.org/10.18280/mmep.050314

Sudha M., Monica M. (2012). Enhanced security framework to ensure data security in cloud computing using cryptography. *Advances in Computer Science and its Application*s, Vol. 1, No. 1, pp. 32-37.

Wang M. M., Zhu G. L., Zhang X. Q. (2018). General survey on massive data encryption. *International Conference on Computing Technology and Information Management*, pp. 150-155.

Zhang B., Peng C. G., Xu Z. P. (2011). Identity-based distributed cloud storage encryption scheme. *International Conference on Reliability, Maintainability and Safety*, pp. 610-614. https://doi.org/10.1109/ICRMS.2011.5979341