Establishing Intent Groups for the Intent-Based Access Control Framework

Pattabhi Mary Jyosthna[1] and Konala Thammi Reddy[2]

[1]Department of Computer Science and Engineering, GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, India
[2]Department of Computer Science and Engineering, GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, India

Abstract

Access control models help the organizations in restricting access to Information Systems in order to minimize internal and external threats. When organizations are required to form cross functional teams and allow them to access the sensitive information, the traditional access control model like Role Based Access Control (RBAC) are inadequate to mitigate internal threats. In this paper, a unique access control approach called Intent Based Access Control (IBAC) is introduced to secure data sharing with cross functional teams. In IBAC, a group of interdisciplinary individuals is formed to achieve the organization's intent. It uses the Weighted Sum Model (WSM) which is one of the Multi Criterion Decision Making (MCDM) approach to choose the best individuals for the Intent Group based on their capabilities, finds their priority level using Bayesian inference model, and it also evaluates their work deviation score using N-Median Outlier Detection (NMOD) method for selecting them to the Intent Group. An employee whose capability score is sufficient as per the intent requirement, the deviation score is less than the role threshold value, priority level is High or Medium, and does not belong to active intents are selected for the Intent Group. The access permissions are assigned to the Intent Group to access the required resources instead of assigning them to the individual user as in RBAC.

Keywords

Internal threats, Access control model, Role Based Access Control, Organization’s intent, Weighted Sum Model

1. Introduction

Organization’s Information Systems are highly prone to internal attacks as they are required to be shared with the employees of the same branch or different branch of the organization [1]. Organizations can use access control models to secure their information systems, resources, and assets against cyber-attacks, data breaches, and security legislation violations. Access control rules are personalized to the company in order to meet the needs of the business. Resources in the academic system, for example, differ from those in the health sector, from those in the financial sector, from those in industrial enterprises, and so on. However, the method of allocating access credentials is the same. If we consider the well-known Role Based Access Control (RBAC) model [2] for the aforementioned organizations, users are associated with roles and access rights are associated with the roles in the organizations and those access rights defined for that specific organization based on the security levels of the resources and user roles.

H. Wang, Y. Zhang, and J. Cao in [3] used the RBAC model to build a secure framework for information sharing in virtual university environment. E. O. Boadu and G. K. Armah in [4] applied the RBAC model to the Hospital Management System for reducing the administration burden and to control the accessing of patient records and other hospital resources based on the defined roles and their permissions. Researchers in [5] considered domain knowledge and purpose of requesting user for accessing the patient record as constraints in current RBAC model to privacy of patient records. B. Tay and A. Mourad in [6] added ML techniques to assess the RBAC access policies enforces in the system, assess the authorization levels based on the user performance and work history to update the policies dynamically. All types of organizations are using the existing RBAC model with some added functionalities depending on their organization’s requirements. The other general requirement of organizations is multi-disciplinary teams.

In general, the employees in an organization must work for the expansion of the organization's reputation in addition to their usual job functions. Each task will be regarded as an organization's objective or intent. A group of interdisciplinary individuals need to be formed to achieve that organization's goal/intent. For example, if we consider a manufacturing company, in addition to job functionalities such as production, marketing, finance, operations, and so on, employees should work in interdepartmental groups to achieve organizational goals such as new innovations for Research and Development (R&D), organizational rankings, accreditations, and so on. For these kinds of cross-functional teams, trust is a crucial challenge [7] for sharing the Information Systems.

This research is mainly focusing on the following:

- Find the priority level of the employee using Bayesian inference model
- Calculate the deviation score of the employee using N-MOD algorithm
- Determine the capability score of the employee using WSM model
- To form the Intent Groups and Compare IBAC model with other access control models

The rest of the paper is organized as follows. Section 2 describes the existing access control models. Section 3 explains the elements and their functionalities in the proposed method. Section 4 discusses the results obtained from each method applied on the dataset. Section 4 summarizes the concept of Intent Based Access Control model.

2. Review on Existing Access Control Models

Researchers on Access Control Models are making many choices to the organizations for choosing suitable access control models for their environments.

S. Oh and S. Park in [8] separated the job functions called tasks from the job role. So that the user in a particular job role can be assigned to a particular job function (Task). A pair of information resources (Objects) and access permissions are assigned to tasks instead of assigning to a job role. L. Zhou et al. in [9] use the RBAC model for securing the access of their data which is stored in cloud data centers. They define the trust models to enforce secure access policies on data at cloud data centers. These trust models help to evaluate trust on roles and on members of a role. Q. Liu et al. in [10] develops an access control model based on RBAC for Manufacturing Internet of Things. MIoT is a collaborative environment for the process of resource sharing. M. Uddin et al. in [11] proposed Authorizing Workflow Task Role-Based Access Control (AW-TRBAC) that grants access permissions to the user who carries the task at that particular instance of time in organizational workflow. They defined the task as a unit of business work to carry the business workflow. Tasks are assigned based on the user's fundamental job role. It also integrates the dynamic Segregation of Duties (DSoD). B. Tay and A. Mourad in [12] provides access to information resources by semantic roles. Here the roles have certain business task and considered the role-task assignment and task-permission assignment for data access.

Researchers also incorporated business constraints and environment constraints in RBAC model. N. Baracaldo, A. Masoumzadeh, and J. Joshi in [13] proposed a framework for secure interoperation between the domains along with SSoD, DSoD and temporal constraints of internal domain policy. Researchers in [14] introduced temporal constraints, periodicity constraints and duration constraints on roles, user-role assignment and role-permission assignment (components of RBAC) in regular RBAC model. G. Milosavljević et al. in [15] proposed an enhancement to the constraints in RBAC with context-sensitive constraints for workflow systems. They defined context conditions as dynamic in nature and they have time duration depending on the constraint type. J. Park et al. in [16] proposed a framework for activity control in collaborative environment. Activity means, resource usage activity, service and control activity.

When all the above researchers focusing on the enhancements to the existing RBAC model like tasks, constrains and context. A. Roy et al. in [17] has focused on the employee assignment to the functional roles in the business. Here, the employees are assigned based on their capabilities and their business constraints. Employee capability will be decided based on their qualification to handle the business role functions. It also considered cardinality constraints for role assignment. They did employee assignment as 1-0 linear programming. Few researchers have addressed the possibility of insider threat in the classical RBAC models due to excess permissions in role hierarchy. S. Mowla et al. in [18] uses genetic algorithm to automate the assignment of access permissions based on their roles. It also evaluates the trustworthiness of an employee in terms of other user's feedback about that user. Mean value of the total number of feedbacks is considered as the threshold value. J. Shahen et al. in [19] has introduced a safety analysis to Temporal RBAC (T-RBAC) model. A security administrator can analyse the consequences of issuing grant permissions to a semi trusted user.

A. S. Salehi et al. in [20] proposed an access control framework for cross-domain teams to satisfy the requirements in healthcare environment. The base access control model they have used is Attribute Based Access Control (ABAC) model. It treats a domain as one healthcare domain not the functionalities within a single domain. S. Mathrani and B. Edwards in [21] described that, the cross-functional teams are helpful for the organizations to develop new products and to go forward in new innovations. In our context, these cross-functional teams are forming to achieve the organizations intents. New product development is also one of the organization's intents. Trust is a major concern for these cross-functional teams as the members are from different domain groups. None of the above works are addressed the access control models for cross-functional teams. The user's work behaviour in their job roles need to be analysed and their knowledge capability need to be calculated before selecting them for cross-functional teams. In RBAC, there is no fine-grained control over individual users in a certain job role. As a result, before selecting an employee for cross-functional team, employees in their job role must be evaluated by the role manager based on their work behaviour as in [22]. The remaining process of employee selection for cross-functional teams is discussed in the next section.

3. Establish Intent Based Groups

The proposed IBAC supports businesses in reducing risks to their reputation and information systems. A group of multidisciplinary individuals is necessary to fulfil the organization's intent, and the resources required to achieve that intent are allotted to the group rather than to the individual. The admin point of the IBAC architecture is where an organization's goals/intents are defined. Every organization's goal/intent may include achieving a national ranking, obtaining accreditation, obtaining projects, obtaining international partnerships, and so on. These are considered as intent requests since they need a group of personnel to complete. This request will be sent to the Configuration agent which is responsible to find the right people for a certain intent.

The Configuration agent maintains a queue to hold the incoming requests. It also maintains the user information database to select the people for the intent. Configuration agent sends the received request to the “Analyse the request” phase for understanding the needs of the intent request. Configuration agent selects the employees based on the intent requirements. The flow of activities for Intent Group creation is shown in Fig.1.

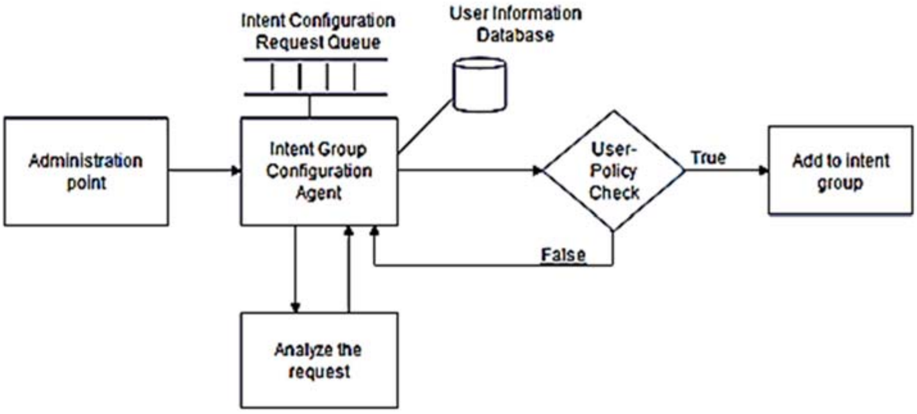

Intent Configuration Request Queue
User Information Database
Administration point
Intent Group Configuration Agent
User-Policy Check
True
Add to intent group
False
Analyze the request

Figure 1. Work flow diagram to from Intent Groups

2.1. Analyse the Intent Request

Organization’s intent request can be represented as a declarative statement. Keywords from these statements are extracted using Natural Language Processing (NLP) techniques [23]. Configuration agent use these keywords for extracting data from the User Information Database (UID). User Information Database contains the attributes and capabilities of employees of a particular organization.

User information Database contains all employees’ details including priority levels which are predicted based on the analysis of insider threat data of the organization, capability score of the employee which are calculated using WSM model and the deviation score of the employee which are calculated using NMOD algorithm.

2.2. Predict the employee priority level

The priority levels of the employee will be predicted by analysing the past insider threat data of the organization using Bayesian inference model. Bayesian inference model is performed based on the Bayes theorem. It produces the value based on the probability rule. Probability value can be treated as the degree of belief. Bayes theorem is as below [24]:

$$P(H/X) = \frac{P(X/H)P(H)}{P(X)} \text{ -------------- (1)}$$

Where,

H is the hypothesis about the employee to be an insider

X is the set of attributes about the employee.

$$X = \{\, hours\ spent, resource\ usage, income, age, no.of\ roles, gender\,\}$$

$P(H)$ is the prior belief on the assumed hypothesis and it is independent on the data

$P(X/H)$ is the probability of likelihood of the employee with attributes X given hypothesis

$P(X)$ is the normalizing constant

$P(H/X)$ is the posterior probability of the hypothesis given the employee attributes

The equation (1) can be written as below equation (2) when the $P(X)$ is considered as the normalizing constant. The posterior probability can be calculated as the product of likelihood and prior beliefs.

$P(H/X) \propto P(X/H)P(H)$ --------------- (2)

If the variables of X are continuous values, then the probability of that variable given hypothesis is calculated as the Probability Density Function (PDF) based on their mean (**μ**) and standard deviation (**σ**). The equation (3) for PDF is mentioned below:

$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}$ ---------------(3)

The probability of the both null hypothesis and alternate hypothesis will be calculated using equation (1) and (3). The hypothesis which yields highest probability will be true.

The proposed model defines 3 different priority levels based on their degree of belief obtained from the Bayesian inference model. Which is shown in the Table. I.

In this level LOW indicates least priority to access the data and level HIGH indicates highest priority to access the data. Based on the requirement MEDIUM level user can have the access rights on data.

Table. I. Priority levels based on the probability value

Level of Priority	**Probability Range (P)**
LOW	0.7 ≥ P ≤ 1
MEDIUM	0.4 ≥ P ≤ 0.6
HIGH	0 ≥ P ≤ 0.3

2.3. Calculate capability score of the employees

The process of user selection from the extracted list of employees will be done by using WSM which is one of the MCDM models [25]. Weights of each capability are decided by the configuration agent and construct a weighted matrix for those employees as shown in the Fig.2. sum of weights of all capabilities of an employee will decide his/her ranks to select for the intent group. This process includes three steps. One is normalization to scale all capabilities and values to the same unit for each alternative (Employees in this case). Second is to perform a product of each normalized value of an alternative with its corresponding weight of the criteria. Third is to calculate the row wise sum of each alternative to decide the rank of each alternative. The process will start by arranging the capabilities of the alternatives in descending order according to their assigned weights.

The values of non-beneficial capability are normalized as follows:

$N_{ij} = \frac{min(C_j)}{E_i(C_j)}$, Where i= 1, 2, 3, …. n and j= 1, 2, 3, …. m --------------------------(4)

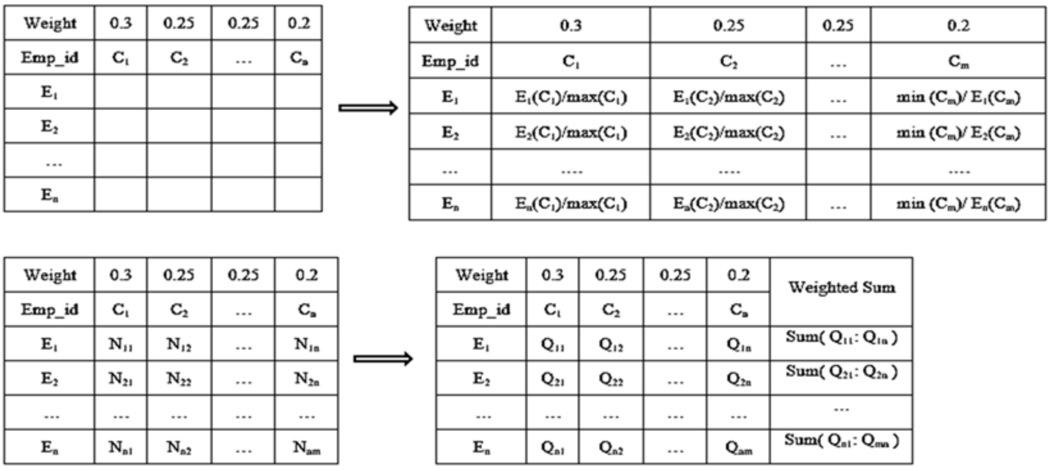
The remaining beneficial capabilities are normalized as follows:

$N_{ij} = \frac{E_i(C_j)}{max(C_j)}$, Where i= 1, 2, 3, …. n and j= 1, 2, 3, …. m --------------------------(5)

The weight of the capability is calculated as follows:

$Q_{ij} = Product\left(N_{ij},\ Weight(C_j)\right)$ ---(6)

The weighted sum of an employee is the sum of weights of all capabilities of that employee. The ranking process will be done in such a way that the list of alternatives is sorted in descending order according to their weighted sum.



Weight	0.3	0.25	0.25	0.2
Emp_id	C_1	C_2	…	C_n
E_1				
E_2				
…				
E_n				

Weight	0.3	0.25	0.25	0.2
Emp_id	C_1	C_2	…	C_m
E_1	$E_1(C_1)/\max(C_1)$	$E_1(C_2)/\max(C_2)$	…	$\min(C_m)/E_1(C_m)$
E_2	$E_2(C_1)/\max(C_1)$	$E_2(C_2)/\max(C_2)$	…	$\min(C_m)/E_2(C_m)$
…	….	….		….
E_n	$E_n(C_1)/\max(C_1)$	$E_n(C_2)/\max(C_2)$	…	$\min(C_m)/E_n(C_m)$

Weight	0.3	0.25	0.25	0.2
Emp_id	C_1	C_2	…	C_n
E_1	N_{11}	N_{12}	…	N_{1n}
E_2	N_{21}	N_{22}	…	N_{2n}
…	…	…	…	…
E_n	N_{n1}	N_{n2}	…	N_{am}

Weight	0.3	0.25	0.25	0.2	Weighted Sum
Emp_id	C_1	C_2	…	C_n	
E_1	Q_{11}	Q_{12}	…	Q_{1n}	Sum(Q_{11}: Q_{1n})
E_2	Q_{21}	Q_{22}	…	Q_{2n}	Sum(Q_{21}: Q_{2n})
…	…	…	…	…	…
E_n	Q_{n1}	Q_{n2}	…	Q_{am}	Sum(Q_{n1}: Q_{mn})

Figure 2. Process to calculate the capability score of the user

2.4. Deviation score of an employee

Every user/employee in an organization is assigned a job position in order to work for the company. Each job position is associated with resources that must be accessed by users/employees of that work function. The work behaviour of an employee in that role group is computed using the N-Median Outlier detection approach [26], and that work behaviour is referred to as the employee's deviation score. Deviation score of an employee is calculated as follows:

The Euclidean distance between an employee (E_{11}, E_{12}) and every employee in its associated job group, say (N_{11}, N_{12}), represents the difference in their work behaviour.

$$E_{dist} = \sqrt{(E_{11} - N_{11})^2 + (E_{12} - N_{12})^2} \text{--} (7)$$

Median distance of that employee to all other n related employees is calculated. where n is the total number of employees under the same job role group. This Median distance is the work deviation score of that employee

Because all users of a role group should behave similarly or exhibit comparable work behaviour. As a result, an employee's deviation score indicates how different his or her work is from that of others in the same position group. This deviation score is one of the criteria used to choose an employee or user for the Intent Group.

2.5. Processing steps in Intent Group creation

An employee is added to the Intent Group if they have a highest capability score in their corresponding role group, a lower deviation score based on their role's threshold value, and do not belong to any of the current Intent Groups. Adding a member to the intent group means allocating access permissions to that member for accessing the required information resources to achieve that intent. The process of creating Intent Group and their access permissions is represented in the control flow graph as shown in Fig.3.

1) Admin sends an intent request to the configuration Agent to create an intent group for achieving that intent and allocate the required resources to that group.

2) This Intent Group creation request is initiated by triggering create_intent_group (req) function. This function subsequently calls Employee_capabilty() function to find the capability score of the employees and then find the suitable employees for the intent group. It then retrieves the employees from the User Information database.

3) The configuration Agent then intimates to work_behaviour to check the deviation score of the selected users by calling emp_dev_score() function.

4) Once they are verified, retrieved from deviation_score database and then get back to Config_Agent with the deviation score of the employees.

5) Selects employees from the User_information database based on their retrieved deviation score.

6) The selected employees are assigned to Intent_Group by calling Assign_IG() function, if the employee is not belonging to any of the active intent group

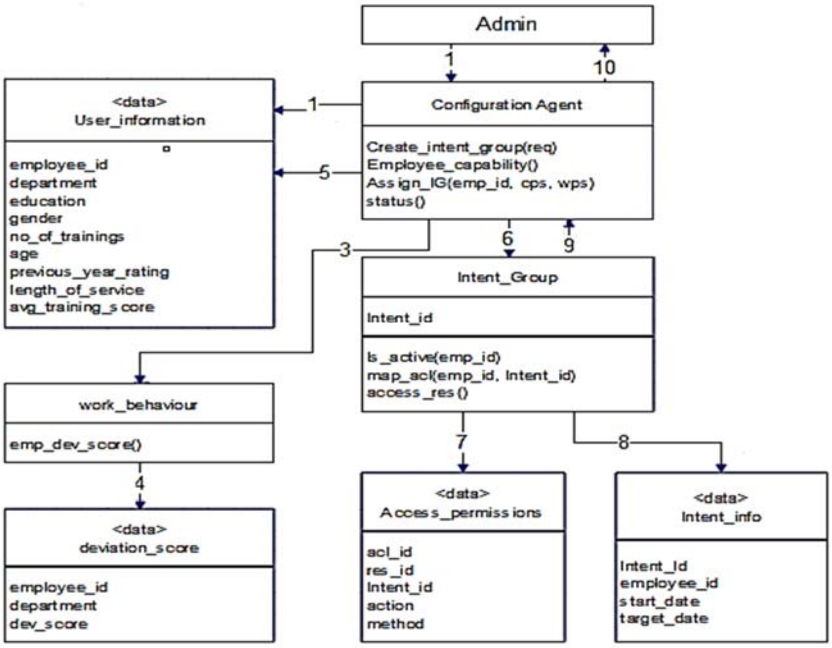


Figure 3. Control Flow Diagram of creating Intent Groups

7) The assigned employee will be mapped with the required resources and access permissions which are already mapped to that particular Intent Group.

8) After successful assignment to Intent group, the employee details will be added to the intent_info database

9) The successful assignment of employees to the Intent group is intimated to configuration Agent.

10) Configuration Agent notify the admin with the finish command after getting the status from the Intent_group for their successful mapping of employees with the Intent Group.

The list of Employees, deviation score, Intent Groups and Permissions are taken as database entities and they are identified with their attributes. The description about each entity, Relationships between entities and their attributes are mentioned in Table.2. An employee is identified with his/her attributes and they are selected to work for achieving the intent of the organization. Each intent group is managed by the single manager and he/she is also an employee. The mapping is one-to-one as an employee manages exactly one Intent Group and an Intent Group is managed by exactly one manager.

Table 2. Details about the database entities in the Intent Based Access Control System

ENTITIES	DESCRIPTION
User_Information	People who work for the organization and access the resources to fulfil their tasks
Intent_Info	Group of employees allotted to achieve the particular intent of the organization
deviation_score	Each role of the organization contains a group of employees and their work behaviour is maintained as deviation score
Access_Permissions	List of access rights and their associated resources

Intent Groups are mapped to required data resources which are already mapped with the defined access rights. Intent Group and Resource mapping is many-to-many as an intent requires multiple resources to access and a resource may be required by many Intent Groups.

3. Results and Discussion

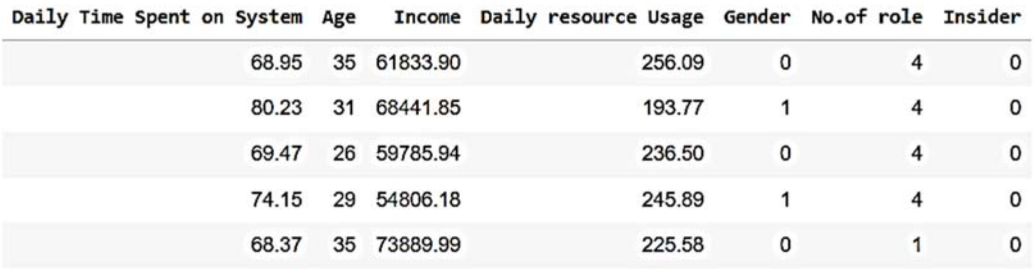
Admin can send the Intent request in the form of declarative statements. In Manufacturing organizations, the regular functional roles are Production, HR, Finance, Technology, Procurement, Marketing & Sales and so on. Organizations use Role Based Access Control (RBAC) model for providing access to the resources to perform their regular job role. Organizations are adopting to form cross-functional teams to achieve a common goal of the organization. Suppose if the manufacturing company wants to form a team made up of individuals from finance, Technology, and sales&marketing to devise a solution to develop a new product. The admin can send the request as follows.

text= "select employees from each of the Salesman, Scientist and SoftwareDeveloper departments"

Natural Language Processing (NLP) techniques are used to analyze the above request and extract Salesman, Scientist and SoftwareDeveloper as the keywords for querying the User Information Database (UID).

3.1. Predict the priority levels

The insider threat data of the organization is shown in the Figure 4. The first four variables Daily_Time_Spent_on_System, Age, Income, Daily resource Usage are continuous variables, independent variables and they are transformed to Normal distribution using standard scaler. Which is shown in Figure 5.



Daily Time Spent on System	Age	Income	Daily resource Usage	Gender	No.of role	Insider
68.95	35	61833.90	256.09	0	4	0
80.23	31	68441.85	193.77	1	4	0
69.47	26	59785.94	236.50	0	4	0
74.15	29	54806.18	245.89	1	4	0
68.37	35	73889.99	225.58	0	1	0

Figure 4. Insider threat data of an organization

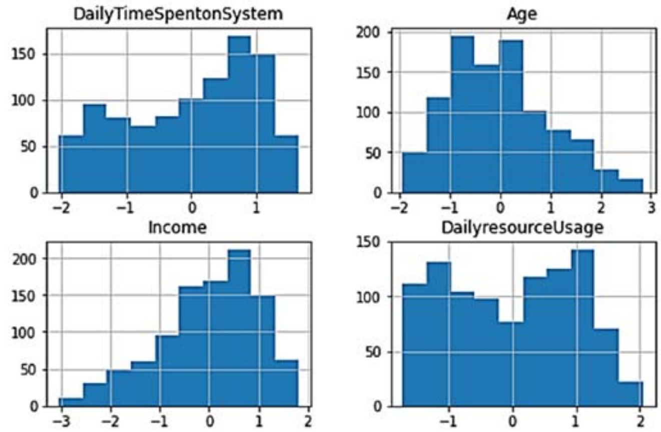
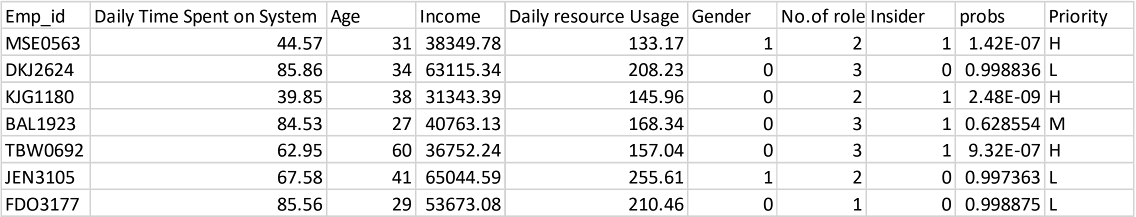


Figure 5. Standard Distribution of continuous variables

The Bayesian inference model has built on the train set and tested on test set. It has given with 96% accuracy and the probability of belief about the users is extracted for each of the employees as in below Figure 6. to decide their level of priority.



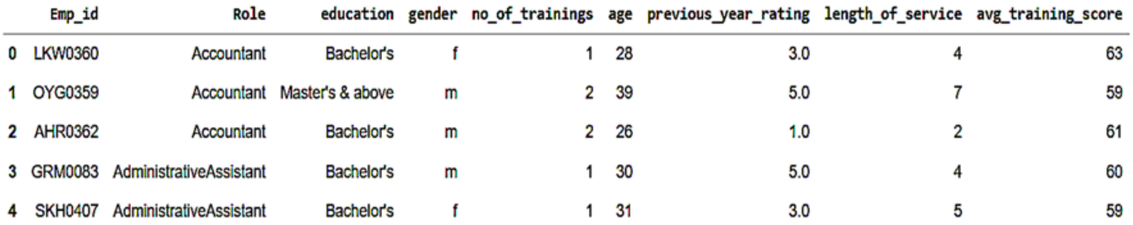
Emp_id	Daily Time Spent on System	Age	Income	Daily resource Usage	Gender	No.of role	Insider	probs	Priority
MSE0563	44.57	31	38349.78	133.17	1	2	1	1.42E-07	H
DKJ2624	85.86	34	63115.34	208.23	0	3	0	0.998836	L
KJG1180	39.85	38	31343.39	145.96	0	2	1	2.48E-09	H
BAL1923	84.53	27	40763.13	168.34	0	3	1	0.628554	M
TBW0692	62.95	60	36752.24	157.04	0	3	1	9.32E-07	H
JEN3105	67.58	41	65044.59	255.61	1	2	0	0.997363	L
FDO3177	85.56	29	53673.08	210.46	0	1	0	0.998875	L

Figure 6. Predicted priority level based on the probability of belief

Based on the probability values between [0, 1], the proposed method has been proposed 3 priority levels to the users for granting data access. When the probability of belief is high, the level of priority is LOW. When the probability of belief is low, the level of priority is HIGH. The level of priority is assigned MEDIUM when the probability of belief is between the range $0.4 \geq P \leq 0.6$ as in Table. I.

3.2. Calculate the capability score of an employees

The sample UID in a manufacturing industry is shown in Figure 7. As per the cross-functional team requirement, gender is not a considerable feature, age is the non-beneficial feature and the remaining features such as education, no_of_trainings, previous_year_rating, length_of_service and avg_training_score are beneficial features.

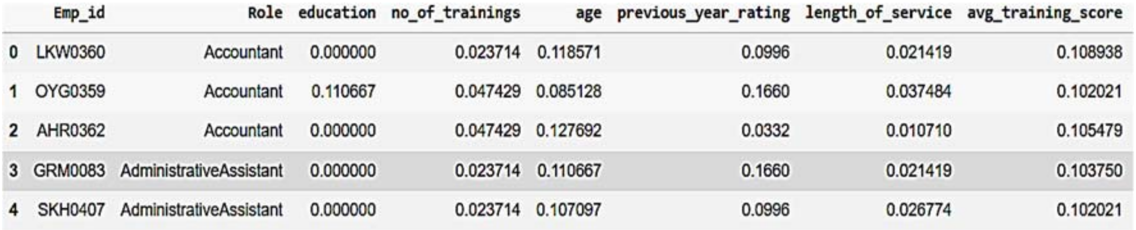


	Emp_id	Role	education	gender	no_of_trainings	age	previous_year_rating	length_of_service	avg_training_score
0	LKW0360	Accountant	Bachelor's	f	1	28	3.0	4	63
1	OYG0359	Accountant	Master's & above	m	2	39	5.0	7	59
2	AHR0362	Accountant	Bachelor's	m	2	26	1.0	2	61
3	GRM0083	AdministrativeAssistant	Bachelor's	m	1	30	5.0	4	60
4	SKH0407	AdministrativeAssistant	Bachelor's	f	1	31	3.0	5	59

Figure 7. User Information Database in a Manufacturing Industry

3.1.1. Normalize the data

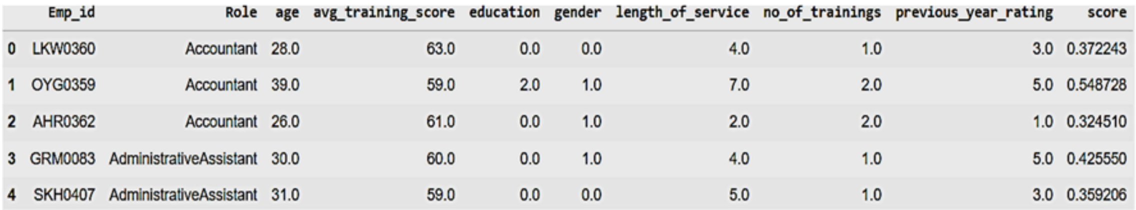
As per the WSM, the features education, no_of_trainings, age, previous_year_rating, length_of_service and avg_training_score in UID table is normalized using the equations (1) & (2) and the resulting values are obtained as shown in Figure 8.



	Emp_id	Role	education	no_of_trainings	age	previous_year_rating	length_of_service	avg_training_score
0	LKW0360	Accountant	0.000000	0.023714	0.118571	0.0996	0.021419	0.108938
1	OYG0359	Accountant	0.110667	0.047429	0.085128	0.1660	0.037484	0.102021
2	AHR0362	Accountant	0.000000	0.047429	0.127692	0.0332	0.010710	0.105479
3	GRM0083	AdministrativeAssistant	0.000000	0.023714	0.110667	0.1660	0.021419	0.103750
4	SKH0407	AdministrativeAssistant	0.000000	0.023714	0.107097	0.0996	0.026774	0.102021

Figure 8. Normalized UID table of data

All attributes that are taken into account when choosing personnel for the requesting intent are assigned equal weightages. According to equation (3), each normalized value is multiplied by its appropriate weightage, and the row-wise summation of that product yields an employee's capability score. According to their score, all of the employees are sorted in descending order. Employees who are ranked first, second, and third in each targeted department, for example, are chosen for the Intent Group. The selected list of employees is shown in Figure 9.



	Emp_id	Role	age	avg_training_score	education	gender	length_of_service	no_of_trainings	previous_year_rating	score
0	LKW0360	Accountant	28.0	63.0	0.0	0.0	4.0	1.0	3.0	0.372243
1	OYG0359	Accountant	39.0	59.0	2.0	1.0	7.0	2.0	5.0	0.548728
2	AHR0362	Accountant	26.0	61.0	0.0	1.0	2.0	2.0	1.0	0.324510
3	GRM0083	AdministrativeAssistant	30.0	60.0	0.0	1.0	4.0	1.0	5.0	0.425550
4	SKH0407	AdministrativeAssistant	31.0	59.0	0.0	0.0	5.0	1.0	3.0	0.359206

Figure 9. List of employees and their capability score

3.3. Deviation Score

The user policy to be a member in the Intent Group is, the selected employee should not have a deviation score greater than 0.5 in their job role group. The deviation score of each employee is calculated using the N-Median Outlier Detection (NMOD) technique based on their work activities within the organization as described in section 2.3. If an organization required to form a multi-disciplinary team for developing new products from Sales, Scientist and Software Developer role groups. First the threshold value of each group is identified by using the N-Median distance plot. The distance plot of Salesman, Scientist and Software Developer role groups is shown in Figures 10(a), 10(b), 10(c). The threshold value of salesman group, Scientist group and SoftwareDeveloper group is identified as 0.5, 0.4 and 0.19. The deviation score of a user in a role group is calculated as:

Dev_score = Median distance of a user in the role group – Threshold value of that group

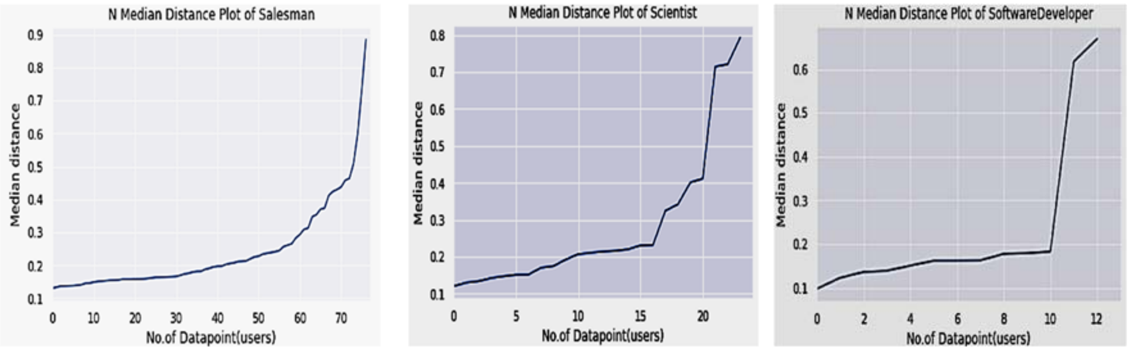
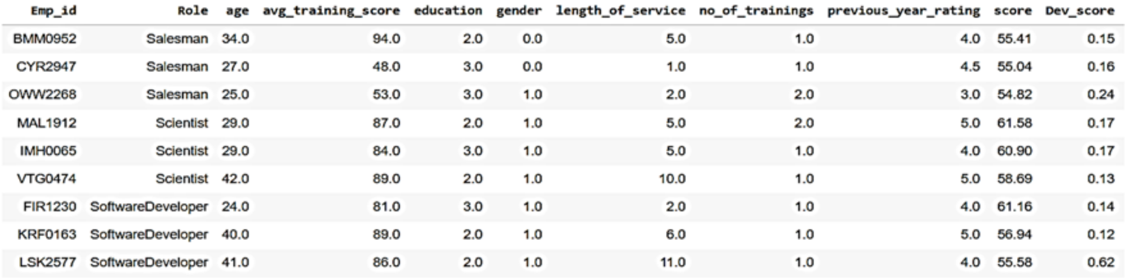


Figure 10(a). Distance plot of Salesman 10(b). Distance plot of Scientist 10(c). Distance plot of SoftwareDeveloper

The deviation score of top 3 employees in each of the required group for new product development team is shown in Figure 11.

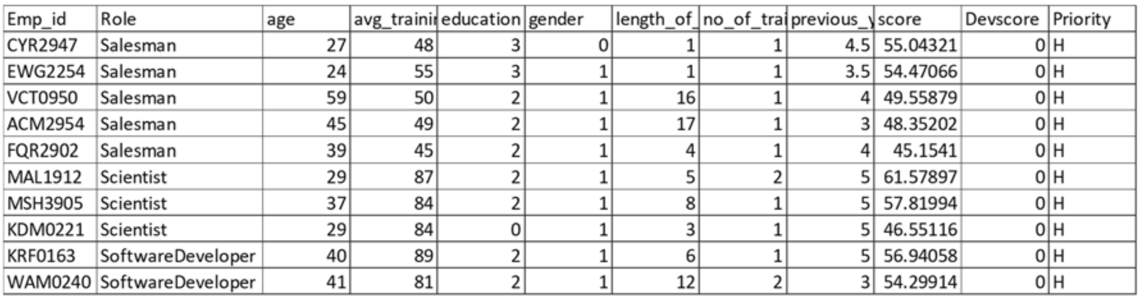


Emp_id	Role	age	avg_training_score	education	gender	length_of_service	no_of_trainings	previous_year_rating	score	Dev_score
BMM0952	Salesman	34.0	94.0	2.0	0.0	5.0	1.0	4.0	55.41	0.15
CYR2947	Salesman	27.0	48.0	3.0	0.0	1.0	1.0	4.5	55.04	0.16
OWW2268	Salesman	25.0	53.0	3.0	1.0	2.0	2.0	3.0	54.82	0.24
MAL1912	Scientist	29.0	87.0	2.0	1.0	5.0	2.0	5.0	61.58	0.17
IMH0065	Scientist	29.0	84.0	3.0	1.0	5.0	1.0	4.0	60.90	0.17
VTG0474	Scientist	42.0	89.0	2.0	1.0	10.0	1.0	5.0	58.69	0.13
FIR1230	SoftwareDeveloper	24.0	81.0	3.0	1.0	2.0	1.0	4.0	61.16	0.14
KRF0163	SoftwareDeveloper	40.0	89.0	2.0	1.0	6.0	1.0	5.0	56.94	0.12
LSK2577	SoftwareDeveloper	41.0	86.0	2.0	1.0	11.0	1.0	4.0	55.58	0.62

Figure 11. List of top three members in each department

If each employee in the selected list satisfies the deviation score and he is not belonging to any of the active Intent Group, then he/she will be assigned to the Intent Group. Otherwise, the configuration agent selects the other alternatives from the remaining UID list. The list of employees assigned to the Intent Group is shown in Table 3 and can observe that the mapping of a user/employee to the Intent Group is One-to-Many.

Table 3. List of employees selected for the Intent Group



Emp_id	Role	age	avg_trainii	education	gender	length_of_	no_of_trai	previous_y	score	Devscore	Priority
CYR2947	Salesman	27	48	3	0	1	1	4.5	55.04321	0	H
EWG2254	Salesman	24	55	3	1	1	1	3.5	54.47066	0	H
VCT0950	Salesman	59	50	2	1	16	1	4	49.55879	0	H
ACM2954	Salesman	45	49	2	1	17	1	3	48.35202	0	H
FQR2902	Salesman	39	45	2	1	4	1	4	45.1541	0	H
MAL1912	Scientist	29	87	2	1	5	2	5	61.57897	0	H
MSH3905	Scientist	37	84	2	1	8	1	5	57.81994	0	H
KDM0221	Scientist	29	84	0	1	3	1	5	46.55116	0	H
KRF0163	SoftwareDeveloper	40	89	2	1	6	1	5	56.94058	0	H
WAM0240	SoftwareDeveloper	41	81	2	1	12	2	3	54.29914	0	H

3.4. Intent Groups to Access Permissions Assignment

Once the Intent Groups have formed as per the sections 3.1. & 3.2., access permissions will be assigned to the groups as in RBAC model. the association between Intent Groups and access rights can be accomplished as a many-to-many connection. That is a group can have many permissions and one permission can be assigned to many groups. The Intent Groups to Access permissions can represented as a matrix consisting Intent Groups as rows and objects as column names and the entries are permissions as shown in the Table 4.

Table 4. Access control Matrix for Intent Groups

Object Intent Group	Customer Feedback	Employee Data	Customer Data	Product data
Product Development	Read		Read	Read Write
Accreditation Group	Read	Read	Read Write	
National Ranking Group		Read		Read

The Product Development team need to analyze the Customer Data about their purchases, Product usage data and Customer Feedback on the current products to develop new products and need to update the product details with write permissions.

3.5. Comparison of IBAC with other access control models

The basic criteria for the comparison of access control models are the requirements of organizations/enterprises. The list of characteristics of an access control model for fulfilling the requirements of an organization are as follows:

A. Support for the policies specific to an organization

Access policies need to be defined based on the business requirement. Therefore, policies should be specific to the organization

B. Support for the use of goal-specific information

Organizations may generate huge data daily by their users or employees. Those data need to be shared securely based on to achieve some specific goal.

C. Support for consistency of resources across multiple Groups

At every state of the access policy enforcement, the resources need to be maintained correctly and assigned correctly among the multiple groups.

D. Support different access control for different goals

Group of people or employees of the organization may work for the different organization’s goals. Each goal may require different access permissions to different resources

E. Support for considering all business constraints while assigning access permissions

Employees/users may work in distributed environments. Access control policies need to be defined by considering all those constraints.

F. Support for fine-grained control of individual users in a Group

When access permissions are assigned to a group of people, there should be some sort of control or monitor the user on every usage of that allotted resource to avoid insider threats.

G. Support for sharing objects with Cross-Functional Groups for achieving organization’s intent

Organizations are adopting cross-functional teams where a group of interdisciplinary people may work together to achieve some sort of organizational goals. While sharing sensitive data with those teams some sort of access control is required to maintain the organization’s reputation. The comparison of access control models with Intent Based Access model will be done by these basic criteria [27] as shown in Table 5.

Table 5. Comparison between access control models

S. No	Access Control Model	Comparison Criteria						
		A	B	C	D	E	F	G
1	PW-RBAC [6]	Y	Y	Y	Y	Y	N	N
2	Task-RBAC [8]	Y	Y	Y	Y	N	N	N
3	AW-TRBAC [11]	Y	Y	Y	Y	N	Y	N
4	Temporal-RBAC [14]	Y	N	Y	Y	Y	N	N
5	CW-RBAC [15]	Y	N	Y	Y	Y	N	N
6	IBAC	Y	Y	Y	Y	N	Y	Y

The percentage of business requirements achieved by the access control models is shown in Figure 12.

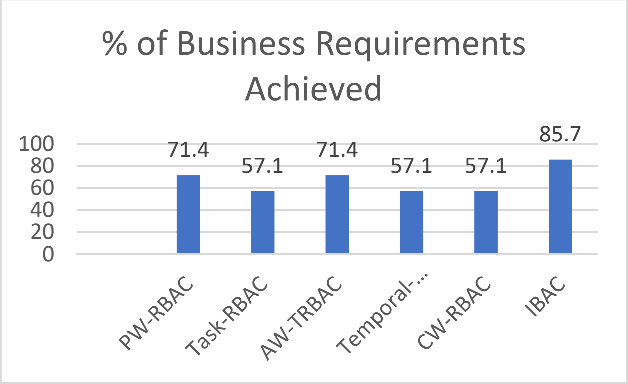


Figure 12. % Of business requirements achieved

The comparison is showing that the proposed IBAC is meeting all the business criteria except the criteria E as it considers only the related constraints not all business constraints. The main focus of this work is to support the business requirements B, F and G as they are trending requirements for business enhancement.

4. Conclusion

Access control models limit an individual's or a group of employees' access to an organization's information systems. The proposed IBAC supports the organization's cross-functional teams, which are intended to meet the organization's goals in a secure manner. Admin's intent request is first analyzed to know the required department and then the WSM was used to choose interdisciplinary individuals depending on their capabilities. It has predected employees priority levels using Bayesian inference model and also calculated each selected employee's deviation score in their job role using N-Median Outlier Detection Method when allocating them to the Intent Group. This paper, for example, looked at employee data of an organization. The comparison of IBAC to alternative access control models reveals that the proposed IBAC model meets 85.7% of business requirements.

Acknowledgments

The authors would like to thank to the R&D departments GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, India for supporting this work. No Funding for this work.

CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare

References

[1] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," *Electronics*, vol. 9, no. 9, pp. 1460, 2020, doi:10.3390/electronics9091460.

[2] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role-based access control: towards a unified standard," in *ACM workshop on Role-based access control*., Jul. 2000, doi: 10.1145/344287.344301

[3] H. Wang, Y. Zhang, and J. Cao, "Effective collaboration with information sharing in virtual universities," IEEE Transactions on Knowledge and Data Engineering, vol. 21, no. 6, pp. 840–853, 2008.

[4] E. O. Boadu, and G. K. Armah, "Role-based access control (RBAC) based in hospital management," *Int. J. Softw. Eng. Knowl. Eng*, vol. 3, pp. 53-67, 2014.

[5] R. Zhang, D. Chen, X. Shang, X. Zhu, and K. Liu, "A knowledge-constrained access control model for protecting patient privacy in hospital information systems," IEEE journal of biomedical and health informatics, vol. 22, no. 3, pp. 904–911, 2017.

[6] B. Tay and A. Mourad, "Intelligent performance-aware adaptation of control policies for optimizing banking teller process using machine learning," IEEE Access, vol. 8, pp. 153403–153412, 2020.

[7] S. S. Webber, "Leadership and trust facilitating cross-functional team success," Journal of management development, vol. 21, no. 3, pp. 201-214, 2002, doi: 10.1108/02621710210420273.

[8] S. Oh, and S. Park, “Task–role-based access control model,” *Information systems*, vol. 28, no. 6, pp. 533-562, Sep. 2003, doi: 10.1016/S0306-4379(02)00029-7.

[9] L. Zhou, V. Varadharajan, and M. Hitchens, “Trust enhanced cryptographic role-based access control for secure cloud data storage,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2381-2395, Nov. 2015, doi: 10.1109/TIFS.2015.2455952.

[10] Q. Liu, H. Zhang, J. Wan, and X. Chen, “An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things,” *IEEE Access*, vol. 5, pp. 7001-7011, 2017, doi: 10.1109/ACCESS.2017.2693380.

[11] M. Uddin, S. Islam, and A. Al-Nemrat, “A dynamic access control model using authorising workflow and task-role-based access control,” IEEE Access, vol. 7, pp. 166676-166689, Oct. 2019, doi: 10.1109/ACCESS.2019.2947377.

[12] R. Ghazal, A. K. Malik, N. Qadeer, B. Raza, A. R. Shahid, and H. Alquhayz, “Intelligent role-based access control model and framework using semantic business roles in multi-domain environments,” IEEE Access, vol. 8, pp. 12253–12267, 2020.

[13] N. Baracaldo, A. Masoumzadeh, and J. Joshi, “A secure, constraint-aware role-based access control interoperation framework,” 2011, pp. 200–207.

[14] J. B. Joshi, E. Bertino, U. Latif, and A. Ghafoor, “A generalized temporal role-based access control model,” IEEE transactions on knowledge and data engineering, vol. 17, no. 1, pp. 4–23, 2005.

[15] G. Milosavljević, G. Sladić, B. Milosavljević, M. Zarić, S. Gostojić, and J. Slivka, “Context-sensitive constraints for access control of business processes,” Computer Science and Information Systems, vol. 15, no. 1, pp. 1–30, 2018.

[16] J. Park, R. Sandhu, M. Gupta, and S. Bhatt, “Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems,” IEEE Access, vol. 9, pp. 151004–151022, 2021.

[17] A. Roy, S. Sural, A. K. Majumdar, J. Vaidya, and V. Atluri, “On optimal employee assignment in constrained role-based access control systems,” ACM Transactions on Management Information Systems (TMIS), vol. 7, no. 4, pp. 1–24, 2016.

[18] S. Mowla, N. Sinha, R. Ganiga, and N. P. Shetty, “Trust Enhanced Role Based Access Control Using Genetic Algorithm.,” International Journal of Electrical & Computer Engineering (2088-8708), vol. 8, no. 6, 2018.

[19] J. Shahen, J. Niu, and M. Tripunitara, “Cree: A performant tool for safety analysis of administrative temporal role-based access control (ATRBAC) policies,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2349–2364, 2019.

[20] A. S. Salehi, C. Rudolph, and M. Grobler, “A dynamic cross-domain access control model for collaborative healthcare application,” 2019, pp. 643–648.

[21] S. Mathrani and B. Edwards, “Knowledge-sharing strategies in distributed collaborative product development,” Journal of Open Innovation: Technology, Market, and Complexity, vol. 6, no. 4, p. 194, 2020.

[22] P. M. Jyosthna, and K. Thammi Reddy, “User Prediction in a Role for Secure Data Sharing Through Cloud,” *IJITEE,* vol. 10, no. 8, pp. 162–166, 2019, doi: 10.35940/ijitee.G5425.0881019.

[23] L. Kof, “Natural language processing for requirements engineering: Applicability to large requirements documents,” *na,* Sep. 2004.

[24] Micheline Kamber and Jian Pei Jiawei Han, Data Mining Concepts and Techniques, 3rd ed., 2012

[25] Z. Chourabi, F. Khedher, A. Babay, and M. Cheikhrouhou, “Multi-criteria decision making in workforce choice using AHP, WSM and WPM,” *The Journal of The Textile Institute*, vol. 110, no. 7, pp. 1092-1101, Jul. 2019, doi: 10.1080/00405000.2018.1541434.

[26] P. M. Jyosthna, and K. Thammi Reddy, “Threat Analysis using N-median Outlier Detection Method with Deviation Score,” *IJACSA*, vol. 12, no. 8, pp. 568-575, 2021, doi: 10.14569/IJACSA.2021.0120866.

[27] E. Sahafizadeh, and S. Parsa, “Survey on access control models,” in *2010 2nd International Conference on Future Computer and Communication*, May 2010, vol. 1, pp. V1-1, doi: 10.1109/ICFCC.2010.5497850.

Author’s Profile

Mrs. P. Mary Jyosthna, received B.Tech. and M.Tech. from JNTUH. Currently she is pursuing Ph.D. in the Department of Computer Science and Engineering at GITAM University (Deemed to be University), Visakhapatnam, Andhra Pradesh. At present she is working as an Assistant Professor in Dept. of CSE at B.V.R.I.T, Narsapur, Hyd., Telangana and she has 16 years of teaching experience. Her research interests include Information Security, Cloud Computing and Machine Learning. Life member of CSI.

Dr. K. Thammi Reddy, received M.Tech (CST) from Andhra University and Doctoral degree from JNTUH, in the area of Data mining. Having 27 years of Teaching & Research experience with an expertise in AI, Data Mining & Security. Published good number of papers in the indexed journals. He is Professor in the Dept. of CSE, Chairperson, Board of Studies, GITAM University. Life member of CSI, ISCA, IE, ISTE.