Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

Data Sensitivity – Similarity Based Access Control Mechanism for Mobile Cloud Computing

Lakshna Arun[1], T.N. Ravi[2]
[1]Research Scholar, [2]Assistant Professor
[1,2]Department of Computer Science, Periyar E.V.R. College (Affiliated Bharathidasan University), Trichy, Tamilnadu, India

ABSTRACT
Cloud computing is probably the most paradigms that dominate the information and knowledge Technology (IT) industry these days. It gives new services that are cost-effective such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). However, along with these services promising benefits and facilities, there are some challenges connected with utilizing cloud computing such as malicious, abuse of cloud services, cyber-attacks, and data security. Among all security specifications of cloud computing, access control is just one of the fundamental requirements to prevent access that is unauthorized systems and protect the organization's assets. These models may not fulfill cloud's access control requirements although, various access control models and policies have been developed for different environments. Simply because cloud computing has a set that is diverse with various units of security conditions. Also, it has security that is unique such as heterogeneity of security domains, rules, and policies, and multi-tenant hosting. The three-models are proposed to enhance the access control for the sensitive data in this paper. An information gain is used to calculate the data sensitivity. The second data similarity computation, Siamese Neural Network is utilized for taking into consideration the semantic similarity. The model is proposed as SNN with MLP classifier given that the Classification process to categorize the info (or allowing the dataset) predicated on data sensitivity and similarity.

KEYWORDS: Cloud Computing, Data Sensitivity, Access Control, Information Gain, TF-IDF, Siamese Neural Network, MLP Classifier, Multi-Tenant Working

1. INTRODUCTION
Cloud computing is an open standard, that could allow ubiquitous computing and supply on-demand network usage of a distributed group of configurable computing resources. It is Internet-centric and provides each of its resources as services such for example storage, communication, and computation [1]. Cloud computing is a unique combination and innovation technologies. It takes management that is minimal from service providers, remote/global access, dynamic infrastructure and delivers pricing, and usage control. Almost three-fourths of 572 reviewed business leaders suggest that their organizations have adopted or managed, the cloud that is considerably implemented within their organizations and 90% would complete this in the next 3 years [2]. Moreover, those companies that possess substantially cloud that is implemented are expected to cultivate from 13% to 41% over the following 36 months.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

Security is just one of the main concerns and an important barrier to consider computing that is the cloud. Cloud computing may suffer from conventional distributed systems' security attacks such as Distributed Denial-Of-Service (DOS) attack, back door, Man-in-the-Middle attack, insecure API, malicious code (Trojan horses, Viruses), nefarious and abuse utilization of cloud computing and malicious insiders [3][4]. Cloud services could be inaccessible as a result of these attacks and generate negative impact. It is an essential and requires that primary cloud service providers to make certain its services are fully functional and offered by in history. Also, cloud computing has new concerns such as moving resources and storing data when you look at the cloud with probability to call home an additional country, which includes regulations that are different. Also, cloud computing is a shared environment, which utilizes infrastructure that is sharing. Hence, data may face issues like privacy and access that is unauthorized. These problems could get more complex during service when different users use lots of different technologies and investigate possible wide ranges of problems. Furthermore, virtualization gives its issues that are own as data leakage [5][6].

1.1 Access Control in Cloud Computing

An access control system [7] is a group of methods and components that discovers the admission with correct strategies by genuine users about pre-configured access privileges and permissions defined when you look at the access security strategy. The goal of access control system is limiting a person to precisely what s/he must be able to do and protect information from unauthorized access. There was a variety that is wide of, administrative capabilities, technologies, and models, utilized to design and propose access control techniques. Thus, every access control system has its attributes that are own methods and procedures, which are based on either an insurance plan or a collection of policies [8].

Cloud computing is a distributed environment which includes its very own features and characteristics such as on-demand mobility and services. Thus, providers of cloud service require an enhanced access control system for controlling admission to the ability to their resources to monitor precisely who accesses them. They need to cope with random behaviors and dynamics of cloud consumers, diversity, and heterogeneity of services. A background about conventional access control models and why cannot be deployed in the cloud are presented in this section. Also, it demonstrates requirements that are fundamental cloud-based access control models and existing proposed solutions [9][10].

2. RELATED WORKS

Sambrekar, Kuldeep, and Vijay S. Rajpurohit [11] introduced a model efficient and fast Multi-View Access Control (FEMVAC) making use of the Amazon S3 public cloud ecosystem for the department of agriculture. The model reduces storage overhead by implementing a binarization technique over UML/ XML system. The metrics like Computation overhead, Storage overhead, and role computation overhead are evaluated in this paper.

Daoud, Wided Ben, et al., [12] proposed a security model that predicts on collaboration among fog and IoT. This model combines access that is an efficient process connected with a screening strategy to make certain secure collaboration among diverse resources and differing

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

functional parts. The authors introduced an access that is distributed predicated on security resource management framework for fog-IoT networks, and proactive security scheme under low-latency and ultra-trustworthiness constraints. Delay and Network usage features are considered and its performance metrics to the proposed algorithm have been calculated.

Singh, Ashish, and KakaliChatterjee [13] suggested an access control model that is based on the user request. This Trust-Based Access Control Model for Healthcare System (TBACMHS) framework consists of the access control, trust model, and mechanism policies which improve the efficiency and accuracy regarding the system. This access control structure will make sure the only trusted and user that is authorized access the info and resources.

Almarhabi, Khalid [14] examined the condition of the current access control mechanism. It offers secure, lightweight, and an approach that is new on Mandatory Access Control (MAC) mechanism called Arbiter. The proposed architecture is designed to lower the cost and energy to replace the entire operating system to fulfill the necessity of a system that is trusted.

Ma, Hui, et al [15] recommended a practical server-aided revocable fine-grained access control mechanism with the aid of cloud's management. The process of computing, and storage capabilities, do not merely reach effective fine-grained attribute-based access control, but also, actualizes immediate and user revocation that is robust. Also, almost all of the complicated operations in decryption are outsourced into the public cloud, leaving one exponentiation when it comes to users.

Khilar, Pabitr Mohan, Vijay Chaudhari, and Rakesh Ranjan Swain [16] recommended a trust evaluation approach based on the machine approach that is learning the trust values of resources and user. The device learning techniques such as Logistic Regression, Decision, Tree, Naive Bayes, and K-Nearest neighbors are believed as important technique to assess the trust management system when the user looks at work that is proposed.

Riad, Khaled, RafikHamza, and Hongyang Yan [17] suggested a sensitive and energetic access control (SE-AC) procedure for handling the cloud-hosted EHRs and supplying a fine-grained access control even yet in vital circumstances. The proposed procedure assures the confidentiality regarding the patients' data, where only licensed people will have permission to review or edit particular regarding the patients' data. Each EHR information is encrypted because of the authority is empowered to submit into the cloud storage. The user is requesting to have dynamically altering permissions predicated on context attributes and authentication.

Zhao, Yang, et al[18] deals the concern of user revocation for attribute-based cloud data sharing. The authors treat cloud application scenarios as targets and suggested a simple yet effective and storage that is a revocable scheme. The authors utilized the remainder that is Chinese to realize direct user revocation without updating users' secret keys periodically.

3. PROPOSED DATA SENSITIVITY MODEL

In this proposed Data Sensitivity model, the proposed IG method is employed to calculate the info sensitivity based on Data Quality, Usage, and Connectivity. The similarity when you look at the information is calculated simply by using the proposed Siamese Neural Network.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

The proposed sensitivity entropy to determine the info sensitivity predicated on these three factors. Shannon's entropy of a discrete random variable X may be calculated from Equation (1).

$$H(x) = \sum_{i=1}^{n} p(x_i)I(x_i) = -\sum_{i=1}^{n} p(x_i)\log p\,(x_i)$$

When you look at the equation (1), the state x_iProbability mass function (PMF) is given by $p(x_i)$ for a method with n various states. When look at the proposed model, it determine the sensitivity of a provided node when look at the data sensitivity graph (DSG) by computing its influence on the operating system upon eliminating it through the DSG. Affectation of elimination of a node through the DSG is calculated information and it is shown in Equation 6. Information Gain is calculated by finding essential difference between the first system entropy and entropy computed after the elimination of the node.

$$IG(X, a) = H(x) - H(x|a) \quad (2)$$

Equation (2), IG(X, a) shows the information and knowledge gain regarding the system after elimination of node a through the DSG, H(X) represents the first entropy regarding the system and H(X|a) represents the entropy regarding the system after elimination of node a. If the elimination of a node disconnects the network through entropy computation then the biggest connected sub-graph is employed to determine entropy.

Data Usage Detection:

Data Usage PMF in the DSG is computed with the equation (3)

$$p(R_i) = \frac{\sum_{i=1}^{m} C_{U_i}, D_j}{\sum_{j=1}^{k}\sum_{i=1}^{m} C_{U_i}, D_j} \quad (3)$$

A request D_j has been accessed by the users; denominator gives the number of times all the other requests have been accessed by all the users in the given equation (3), numerator represents the number of times. The usage entropy is computed for the nodes that represent requests (D_i) when look at the DSG.

Data Connectivity Detection:

The Connectivity PMF can be computed with the help of equation (4):

$$p(R_i) = \frac{\sum_{j,m,n=1,1,1}^{j,m,n=a,b,c} d_{Ri,j,R_{m,n}}}{\sum_{i,j,m,n=1,1,1,1}^{i,j,m,n=d,a,b,c} d_{Ri,j,R_{m,n}}} \quad (4)$$

A dataset might act as a link point among different datasets. Data items, that are comparable to data items various other datasets, are sensitive while they provide usage of data items, that are potentially sensitive to various other datasets. When you look at the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

equation (4), numerator represents the true wide range of arcs of routes incident to node R_i, and denominator could be the amount of the sum all arcs or paths incident to all the nodes R_i.

Data Quality Detection:

The data quality PMF can be computed by using the equation (5). The greater the info quality higher the info sensitivity. The data quality is represented in the term of missing data and erroneous/corrupted data in this proposed model.

$$p(R_i) = \frac{\frac{\sum_{S_r} co(R_j)}{S_r}}{\sum_{i=1}^{n} \frac{\sum_{S_i} co(R_i)}{S_i}} \quad (5)$$

Data quality is displayed because of the provided equation (5), $co(R_j)$ presents the sheer number of current entries of all of the data items in R_i, S_i provides the final number of entries of all of the data items in R_i, numerator provides the percentage of correct data in one single dataset; denominator provides the final number of ideal data entries in every dataset.

The blended measure of entropy could be the product of all of the three measures that are entropy with equations (3) (4) and (5). The blended measure of entropy is portrayed as the following:

$$H(x_i) = H(C_{u,d_i}).H(d_{r_i}).H(N_{r_i}) \quad (6)$$

When you look at the above equation (6), for dataset D_i, the blended entropy measure is denoted by $H(x_i)$, with the help of equation (7), the entropy measure of data usage is given by $H(C_{u,\,d_i})$. Using equation (8), the data similarity entropy measure is denoted by $H(d_{ri})$. With equation (9), the measure of data quality entropy is denoted by $H(N_{ri})$.

$$H(C_{u,d_i}) = -p(R_i)\log p(R_i) \quad (7)$$

$$H(d_{r_i}) = -p(R_i)\log p(R_i) \quad (8)$$

$$H(N_{r_i}) = -p(R_i)\log p(R_i) \quad (9)$$

The sensitivity score of a dataset is dependent upon the result of the elimination of the dataset when you look at the DSG. This is the difference regarding the amount of the measure of blended entropy of all of the datasets in addition to entropy regarding the dataset.

$$C(x_i) = \sum_{i=1}^{n} H(x_i) - H(x_i) \quad (10)$$

The above equation (10), the dataset i sensitivity is given by $C(x_i)$, the dataset i entropy scores is denoted by $H(x_i)$, the n datasets sum of the entropies is denoted with i, $\sum_{i=1}^{n} H(x_i)$.

Using equation (11), the measure of adjusted sensitivity is computed:

$$C_{adj}(x) = \alpha.C(x) \quad (11)$$

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

The equation (11), α provides a score allocated by an expert of domain. It is weight this is certainly fond of the dataset implying the sensitivity. A dataset with a top $C(x)$ score but that will be not considered to be extremely sensitive because of the expert of the domain will get a low α value. This score varies between 1 and 0.

Characteristics regarding the dataset, which made the expert of domain specify the score, are widely used to train a Siamese Neural Network, which often should determine the score once a dataset that is similarly encountered as time goes by.

4. PROPOSED COMPUTATION OF DATA SIMILARITY WITH SIAMESE NEURAL NETWORK

Siamese neural networks (S2Nets) [19] [20] and their DNN variants, referred to as Deep Structured Semantic Models (DSSMs) were created for text matching. S2Nets are made from a couple of DNNs f_1 and f_2 which maps inputs x and y into corresponding vectors into a standard low-dimensional space that is semantic. Then your similarity of y and x is measured because of the cosine distance regarding the two vectors. The same architecture and even the same parameters, in DSSMs, f_1 and f_2 can be of different architectures depending on x and y while s2Nets assume that f_1 and $f_2$shared.

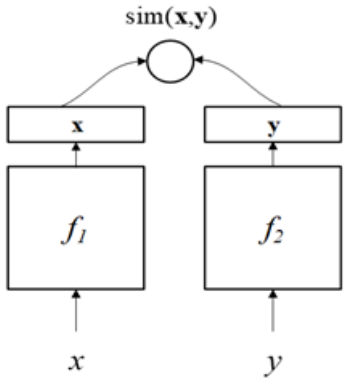

Figure 1: Architecture of Computing the Data Similarity in the dataset

Consider (x,y) could be a document pair for document ranking. The model parameters θ are frequently optimized with a pair-wise rank loss. Undertake document ranking as one example. Choose a query x (this x should be data sensitivity value acquired because of the proposed Data Sensitivity Computation) as well as 2 candidate documents$y^+$and y^-, where y^+ applies to x, $y^-$is certainly not. Let $sim_\theta(x, y)$ end up being the cosine similarity of x and y when you look at the space that is semantic by θ. Working out objective will be to reduce the margin-based loss

$$L(\theta) = [\gamma + sim_\theta(x, y^-) - sim_\theta(x, y^+)]_+$$

Where the margin hyper meter is given by γin $[x]_+ := \max(0, x)$.

4.1 Hybrid Siamese Neural Network Classifier

In this SNN that is hybrid classifier Multi-Layered Perceptron, NN is presented when look at the SNN architecture. So, SNN has two MLP-NN that is the same for classification regarding the dataset predicated on their measure of data sensitivity and similarity. The dataset with maximum data sensitivity and data similarity is given, where for the second block of SNN, the dataset with minimum data sensitivity and similarity is given in the first

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

block of SNN. A 3-layer MLP consisting of input, output, and one hidden layer in this proposed Hybrid SNN classifier.

4.1.1 Three-Layer MLP

An MLP is a NN that is feed-forward, the activation regarding the neurons is propagated layer-wise through the input into the output layer [21]. Also, the activation function of the neurons has got to be differentiable so can update the network parameters through the Back-propagation algorithm. Widely used non-linear activation functions through the sigmoid function together with tanh function (i.e., the hyperbolic tangent function). The tanh function produces both negative and positive output values in contrast with that the sigmoid function allows only positive output values. Since negative values are essential at the proposed Hybrid SNN model, now it have selected tanh function in this model that is proposed. The function that is tanh its derivates is written by:

$$tanh = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}} \qquad (1)$$

$$tanh' = 1 - tanh^{2}(x) \qquad (2)$$

Feed Forward

For almost any considering input sample x_i, accepting its output as a_i. In the step that is first through the input layer towards the hidden layer, using the parameter matrix$W^{(1)}$ in addition to bias vector $b^{(1)}$, the values when look at the hidden layer are calculated as $h_i = tanh\left(W^{(1)}x_i + b^{(1)}\right)$. In the step that is second through the hidden layer into the output layer, using the parameter matrix $W^{(2)}$ in addition to bias vector $b^{(2)}$, the output values are calculated as $a_i = tanh\left(W^{(2)}h_i + b^{(2)}\right)$. Finally, the function that is objective of the MLP classifier is probably the Mean Square Error (MSE) amongst the calculated outputs and their preferred targets from most of the training samples.

$$J = \frac{1}{2N}\sum_{i=1}^{N}(a_i - g_i)^2 \qquad (3)$$

where N could be the wide range of all training that is possible, g_i is the goal vector when it comes to output sample a_i.

Back Propagation

The back-propagation algorithm is employed to update the collection of parameters P:$\{W^{(1)}, b^{(1)}, W^{(2)}, b^{(2)}\}$, using the method of Equation (3), the ith sample gradient is given by

$$\frac{\partial J_i}{\partial P} = (a_i - g_i)^T \frac{\partial a_i}{\partial P} \qquad (4)$$

In addition to differentiate from the output layer, about $z_i^{(2)} = W^{(2)}h_i + b^{(2)}$is,

$$\delta_i^{(2)} = (1 - a_i \odot a_i) \odot (a_i - g_i) \qquad (5)$$

Where the notation $\odot$ indicates element-wise multiplication. Eventually, the differential from the layer that is hidden about$z_i^{(1)} = W^{(1)}x_i + b^{(1)}$is

$$\delta_i^{(1)} = (1 - h_i \odot h_i) \odot \left[\left(W^{(2)}\right)^T \delta_i^{(2)}\right] \qquad (6)$$

In addition to differentials regarding the computation of network parameters are given as:

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

$$\Delta_i W^{(2)} = \delta_i^{(2)} h_i^T \quad (7)$$

$$\Delta_i b^{(2)} = \delta_i^{(2)} \quad (8)$$

$$\Delta_i W^{(1)} = \delta_i^{(1)} X_i^T \quad (9)$$

$$\Delta_i b^{(1)} = \delta_i^{(1)} \quad (10)$$

From then on, the parameters $P: \{W^{(2)}, b^{(2)}, W^{(1)}, b^{(1)}\}$: maybe updated utilizing the appropriate gradient descent function:

$$P = P - \mu \sum_{i=1}^{N} \Delta_i P \quad (11)$$

Where the learning rate is given by μ. The default learning rate is scheduled to 10^{-4} in this model that is proposed.

5. RESULT AND DISCUSSION

In this paper, a dataset is considered from Twitter and obtained by using API. The datasets in varying size from 100 MB to 1000MB is considered for this evaluation of the proposed Data Sensitivity-Similarity based access control method. Running time (in seconds) and Number of Sensitive in the dataset are the performance metrics in this work. The performance of the proposed Data Sensitivity and Similarity-based Access Control (DSSBAC) is compared with the Content-Based Access Control (CBAC) method [22]. Table 1 depicts the running time (in seconds) by the proposed DSSBAC method and the existing CBAC method for the different sizes of the datasets. Figure 2 depicts the graphical representation of the Running Time (in Seconds) for the Proposed DSSBAC method and existing CBAC method for different size of Datasets. From table 1 and figure 2, it is clear that the proposed DSSBAC method takes less running time (in seconds) than the existing CBAC method.

Table 1: Running Time (in Seconds) for the Proposed DSSBAC method and existing CBAC method for different size of Datasets

Size of the Dataset (in MB)	Running Time (in Seconds) by Access Control Methods	
	Proposed DSSBAC method	**Existing CBAC Method**
100	23	41
200	39	65
300	52	88
400	71	102
500	94	132
600	113	159
700	133	188
800	158	203
900	196	269
1000	216	297

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

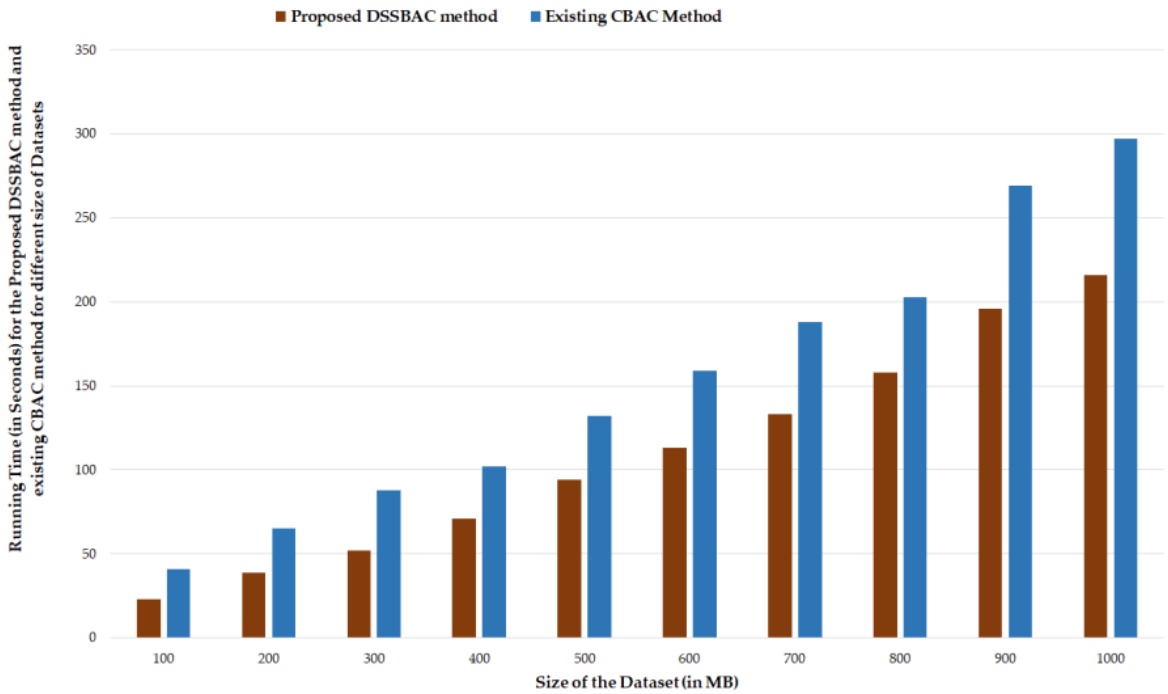

Figure 2: Graphical representation of the Running Time (in Seconds) for the Proposed DSSBAC method and existing CBAC method for different size of Datasets

Table 2 gives the number of sensitive items identified by the proposed DSSBAC method and the existing CBAC method for the different sizes of the datasets. Figure 3 depicts the graphical representation of the Number of sensitive items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets. From table 2 and figure 3, it is clear that the proposed DSSBAC method identifies more sensitive items when compared with the existing CBAC method.

Table 2: Number of sensitive items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets

Size of the Dataset (in MB)	Number of Sensitive Items identified by Access Control Methods	
	Proposed DSSBAC method	**Existing CBAC Method**
100	8	3
200	14	5
300	17	8
400	22	11
500	25	16
600	30	17
700	38	21
800	45	26
900	53	29
1000	65	34

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

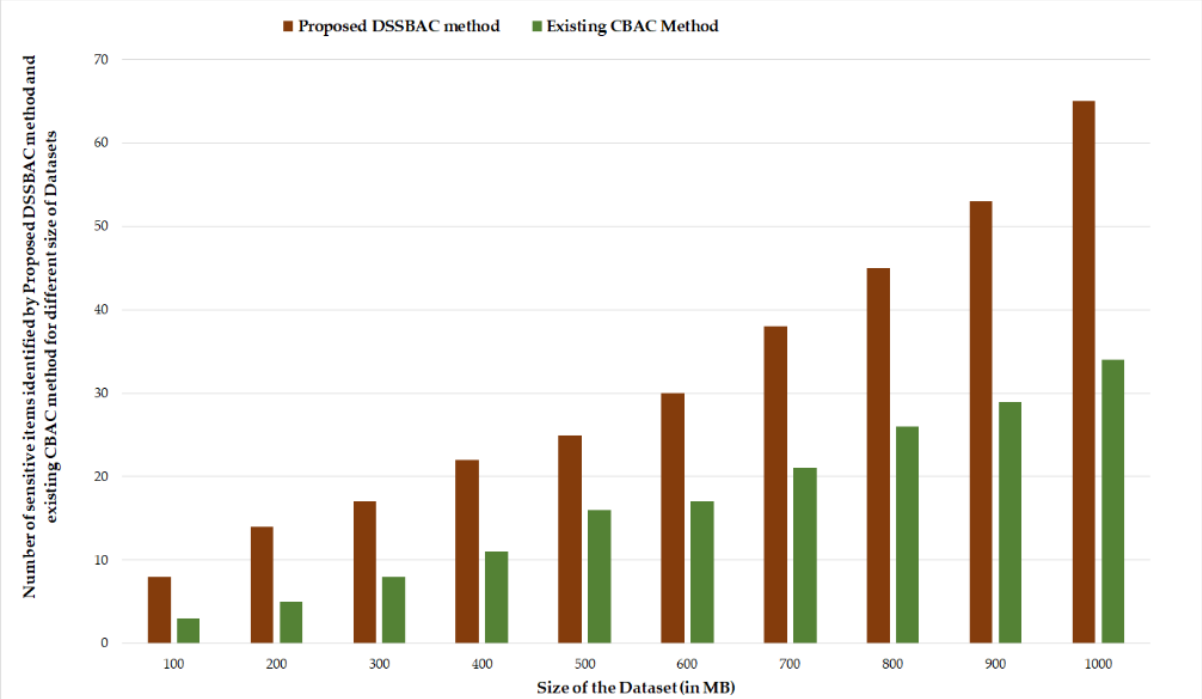

Figure 3: Graphical representation of the Number of sensitive items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets

Table 3 gives the number of similar items identified by the proposed DSSBAC method and the existing CBAC method for the different sizes of the datasets. Figure 4 depicts the graphical representation of the Number of Similar items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets. From table 3 and figure 4, it is clear that the proposed DSSBAC method identifies more similar items when compared with the existing CBAC method.

Table 3: Number of Similar items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets

Size of the Dataset (in MB)	Number of Similar Items identified by Access Control Methods	
	Proposed DSSBAC method	Existing CBAC Method
100	21	11
200	36	18
300	49	21
400	53	26
500	78	34
600	90	47
700	109	52
800	128	63
900	136	79
1000	159	94

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

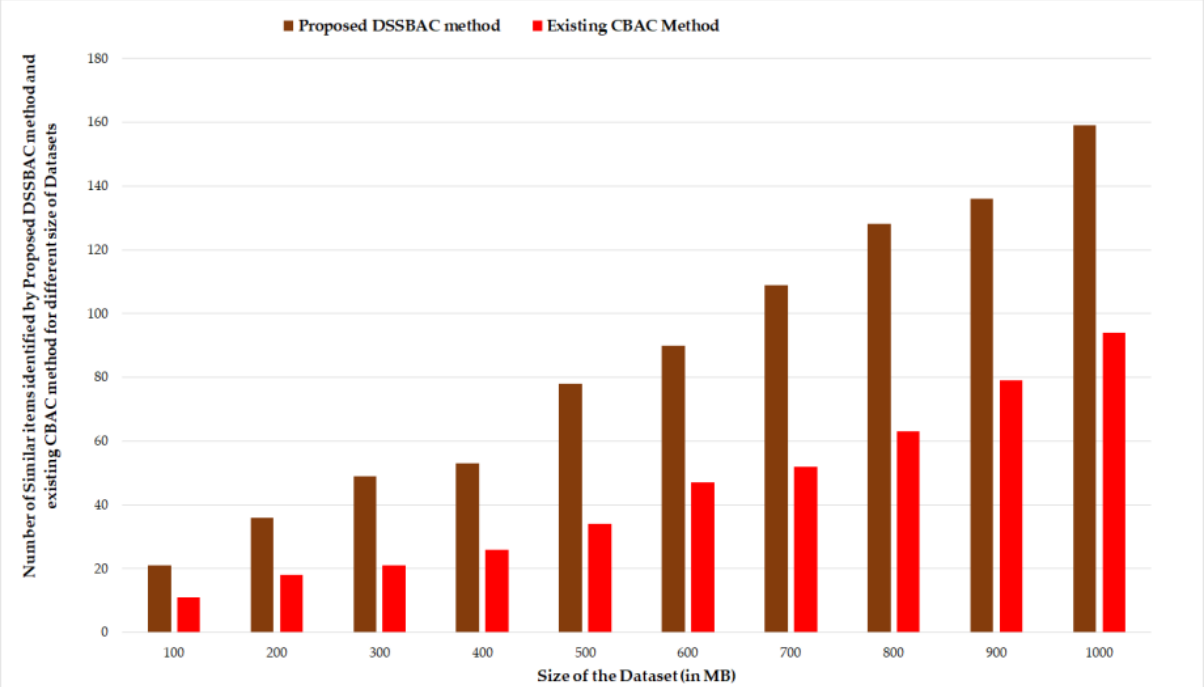

Figure 4: Graphical representation of the Number of Similar items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets

Table 4 depicts the accuracy of the proposed DSSBAC with the proposed Siamese Neural Network classifier. The performance of the proposed Siamese Neural Network classifier with other existing classifiers like Artificial Neural Network, Support Vector Machine with varying dataset size. Figure 5 depicts the graphical representation of the Classification Accuracy obtained by Proposed SNN classifier, ANN, SVM in Pro-posed DSSBAC Method. From table 4 and figure 5, it is clear that the proposed SNN classifier in the classification of dataset gives more accuracy than the ANN and SVM classifiers.

Table 4: Classification Accuracy obtained by Proposed SNN classifier, ANN, SVM in Proposed DSSBAC Method

Size of the Dataset (in MB)	Classification Technique		
	Proposed SNN	**ANN**	**SVM**
100	95.8	78	65
200	95.85	77.8	64.5
300	95.77	77	63.9
400	95.72	76.6	63.2
500	95.65	76.8	63.1
600	95.55	75.54	62.96
700	95.42	75.24	62.84
800	95.31	74.98	62.75
900	95.03	74.82	62.53
1000	94.92	74.77	62.31

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6594 - 6607
Received 16 February 2021; Accepted 08 March 2021.

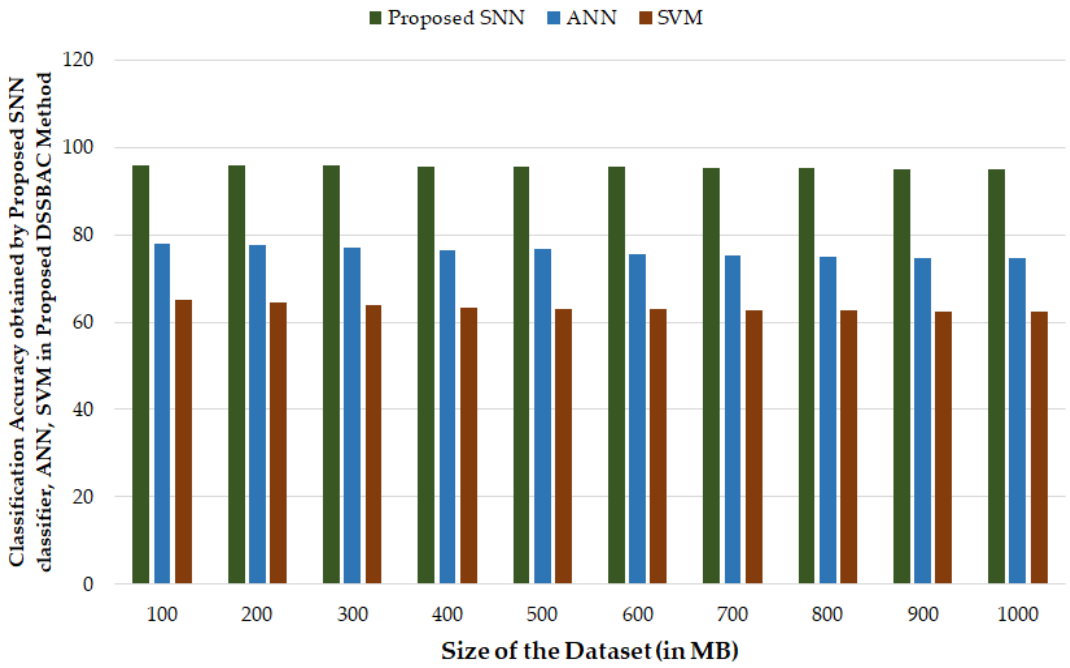

Figure 5: Graphical representation of the Classification Accuracy obtained by Proposed SNN classifier, ANN, SVM in Proposed DSSBAC Method

6. CONCLUSION

In this paper, Data Sensitivity-Similarity based Access Control mechanism is proposed to ensure the security of the sensitive data. In this paper, the proposed DSSBAC mechanism uses three models viz data sensitivity computation based on Information Gain, Data Similarity computation with Siamese Neural Network, and Proposed SNN classifier (which has MLP in the twin layer of SNN). From the result analysis, it is clear that the proposed DSSBAC method performs in less time, and it detected the more sensitive items than the existing CBAC method. Using the proposed SNN classifier model, the classification accuracy obtained is more than the using ANN and SVM classifier in the classification of the dataset which is again based on data sensitivity and data similarity.

REFERENCES

[1] Kalaiprasath, R., R. Elankavi, and Dr. R. Udayakumar. "Cloud.security and compliance-A semantic approach in the end to end security." *International Journal Of Mechanical Engineering And Technology (Ijmet)* 8.5 (2017): 987-994.

[2] Nakagawa, Ikuo, and Shinji Shimojo. "IoT agent platform mechanism with transparent cloud computing framework for improving IoT security." *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*.Vol. 2.IEEE, 2017.

[3] Bonguet, Adrien, and Martine Bellaiche. "A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing." *Future Internet* 9.3 (2017): 43.

[4] Imran, Muhammad, et al. "Toward an optimal solution against denial of service attacks in software defined networks." *Future Generation Computer Systems* 92 (2019): 444-453.

[5] Yadav, Arun Kumar, Rajendra Kumar Bharti, and Ram Shringar Raw. "Security Solution to Prevent Data Leakage Over Multitenant Cloud Infrastructure." *International Journal of Pure and Applied Mathematics* 118.7 (2018): 269-276.

[6] Kirar, Anshu, Arun Kumar Yadav, and SupriyaMaheswari. "An efficient architecture and algorithm to prevent data leakage in Cloud Computing using multi-tier security approach." *2016 International Conference System Modeling& Advancement in Research Trends (SMART)*.IEEE, 2016.

[7] Almarhabi, Khalid. "Arbiter: a lightweight, secured and enhanced access control mechanism for cloud computing." *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*.IEEE, 2019.

[8] Xu, Yang, et al. "An efficient privacy-enhanced attribute-based access control mechanism." *Concurrency and Computation: Practice and Experience* 32.5 (2020): e5556.

[9] Sun, Panjun. "Research on cloud computing service based on trust access control." *International Journal of Engineering Business Management* 12 (2020): 1847979019897444.

[10] Sookhak, Mehdi, et al. "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues." *Future Generation Computer Systems* 72 (2017): 273-287.

[11] Sambrekar, Kuldeep, and Vijay S. Rajpurohit. "Fast and efficient multiview access control mechanism for cloud-based agriculture storage management system." *International Journal of Cloud Applications and Computing (IJCAC)* 9.1 (2019): 33-49.

[12] Daoud, Wided Ben, et al. "TACRM: trust access control and resource management mechanism in fog computing." *Human-centric Computing and Information Sciences* 9.1 (2019): 28.

[13] Singh, Ashish, and KakaliChatterjee. "Trust based access control model for securing electronic healthcare system." *Journal of Ambient Intelligence and Humanized Computing* 10.11 (2019): 4547-4565.

[14] Almarhabi, Khalid. "Arbiter: a lightweight, secured and enhanced access control mechanism for cloud computing." *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*.IEEE, 2019.

[15] Ma, Hui, et al. "Server-Aided Fine-Grained Access Control Mechanism with Robust Revocation in Cloud Computing." *IEEE Transactions on Services Computing* (2019).

[16] Khilar, Pabitr Mohan, Vijay Chaudhari, and Rakesh Ranjan Swain. "Trust-based access control in cloud computing using machine learning." *Cloud Computing for Geospatial Big Data Analytics*.Springer, Cham, 2019.55-79.

[17] Riad, Khaled, RafikHamza, and Hongyang Yan. "Sensitive and energetic IoT access control for managing cloud electronic health records." *IEEE Access* 7 (2019): 86384-86393.

[18] Zhao, Yang, et al. "An efficient and revocable storage CP-ABE scheme in the cloud computing." *Computing* 101.8 (2019): 1041-1065.

[19] Vinayakumar, R., and K. P. Soman. "Siamese neural network architecture for homoglyph attacks detection." *ICT Express* 6.1 (2020): 16-19.

[20] Gabrielli, Leonardo, et al. "Processing Acoustic Data with Siamese Neural Networks for Enhanced Road Roughness Classification." *2019 International Joint Conference on Neural Networks (IJCNN)*.IEEE, 2019.

[21] Driss, S. Ben, et al. "A comparison study between MLP and convolutional neural network models for character recognition." *Real-Time Image and Video Processing 2017*.Vol. 10223.International Society for Optics and Photonics, 2017.

[22] Zeng, Wenrong, Yuhao Yang, and Bo Luo. "Content-Based Access Control: Use data content to assist access control for large-scale content-centric databases." In Big Data (Big Data), 2014 IEEE International Conference on, pp. 701-710, 2014.