IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 68-73

Hopfield Neural Network Based Cloud Security-State (Hnnbcss) Prediction for Monitoring Data

Dr. N. Revathy[1], Dr. V.Kavitha[2], Mr.T.Guhan[3] Ms.M.Sherlyn Sandhya[4], Ms.R.Gandhi Mathi[5]

[1] *Associate Professor, Department of MCA, Hindusthan College of Arts and Science, Coimbatore.*
[2] *Associate Professor, Department of MCA, Hindusthan College of Arts and Science, Coimbatore.*
[3] *Assistant Professor(Sr.grade), Department of CSE, Sri Ramakrishna Engineering College, Coimbatore.*
[4 & 5] *III MCA, Department of MCA, Hindusthan College of Arts and Science, Coimbatore.*

Abstract: *Security issue of Cloud Computing (CC) is very significant and it is able to prevent the fast improvement of new methods. This work aims in the direction of calculate the security level with numerous huge-scale attributes in CC. A new classifier based Hopfield Neural Network(HNN) is proposed in this paper for predicting the security state of CC, where the Evidential Reasoning(ER) technique is employed in the direction of combine the various system indicators of real CC system and formulate a practical evaluation in the direction of explain the cloud security state. To show the efficiency of the proposed HNNBCSS prediction model is experimented in engineering, the valuation of security condition in the CC platform will be computed by using logs with 100 days. Ten-fold cross validation is performed to verify the security state of the classifier results further successful and satisfactory; where interval determination is used in order verify the accuracy and security of the CC model.*

Keywords: *Cloud Computing (CC), Hopfield Neural Network (HNN), classifier, security, evidential reasoning (ER), logs.*

I. INTRODUCTION

Distributed computing is one more name for Internet computing. CC is a model for allowing on-request and helpful system access to a widespread pool of configurable registering assets with the purpose of is able to be quickly provisioned and absolved with unimportant administration application or professional organization communication [1]. For some it is a worldview that gives computing assets and capacity while for others, it is only an approach to get to programming and information from the cloud.

Distributed computing is mainstream in association and scholarly today since it gives its clients versatility, adaptability and accessibility of information. Likewise CC lessens the cost by empowering the sharing of information to the association. Anyway cloud gives different office and advantages yet at the same time it has a few issues with respect to safe access and capacity of information. A few issues are there identified with cloud security as: merchant secure, multi-occupancy, loss of control, profit interruption, and so forth are a portion of the examination issues in CC [2].

Be that as it may, the consideration of the security of cloud condition is substantially higher than the genuine scale development of cloud framework. Along these lines, the cloud security state is the huge security data in the direction of assurance framework unwavering quality [3], where it can completely mirror the security condition of the CC.

The expectation method might influence an early consciousness of the security to level. All the more significantly, it gives a hypothetical premise to leaders to take measures for maintaining a strategic distance from misfortunes. The early systems most utilized by utilizing sorts of channels and measurable models, for example, Kalman channel [4], particle filter [5], Key Performance Indicators (KPI) approach [6] and Partial Least Squares (PLS) approach [7]. These strategies can be utilized to anticipate and examine as indicated by the framework attributes. Be that as it may, for a complicated CC framework, a sensible numerical model is normally hard to get. Therefore, it is difficult to accomplish a sensible and exact outcome for cloud security state.

II. LITERATURE REVIEW

Wei et al [8] clarified the new risks that face management and of a cloud's image storage. To address those challenges, proposed an image administration framework that controls access to images, tracks the provenance of pictures, and furnishes clients and managers with effective picture channels and scanners that distinguish and repair security violation. Channels and scanners accomplish proficiency by misusing excess

among pictures; an early execution of the framework demonstrates that this approach scales superior to a susceptible approach that treats each picture freely.

Yan et al [9] presents distributed computing and security circumstance, contemplates the fundamental security issues of CC, and concocts a CC security structure which can viably tackle these security issues, and indicates out that lone take care of the security issues, CC can continuously extended, and the application will be increasingly widely.

Rosado et al[10] proposed framework gives a protection criticism to advise clients of the distinctive protection activities connected on their information and to make them mindful of any information breaks or dangers with the purpose of may cause danger to the privacy of their delicate data. Giving a protected security criticism builds the clients' trust in the CC administrations, calms their security concerns, and backings an arrangement of responsible reviewing administrations required to accomplish legitimate consistence and accreditation.

Muñoz et al[11] presents another engineering designed for dynamic security checking and implementation exceptionally intended for CC situations. The arrangement is in this manner an entire one including a three-layered engineering, another dialect for communicating checking rules and a technique in view of the age of a limited state machine to enhance the execution of the observing motor.

Petcu [12] outline and actualize such an administration an initial step is the ID of the fundamental necessities. The scientific categorizations accessible for the fields of CC, observing, security and Service Level Agreements (SLAs) are relied upon to be utilized. This short note proposes a visual scientific categorization expected to serve the plan of a SLA-based Cloud security observing.

Frigault et al [13] proposed a Dynamic Bayesian Networks (DBNs) classifier in the direction of fuse fleeting variables, for instance, the accessibility of adventure codes or fixes. Beginning from the model, additionally examine two cases to show the potential applications. This novel model gives a hypothetical establishment and a reasonable structure for constantly estimating system security in a dynamic situation.

Wei and Qiao [14] proposed a dependability evaluation strategy in view of Evidential Thinking (ER) manage and semi-quantitative data, where another unwavering quality appraisal design incorporating four viewpoints with both quantitative information and subjective learning is built up. Also, the ER administer which has great execution for numerous attribute decision making issue is utilized to incorporate diverse sorts of the properties in evaluation engineering, which can acquire more precise appraisal results. The appraisal consequences of the contextual analysis in an actual CC stage check the viability and the upside of the proposed strategy.

Hussain et al [15] exhibited a novel multilevel characterization model of various security assaults crosswise over various cloud administrations at each layer. It additionally distinguishes assault types and hazard levels related with various cloud administrations at these layers. These risks are positioned as low, medium and high. The force of these hazard levels relies on the situation of cloud layers. The multilevel order show prompts the arrangement of dynamic security contract for each cloud layer that powerfully chooses about security prerequisites for cloud purchaser and provider.

Arvind and Manimegalai [16] proposed a specialist characterizes the client's information into three distinct clusters in particular, low, medium, high. At that point, the information is encoded utilizing Advanced Encryption Standards (AES). Stored information is exchanged to the representative for choosing for reasonable administration specialist. The put away information is then homomorphically encoded which empowers the cloud supplier and cloud client to process the information without the requirement for decryption. Execution investigation shows that proposed technique decreases order time and gives better security and trustworthiness on mobile cloud information.

Dorairaj and Kaliannan [17] recommended a new multilevel security structure in view of cryptography procedures with the purpose of give sufficient security to the characterized information put away in cloud. The proposed security framework adjusts well for cloud condition and is additionally adaptable and more dependent to meet the required level of security of information with various affectability those progressions with business needs and business conditions.

Wei et al [18] proposed a twofold layer strategy for anticipating the security condition of CC framework in view of the conviction run base model, where the evidential thinking (ER) calculation is utilized to combine the different framework pointers of real cloud framework and influence a sensible appraisal to portray the cloud security to state.

III. PROPOSED METHODOLOGY

A new classifier based method is proposed in this paper for predicting the security state of CC depending on the Hopfield Neural Network(HNN), where the Evidential Reasoning(ER) technique is employed in the direction of combine the various system indicators of real CC system and formulate a practical evaluation in the direction of explain the cloud security state.

3.1 Cloud Security State Model

Before anticipating of the security condition of CC framework, it is important to make a far reaching appraisal in light of the present indicators. As per the framework normal for CC, a multi-level indicators structure for the appraisal of CC security framework is set up with the security risk of real framework [19]. It is accepted that Y is the arrangement of the entire pointers for mirroring the real cloud framework, which is characterized as $Y = [y_1(t), \dots, y_p(t)]^T$. In the useful framework, as indicated by the physical normal for framework, the evaluation structure is isolated into three levels, including equipment security, programming security and administration security. When taking the noteworthiness of the entire related properties, the arrangement of y as the screened trademark chose from the arrangement of Y, indicated as y $Y = [y^1(t), \dots, y^L(t)]^T$. L signifies the reordered number of the rescreened pointers, and notes that L≤P. y(t) implies the checking information at the time moment t. The remained indicators are not considered considering for lessening the exertion size of the proposed system.

From the above definition, they chose indicators comprise of three highlights as per encounter. In the level of the equipment security, the adaptability of cloud framework implies with the purpose of the load ability to ensure the typical task of the framework. The fault tolerant rate of cloud stage implies the precarious likelihood that the framework will decrease some factor or the typical task of the framework. These pointers are for the most part hard to be seen by the screen precisely and the genuine incentive to be acquired requirements encounter as a help. In the level of the product security, the indicators of controllability of access terminal and resistance of cloud working framework can be delegated subjective information, which implies that it can't be seen by the perception and got genuine information.

Administration security is one of the imperative markers that evaluate consumer loyalty in CC framework, and its appraisal is additionally needs the specialists' involvement. The difference in its record demonstrations an unequivocal part in evaluating the cloud security condition of the framework. Evidential Reasoning (ER) calculation can well managing the property with the purpose of contains subjective and quantitative information. Thinking about this preferred standpoint, the ER calculation is utilized to incorporate the various pointers, and afterward the in general and precise security condition of framework is able to be acquired. This proposed evaluation structure can be examined from numerous parts of framework security.

In this way, the ER calculation is utilized to meld the indicators of the framework with the goal that it can influence an exhaustive appraisal of cloud security to state. The ER calculation is a Multi-Criteria decision Analysis (MCDA) strategy for increasing quality choice and D-S hypothesis [20]. It can manage clashing confirmation indicators exceptionally well, and has preference to address diverse kinds of data in the perplexing CC framework. After all the screened markers are incorporated, the yield appraisal regard is gotten, of which the range is 0 to 1. The physical meaning of the information can be abridged as takes after:

- The evaluation estimation of the cloud security state is quantized in the genuine number interim of [0,1].
- The higher of the evaluation regard is the greater security dangers got on cloud stage.
- At the point when the security state surpasses the edge extend, the suitable arrangements is expected to ensure that the cloud framework ceaselessly works legitimately.

3.2 Hopfield Neural Network(HNN)

At the point when the evaluation of the security state is finished utilizing ER calculation, next segment is to build the HNN classifier. In this HNN (owner) yield vector creates a secret state level. Another system (cloud client) has been synchronized with the sender side system to create a similar results vector. This result is able to be utilized to shape the mystery state expectation between the sender and user. In this system private key cryptography have been utilized however with some exclusion, no sharing of key happened here i.e. mystery key is never transmitted. Here HNN has been utilized at the two finishes for shaping same privacy enter utilized as a part of expectation state. Sharing of secrecy key isn't required any more with the assistance of HNN. On the off chance that cloud owner sends any message scrambled with the secrecy key client can without much of a stretch decode it with the indistinguishable self-produced secrecy key.

Input*: - Random input vectors for both Hopfield Network.*
Output*: Secret state prediction.*
Method: *Secret key through synchronization of input and output neurons as vectors.*

Step1: *Input two vectors randomly. They are vect_zero and vect_one. Then convert these two vectors into bipolar format using the formulae*
fn-sgn(a)=(a-0.5)×2 . (1)
Step 2: *Multiply vect_zero[i] with vect_zero[j] and vect_one[i] with vect_one[j].*
Then add these two matrices.
Step 3: *Set the diagonal elements of the matrix to zero.*
Step 4: *Take inputs as input vector and the convert them to bipolar form using the above formula (1).*
Step 5: *Formulate the result vector using two recursive loops. The result vector is formulated by*
result_vec[i]=result_vec[i]+input_vect[j]×weight[i][j] . (2)
Step 6: *Apply conditions to limit the result vector.*
a. *If result vector is greater than zero then set result vector as 1.*
b. *If result vector is equal to zero then the result vector is equal to the input vector.*
c. *Else the result vector is -1.*
Step 7: *The current result vector will be set as the new input to the network.*

All equations are numbered and referred to in the text solely by a number enclosed in a round bracket (i.e., (3) reads as "equation 3"). Ensure that any miscellaneous numbering system you use in your paper cannot be confused with a reference [4] or an equation (3) designation.

IV. RESULTS AND DISCUSSION

To show the efficiency of the proposed HNNBCSS prediction model is experimented in engineering, the valuation of security condition in the CC platform will be computed by using logs with 100 days. Ten-fold cross validation is performed to verify the security state of the classifier results further successful and satisfactory; where interval determination is used in order verify the accuracy and security of the CC model. Initially, the genuine security occasions of pointers among 100 days are gathered by the framework Monitor in CC stage. As indicated by the evaluation system proposed over, a few information of these markers are acquired by implication on account of the particular factors that need master's learning heretofore. Likewise, a few information is of the properties with subjective learning that can't be straightforwardly estimated. Along these lines, the first perception information that can be crawled specifically is appeared in Figure 1.

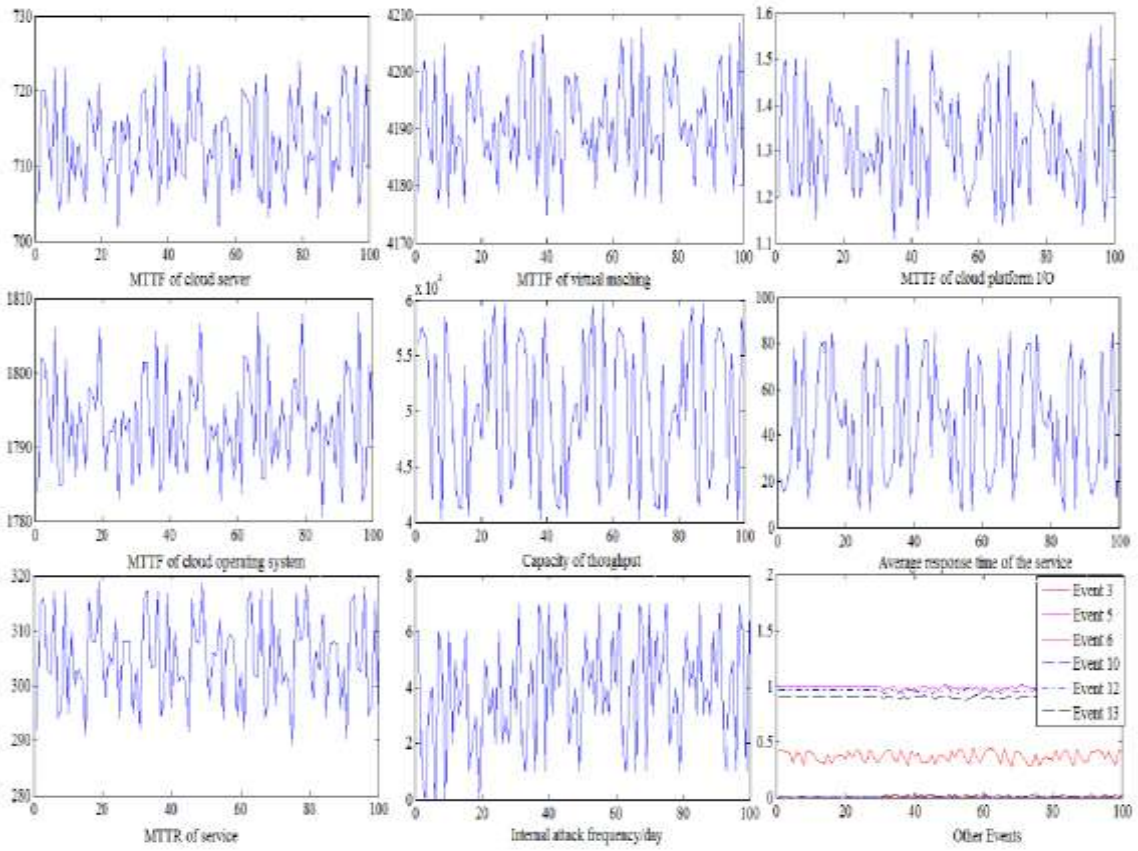
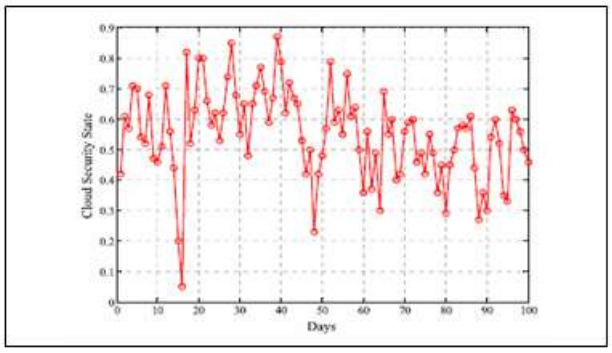


Figure1. Observation data during 100 days

Ten fold cross approval is utilized to make the prescient outcomes more reasonable and valid, and interim estimation is utilized to check the exactness. In this manner, the informational collection of cloud security states in Figure 2 is isolated into 10 sections, where 9 sections are utilized as the preparation information, and 1 section is utilized as the testing information. Four referential focuses are allotted to the security states and the relating ranges are shown in Table 2.



For this situation, the quantized security conditions of a CC stage among 100 days are acquired by utilizing the proposed strategy, as appeared in Figure 2. The estimations of these security states are standardized, and the more noteworthy esteem speaks to more risky state.

The underlying informational index is upheld by Mobike Technology Ltd. in China, whose framework is running on the Tencent Cloud stage. An aggregate of 100 days' logs of server security state were gathered by screen from the framework occasion logs, which recorded the security related occasions.

Before surveying these huge scale pointers, the specific weights of every ascribe should be is set by the specialists. The reference purposes of info parameters are set as Low (L), Medium (M), High (H), Very High (VH), and the limit estimations of each level.

Table1. Mean Square Errors of the prediction methods

Round	1	2	3	4	5	6	7	8	9	10
MM	0.054	0.059	0.0038	0.0012	0.002	.000301	.00012	.000148	.00016	.00022
RBF	0.0160	0.075	0.017	0.015	0.028	0.014	0.029	0.0093	0.019	0.014
BRB	.000164	.00032	.00038	.00036	.000302	.000301	.00012	.00082	.00016	.00022
HNN	.00012	.00027	.00031	.00028	.00025	.00027	.00010	.00073	.00012	.00018

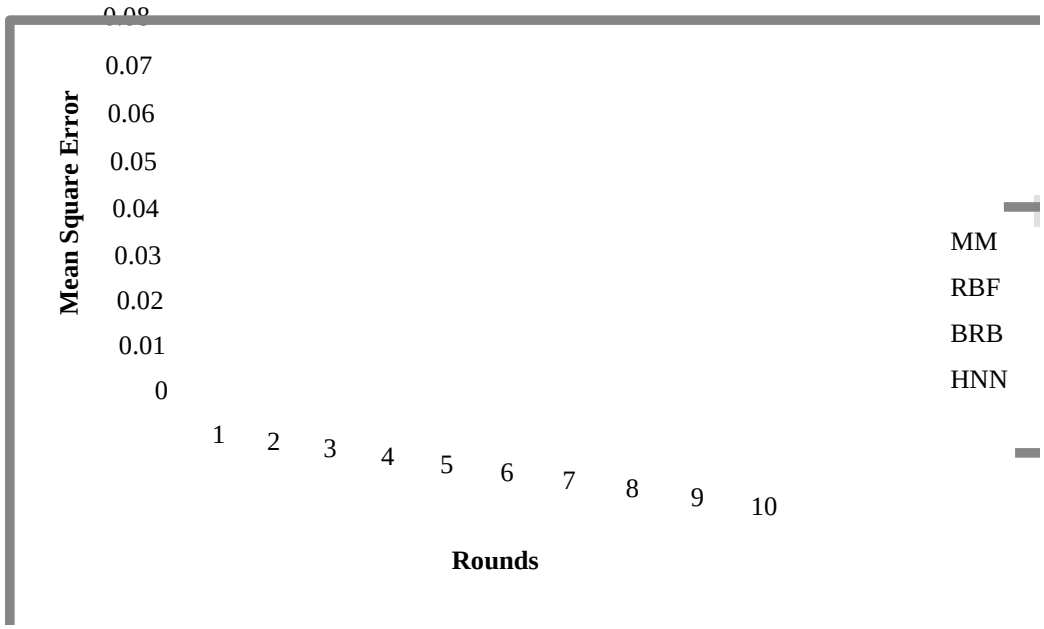


Figure3. Mean Square Errors of the prediction methods

Cross validation experiments are picked in 10 times, and prediction results generated by different models such as Markov forecasting Model (MM), NN with Radical Basis Function (RBF), Belief rule base (BRB) and proposed HNN are listed in Figure 3. The mean square errors of these results are listed in Table 1.

V. CONCLUSION AND FUTURE WORK

A new classifier based method is proposed in this paper for predicting the security state of CC depending on the Hopfield Neural Network(HNN), where the Evidential Reasoning(ER) technique is employed in the direction of combine the various system indicators of real CC system and formulate a practical evaluation in the direction of explain the cloud security state. In this HNN (owner) yield vector creates a secret state level. Another system (cloud client) has been synchronized with the sender side system to create a similar results vector. This result is able to be utilized to shape the mystery state expectation between the sender and user. Evidential Reasoning (ER) calculation can well managing the property with the purpose of contains subjective and quantitative information. The proposed HNNBSS prediction is verified and implemented in the practical environment it concludes that the proposed method in the direction of indicates the potential applications regarding the CC platform. Consequently, additional security factors must be taken addicted to further works consequently with the purpose of the real CC environment be able to be real discussed and implemented.

REFERENCES

[1]. Rawat, S.S. and Sharma, N., 2012. A survey of various techniques to secure cloud storage. *International Journal of Computer Science and Network Security (IJCSNS)*, *12*(3), p.116.

[2]. Behl, A. and Behl, K., 2012, October. An analysis of cloud computing security issues. World Congress on Information and Communication Technologies (WICT), pp. 109-114.

[3]. D. G. Rosado, D. Mellado, E. Fernandez, and M. Piattini, Security Engineering for Cloud Computing: Approaches and Tools. Hershey, PA, USA: IGI Global, 2012, pp. 1-19.

[4]. S. Vakilinia, B. Heidarpour and M. Cheriet, ``Energy efficient resource allocation in cloud computing environments," IEEE Access, vol. 4, pp. 85448557, 2016.

[5]. T. Boukra, ``Identifying new prognostic features for remaining useful life prediction using particle filtering and neuro-fuzzy system predictor," in Proc. IEEE 15th Int. Conf. Environ. Elect. Eng. (EEEIC), 2015, pp. 15331538.

[6]. S. Yin, X. Xie, J. Lam, K. C. Cheung, and H. Gao, ``An improved incremental learning approach for KPI prognosis of dynamic fuel cell system," IEEE Trans. Cybern., vol. 46, no. 12, pp. 31353144, 2016.

[7]. X. Xie, W. Sun, and K. C. Cheung, ``An advanced PLS approach for key performance indicator-related prediction and diagnosis in case of outliers," IEEE Trans. Ind. Electron., vol. 63, no. 4, pp. 25872594, 2016.

[8]. Wei, J., Zhang, X., Ammons, G., Bala, V. and Ning, P., Managing security of virtual machine images in a cloud environment. Proceedings of the ACM workshop on Cloud computing security, pp. 91-96, 2009.

[9]. Yan, X., Zhang, X., Chen, T., Zhao, H. and Li, X., 2011. The research and design of cloud computing security framework. In Advances in Computer, Communication, Control and Automation (pp. 757-763). Springer, Berlin, Heidelberg.

[10]. D. G. Rosado, D. Mellado, E. Fernandez, and M. Piattini, Security Engineering for Cloud Computing: Approaches and Tools. Hershey, PA, USA: IGI Global, 2012, pp. 119.

[11]. A. Muñoz, J. Gonzalez, and A. Maña, ``A performance-oriented monitoring system for security properties in cloud computing applications," Comput. J., vol. 55, no. 8, pp. 979994, 2012.

[12]. D. Petcu, ``A taxonomy for SLA-based monitoring of cloud security," in Proc. IEEE 38th Annu. Comput. Softw. Appl. Conf. (COMPSAC), 2014, pp. 640641.

[13]. M. Frigault, L. Wang, A. Singhal, and S. Jajodia, ``Measuring network security using dynamic Bayesian network," in Proc. 4th ACM Workshop Quality Protection, 2008, pp. 2330.

[14]. H. Wei and P. L. Qiao, ``Reliability assessment of cloud computing platform based on semiquantitative information and evidential reasoning," J. Control Sci. Eng., vol. 2016, Sep. 2016, Art. no. 2670210.

[15]. Hussain, S.A., Fatima, M., Saeed, A., Raza, I. and Shahzad, R.K., 2017. Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), pp.57-65.

[16]. Arvind, K.S. and Manimegalai, R., 2017. Secure data classification using superior naive classifier in agent based mobile cloud computing. Cluster Computing, 20(2), pp.1535-1542.

[17]. Dorairaj, S.D. and Kaliannan, T., 2015. An adaptive multilevel security framework for the data stored in cloud environment. The Scientific World Journal, 2015, pp.1-11.

[18]. Wei, H., Hu, G., Han, X., Qiao, P., Zhou, Z., Feng, Z. and Yin, X., 2017. A New BRB Model for Cloud Security-state Prediction based on the Large-scale Monitoring Data. IEEE Access, pp.11907-11921.

[19]. H. Wei and P. L. Qiao, ``Reliability assessment of cloud computing platform based on semiquantitative information and evidential reasoning," J. Control Sci. Eng., vol. 2016, Sep. 2016, Art. no. 2670210.

[20]. Y. M. Wang, J. B. Yang, D. L. Xu, and K. S. Chin, ``The evidential reasoning approach for multiple attribute decision analysis using interval belief degrees," Eur. J. Oper. Res., vol. 175, no. 1, pp. 3566, 2006.

[21]. Sivanandam, S.N., Deepa, S.N.: Principles of Soft Computing. Wiley-India (2008), Reprint (2012)