Research Journal of Applied Sciences, Engineering and Technology 13(5): 354-364, 2016
DOI:10.19026/rjaset.13.2953
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 9, 2015 Accepted: April 5, 2016 Published: September 05, 2016

**Research Article**

# Steganography Based Secure Data Storage and Intrusion Detection for Cloud Computing Using Signcryption and Artificial Neural Network

[1]J. Anitha Ruth, [2]H. Sirmathi and [1]A. Meenakshi
[1]SRM University,
[2]COE SRM University, Sikkim SRM University, SRM Nagar, Kattankulathur, Kancheepuram District-603 203, Tamilnadu, India

**Abstract:** An efficient approach for providing very high secure storage data to the cloud system is proposed in this study. In order to effectively access data from the cloud server, a secure authentication is highly essential. After the authentication the user data is examined to ascertain whether the specified data is normal or intrusive in accordance with the intrusive recognition system, such as the Artificial Neural Network (ANN). It is accompanied by the encryption of the file by means of the signcryption technique. For the purpose of enhancing the storage safety of the novel approach, the steganography methods are carried out immediately after the encryption technique. In the innovative technique, the linguistic steganography approach is employed to conceal the data from the TPA. Subsequently, the data is subdivided arbitrarily and is amassed into cloud. The epoch-making steganography based secure storage and intrusion recognition technique is performed with the mighty assistance of the Cloud simulator in the working platform of Java software.

**Keywords:** Artificial neural network, Intrusive detection system, linguistic steganography, signcryption, steganography

## INTRODUCTION

Cloud computing is one of the significant and improving topic for both the developers and the users. Cloud computing is a suitable platform for persons who are interconnected with the networking surrounding (Nafi *et al*., 2012). Cloud computing is depend on internet and it is one of the basic of the next generation of computing. Computing applications such as data, storage, software, computing and application are distributed to local devices with the help of internet (Gonzalez *et al*., 2012). Nowadays, cloud storage service gives a comparably low cost, scalable, position-independent platform for clients so it becomes a rapid profit growth service. It has the ability to integrate multiple internal and/or external cloud services mutually to give high interoperability, since a cloud computing surroundings is created depend on open architectures and interfaces (Zhu *et al*., 2012). By the review of IDC, security is one of the important open problems in adopting the cloud computing model.

Security is one of the greatest problems for the adoption of cloud computing. And also security is a big problem associated to several features (Chen *et al*., 2012). The organization of cloud computing security standards and evaluation system with the center of security goal validation and security service level estimate is one of the security confront of cloud computing (Vouk, 2008). Three security necessities are frequently considered: confidentiality, integrity and availability for the majority internet service providers and cloud users (Zhao *et al*., 2014). Data security engages encrypting the data as well as make sure that suitable strategy are imposed for data sharing (Hamlen *et al*., 2010). We tackle the difficulty of the security of cryptographic protocols in face of prospect advances in computing technology and algorithmic research. The difficulty stems from the reality that calculation which at a given point in time may be considered infeasible in the course of years or decades, be prepared probable with enhanced hardware and/or penetrates in code-breaking algorithms. In such situation, the security of historical is highly secret data may be in jeopardy (Aumann *et al*., 2002).

Essentially, network security contain the hardware and software of network systems, mutually with the security of information conveyed on the network, which, we should make sure, would not be damaged by

**Corresponding Author:** J. Anitha Ruth, SRM University, SRM Nagar, Kattankulathur, Kancheepuram District-603 203, Tamilnadu, India

chance or wicked attack. Network security engages both the technical and the management troubles (Fernandes *et al*., 2014). Security is an important necessity for cloud computing unite as a robust and practicable adaptable result (Sahu *et al*., 2014). This security has been separated as numerous divisions and one of the mainly significant divisions is guarantee about the user authentication procedures and supervision contact when users outsource sensitive data distribute on public or private cloud servers (Moghaddam *et al*., 2014). The majority vital security necessities are user identification and authentication (Zwattendorfer and Tauber, 2012). Authentication is to verify the uniqueness of the user, which means whether the person is similar as he imagines being (Emam, 2013). The authentication reflected on the center of security in the cloud computing. Therefore, it is essential to permit that only authorized user can contact stored data (Yassin *et al*., 2012). User authentication in cloud computing surroundings has been separated to two major procedures: examining exclusive identifiers of users on the early registration segment and user authentication and authenticating user legal uniqueness and obtaining their access control rights for the cloud-based resources and services on the service process segment (Moghaddam *et al*., 2014). The overall objective of the proposed work is to improve the security of data storage in cloud using steganography methods after the encryption technique.

## LITERATURE REVIEW

Numerous methods were projected by different authors for Secure Storage and intrusion detection system in Clouds and some of them are given detailed below:

Cloud computing is a "network of networks" through the internet, so probability of interruption is further with the sophistication of intruder's assaults. Dissimilar IDS methods are employed to oppose malicious assaults in conventional networks. For Cloud computing, huge network contact rate, resigning the handle of data and applications to repair supplier and circulated assaults susceptibility, a competent, consistent and information transparent IDS is necessary (Shelke *et al*., 2012). A multi-threaded cloud IDS representation was projected which could be directed by a third party observing service for a superior optimized effectiveness and transparency for the cloud user. To switch large scale network contact traffic and managerial control of data and application in cloud, a new multi-threaded circulated cloud IDS representation has been projected. Their projected cloud IDS switches huge flow of data packets, examine them and create reports competently by incorporating knowledge and performance study to identify interruptions.

Facing the difficulty of Cloud design, Mathew and Jose (2012) have centered on suggesting operation design of Intrusion Detection Systems in the Cloud. They have conversed and list numerous existing intimidations for a Cloud communications and were provoked to utilize Intrusion Detection Systems (IDS) and its organization in the Cloud. They projected the consumption of incorporated and covered IDS on cloud that intended to wrap different attacks. That IDS incorporate facts and performance study to amplify a cloud's safety. The two interruption finding methods were different. But the lack of one method will be complimented by other one. The aim of the study was to suggest a technique that allows Cloud Computing System to attain both efficiency of using the system possessions and power of the safety service without transaction between them.

The dispersed and open arrangement of cloud computing and services becomes an impressive aim for possible cyber-attacks by impostors. Patel *et al*. (2013) have obtainable a complete categorization and state of the art of interruption finding and obstacle systems to pull investigators concentration for probable results to interruption finding and obstacle in cloud computing. A precise notice was specified to cloud systems uniqueness and present disputes prohibition IDPS expansion for cloud. Allowing for the preferred uniqueness of IDPS and cloud computing systems, a directory of germane necessities for a cloud based interruption finding and obstacle system was offered and four model so autonomic figuring self-management, ontology, risk management and fuzzy theory are leveraged to gratify these necessities.

Cloud computing is the liberation of computing possessions through the Internet. Cloud stores roughly unlimited amount of data using virtualization. There may be an option of data loss in cloud. Kumar and Ramasubash (2014) have recommended a method called multi tier intrusion detection system. Presenting safety is to circulate systems requirements to more than user certification with passwords or digital certificates and isolation in communication of data. Distributed design of cloud construct is the susceptible and flat to complex circulated interruption assaults parallel to Cross Site Scripting as well as Distributed Denial of Service. To grasp large scale network contact traffic and managerial control of information and function in cloud, new multi-threaded dispersed cloud IDS design has been predictable. Our anticipated cloud IDS embrace vast flow of data packets, observe them and generate information capably by incorporating information and presentation study to become conscious of interruptions.

Velumadhava Rao and Selvamani (2015) has planned a Cloud Computing movement is quickly rising that has a technology association with Grid Computing, Utility Computing and Distributed Computing. Cloud service providers such as Amazon, IBM, Google's Application and Microsoft Azure etc; offer the users in increasing applications in cloud surroundings and to

contact them from everywhere. Cloud data are accumulated and contacted in a remote server with the aid of services offered by cloud service providers. Supplying safety is a main concern as the data is broadcasted to the remote server over a channel (internet). Before applying Cloud Computing in a group, safety challenges requirements to be tackled initial. In this study, we underline data linked safety challenges in cloud based situation and results to defeat.

Cloud computing has become an ingredient of the aggressive promote today. Different cloud computing service providers are obtainable with their services in the cloud background Methods approved by different providers to accomplish safety are of changeable environment. To examine and compute an exacting service depends on its safety possessions is a dispute. Shaikha and Sasikumar (2015) has obtainable such a quantity by using a trust form. A trust form computes the safety power and calculates a trust value. A trust value encompass of different limits that are essential magnitude beside which safety of cloud services can be deliberate. CSA (Cloud Service Alliance) service confronts are used to review safety of a service and legality of the form. Sufficiency of the form is also confirmed by estimating trust value for obtainable cloud services. Trust form acts as a standard and position service to compute safety in a cloud computing surroundings.

**Problem definition:** Cloud computing has produced important attention in both academia and industry, but it's still a developing model. One of the main dangerous concern of cloud computing is data security. The general difficulty in existing cloud security and privacy methods are given below:

- Cost and efficiency is the main difficulty of the existing security and privacy methods.
- The major two problems in cloud computing is the user meeting when using cloud computing services. The first one is users concerns about hacking threats whether inside or on the outside. The other one is the infeasibility of encrypting all data without intriguing into thought of its privacy level.
- The major difficulty of existing cloud security and privacy method is security difficulty.
- The major plan of IDS is to identify the assaults and produce the appropriate reply. But the existing signature based intrusion detection technique cannot identify the novel or alternative of recognized attacks.
- Extra time is necessary to recognize the attacks in different existing intrusion detection system.

These are the major disadvantage of different existing works, which stimulate us to do this investigate on Cloud Security Storage and intrusion detection system. We are planned to suggest an appropriate technique to accomplish secure data storage and intrusion detection in cloud computing.

**Proposed method:** In the current investigation, an effectively technique is elegantly launched for furnishing very superior confidential storage data to the cloud system. At the outset, the user is required to register his records in the cloud and generate his own user name and password and thus obtain the public and private keys. If the user details are already registered in the cloud server then he has to enter his user name and password. Thereafter, the cloud server examines the authentication of the user. If the authentication is successful the user gets linked to the server, or else the server rejects the request of the user. Subsequently, an assessment is made regarding whether the data is regular or intrusive, with the help of the intrusion recognition system. This is followed by the encryption of the data by means of the cryptography approach. To enhance the storage safety of the novel technique, the steganography methods are employed immediately after the encryption approach. Now, the data is arbitrarily subdivided and amassed into the cloud. The overall procedure of the suggested approach is colorfully pictured in the block diagram (Fig. 1).

The new-fangled technique flows through the following four phases such as the authentication, Intrusion detection, encryption and decryption and steganography. In the authentication stage, the user authentication is examined. Later on, the intrusion recognition is effectively performed by the artificial neural network in accordance with the classification such as the regular or intrusive data. Thereafter, the regular data is subjected to encryption by means of the signcryption technique. The encryption is followed by the steganography with the intention of enhancing the storage safety. The total process of the four phases is broadly discussed as follows.

**Phase 1: Authentication phase:** The data owner has the obligation to encrypt the file and thereafter amass it in the cloud. In the event of a stranger succeeds in his effort to download a specific file, they are competent to observe the record if they are in possession of the key utilized to decrypt the encrypted file. At time, it may end in failure on account of the technology advancement and the incapacity of the hackers. While effectively addressing the related hassle, the authentication stages assume supreme significance in view of the fact that it is capable of authenticating the user data in the cloud first. In the proposed technique, the user authentication is a big must. If the

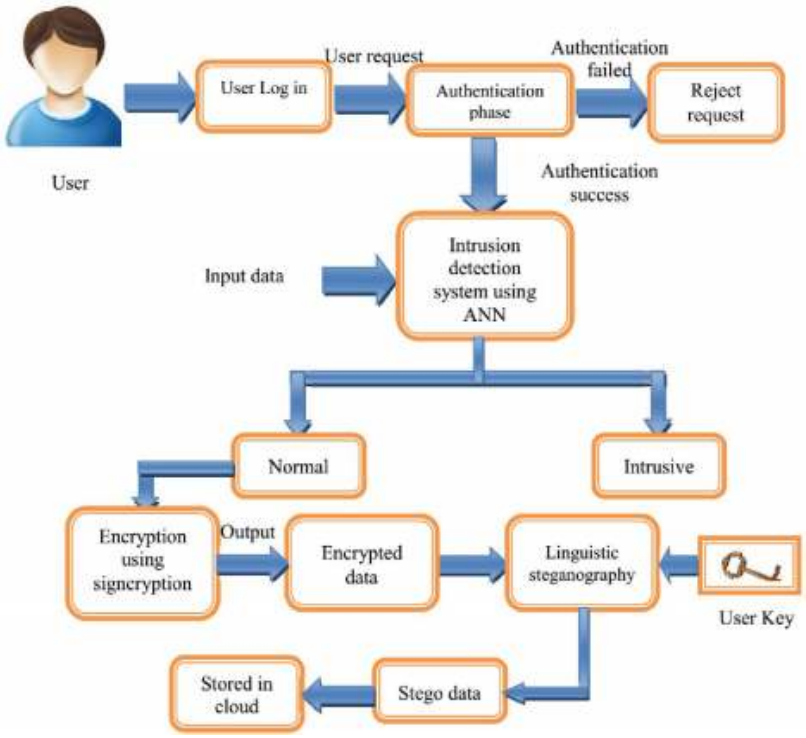


Fig. 1: The block diagram of the proposed method

authentication ends up in success the user gets linked to the server, or else the server squarely rejects the request of the user. Subsequent to the authentication of the user, the user data is examined, to assess the nature of data such as the regular or intrusive the innovative technique effectively employs the artificial neural network for the sake of the corresponding categorization into the standard and intrusive data. The modus operandi of the intrusion recognition stage is beautifully pictured in the upcoming section.

**Phase 2: Intrusion detection phase:** The innovative approach employs the Artificial Neural Network (ANN) for the intrusion recognition system, with the ultimate objective of categorizing the data into two categories such as the standard or intrusive. Further the brand of ANN employed in the suggested technique is the Back Propagation (BP) approach. Thus, the ANN based intrusion recognition system emerges as an effective solution for amorphous network data.

**Artificial neural network using back propagation algorithm:** The Artificial neural network based back propagation technique is taught with the help of the input data. The neural network invariably comprises m number of input units, h hidden units and a single output unit. In the innovative technique, the back propagation technique is elegantly employed as the training method. The configuration of the proposed artificial neural network is effectively exhibited as follows. The overall structure of artificial neural network is plotted in Fig. 2; it is shown in beneath.

**The bias function of the neural network:** The bias function represents the product of weights and input data of the neural network as illustrated in the following Equation:

$$BF(t) = \alpha + \sum_{n=1}^{h} (w_{11}d_1 + w_{12}d_2 + \ldots\ldots + w_{tn}d_m) \quad (1)$$

Here, ($w_{11}$, $w_{12}$, … $w_{tn}$) characterize the weights of neuron and ($d_1$,$d_2$…$d_m$) depict the input data.

**Activation functions for the neural network:** The Activation function is represented as a non-linear function as described in the Equation shown below:

$$H = \frac{1}{1+\exp^{-BF(t)}} \quad (2)$$

**Calculation of learning error obtained is given below:** The learning error is achieved by means of the following Equation:

$$O = \frac{1}{2}\sum_{n=0}^{h-1} (desired - actual) \quad (3)$$

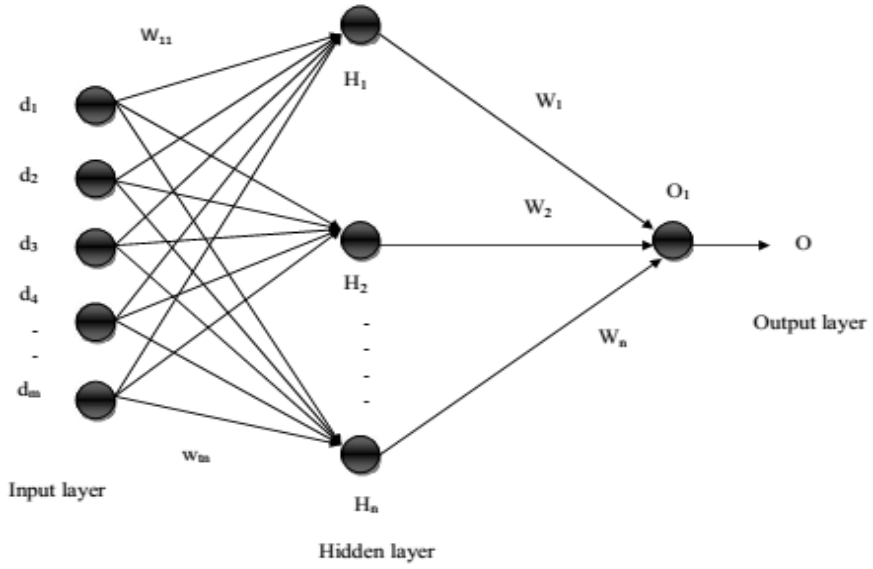


Fig. 2: The structure of artificial neural network

Here, O corresponds to the neural network output and h signifies the total number of neurons in the hidden layer.

In the artificial neural network the error is cutback considerably to the extent of the least value in order that it is well-educated for carrying out the testing phase. Further the threshold value which fulfils the minimum benchmark is allocated. Thereafter the threshold value $\omega$ and the upshot of the neural network (O) are assessed and contrasted by means of the following equation:

$$result = \begin{cases} normal, O \geq \omega, \\ \text{int}\, rusive, O < \omega \end{cases} \quad (4)$$

If the upshot of the neural network output exceeds the threshold value it indicates that the offered input data is regular, or else it represents the intrusive data. Subsequent to the categorization of the input data in to regular or intrusive, the regular input data is shortlisted for additional processing.

**Phase 3: Encryption and decryption phase:** In the document, the encryption and decryption functions are executed with the help of the signcryption algorithm.

**Utilization of signcryption algorithm:** The Signcryption, in quintessence, represents a public-key primitive which simultaneously performs the tasks of the digital signature and encryption, which constitute two vital cryptographic gadgets which are capable of ensuring the privacy, honesty and non-repudiation. The Sender encloses the specified data, with the intention of forwarding it to the receiver in an unprotected channel and hence he borrows the assistance of signcryption technique to communicate the message to receiver in such a way that the data remains protected and confidential:

**Parameter initialization:**

P: Large prime number
Q: Large prime factor
G: Integer with order Q modulo P, chosen randomly from [1, … P-1]

Hash-one way hash function, whose output has at least 128 bits, KH-Keyed one way hash function V-value, chosen randomly [1,…Q-1]
Sender key initialization:

**$A_{k1}$:** Sender private key, chosen randomly [1,…Q-1]
**$B_{k1}$:** Sender public key,

$$B^{k1} = G^{A}_{k1} \bmod P$$

**Receiver key initialization:**

$A_{k2}$ : Receiver private key, chosen randomly [1, … Q-1]
$B_{k2}$ : Receiver public key,

$$B_{k2} = G^{A}_{k2} \bmod P$$

The roadmap with various stages involved in the signcryption procedure is drawn and the comprehensive process elegantly exhibited in Fig. 3 shown.

**Steps for signcryption:**

- At the outset, the sender shortlists an appropriate Value (V) from the range of [1 …. Q-1]
- With the intention of evaluating the hash value, he utilizes the receiver public key and the value (V). The output of hash value (OH) is estimated as a 128 bit as detailed below:

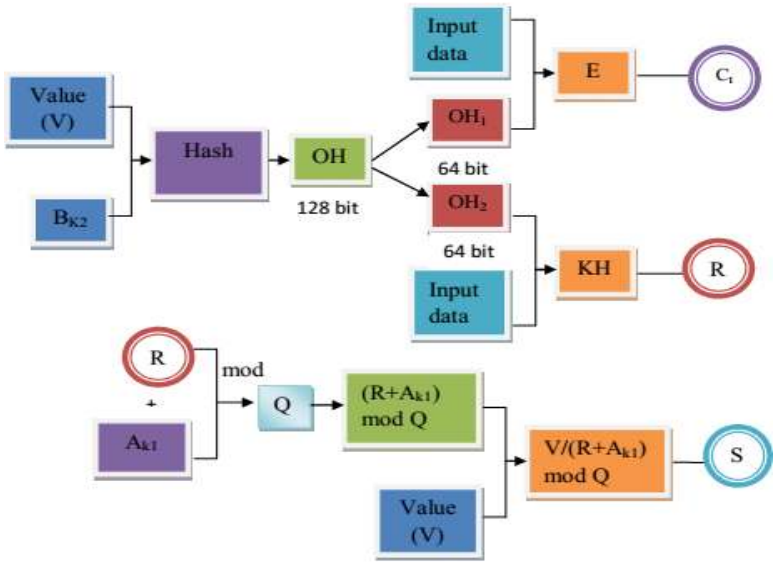


Fig. 3: Process of signcryption

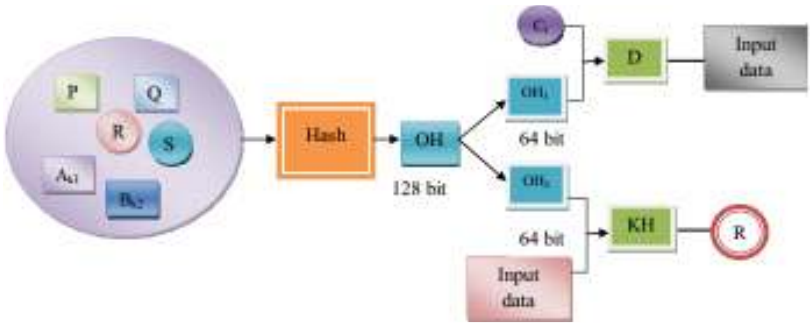


Fig. 4: Process of unsigncryption

$$OH = hash(Y_{k2}{}^{V} \bmod P_{rn}) \quad (5)$$

- Subsequently he subdivides the 128 bit Output Value (OH) into two distinct 64 bit values such as OH1 and $OH_2$.
- Then, he performs the encryption of the data with the assistance of the encryption (E) algorithm with $OH_1$. Thus, he gets hold of the sender cipher text ($C_t$) as illustrated in the following Equation:

$$C_t = E\,OH_1(data) \quad (6)$$

- Now, he effectively utilizes the $OH_2$ value in the one-way keyed hash function KH to achieve a hash of the data, which leads to the 128-bit hash, labeled as the R:

$$R = KH\,OH_2(data) \quad (7)$$

- Finally, he evaluates the value S by means of Equation 11 shown hereunder:

$$S = \frac{V}{(R + V_{OH1}) \bmod Q} \quad (8)$$

- Thus, the send pockets three distinct values such as the Ct, R and S, which are subsequently communicated to the receiver.

**Unsigncryption algorithm:** The receiver at his end performs the function of decryption of the data by carrying out the successive steps in the unsigncryption phase, immediately after receipt of the $C_t$, R and S from the sender. In the process, he follows the steps detailed below. Further, the overall procedure is beautifully pictured in Fig. 4.

**Steps for Unsigncryption:**

- The sender effectively utilizes the values of $C_t$, R, S, receiver private key, sender public key, P and G to estimate a hash which ultimately offers the 128 bit output:

$$OH = hash((B_{k1} * G^{R})^{s} * ^{A_{k2}} \bmod P) \quad (9)$$

- Thereafter, the 128 bit output is subdivided into two 64 bit halves which offer the key pair of ($OH_1$, $OH_2$).
- The receiver subsequently uses the key $OH_1$, to decrypt the cipher text $C_t$, which eventually ushers in the data:

$$data = D\,OH_1(C_t) \quad (10)$$

- The data is accepted as valid if KH $OH_2$ (data) = R

**Phase 4: Steganography phase:** With an eye on enhancing the storage safety of the novel approach, the steganography methods are initiated subsequent to the encryption technique. The underlying motive of the steganography is dedicated to hiding the data from a stranger. In this regard the steganography may be broadly categorized into diverse types such as the image, text, audio and the video steganography based on the cover media utilized to implant the confidential data. In the document, the text steganography is effectively used for the additional processing, as it is competent to include anything from modifying the formatting of a modern text, to varying the words within a text, to producing arbitrary character sequences or employing the context-free grammars to create legible texts. In fact, galore are the diverse methods which can be employed to implant the confidential data in the text files:

- Format Based technique
- Random and Statistical approach
- Linguistics Method

In fact, the encoding of confidential messages in text has turned out to be a very daunting challenge these days. The vital cause of is on account of the fact that the text files contain an infinitesimal quantity of superfluous data for substitution with the confidential message. A different type of deficiency is the simplicity with which the text based Steganography can be modified by an unscrupulous stranger by merely varying the text itself or a slight modification of the text format into a different one very easily. In the innovative technique, the linguistic steganography approach is effectively employed to conceal the data from the TPA.

**Linguistic steganography:** The Linguistic approach which exclusively takes into account the linguistic qualities of the created and adapted text habitually employs the linguistic framework as a haven for the concealed messages. As a matter of fact, it is very easy and convenient to conceal the steganography data within the syntactic framework itself. Further, the encrypted data emerges as the input for the steganography approach. With the motive of concealing the encrypted data, at the outset, the user key is derived to locate the appropriate place where the encrypted data has to conceal the data. As per the user key, the fitting position is chosen and the data is substituted with their related information. Subsequent to this procedure, the stego data is attained, which is amassed into the cloud with high safety. Therefore, it is necessary to subdivide the data and stockpile them arbitrarily in the cloud. In the document, the run time, memory utilization and the expenditure are assessed and are considerably scaled down for establishing the excellence in performance of the novel technique. From the charismatic outcomes, it becomes crystal clear that the new-fangled technique has come out in flying colors in highlighting its superlative efficiency with regard to various factors and contrasted with the modern method.

## RESULTS AND DISCUSSION

This section gives the detailed view of the result that is obtained by our proposed method of steganography based secure data storage and intrusion detection is performed in the working platform of JAVA with CloudSim. To develop a secure storage signcryption algorithm is used in our method. Signcryption algorithm is applied for encryption and decryption process. In order to improve the secure storage steganography is applied after the encryption. The experimental result and the performance of the proposed method are given below in detail. At first the user registers their details in the cloud server. The new registration of the user is shown in Fig. 5.

**Performance analysis:** The performance analysis of our proposed technique is shown in the below section. Table 1 shows various file size and the corresponding encryption and decryption time. In our method we take the file size as 10, 20, 30 and 40 kb, respectively. To encrypt the file contain 10kb it takes the 1562 milliseconds and if the file size vary the time consumption to encrypt the file also vary (Table 1).

To encrypt the 10kb file our method takes 1562 milliseconds for encryption and 1634 milliseconds for decryption. Varying the file size like 20, 30 and 40kb encryption time and decryption time is also varying. Here 2134 milliseconds to take to encrypt the 20kb file and 1987 milliseconds obtain to decrypt the same file

Table 1: Encryption and decryption time for various file size

| File size | Encryption time | Decryption time |
|---|---|---|
| 10 kb | 1562 | 1634 |
| 20 kb | 2134 | 1987 |
| 30 kb | 2654 | 1846 |
| 40 kb | 3681 | 3179 |


Fig. 5: New registration of the user

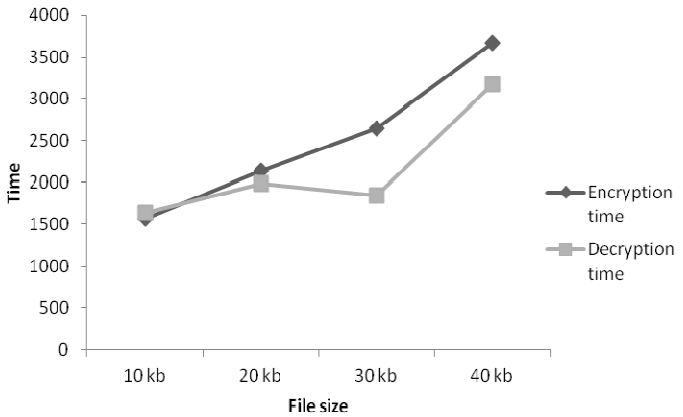


Fig. 6: Encryption and decryption time by varying the file size

Table 2: Memory value and execution time of the proposed method

| No of iterations | Memory | Time |
|---|---|---|
| 10 | 563416 | 2347 |
| 20 | 764111 | 3478 |
| 30 | 816546 | 3961 |
| 40 | 923464 | 3926 |
| 50 | 946467 | 4367 |

Table 3: Accuracy value of proposed method

| Classifier | Accuracy value for testing |
|---|---|
| ANN (Back propagation algorithm) | 91% |

size. The graphical representation of the proposed encryption and decryption time by varying the file size is shown in Fig. 6.

In our proposed technique Table 2 shows the overall memory value and execution time of the proposed method. In Table 2 we vary the number of iteration and evaluate the memory value and execution time.

Figure 7 and 8 shows the graph value for no of iteration with memory value and execution time. It is plotted in the below section.

The overall memory value of proposed method achieves 802800.8 by varying the number of iteration, the memory value is varying for number of iteration. The overall execution time of the proposed methods achieves 3615.8 milliseconds. Figure 8 shows the execution time for the proposed method by varying the number of iteration.

The overall classification accuracy of the proposed artificial neural network based back propagation algorithm is tabulated in Table 3. Here the proposed ANN achieves 91% of the accuracy value. It is tabulated in beneath.

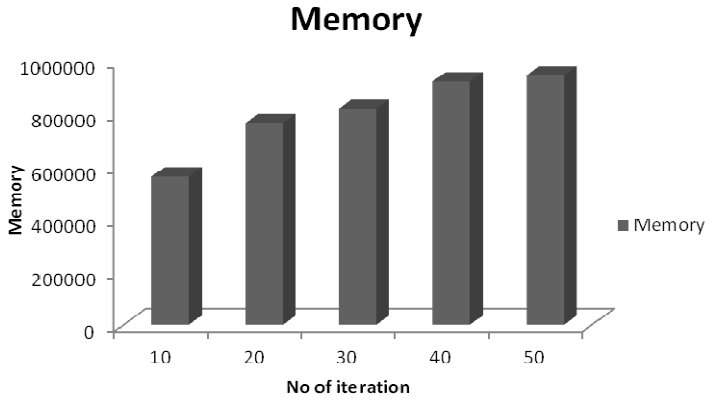


Fig. 7: Memory value for the proposed technique

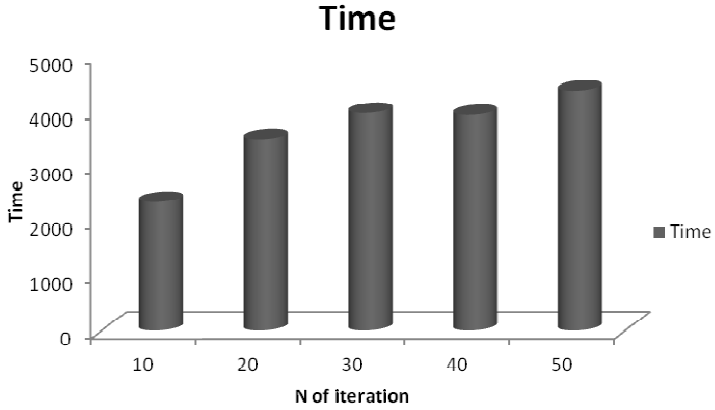


Fig. 8: Execution time for the proposed technique

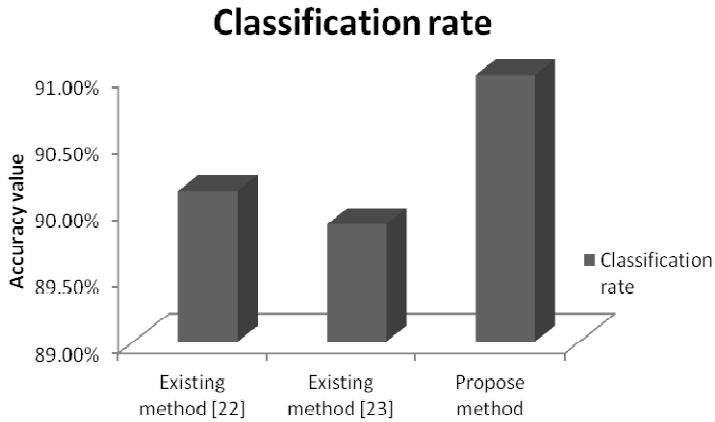


Fig. 9: Comparative analysis of classification rate

**Comparative analysis:** The comparative analysis of our proposed method is compared with the various existing method is tabulated and the result are plotted given below. Table 4 shows the classification accuracy of the proposed method compared with existing method (Moradi and Zulkernine, 2004; Ibrahim, 2010). In existing method (Moradi and Zulkernine, 2004; Ibrahim, 2010). The intrusion is detected with the help of neural network based MLP and RNN with MLP. The method (Moradi and Zulkernine, 2004) achieves 90.13% of accuracy value and Ibrahim (2010) is achieves 89.88% of classification rate. These values are tabulated in the below section.

Table 4 reveals the overall accuracy value of the proposed method is high when compared to other existing method. The graphical representation of the proposed comparative analysis for the classification rate is plotted in Fig. 9.

Table 4: Comparative analysis of classification rate

| Methods | Existing method (Moradi and Zulkernine, 2004) | Existing method (Ibrahim, 2010) | Propose method |
|---|---|---|---|
| Classification rate | 90.13% | 89.88% | 91% |

Table 5: Comparative analysis of execution time

| | | Existing method (Babu *et al*., 2015) | | |
|---|---|---|---|---|
| Methods | Proposed method | Blowfish algorithm | RSA | DES |
| Execution time (ms) | 3615.8 | 35379 | 173514 | 49540 |

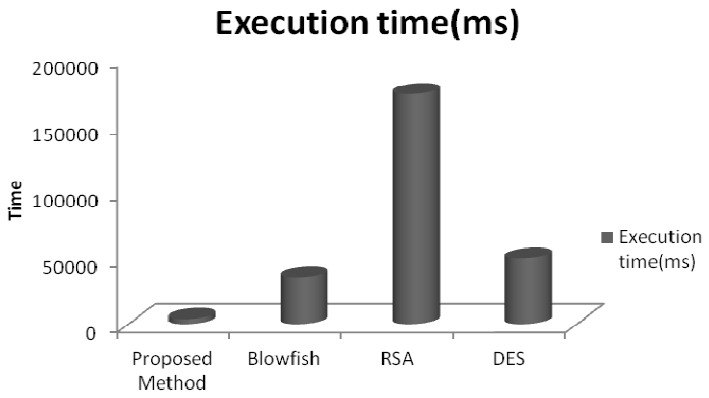


Fig. 10: Comparative analysis of execution time

The overall execution time of the proposed method is less when compared to the existing method. It is tabulated in Table 5 in below section.

Figure 10 reveals the overall execution time for both proposed and existing method; here we consider blowfish algorithm, RSA and DES method. When compared with existing method our method takes minimum time for execution. Here the proposed method takes3615.8ms and existing blowfish takes 35379ms RSA takes 173514ms and DES algorithm takes 49540ms for execution.

## CONCLUSION

In the document, the steganography based safe storage and intrusion recognition technique, is proudly presented. With the mighty assistance of the CloudSim, the epoch-making approach has been elegantly executed. At the outset, the user authentication is examined and an assessment is made regarding the state of the data such as standard or intrusive by means of the artificial neural network. It is followed by the encryption function which is well-discharged by the unique signcryption technique. With an eye on enhancing the safe storage data in the cloud the steganography technique is employed subsequent to the encryption by means of the linguistic steganography approach. Subsequently, the data is subdivided arbitrarily and stockpiled in the cloud. The efficiency in accomplishment of record-breaking technique is appraised, assessed and contrasted with the peer approaches. The cheering outcomes reveal the undeniable fact that the novel method is well-geared to yield superlative safety vis-à-vis and high classification rate that offered by the parallel modern methods.

## REFERENCES

Aumann, Y., Y.Z. Ding and M.O. Rabin, 2002. Everlasting security in the bounded storage model. IEEE T. Inform. Theory, 48(6): 1668-1680.

Babu, A.M., G.A. Ramachandra and M.S. Babu, 2015. Implementation of security in cloud systems based using encryption and steganography. Int. J. Elec. Electron. Comput. Syst., 3(11): 80-84.

Chen, J., X. Wu, S. Zhang, W. Zhang and Y. Niu, 2012. A decentralized approach for implementing identity management in cloud computing. Proceeding of the 2nd IEEE International Conference on Cloud and Green Computing (CGC, 2012). Xiangtan, pp: 770-776.

Emam, A.H.M., 2013. Additional authentication and authorization using registered email-ID for cloud computing. Int. J. Soft Comput. Eng., 3(2): 110-113.

Fernandes, D.A.B., L.F.B. Soares, J.V. Gomes, M.M. Freire and P.R.M. Inácio, 2014. Security issues in cloud environments: A survey. Int. J. Inf. Secur., 13(2): 113-170.

Gonzalez, N., C. Miers, F. Redígolo, M. Simplício, T. Carvalho, M. Näslund and M. Pourzandi, 2012. A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput. Adv. Syst. Appl., 1: 11-18.

Hamlen, K., M. Kantarcioglu, L. Khan and B. Thuraisingham, 2010. Security Issues for Cloud Computing. Int. J. Inf. Secur. Priv., 4(2): 39-51.

Ibrahim, L.M., 2010. Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN). J. Eng. Sci. Technol., 5(4): 457-471.

Kumar, K.V. and M.P. Ramasubash, 2014. Distributed cloud multi tier intrusion detection system. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 4(2): 791-795.

Mathew, S. and A.P. Jose, 2012. Securing cloud from attacks based on intrusion detection system. Int. J. Adv. Res. Comput. Commun. Eng., 1(10): 753-759.

Moghaddam, F.F., S.G. Moghaddam, S. Rouzbeh, S.K. Araghi, N.M. Alibeigi and S.D. Varnosfaderani, 2014. A scalable and efficient user authentication scheme for cloud computing environments. Proceeding of the IEEE Region 10 Symposium. Kuala Lumpur, pp: 508-513.

Moradi, M. and M. Zulkernine, 2004. A neural network based system for intrusion detection and classification of attacks. Proceeding of the IEEE International Conference on Advances in Intelligent Systems Theory and Applications.

Nafi, K.W., T.S. Kar, S.A. Hoque and M.M.A. Hashem, 2012. A newer user authentication, file encryption and distributed server based cloud computing security architecture. Int. J. Adv. Comput. Sci. Appl., 3(10): 181-186.

Patel, A., M. Taghavi, K. Bakhtiyari and J. Celestino Júnior, 2013. An intrusion detection and prevention system in cloud computing: A systematic review. J. Netw. Comput. Appl., 36(1): 25-41.

Rao, R.V. and K. Selvamani, 2015. Data security challenges and its solutions in cloud computing. Proc. Comput. Eng., 48: 204-209.

Sahu, V., B. Dubey and S.M. Ghosh, 2014. An analysis of current security issues and solutions for cloud computing. Int. J. Res. Appl. Sci. Eng. Technol., 2(5): 365-372.

Shaikh, R. and M. Sasikumar, 2015. Trust model for measuring security strength of cloud computing service. Proc. Comput. Sci., 45: 380-389.

Shelke, P.K., S. Sontakke and A.D. Gawande, 2012. Intrusion detection system for cloud computing. Int. J. Sci. Technol. Res., 1(4): 67-71.

Vouk, M.A., 2008. Cloud computing – issues, research and implementations. J. Comput. Inform. Technol., 4: 235-246.

Yassin, A.A., H. Jin, A. Ibrahim and D. Zou, 2012. Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. Proceeding of the 2nd International Conference on Cloud and Green Computing (CGC, 2012), pp: 282-289.

Zhao, F., C. Li and C.F. Liu, 2014. A cloud computing security solution based on fully homomorphic encryption. Proceeding of the 16th International Conference on Advanced Communication Technology. Pyeongchang, pp: 485-488.

Zhu, Y., H. Hu, G.J. Ahn and M. Yu, 2012. Cooperative provable data possession for integrity verification in multicloud storage. IEEE T. Parall. Distr., 23(12): 2231-2244.

Zwattendorfer, B. and A. Tauber, 2012. Secure cloud authentication using eIDs. Proceeding of the IEEE 2nd International Conference on Cloud Computing and Intelligent Systems. Hangzhou, 1: 397-401.