International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-9 Issue-2S, December 2019

Recommender System for Geo-Social Access Control Framework

Priyanka C Hiremath, Raju G T

***Abstract:** A malicious attack or threat can happen within any organization, from their own employees, administrators, contractors or former employees, who pose the important resources of a company such as database, physical laboratories and financial resources. In an organization insider attacks are most common as well as most costly affair. According to United States cyber security 2018 statistics, insider threat holds the risk of 74% out of surveyed organizations. The insider threat has caused immense loss to data as well as monetary assets. Among the surveyed organization by US cyber securities, 53% of organization claimed their remediation cost was around $ 100000 and in 2018 the number raised to 66%. Higher number of organization claimed insider attackers were most costly attacks in comparison with external attacks. Some of the probable reasons, why it is difficult to stop an insider attack are, firstly insider threat may be unintentional and all of sudden. Second is distinguishing regular work by employee and malicious work is difficult. Third is most of the insider attackers are technologically sound to mask their intentional activities or easily erase the intentional activity signs from the system before anyone observes it. Lastly and the worst case is employees simply say their intentional act was by mistake and escape from scenario. To avoid such malicious insider attacks lots of research is done on access control. Access control is a method or technique to control the access of an insider to the organizations valuable resources. There are different types of access control models, having their own access control policies and criteria to grant the authority, to have an access to specific resources of an organization. In this paper we discuss the different types of technical access control models that have been developed with certain parameters and their advantages and limitations.*

***Keywords:** Insider attack, Context, Attributes, Roles, Resources, Geo-Social Data, Access control.*

I. INTRODUCTION

To develop or build any organization, first and foremost importance is given to resources. Organizations data and resources must be secured from illegal or unauthorized access. Access control is a feature of security, which controls users and systems from the important data and resources. It gives ability to an organization to authorize, monitor, control, protect and restrict resources such that the resources are neither over protected nor loosely disclosed. The access to any organization is controlled through practically three types of access control techniques: Administration Access Control, Physical Access Control and Logical Access Control.

A. Administration Access Control

The whole organizations polices, practices and procedures are decided by administrative people. Administrative access control defines the organization requirement in terms of technical and physical access control. It also defines the loss and consequences to an organization if access controls are not set. Few examples are: hiring practices, training levels, checking employee backgrounds, software development policies and procedures, review and reports, classification of data and labeling setting rules for increment, holding leave history, holding personal performance records, controlling contractors, auditing , supervising and testing.

B. Physical Access Control

Restricting control physically to the campuses, buildings, properties or room some of the examples for physical control are: security guards, finger prints, retina recognition, face recognition, using manual and digital lock systems, applying badges, constructing fences, swiping cards, sealing windows, protecting cables, having guard dogs, installing video cameras and motion detectors, alarms and mantraps. All these control methods are physically something you can touch.

C. Logical or Technical Access Control

It means restricting access control technically. The main aim is to provide secure network connections to system files, computer networks and data. In today's modern world, with increase of digital devices and applications, easily we get the information of user's social and location details. Such information allows us to provide security at high levels. Due to such growing digital world much of research is done to combine administrative, physical and technical control, which has led to modern access control systems. Few examples of logical access control are digital forensic tools, antivirus and intrusion detection systems. It is generally software component such as programs and process which enforce restrictions and control the organization. Fig. 1 shows the benefits of access control (AC) and Fig. 2 shows taxonomy of access control models.

Protect staff and systems
Prevent intruders and theft
Audit trail and compliance with regulations
Integration across physical and logical access

Fig. 1. Benefits of AC

Revised Manuscript Received on December 12, 2019.

* Correspondence Author
Priyanka C Hiremath*, Research Scholar, Department of Computer Science and Engineering, RNS Institute of Technology, Bengaluru, India. Email: hiremath.priyanka1@gmail.com
G T Raju, Department of Computer Science and Engineering, RNS Institute of Technology, Bengaluru, India. Email: gtraju1990@yahoo.com

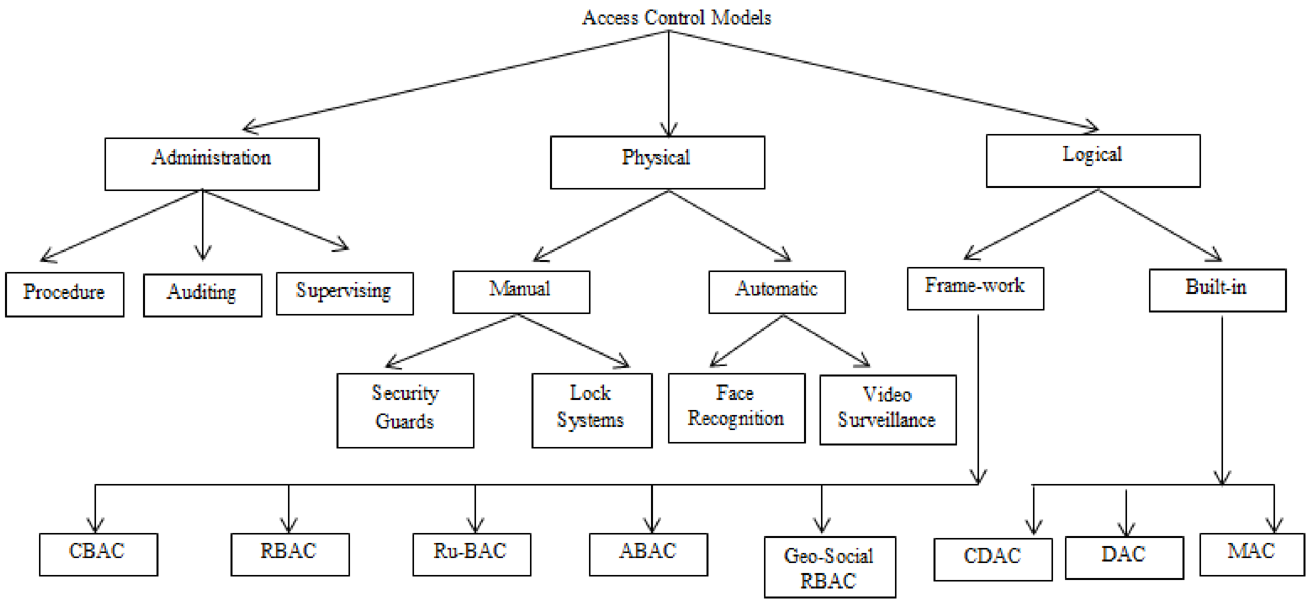

Fig. 2. Taxonomy of Access Control Models

In this paper we explore technical access control models, such as Content Dependent Access Control (CDAC), Context Based Access Control (CBAC), Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC), Rule Based Access Control (Ru-BAC), Attribute Based Access Control (ABAC) and Geo-Social Role Based Access Control (Geo-Social RBAC), against various parameters listed below.

- *Resource Classification*: In access control models resources are classified or categorized to ease the authorization.
- *Generic functionality*: The access control models can either be built-in the operating system or can be framework for particular application area.
- *Environment*: The Environment is categorized or distinguished by the static or dynamic nature of access control model. If the input data is already updated and cannot be updated during the execution time is static in environment. If the input data gets updated even during execution time is dynamic in environment.
- *Availability of resources to users*: Organization resources should be provided to users such that resources are neither overprotected nor loosely disclosed. We analyze them as high, moderate and low restrictions on users to avail resources.
- *Type of Data*: The input data can either be homogenous, heterogeneous or neutral. If the data is same or alike type, it is homogeneous else the data is heterogeneous. Few access control models do not depend on the type of data. Input data maybe homogeneous or heterogeneous. Such models are analyzed as neutral.
- *Execution Complexity*: Execution complexities depend on data size and environment in which models are executed. In static environment execution complexity is low during run time. In dynamic environment it is little low.

II. ACCESS CONTROL MODELS

Lot of research has been done on enhancement and improvement of access control models. Following section provides description of access control models. Table I summarizes these models against described parameters.

A. Discretionary Access Control Model (DAC)

DAC model permits users to access to organization resources by taking permissions from the administrators. It was found in the year 1970 [1]. Here importance is given to administrators or owner he / she can either grant access or deny. Once the resources are granted, users can modify or alter the features of resources also change or specify whether the resource are accessible or not to other users. Simple example of DAC is password file. DAC models are used in both centralized and distributed level. This model is built-in in all operating system. Example of this is file permission model. It has moderate restriction on users to avail resources but integrity of resources is not maintained properly as authority of determining policies is left to users. DAC shares the resources fundamentally but faces difficulty in protecting resources. One of the major disadvantage of DAC is, it cannot recognize or differentiate between a computer and human.

B. Mandatory Access Control (MAC)

MAC was also found in the year 1970 [1]. Here resources are classified for users on bases of labeling. For example, top secret is labeled as label 1, secret is labeled as 2 and free is labeled as 3. Now users are authorized such that a user must have certain clearance level. If user has clearance level 2, he can access secret and free resources. If clearance level is 3, he can access all three resources that is top secret, secret and free. Meanwhile apart from labeling MAC does not allow users to override the policy.

For example, suppose a mail server is predetermined with particular message size to be sent or received. Here neither the recipient nor the sender can disobey or disregard the mail It means no users can override the policy. These two characteristics of MAC model, results in strict security formalization. This is very helpful and useful in defense or military environment. The drawback of MAC is, practically in business world implementation is not possible with standard tools of operating system

C. Content Dependent Access Control (CDAC)

CDAC is a model was found by Moffet in 1991 [2] which decide the access of users to resources on the bases of content present in the resources. It is specially used to preserve and safe guard the sensitive information. An example of CDAC is parental control application in phones and patient record management in hospitals. Each and every detail of patient is not shown to everyone. The main drawback of CDAC is lot of intensive scanning is done on resources. To decide which information is to be shared with resources this results overhead and slow down users. This model is difficult to maintain and manage as well as labor intensive to achieve fine granularity. Fig. 3 depicts access is granted depending upon the content.

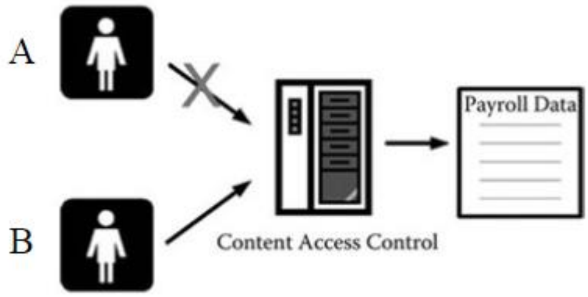

Fig. 3. Content Dependent Access Control

D. Role Based Access Control (RBAC)

In 1992 author Ferraiolo and Kuhn [3] came up with RBAC model. They defined roles, role hierarchies, permissions as well as relationship between user, role and resources. In the year 1994 Nyanchama and Osborn [4] developed model for role organization. In the year 1995 Ferraiolo and Kuhn [5] gave additional insight to RBAC model. In the year 1996 Sandhu, Coyne, Feinstein and Youman [6] described reference models to understand RBAC more clearly and categorized implementation in different ways. In RBAC model users are centralized to set of controls determined by system, not by the administrator or owner to determine how resources are permitted to users. Interaction between users and resources are assigned through permissions, which are associated with roles of users. The appropriate roles are defined to users, to avail resources as shown in Fig. 4.

Merits of RBAC are, firstly administrator cost is reduced. Second is managing resources is simplified through roles. Third is integrity and availability of system is maintained explicitly. Lastly it is comfortable to implement enterprise specific security policies. Demerits of RBAC are, firstly if users have multiple and complex roles RBAC do not support such applications. Managing complex roles, user resources and their interrelationships is daunting task. This is known as role explosion. Secondly RBAC model is static in environment. Users, roles, resources and their relationship are predefined and standardized. RBAC cannot use information that is contextual such as device types, location of user and at what time. Thirdly it is hectic and overhead to maintain and manage. Very often users and different roles get added and admin forgets to remove old roles. During access reviews situations are error prone, time consuming and painful.

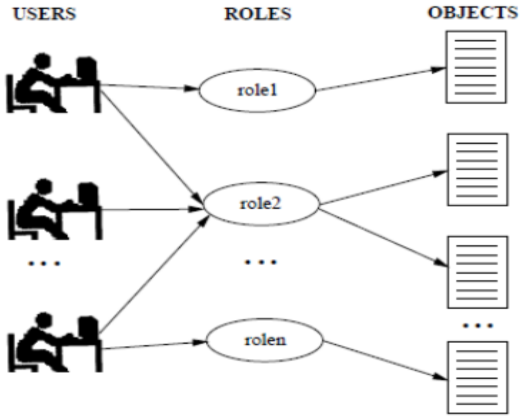

Fig. 4. Role Based Access Control

E. Rule Based Access Control (Ru-BAC)

Ru-BAC is especially used to take off burden of programmers and enhanced security in applications. It was found in the year 1997 [8]. It applies specific rules to decide what all information can flow between users and resources. Generally the logic behind is, If rule X then resource Y. Before a user meets the resources he must satisfy set of predefined rules. Ru-BAC is also known as compulsory access control because rules are enforced stringently and a user must meet those requirements. Rules are not modifiable by users. Its measured drawback is the model doesn’t deal with specific user identity and authorization. Simple example of Ru-BAC is, mangers only accept emails less than fifty. Other great examples are routers and firewalls, they work on Ru-BAC mechanism.

F. Context Based Access Control (CBAC)

Many confuse as content and context sound similar in manner, but both are completely different models. The approach towards CBAC [9] is, it doesn’t solely depend on user’s identity, resources or content of resources but also includes sequence of situation or reviews system events and make decision. Example of CBAC, for certain medical images repository, allows access to body imagery data. If the previous and earlier web history is also referencing to medical related data, based on context authorization is either granted or denied. Another example is firewall which performs inspection. It updates the state of each and every connection whenever new packet arrives. Here on the context of connection, further packages will be allowed. The major drawback of this model is it requires strong and depth knowledge of domain.

Table – I: Summary of various Access Control Models against parameters

policies that are specified in terms of those attributes and

Access Control Models	Parameters						Limitations
	Resource Classification based on	*Generic Functionality*	*Environment*	*Restrictions on Availability of Resources to users*	*Type of Data*	*Execution complexity*	
DAC [1], 1970	Resources are either granted or denied by owners discretion	Built-in	Static	Moderate	Homogeneous	Low	Theoretically this model can be finely grained, actually in reality it is abundantly labor intensive
MAC [1], 1970	Labels and by not allowing user to override policy	Built-in	Static	High	Homogeneous	Low	It is impossible to apply practically in business world using standard tools of O.S
CDAC [2], 1991	Content and type of data	Built-in	Static	High	Neutral	Low	Adds complexity and performance to system
RBAC [3], 1992	User roles	Frame-work	Static	Low	Homogeneous	Low	It limits to deal with sequence of operations in a particular situation
Ru-BAC [8], 1997	Classified between subject and object using appropriate rules	Frame-work	Dynamic	High	Neutral	Low	A specific rule is set to allow usage of resources, but doesn't deal with authorization and identity.
CBAC [9], 2003	Reviews of situation in system	Frame-work	Dynamic	High	Neutral	Moderate	It is not easy to implement, it requires strong and detailed knowledge of domain
ABAC [10], 2010	Attributes	Frame-work	Dynamic	Moderate	Heterogeneous	High	It is flexible but most complex in maintenance once implemented
Geo-Social RBAC [14], 2014	Geo-social constraints	Frame-work	Dynamic	High	Heterogeneous	High	Difficult to implement practically as social ethics may come into role

G. Attribute Based Access Control (ABAC)

To overcome the drawbacks of RBAC, model ABAC was developed [10]. ABAC is unique and different from other approaches as resources are classified on bases of attributes. Access is granted to users on bases of policy formulated with help of attributes. Attributes are building blocks of ABAC, to formulate policies and rules. Formulation of policies is done through Extensible Access Control Markup Language (XAML). It is structured language and comfortable to write and read just as natural language. It is flexible to use RBAC and ABAC model, both combine together in hierarchical manner. RBAC is used to control users and what resources they can see. ABAC can be embedded inside resources to control what they can do in resources.

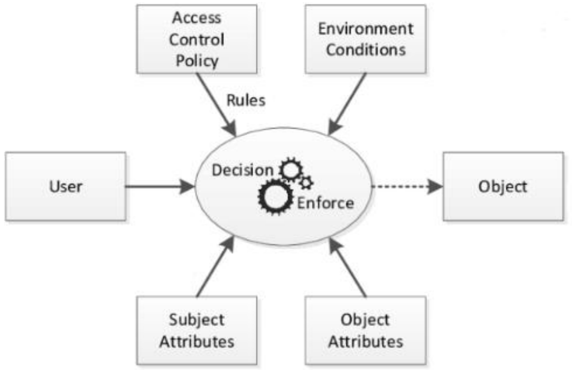

Fig. 5. Attribute Based Access Control

The National Institute of Standards and Technology (NIST) defines ABAC as "An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of conditions." Fig. 5 shows mechanism and logic of ABAC. Advantages of ABAC are, firstly, it allows achieving fine grained control.

Secondly, it has centralized policies and dynamic in environment. ABAC is powerful and flexible model in comparison with DAC, MAC and RBAC. Meanwhile this model is most complex in maintenance and management. Due to heterogeneity of data it introduces complexity during runtime. Example of ABAC, Only managers in India can view the balance of a India_based customer bank account. Here role is the manager (subject), user_location (subject attribute) is India, action is view, resource (object) is balance, resource type is bank account, resource location (object attribute) is India. Access control to manager is granted or denied by taking decision dynamically at run time.

H. Geo-Social Role Based Access Control (Geo-Social RBAC)

The utilization of mobile devices has increased. Most of them are GPS enabled devices, hence it is easy to gather location and social information of user. Geo-Social RBAC is the enhanced model of RBAC model [14]. It utilizes the Geo-Social data that is location and social behavior of a user for granting authorization. To the best of our knowledge this is the first model to include attributes such as location and social data of a user rather than just using geo-social data it also includes geo-social cardinality constraints. Cardinality constraints depicts how many people are related or have connection particularly by a social relation that are required to be in the specified location at the time of resource access.

Geo-Social advantages over RBAC as it supports geo-social constraints and provide high security to an organization. It is also easy to incorporate where RBAC is already working in organization. Overall it helps in enforcing better security than other models. Meanwhile it is complex in implementation and practically during implementation social ethics may come in role.

III. RESULTS AND DISCUSSIONS

Organizations invest heavily to enforce security that is efficient and effective. Current access control models hold one or the other limitations and make them suitable to only particular application areas. Here are the few major limitations listed.

- Static environment access control models are not much suitable to present situations of organizations. Most of the organizations have their own policies and practices, which needs organization to keep on updating the current status and situation to the access control models, which is highly time consuming and labor intensive.

- Availability of resources to users should be such that information should neither be overprotected nor easily or loosely disclosed to users. If there are high restrictions on the availability of resources loyal users get irritated and frustrated. On the other hand if there are low restrictions on the availability of resources, administrators are not happy and confident on their employees. Models lack in knowing the trust level of users of administrators.

- Dynamic environment access control model and heterogeneity of data, increases execution complexity during run time. Practically during the access review time and during classification of resources. It is difficult to maintain the integrity of the information.

IV. CONCLUSION AND FUTURE WORK

We have presented various types of technical access control models their advantages and limitations. We also summarized models against variety of parameters. The parameters analyzed are strong enough to know the characteristics and get insight of each access control models described.

In this modern world, varieties of organizations are present and require different types and levels of securities. Each access control model has its own uniqueness and specialty. Either the specific access control model can be applied or models can be combined to get the best security to an organization. The static models are hectic during maintenance and management as they are very lengthy, painful and time consuming on the other hand dynamic and heterogeneous models introduce complexities during run time as well as they face difficulties to maintain the integrity of the information.

We conclude that efficient, dynamic and trust aware access models are in demand to achieve better securities in organization. Our future work would focus on addressing these issues so as to develop Recommender System for Geo-Social Access Control Framework.

REFERENCES

1. Ling Liu, M. Tamer Ozu, “Orange book” [Online], Available: https://link.springer.com/referenceworkentry/10.1007%2F978-0-387-39940-9_135
2. Moffet, Sloman “Content Dependent Access Control” ACM SIGOPS Operating System review, volume 25, issue 2, pages 63-70, April 1991
3. D.F. Ferraiolo and D.R. Kuhn (1992) "Role Based Access Control" ISth National Computer Security Conference, Baltimore, pp. 554 - 563 October 1992.
4. M. Nyanchama and S.L. Osborn. "Access Rights Administration in Role-Based Security Systems". Proceedings of IFIP WG 11.3 Working
5. D.F. Ferraiolo, J. Cugini, D.R. Kuhn, "Role Based Access Control: Features and Motivations", International Conference on Computer Security Application, Volume 2 Issue 1,Pages 34-64 1995.
6. R. Sandhu, "Role Hierarchies and Constraints for Lattice Based Access Controls", 4th European Symposium on Research in Computer Security, Rome, Italy, pp. 3-33 Sept. 2S - 27, 1996.
7. D.R. Kuhn, "Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-Based Access Control Systems" 2nd ACM Workshop on Role-Based Access Control, 1997.
8. Acevedo, Teresa; Fillingham, David; Nicolettos, John, Enterprise Security Applications of Partition Rule Based Access Control (PRBAC), WET ICE Conference Minutes, June 1997
9. P. McDaniel, “On Context in Authorization Policy”, ACM, SACMAT’03, Como, Italy, June 2003.
10. D. Richard Kuhn ; Edward J. Coyne ; Timothy R. Weil “ Adding attributes to Role based access control” Computer Volume: 43, Issue: 6, pp**:** 79 – 81, June 2010
11. J. Adibi, H. Chalupsky, E. Melz, A. Valente et“The kojak groupfinder: Connecting the dots via integrated knowledge-based and statistical reasoning,” *in Proceedings of the National Conference on AI, 2004.*
12. M. S. Kirkpatrick, M. L. Damiani and E. Bertino, “Prox-rbac: aproximity-based spatially aware rbac,” in Proc. of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, 2011.
13. N. Baracaldo, B. Palanisamy and J. Joshi, “Geo-social-rbac: A location-based socially aware access control framework,” in In Proceedings of the 8th International Conference on Network and System Security, 2014.
14. S. Chakraborty and I. Ray, “Trustbac: integrating trust relationships into the rbac model for access control in open systems” in Proceedings of the 11th ACM SACMAT, 2006.
15. F. Feng, C. Lin, D. Peng and J. Li, “A trust and context based access control model for distributed systems,” in Proceedings of the 10th IEEE International Conference on High Performance Computer and Communications, 2008
16. N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon and K. Moody, “Using trust and risk in role-based access control policies,” In Proceedings of the 9th ACM SACMAT, 2004.
17. B. Aziz, S. N. Foley, J. Herbert and G. Swart, “Reconfiguring role based access control policies using risk semantics,” in Journal of High Speed Networks: Special Issue on Managing Security Policies, Modeling Verification and Configuration, Volume 15 Issue 3, Pages 261-273 , July 2016.
18. L. Chen and J. Crampton, “Risk-aware role-based access control,” in Proceedings of the 7th International Workshop on Sec. and Trust Management, 2011.
19. N. Baracaldo and J. Joshi, “An adaptive risk management and access control framework to mitigate insider threats,” Computers & Security, Volume 39, Part B, pages 237-254, 2013
20. E.EugeneSchultz , “A framework for understanding and predicting insider attacks” Computer and Security, Volume 21, Issue 6, pp 526-531, 1 October 2002
21. Malek Ben Salem, Shlomo Hershkop Salvatore J. Stolfo, “A Survey of Insider Attack Detection Research” Issues in Security, Volume 39, pp. 69-90, 2010.
22. Balaji Palanisamy and James Joshi “A Dynamic Privacy Aware Access Control Model for Location Based Services” IEEE 2nd International Conference on Collaboration and Internet Computing, pp.554-557,DOI: 10.1109/CIC.2016.829,2016
23. William R. Claycomb and Carly “Identifying Indicators of Insider Threats:Insider IT Sabotage” 47th international conference on security Technology(ICCST), DOI: 10.1109/CCST.6922036, 2013
24. Yi-Lu Wang and Sang-Chin Yang “A Method of Evaluation for Insider Threat” 2014 International Symposium on Computer, Consumer and Control, pp. 438 to 441, DOI: 10.1109/IS3C.2014.121, 2014

25. Fatma Alrayes and Alia Abdelmoty "Towards Location Privacy Awareness on Geo-Social Networks" 10th International Conference on Next Generation Mobile Applications, Security and Technologies, pp.105-114, DOI:10.1109/NGMAST.2016.26, 2016
26. Yong Wang , Yuan Ma, Keyu Xiang, Zhenyan Liu, Ming Li "A Role-Based Access Control System Using Attribute-Based Encryption" International Conference on Big Data and Artificial Intelligence(BDAI),2018
27. BoCu, Zhikun, Lan, Xiangyu, Bai "Research on Role-based Access Control in IPv6 Smart Home" IEEE 9th International Conference onElectronics Information and Emergency Communication,2018
28. Shareeful Islam, "A dynamic access control model using authorising workflow and task-role based access control" IEEE early access, DOI: 10.1109/ACCESS.2019.2947377, 2019

AUTHORS PROFILE

Priyanka C Hiremath is a Research Scholar at RNSIT. She earned her M.tech and B.E degrees in Computer Science and Engineering from Visvesvaraya Technological University in 2016 and 2014 respectively. She has got best paper award for paper titled "GSKCG Queries for Collaborative Activity Planning" Her research interests are Access Control Models, information security, privacy, trust management and machine learning.

Dr G T Raju currently working as Head of CSE Dept. RNSIT. He has 25+ years of teaching and 12+ years of research experience. He has published 55 papers in international Journals, conferences. He has organized 28 workshops/FDP/conferences & delivered 30 invited talks. He has received 21 lakhs research grants from AICTE and VTU . He is life member of ISTE and CSI. His research interests are pattern recognitions, web mining, image processing & information retrieval, machine learning and artificial intelligence. He has held various positions at university.