International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 6, December 2018, pp. 4724~4734
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp4724-4734

Trust Enhanced Role Based Access Control Using Genetic Algorithm

Saleh Mowla, Niharika Sinha, Raghavendra Ganiga, Nisha P. Shetty
Department of Information & Communication Technology, Manipal Institute of Technology, India

Article Info

Article history:

Received Mar 13, 2018
Revised Jun 26, 2018
Accepted Jul 11, 2018

Keyword:

Algorithm
Data privacy
Genetic
Healthcare
RBAC
Trust

ABSTRACT

Improvements in technological innovations have become a boon for business organizations, firms, institutions, etc. System applications are being developed for organizations whether small-scale or large-scale. Taking into consideration the hierarchical nature of large organizations, security is an important factor which needs to be taken into account. For any healthcare organization, maintaining the confidentiality and integrity of the patients' records is of utmost importance while ensuring that they are only available to the authorized personnel. The paper discusses the technique of Role-Based Access Control (RBAC) and its different aspects. The paper also suggests a trust enhanced model of RBAC implemented with selection and mutation only 'Genetic Algorithm'. A practical scenario involving healthcare organization has also been considered. A model has been developed to consider the policies of different health departments and how it affects the permissions of a particular role. The purpose of the algorithm is to allocate tasks for every employee in an automated manner and ensures that they are not over-burdened with the work assigned. In addition, the trust records of the employees ensure that malicious users do not gain access to confidential patient data.

Corresponding Author:

Raghavendra Ganiga,
Department of Information & Communication Technology,
Manipal Institute of Technology, Manipal, Karnataka, India.
Email: raghavendra.n@manipal.edu

1. INTRODUCTION

Role-Based Access Control is a model through which users can access resources that they are qualified for. This can be achieved by mapping the permissions or functionalities to certain roles and then based on certain criteria, the users are assigned the role and are hence permitted to access the resources. The paper discusses a model of RBAC which can be easily adopted by healthcare organizations such as hospitals, clinics, etc. Besides task allocation by the genetic algorithm, the system will also record feedback given by patients for concerned employees to ensure that they are trustworthy and reliable so as to access patient record details.

1.1. Background

1.1.1. Role-Based Access Control

Role Based Access Control is a method through which user access to computer or network resources is regulated on the basis of the roles they have been assigned [1]. There are different models that have been implemented in this regard. A user can have multiple roles and each roles can be assigned with multiple functionalities as shown in Figure 1. Various factors are considered when it comes to assigning users their roles (based on the application or system) and once the criteria has been fulfilled, the user can access the resources and functionalities mapped to the respective role. This leads to the description of two jargons i.e. roles and permissions. An *organizational role* is a way to provide authoritative entitlement to people entities

working in the organization. Depending on the number of responsibilities and significance of the role, the organization builds a hierarchical system so as to follow a smooth chain of command. *Permissions* can be referred to as the functionalities or authority that has been delegated to a role. It is the duty and responsibility of the person assigned a role to perform the assigned permissions satisfactorily as required.

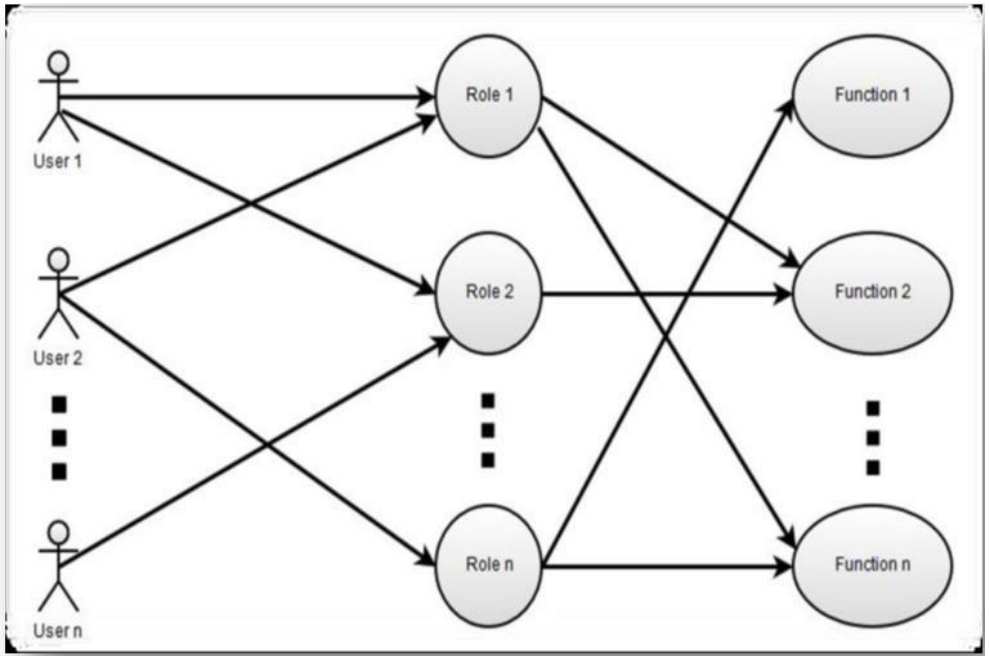

Figure 1. General overview of an RBAC System

1.1.2. Genetic Algorithm

The genetic algorithm was inspired by the process of generation of DNA in animals and follows Darwinian's principle of "survival of the fittest". The use of this algorithm has had various successes in areas like problems related to global optimization, security (and cryptography) as well as time-tabling. The algorithm considers a number of parameters which are taken into consideration and are applied on the basis of the requirements and the purpose of the applications.

1.1.2.1. Selection

Selection is the process of selecting better solutions than the ones available. The idea is to select the best genes so that they can pass over to the next generation thus aligning itself with Darwin's "survival of the fittest" theory. Selection mainly involves the selection of appropriate parents so that they can generate off-springs of the further generations. With respect to the algorithm, the selection process is facilitated by the evaluation of a 'fitness' function. If the fitness level of a solution is above a certain user-defined threshold, it is selected. Fitness function can be objective or subjective. An objective function is one which selects solutions based on a mathematical model or a computer solution whereas a subjective function is one where the solution is chosen by humans who consider the solution better than the worse ones.

1.1.2.2. Crossover and Recombination

Crossover in genetic algorithm is analogous to the crossover in biological reproduction. More than one parent is selected. Using the genetic content of the selected parent, one or more off springs are produced. This step, along with mutation, is mainly to generate another generation of solutions from the selected parents. To produce a new solution using the existing ones, a pair of parents is selected from the remaining solutions. The new solution that is obtained generally shares many of its parents' characteristics. The process of generation of new solutions from existing ones continues till a solution of required size is obtained.

There are many different types of crossover. The first type of crossover uses a single crossover point in both the parent strings [2]. The part of the string beginning from one chromosome till its crossover point is taken from one parent, and from the second parent, its part of the string from the crossover point till the end is taken as shown in the Figure 2.

Figure 2. Single Point Crossover

The second type is a two point crossover, wherein the part of the string starting from the beginning of the chromosome till the first crossover point is taken from the first parent, the part of the string from the first to the second crossover point is taken from the second parent, and from the second crossover point till the end of the chromosome is taken from the first parent [2] as shown in the Figure 3.

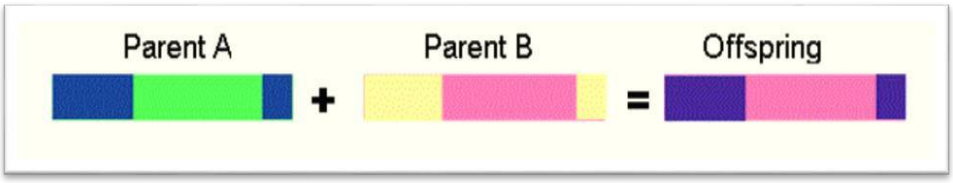

Figure 3. Two Point Crossover

Uniform crossover has the child carrying parts of the string randomly copied from the first as well as the second parent. Cross points can be randomly chosen along the strings of the parents. If the mixing ratio of both the parents is 50-50, then the child will approximately have half the string from the first and half from the second parent [2] as shown in the Figure 4.

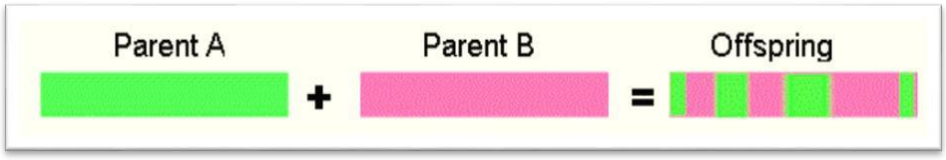

Figure 4. Uniform Crossover

An arithmetic operation can also be decided upon beforehand. This arithmetic operation is performed on the parent bits and can hence be used to calculate the resulting child bits. The arithmetic operation can be any as shown in Figure 5.

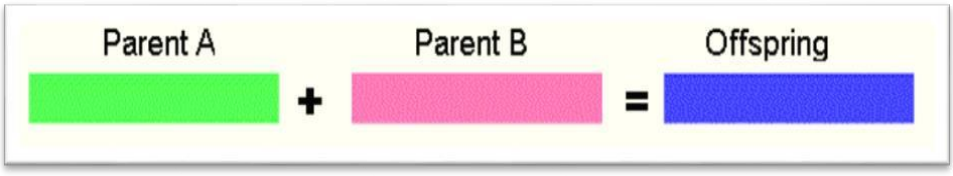

Figure 5. Arithmetic Crossover

Sometimes, three parents are used to produce one offspring. In this case, bit-wise comparison takes place with bits from all the three parents. Accordingly, the resulting corresponding child bit is set to 0 or 1.

1.1.2.3. Mutation

Mutation refers to the modification done in the chromosome in order to obtain new solutions. It is done so as to increase the diversity of the population chromosome content. Like crossover, even mutation in genetic algorithm is analogous to genetic mutation. There are different kinds of mutation methods or mutation operators. A combination of the methods known can also be used [2]. Flip bit mutation is a mutation method in which the bits of the available genome are inverted. A mutation operator can work on integer, float, string, etc. genes. In swap mutation, two positions are chosen on the selected chromosome and the values at these positions are swapped as shown in the Figure 6.

Figure 6. Swap Mutation

There is a mutation method called scramble mutation in which a subpart of the chromosome is taken and the values in this subpart is shuffled randomly as shown in the Figure 7.

Figure 7. Scramble Mutation

In inversion mutation, a subpart of the chromosome is selected and the subset string gets inverted as shown in the Figure 8.

Figure 8. Inversion Mutation

In uniform mutation the value of the selected gene is replaced by a value within the upper bound and lower bound that is specified by the user. Bit string mutation inverts the bits of the chromosome at random positions [2] as shown in the Figure 9.

Figure 9. Bit String Mutation

1.2. Problem Definition

Using the RBAC model, it is possible for users to simply login and based on their credential i.e. role, they are able to access the resources or permissions mapped to that role. This mapping of roles and users can be done by the admin or the head of the organization that will have the authority over the entire system. However, it is not possible for a single admin to manage the roles and the permissions mapped to them for a large organization with hundreds and thousands of employees. In addition to managing the roles and the permissions, the admin will have to manage the number of users, allocate roles to the users and ensure that only qualified users are eligible to access the resources or perform functionality. Bearing this problem in mind, the idea is to implement a 'Genetic Algorithm' which can be applied to the RBAC model of healthcare organizations. Using this algorithm, users will be authorized for their permissions automatically.

The admin simply has to maintain the database for the employees and the permissions of each role. Once an employee logs into the system, the Genetic Algorithm will take into account the role of the user and assign him his tasks and permissions of the day. At the same time, it is imperative that users of such a system are reliable and trustworthy enough to access confidential information because leakage of private patient information leads to the healthcare organization incurring heavy losses in terms of finance as well as credibility. Thus it is essential to evaluate the trustworthiness of the employee so that the probability of malicious users gaining access to sensitive information becomes minimal.

1.3. Literature Review

A good amount of research has been conducted in both access control systems as well as genetic algorithms. Ferreira et al. proposed a model call BTG-RBAC which facilitates the users to break the glass rather than be denied access [3]. Bindiganavale and Ouyang introduced RBAC in a typical J2EE enterprise application [4]. In order to minimize the disadvantages of RBAC systems, a model was developed which added attributes (ABAC) to the existing RBAC system [5]. To further improve the system, the Bi-layer Access Control model was proposed by Alshehri and Raj which combined the benefits of RBAC and ABAC [6]. Wonohoesodo and Tari proposed two models viz. SWS-RBAC (for single web services) and CWS-RBAC (for global web services) [7]. With respect to healthcare organizations, contribution has been made to secure communication channels by means of an access control system for mobile agents between healthcare organizations [8] and threat models have also been designed and developed for regulating access in healthcare institutes [9].

Khan and Sakamura [10] proposed a Discretionary Access Control (DAC) framework that provides healthcare organizations against security attacks and ascertains confidentiality of patient data. A trust-aware RBAC model has been used to demonstrate social healthcare networks application in a cloud environment [11]. A similar cryptographic RBAC model has also been designed that considers inheritance of the roles as well their hierarchy in the evaluation of trustworthiness of the users and how it can be deployed on the cloud [12]. Yu, Wang, Ren and Lu have combined Attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve user access privilege confidentiality and secret key accountability of the users [13]. An emergency medical system has also been developed to enable ubiquitous access to medical services [14]. A role-based trust management model has also been proposed along with a detection algorithm to avoid violation of the least-privilege principle of RBAC [15]. Suryani, Sulistyo and Widyawan used a Modified Ant Colony algorithm to calculate the selection processes of trustable objects [16].

2. THE PROPOSED METHOD

There have been different implementations and modified use of this algorithm. Shiu and Szeto developed a mutation-only genetic algorithm to optimize airport capacity utilization [17]. With the help of the algorithm, it was possible to realize a rostering solution that experiments with work shifts of doctors while maintaining quality of services [18]. An adaptive local search and immigrant scheme in [19] combined with an adaptive genetic algorithm has helped solved staff routing problem in healthcare organizations along with improving the performance of the original genetic algorithm. Cai et al. [20] minimized the costs of allocating staff for over-time work and optimized a solution for scheduling staff of mixed skills under multiple criteria using genetic algorithm. Chang-Chun Tsai et al. [21] proposed a method to reduce infeasible solutions in genetic algorithm. This paper approaches the development of an RBAC system for healthcare organization by automating the role-permission mapping process with the help of a variant genetic algorithm. In this section, the proposed architecture is discussed with respect to a scenario in a healthcare organization.

2.1. Healthcare Organization

The model assumes that a number of hospitals and clinics have access to the database containing patient record files and the department assigned to them. The model can be applied to a single healthcare

organization and can also be scaled to include others easily. The constraint with accessing the database is that the patients themselves need to authorize the hospitals to access their records. Consider a scenario where a patient is dissatisfied with the services and treatment provided by a healthcare organization. He can opt to seek for treatment provided by another hospital or clinic integrated into the RBAC system by providing them the consent to access his health records. It avoids unnecessary documentation and potential miscommunications between the hospitals regarding the patient since the details can be accessed from the database.

2.2. Specialization departments

The model takes into consideration four health departments present in each organization, namely Cardiology, Neurology, Gynecology and General Surgery. Addition and removal of departments specific to every healthcare organization can be easily accommodated. Each department will have their own set of patients that they are responsible for and need to keep track of. The system has been designed in such a way that the departments can recommend the patient for further treatment by another department through the RBAC system. The recommended department thus gains access to the patient records without the involvement of any paperwork. For example, after a gynecologist delivers a new born baby, the doctor may recommend the patient to seek additional care from a pediatrician.

2.3. Authoritative Roles

The initial system assumes that there are many employees in each healthcare organization broadly divided into four roles viz. Receptionist, Nurses, Interns and Doctors. The system can accommodate the addition of other distinctive roles as well. Each role has its own set of functionalities and permissions which it is responsible for. Table 1 gives a brief overview of the functionalities assigned to each role recognized in the healthcare organizations.

Table 1. Overview of Roles and Permissions in Healthcare Organization

Sr. No.	Role	Permissions
1.	Receptionist	Access Patient Information and File Records
		View Appointments of the Department
		Schedule Appointments
		Delete Appointments
		Notify patients and other users of the system
2.	Nurse	Access Patient Information and File Records
		View Appointments of the Department
		Send details for testing
		View Test Results
3.	Intern	Access Patient Information and File Records
		View Appointments of the Department
		View Test Results
		Write Reports
		Assist in Surgery
4.	Resident Doctor	Access Patient Information and File Records
		View Appointments of the Department
		Perform Surgery
		View Reports and Test Results
		Supervise and teach interns

2.4. Employee Credentials

In order to apply the Genetic Algorithm to the RBAC model, we will be assigning the users of the system with an ID where the digits themselves signify an aspect of the organization. The User ID is of the form AB-CD-EF-GH where A, B, C, D, E, F, G and H represent digits from 0-9. The model assumes that more than one healthcare organization are sharing a common central database. This ensures that patient information can be shared with another hospital provided the patient gives his consent. Table 2 gives the description of the employee ID.

Table 2. Description of Employee ID

Digits	Significance	Description	Example
AB	Hospital	The first two digits signify which hospital or healthcare organization the user is working in	11- Hospital A 12- Hospital B 13- Clinic A 14- Hospital C
CD	Department	The third and the fourth digit together signify the department the user belongs to in the organization	10- Cardiology 20- Neurology 30- Gynecology 40-General Surgery
EF	Role	The fifth and the sixth digit represent the role of the user	10- Receptionist 20- Nurse 30- Intern 40- Resident Doctor
GH	Registration Number	The last two digits represent the registration number allotted to the user by the organization.	01- User 1 02- User 2 03- User 3 04- User 4

2.5. Patient Role and Trust

The patients getting treated in the healthcare organizations are also a part of the system and have their own interface to login and use the system. The patients have the privileges of viewing their health record files and most importantly provide the hospitals using the RBAC system permission to access their records. The patient may also choose to deny granting access rights to the hospital as per their preference. In instances where patients have been provided inadequate care, it is sometimes however, impractical to disregard the merits of the healthcare organization due to mishaps and incompetency of a few employees.

In order to prevent the credibility of an organization from getting lowered as a whole, the patients are also given the privilege to provide feedback to the employees who have treated them which will be stored in the form of a trust record. The trust record of an employee will be stored in the form of $<X_{rc}, X_{tr}>$ where X_{rc} denotes the count of the total number of trust records of the employee and X_{tr} denotes the total value of the trust records provided by the patients for the employees. After evaluating the total trust value of the employee from his trust tuple, the mean value is calculated. It is the authority of the department to determine a trust threshold value for its employees. If the mean trust value of the employee is above this threshold limit, then he or she is considered trustworthy and can gain access to the patient's medical records. However, if the mean trust value is lower than that of the threshold, the system will ensure that such employees are denied access rights to patient's medical records. This feature will not only ensure privacy of patient data but can also be used as a metric to evaluate the patient relationship management of the employee.

3. RESEARCH METHOD

In this section, fitness and mutation functions are discussed with respect to RBAC system.

3.1. System Overview and Process Workflow

The model designed has been implemented in Java using NetBeans IDE and Derby database. The GUI of the RBAC system has been developed using Java Server Pages (JSP). The use of servlets has ensured a dynamic system where any changes and updates made by the user are reflected immediately in the GUI. The process workflow can be summarized from the following pseudocode. The fitness and mutation function of the above algorithm are mentioned in sections 3.2 and 3.3 respectively.

```
a.  Enter Employee ID (i.e. AB-CD-EF-GH) and Password
b.  If (credentials are fit)
c.      Login Successful
d.      If (starting of new week)
e.          C'D' = mutate(CD)
f.          fetchTasks(C'D')
g.          Working_Department = C'D'
h.      Else
i.          fetchTasks(Working_Department)
j.  End If
```

3.2. Selection and Fitness Function

The fitness function of the algorithm will evaluate the validity of the user's input. It will validate the login of the user based on the following criteria:

a. The length of his user ID is 8.
b. The Hospital the user works in exists in the database.
c. The Department exists in the database for the organization.
d. The Role is accounted for in the database.
e. The user has been registered in the organization.

If the above criteria are met satisfactorily, the user is considered to be fit and the algorithm will proceed with assigning the permissions to the user according to his role.

3.3. Mutation

The genetic algorithm will ensure that the role and hospital of a user does not change because in a practical scenario, it is implausible for a nurse to have the permissions of a resident doctor or for an employee working in one organization get access to resources of another. Keeping the role and working organization same, the algorithm will mutate digits CD. Since the mutation will depend on the existing infrastructure of the organization, the mutation will always be valid; this ensures that the algorithm is not applied all over again and thus saves on time and increases performance.

Another factor that has been taken into consideration is the fact that it is not feasible for the algorithm to mutate the department every time the employee logs in. If this is allowed, then it would become tedious and almost impossible to get used to the work culture of the health organization in which he is working in since different departments have different policies. In view of this problem, the implemented model mutates the department of the employee once in a week, a policy which can be changed easily as well. This ensures that the algorithm won't mutate the department unnecessarily further increasing efficiency.

3.4. Task allocation

Once the algorithm has mutated the department credentials in the user ID, it will need to fetch the tasks that the employee needs to perform on that particular day. . Depending on the working organization, mutated department and role of the user, the algorithm will determine the tasks that the employee will have to perform and the resources he can get access to. The algorithm needs to take into account two considerations-

1. Every department has many employees.
2. Every role has been delegated many permissions and functionalities.

It would be physically impossible for a single employee to perform all the duties and task mapped to his role. Therefore, while fetching the tasks the algorithm will ensure that each employee will be allocated not more than 3 tasks each day (policy subject to change according to the organization). The algorithm thus ensures that employees are not overburdened and due to the automated mechanism, it reduces the burden of the administrative head of every department.

3.5. Trust Factor

When a patient logs into the system, he or she has the option of providing feedback to the employees belonging to the department that is taking care of the patient from a range of -1 to +1 where -1 denotes untrustworthy and +1 denotes trustworthy. The implementation can be summarized from the pseudocode shown below.

```
Patient:
1.  x = getPatientFeedback(Employee_ID)
2.  If(x > 0)
3.    Increment count of X_rc
4.    Increment count of X_tr in database
5.  Else If(x < 0)
6.    Increment count of X_rc
7.    Decrement count of X_tr
8.  Else
9.    Increment count of X_rc
10. End If
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Employee:
1.  numRecords = fetchTrustRecordCount(Employee_ID)
2.  trustValue = fetchTrustValues(Employee_ID)
3.  meanTrust = trustValue / numRecords
```

4. If(meanTrust ≥ departmentTrustThreshold)
5. Patient Data Access Granted
6. Else
7. Patient Data Access Denied
8. End If

4. RESULTS AND ANALYSIS

The system has been designed to take into consideration the fact that each and every health department will have their own policies and guidelines that need to be implemented and followed. The model factors in the experience of the employee with respect to his or her role. For example, it may be required for an intern working in the General Surgery Department to have at least 4-6 weeks of experience to get permitted to perform a task but that required by an intern working in the Neurology Department may be 8-10 weeks for the same task. The system design has accommodated that each and every department will have their own policies specific to the different roles working in the department.

The experience mentioned by a person entity working in the organization refers to the work experience of the entity in a particular department and not the total number of days that the employee has worked in the organization. Figure 10 shows a sample scenario of department policies where the X-axis represent the number of weeks the employee has worked in each department and Y-axis represents the number of tasks and operations the employee has been permitted to perform as shown in the Figure 10. In a scenario where patients are not comfortable and do not trust an employee, they can rate the employee and give their feedback. Based on the guidelines and policies of the department, if an employee is considered untrustworthy then he will be denied access to any patient records.

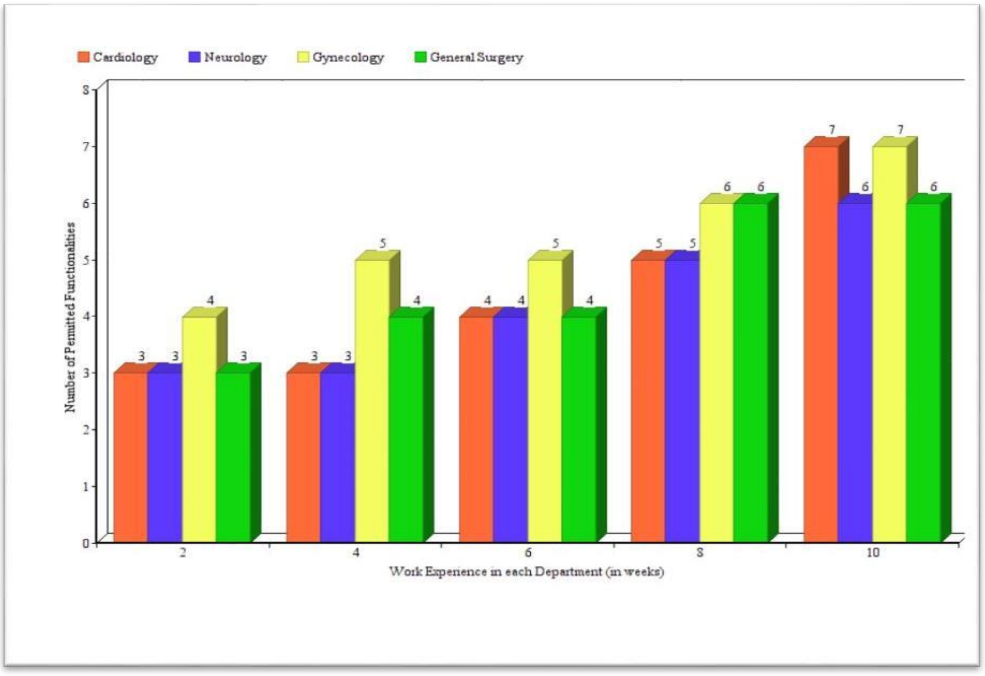

Figure 10. A Sample Scenario of Department Policies

In addition to the above, the model assumes that an employee working in a particular department can only access records of patients belonging to that department. A patient cannot decide which department gets to treat him since it is the assumption that the doctors would be more informed about that decision. In case the doctor feels that the patient should be treated by an employee belonging to another health department, he can authorize that department to gain access to the patient's records. For example, after the delivery of a baby and initial treatment of the mother, the Gynecology department may recommend the mother to seek further treatment, attention and care from a pediatrician. With the help of the implemented

model, the Gynecology department can authorize the Pediatrics department to gain access to the said patient's and baby's medical records.

5. CONCLUSION

For the purpose of the developing an RBAC system for healthcare organizations, the genetic algorithm had been modified to include only selection and mutation. The need for crossover was not felt since it would result in the production of new offspring (i.e. employee entities) which may not exist in the database. Such entities would be considered unfit and the genetic algorithm would have to re-compute a valid solution in order for the system to fetch and allocate the tasks to the employee. This redundant computation is avoided thereby making the system faster and more efficient (similar to the objective of reducing overhead computation achieved by Meneka and Meenakshisundaram [22]).

The model implemented can be used by healthcare organizations where employees are trained and taught in different fields of the organization. The model also takes into account the possibility of different trust policies and experience requirements by different departments for the employee to gain access to certain resources or perform certain operations and tasks. The objective of developing an automated system where employees are allocated tasks according to their role and experience was successfully achieved. The integration of the trust factor has ensured that confidential patient data is safe from the hands of potential malicious users. Future work with respect to the RBAC model would be to implement cryptographic algorithms and integrate it with the system to guarantee entity authentication and thus further increase the security.

REFERENCES

[1] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," Computer, vol. 29, no. 2, Feb 1996.
[2] Sastry K., Goldberg D., Kendall G. (2005) Genetic Algorithms. In: Burke E.K., Kendall G. (eds) Search Methodologies. Springer, Boston, MA
[3] A. Ferreira et al., "How to Securely Break into RBAC: The BTG-RBAC Model," 2009 Annual Computer Security Applications Conference, Honolulu, HI, 2009, pp. 23-31, doi: 10.1109/ACSAC.2009.12
[4] V. Bindiganavale and J. Ouyang, "Role Based Access Control in Enterprise Application - Security Administration and User Management", 2006 IEEE International Conference on Information Reuse & Integration, Waikoloa Village, HI, 2006, pp. 111-116, doi: 10.1109/IRI.2006.252397
[5] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," Computer, vol. 43, no. 6, pp. 79–81, Jun. 2010.
[6] Alshehri and R. Raj, "Secure Access Control for Health Information Sharing Systems," in IEEE International Conference on Healthcare Informatics (ICHI 2013), Philadelphia, 2013.
[7] R. Wonohoesodo and Z. Tari, "A role based access control for Web services," IEEE International Conference onServices Computing, 2004. (SCC 2004). Proceedings. 2004, 2004, pp. 49-56. doi: 10.1109/SCC.2004.1357989
[8] C. Santos-Pereira, A. B. Augusto, R. Cruz-Correia and M. E. Correia, "A secure RBAC mobile agent access control model for healthcare institutions," Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems, Porto, 2013, pp. 349-354, doi: 10.1109/CBMS.2013.6627814
[9] S. Alshehri, S. Mishra and R. K. Raj, "Using Access Control to Mitigate Insider Threats to Healthcare Systems," 2016 IEEE International Conference on Healthcare Informatics (ICHI), Chicago, IL, 2016, pp. 55-60, doi: 10.1109/ICHI.2016.11
[10] M. F. F. Khan and K. Sakamura, "A smartcard-based framework for delegation management in healthcare Access Control systems," *2016 IEEE Region 10 Conference (TENCON)*, Singapore, 2016, pp. 2739-2742, doi: 10.1109/TENCON.2016.7848538
[11] R. Wooten, R. Klink, F. Sinek, Y. Bai and M. Sharma, "Design and Implementation of a Secure Healthcare Social Cloud System," 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012), Ottawa, ON, 2012, pp. 805-810, doi: 10.1109/CCGrid.2012.131
[12] L. Zhou, V. Varadharajan and M. Hitchens, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2381-2395, Nov. 2015, doi: 10.1109/TIFS.2015.2455952
[13] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9, doi: 10.1109/INFCOM.2010.5462174
[14] V. Koufi, F. Malamateniou and G. Vassilacopoulos, "Ubiquitous access to cloud emergency medical services," Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine, Corfu, 2010, pp. 1-4, doi: 10.1109/ITAB.2010.5687702
[15] X. Guo, J. Zheng, Q. Zhang, H. Liu. "Role-based Trust Management Model in Multi-domain Environment". *Indonesian Journal of Electrical Engineering and Computer Science.* 2013, Vol. 11, No. 1.

[16] V. Suryani, S. Sulistyo, W. Widyawan. Trust Based Privacy for Internet of Things. *International Journal of Electrical and Computer Engineering.* 2016, Vol. 6, No. 5.
[17] Shiu K.L., Szeto K.Y. (2008) Self-adaptive Mutation Only Genetic Algorithm: An Application on the Optimization of Airport Capacity Utilization. In: Fyfe C., Kim D., Lee SY., Yin H. (eds) Intelligent Data Engineering and Automated Learning – IDEAL 2008. IDEAL 2008. Lecture Notes in Computer Science, vol 5326. Springer, Berlin, Heidelberg
[18] H. A. Majid, L. M. Yusuf, A. A. Samah, M. S. Othman and A. N. W. Ren, "Application of genetic algorithm for doctor rostering at primary care clinics in Malaysia," 2017 6th ICT International Student Project Conference (ICT-ISPC), Johor, Malaysia, 2017, pp. 1-4, doi: 10.1109/ICTISPC.2017.8075351
[19] T. Sinthamrongruk, K. Dahal, O. Satiya, T. Vudhironarit and P. Yodmongkol, "Healthcare Staff Routing Problem using adaptive Genetic Algorithms with Adaptive Local Search and Immigrant Scheme," 2017 International Conference on Digital Arts, Media and Technology (ICDAMT), Chiang Mai, 2017, pp. 120-125, doi: 10.1109/ICDAMT.2017.7904947
[20] X. Cai and K. N. Li, "A Genetic Algorithm for scheduling staff of mixed skills under multi-criteria," European Journal of Operational Research, vol. 125, no. 2, pp. 359-369, 9/1/ 2000.
[21] C.-C. Lin, J.-R. Kang and T.-H. Hsu, "A Memetic Algorithm with Recovery Scheme for Nurse Preference Scheduling", Journal of Industrial and Production Engineering, vol. 32, no. 2, pp. 83-95, 2015/02/17 2015.
[22] M. Meneka and K. Meenakshisundaram. An Enhancement Role and Attribute Based Access Control Mechanism in Big Data. *International Journal of Electrical and Computer Engineering;* 2018, Vol. 8, No. 5