Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2019, 6(4):57-64

Research Article ISSN: 2394 - 658X

Role-Based Access Control (RBAC) in Modern IAM Systems: A study on the effectiveness and challenges of RBAC in managing access to resources in large organizations

Sri kanth Mandru

Mandrusrikanth9@gmail.com

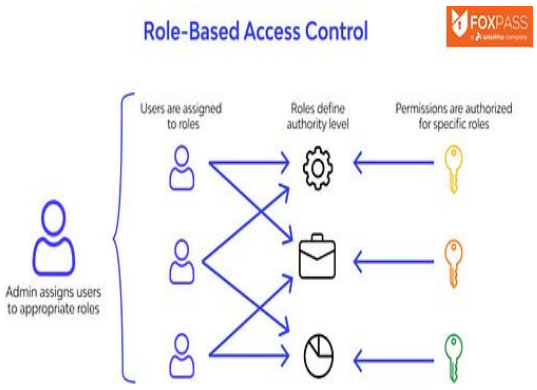
ABSTRACT

Modern Identity and Access Management, IAM, solutions designed for today's organizations cannot be complete without considering RBAC, particularly for large organizations. This paper aims to review the computational results of employing RBAC to enhance the security features and reduce the level of administrative cost, as well as weigh the advantages and disadvantages of this resource access management system. RBAC ensures compliance with the organizational requirements and brings simplicity to access control through the formation of roles that come with certain privileges. However, it is problematic to implement RBAC in large organizations; this remains ongoing and needs to maintain roles, leads to the explosion of roles, and is also complex in role assignment. These are the issues that are discussed in this work, together with possible solutions that include the employment of practical automated role management tools and the introduction of more complex RBAC models. Where and how RBAC is advantageous is also discussed in the paper through the use of case studies and real-life examples, as well as pointing out its weaknesses and the possibility of its development in the future. The findings thus underscore how strategic RBAC is to achieve agile and safe access control in the dynamic business environments of the current world.

Keywords: Role-Based Access Control, Identity and Access Management, RBAC, IAM, access control, security, authorization.

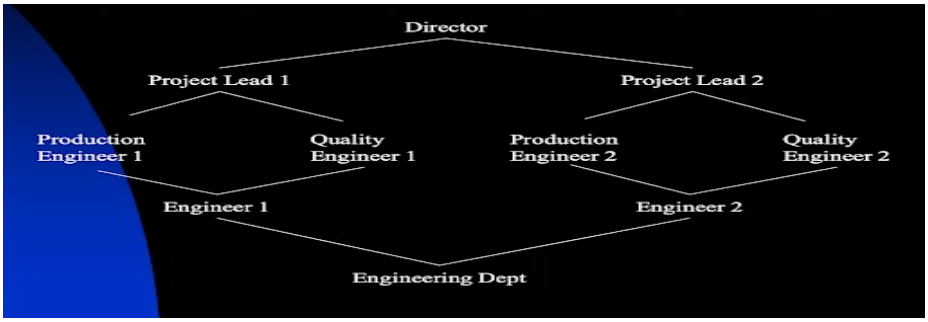
INTRODUCTION

In today's IAM systems for large enterprises, one of the most important components for turning resource access is RBAC, which is short for role-based access control. This is because as the companies grow bigger and more organized, more complexities are experienced, especially in the planning process of making sure that only the right people get the right resources.



Role-Based Access Control

As illustrated above, each user has their own set of permissions for the resources they can access in the growing business. Therefore, only specific staff can carry out the specified roles, which ensures the privacy of the business information. RBAC offered access to some roles instead of concrete individuals. Then, roles are distributed among users, and their positions in an organization are corresponding. In this way, the method secures and optimizes the control of access rights, as it is guaranteed that users have access only to those resources that they need for their work. In addition, because the proposed access controls are easily visible and traceable, RBAC helps organizations adhere to the requirements of regulations. While RBAC implementation has become more established in large-scale corporations, this comes with certain challenges as well [1]. Issues such as role proliferation, where there are just too many roles, and role assignment issues might even make it hard to implement, such as a director who has to oversee several staff as illustrated below;

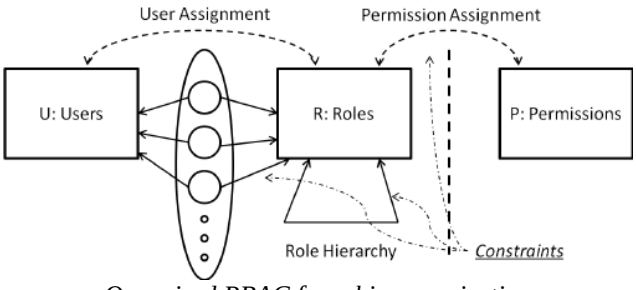


RBAC model of a director overseeing other staff

Thus, the objective of this research is as follows: To identify the problems associated with RBAC and its effectiveness in large organizations. It talks about the issues concerning the deployment of RBAC and covers those for implementing RBAC, including the following Advantages of RBAC. Savings on overhead costs and security. The remainder of this paper brings suggestions on how to overcome general issues. It introduces guidelines on how to successfully implement the RBAC model through the discussion of case studies and examples. Consequently, the findings indicate the significance of RBAC in achieving optimum and safe access control in today's competitive corporate environments.

PROBLEM STATEMENT

A complex problem is the control of resource access in large enterprises. Access management tends to be complex with the increasing size of an organization because size is indicative of a direct proportional growth in the population, systems, and data assets. The workers would probably not have the right access privilege to perform their duties without compromising security. Many intenders of Implementation of mandatory access control, MAC, and discretionary access control, DAC, based access control systems reveal that large businesses discover that other traditionally successful access controlling types are inadequate to meet their goals, as illustrated below, where a complex system has been organized effectively using RBAC.



Organized RBAC for a big organization

Permissions could be granted, and the resource owners decide this lever with the help of DAC; hence, there could be inconsistent and unregulated permissions [2]. Nevertheless, MAC may well be highly structured much of the time and, therefore, even more rigid and difficult to manage, especially in the constantly changing environment of most organizations, roles, and responsibilities of employees. These conventional approaches cannot easily be scaled up, and that leads to either under or over-permissions, which decreases productivity and raises security risks. Another concern that has been identified in the access management research is scalability. The escalation of expansions brings about new management and enforcement of rules across the business; intentions significantly increase with access control policies and permission. Security issues are concerns that can also be noted, and learning is yet another fundamental concern that has been reported as disturbed [3]. The problem of insufficient access control may result in information leakage and unauthorized access to personal information, as well as non-

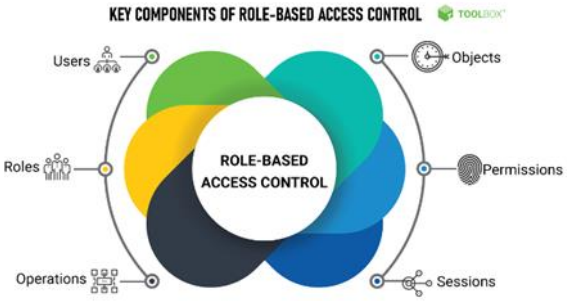
adherence to the requirements of legal acts. Traditional paradigms do not offer enough capability and scale to accomplish these security requirements. Therefore, one can conclude that it is necessary to introduce a more elaborate concept of access control, namely Role-Based Access Control (RBAC). That is the reason why, in RBAC, permissions are assigned to roles, not to concrete users; it is scalable, controllable, and safe. It also makes permission control easier and enhances security through standardized and traceable methods.

SOLUTION

They are highly organized for controlling access to resources because RBAC assigns rights to roles rather than users. Since several users are not allowed to gain direct access to the resources needed for work, only the administrator has access; this method enhances security and organizational efficiency. RBAC mainly includes role assignment, role authorization, and permission assignment. It is granted to the roles that are defined according to the employee's job titles or tasks within the organization. After role assignment, people are endowed with authority that is attributed to their responsibilities. RBAC is beneficial in matters of security concerning access control since it is relatively easy to implement and keep track of. The approach of role-based permission makes it easier to enforce standard measures across the organization. This enhances the level of compliance with the law and reduces the probability of unauthorized entry into one's house [4].

Tracking of each entry to private information

As illustrated above, each entry to the private information is tracked. Hence, unauthorized personnel trying to access the information would be detected promptly. They might also ensure that their access control rules remain relevant to their security objectives and the organization's processes by periodically reviewing roles and permissions, as illustrated below;



Role-Based Access Control in assigning roles and permission

Position hierarchies and constraints are concomitant elements that allow a certain position to obtain permissions from other roles and division of tasks, respectively. Contemporary IAM systems consist of RBAC through the help of administration consoles that allow one to put in place, transform, and dispense roles and privileges. Managers can define and identify roles with the help of tools that tend to be implemented in these systems and act according to the actual usage statistics. It is obvious that to incorporate RBAC into modern IAM concepts; it is vital to link the concept to present permission and authorization mechanisms.

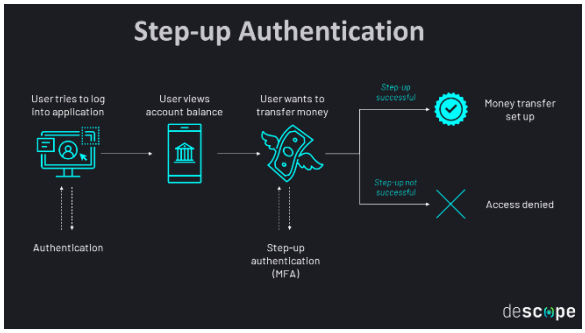
USES

RBAC is among the most effective and versatile methods for controlling access to some or all of the resources within an organization. They have created product layout applications through the employment of the Internet in numerous fields, excluding production, analysis, development, telecommunications, and many others. The industrial sector relies on RBAC. Large supply chains, technical processes, and complex tools are incurred in manufacturing fields. RBAC helps to minimize the worker’s access to effective product production details and tools to only those workers who ought to access such resources on the production floor. Operational security also ensures

compliance with safety measures and practices regarding the operations of the business. If you wish to guarantee that only individuals in the maintenance department can set the machine, you can give them a role that only enables them to run the equipment. Due to the effectiveness with which it is able to enhance security and bring in automation in access control, RBAC is quite versatile in its applicability to several organizational contexts. RBAC is widely used in IT, health care, finance, government sectors, and the educational field, to name but a few, as all these benefit from the structured and scalable RBAC model. RBAC is crucial in managing access to such valuable information as patients' data in the healthcare sector [5]. Implementing a system that supports passkeys such as fingerprints becomes very secure, as illustrated below;

Illustration of fingerprint-enabled system

Healthcare companies may ensure that according to the RBAC, administrative personnel, physicians, and nurses can only access the data that is necessary for their work. For example, administrative staff may be able to see only billing details, while doctors may be able to see all the details of the patient. Besides helping to monitor compliance with HIPAA, this minimizes the potential for unlawful disclosure of data [6]. By applying RBAC, R&D managers may delegate responsibilities based on the researcher's involvement in the particular project, thus restricting researchers' access to the necessary resources only. This enhances a safe research environment because the respondent can disclose sensitive information to the wrong people. Organizations may ensure that within a certain department, different tasks are assigned to network administrators, customer service attendants, and technical support personnel in equal measure to ensure everyone gets a fair share of telecom company work. This has the side effect of increasing safety and decreasing the complexity of work by providing the necessary data and tools to the employees. For example, network engineers get to work with the configuration files, but the customer service representatives only get to work with the billing section. Scarcely, a school or college, starting from elementary and high school and going up to the universities today, does not apply RBAC to restrict or permit who may access what in their administrative systems, research data banks, and students' records. Access rights may be restricted to organizational roles such that each role is required to perform, and their status may be configured as a student, a teacher, or an official. Instructors are the only ones who can view one student's or many students' data; students can only view their profile and what is expected from them in their class. This preserves any specific data and, at the same time, avoids disagreements with the laws of education, among them being the FERPA. In the same respect, RBAC benefits the financial sector profoundly. Security measures have to be applied to the banks and other large financial organizations' data due to the great amount of sensitive information that fraudsters and hackers can potentially exploit, which demands secure procedures such as those illustrated below.



Step-up authentication

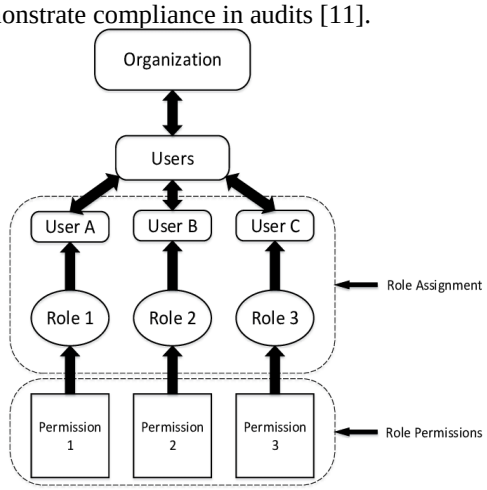
Since the permissions are granted based on organizations' positions, RBAC helps such businesses ensure that tellers, loan officers, and IT personnel get optimal access levels [7]. In government organizations, RBAC is employed to provide access to different degrees of government data and protect secret data. An agency may be able to control data access by implementing roles and access rights, thus ensuring that only those with the right clearance will be able to view the information that is critical to their functioning [8]. This strategy thus helps in the

preservation of national security and compliance with laws like the Federal Information Security Management Act. Colleges and universities in the education sector implement RBAC in order to regulate the access of student records, research-related data, and administration systems. The relations that characterize who has access to the important data of a faculty, students, or administrative personnel safeguard the information and ensure the best outcome. Some of the advanced RBAC applications include smart city and Internet of Things (IoT) domains. Transport, safety, and facilities that function in a smart city under the government rely on each other since they are joined. Thus, through the allocation of responsibilities that various municipal authorities and service providers manage, RBAC can help in controlling access to the mentioned systems. For instance, positions in public safety may lead to monitoring systems and emergency response equipment, and other related jobs may lead to traffic lights and their operations. This is an organized access control aimed at the protection and efficient running of systems that are essential in societies. Legal departments and companies themselves may ensure that the information about a particular case is only disclosed to individual employees such as lawyers, paralegals, and administrative assistants who are involved in the completion of the particular case. It helps to maintain compliance with all the legal requirements of the privacy regulations and ethical practice in law while at the same time respecting the do-no-harm principle of clients' rights to privacy.

Regarding the access control issues of hybrid and remote workplaces, RBAC rules the world. Thus, there is a benefit in RBAC, where workers are allowed to have access to the company's resources regardless of location, which is crucial in today's environment, where working from home is becoming normal. It is possible to maintain the security and efficiency of the distributed workforce by creating roles, meaning that the position of the employee will determine access levels.

IMPACT

In terms of the clear system of roles and permissions for access, RBAC is a significant enhancement for the corporations' security and performance. Business highlights of RBAC are its ability to execute the ideas of least privilege and ensure that the users are only granted access to what is necessary for their roles within the organization. This increases general security as it reduces the risks of unauthorized access to valuable information. In addition to keeping the company's information secure, RBAC helps to minimize internal risks and prevent the leakage of information due to the ability to monitor all actions within the framework of access control. RBAC helps to control user authorization in a better manner; it decreases administration costs, and the cost takes less time [9]. While assigning some rights to the user, administrators may assign roles to users, which makes this procedure faster and reduces the chance of mistakes. It eliminates chances of establishing access control in some areas while leaving others; it essentially ensures even distribution of access control throughout the company and is time-saving, too [10]. In addition, RBAC is easier when it comes to the introduction and dismissal of certain staff members since authorities may be quickly assigned or removed as needed. Documentation of the roles and permissions assigned to the staff helps the firms easily demonstrate compliance in audits [11].

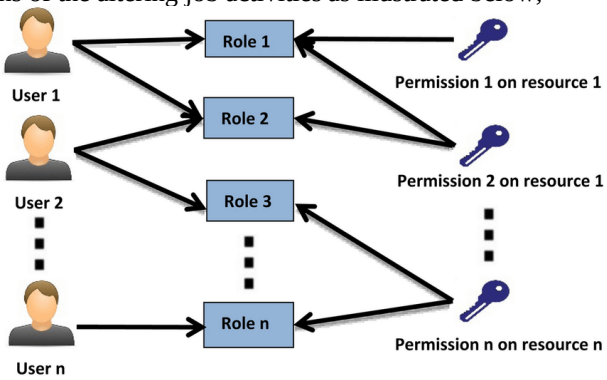


Format of a Role-Based Access Control Policy

It can be concluded that one of the greatest advantages of RBAC is that it is structured. Thus, it enhances access control enforcement that meets the required regulatory regulations, with minimal chances of incurring fines resulting from non-compliance.

RBAC is not without its drawbacks, however. The problem of role explosion, that is, a man can become a member of an uncontrollable number of groups and receive an incredible number of different roles, which creates difficulties and confusion, is one of the constraints. This can, however, be reduced through proper job design and addressing issues relating to role mining, a process whereby organizational inefficiencies in Terms of locating and eliminating

insignificant responsibilities are identified [12]. Moreover, constant efforts are required to maintain relevant roles and provide accurate reflections of the altering job activities as illustrated below;



Principles of role-based access control model

To ensure that the RBAC system is working optimally and aligned with the organization's needs, one might consider conducting periodic assessments and adjustments of roles and privileges. The first resource deployment for RBAC is likely to be costly. It demands considerable time to allocate for planning and the coordination of activities, which is another challenge. To address this, organizations may apply a phased approach in implementing RM for the core systems first and then gradually spread it to the other domains.

SCOPE

Considering contemporary IAM systems, RBAC has more extensive significance compared to its traditional approach to Access Management, addressing new technology advancements and cybersecurity factors [13]. This is more so because more and more enterprises are implementing sophisticated IT systems where RBAC's capability to offer sound and hierarchical access control is critical.

Growing need for RBAC systems for expanding businesses

Contemporary IAM systems use RBAC because it is more efficient and structured than other methods of access control. It affects many facets of a company and the cybersecurity field, not strictly limited to methods of access management. One of the many uses of RBAC is the building up and integration of other existing enhanced security mechanisms such as PBAC, ABAC, and FGAC. Organizations might adopt fine-grain access control to provide precise on how data can be accessed and used since it allows them to set permissions at the item level. To further enhance the access control granularity, Role Base Access control introduces a tap in which different extents of access to individual data items are granted to specific roles. This integration also brings a significant enhancement in the level of security since only the permitted personnel get access to such details. RBAC must be supplemented with other IAM components that contribute to the creation of solid and long-lasting security systems such as SSO, AAC, and MFA [14]. However, ABAC is also effective in granting access rights because the access rights depend on the user's attributes, such as job position, department, or location. Therefore, as an additional measure of security, the ABAC checks on real-time characteristics to further enhance the RBAC's system of access control. Accordingly, the integration of the two approaches provides a better solution to access control compared with the single approaches of RBAC or ABAC, combining flexibility with security. RBAC is also widely utilized in PBAC environments. Based on the organizational policies and regulations, PBAC defines access control decisions. Because RBAC assigns an organization's role structure in harmony with its tasks and duties, it may enhance the smooth functioning of such policies. With such cooperation, the currently valid access control rules of the company and the appropriate actions are always in force and applied consistently.

Within modern IT environments, apps, devices, and services alongside human employees and contractors are managed by RBAC and, therefore, fit the definition well. Thus, by leaving the tasks to these entities, businesses can regulate who utilizes which capacities and access to what assets, and thus, only those applications and devices that are allowed may in any way interact with the private data. RBAC continues to serve a crucial purpose, even more so

where the topology is fragmented and cloud environments are in use. Many organizations adopt a great number of cloud productions and providers, each of which provides its way of addressing the access control problem. Li preceded by proposing that in all of these different contexts, there is only one way to sustain reliable and coherent access control, which is by using RBAC. Especially in matters concerning all regulations and standards of the market, this has to be done in many cases. Therefore, the main expected, driven enhancements of RBAC technology are thought to be the integration of role assignment and permissions through machine learning and artificial intelligence and the enhancement of integration abilities. These innovations will also assist businesses in understanding shifting security risks and business environments to make better decisions. Other factors that are likely to shape future RBAC implementations include the emergence of new zero-trust models that proactively assume that threats could be internal or external. Here, RBAC will have to be more proactive in responding to users' actions and constantly adjusting permissions based on the levels of risk identified. RBAC is highly effective in the modern, ever-developing areas of cybersecurity and data privacy [15]. RBAC offers a lasting approach for assuring compliance with regulatory requirements and data protection laws while at the same time ensuring the access controls identified are overt and traceable. Due to the growing emphasis on data confidentiality, RBAC helps companies implement detailed access control measures that protect lost data.

CONCLUSION

Contemporary IAM solutions cannot but incorporate such security measures as RBAC, specifically in large companies. Moreover, to demonstrate the applicability of RBAC with regard to advantage in security enhancement, reduction of the number of workers' administrative tasks, and compliance with legislation, it is possible to assess the specifics of various benefits and limitations of this approach to resource management. Thus, RBAC facilitates the management of access rights as it relates to roles, not people. It also provides a feasible solution to volumes' difficulties related to complex organizational structures. Even while involving RBAC has its advantages, it is not without its challenges, such as role proliferation and subsequent constant role management. Perhaps one of the most crucial prerequisites to RBAC is the careful planning of such a move that includes regular audits and even the use of innovative solutions that will help manage responsibilities adequately. The ability of RBAC to offer dependable means of access control together with methods of audit capability will progressively become valuable in the future, given the dynamic state of cybersecurity and increased stringency of data protection legislation. Thus, organizations have to develop their RBAC policies further to meet their security and compliance objectives as well as address new risks and ensure that access controls are integrated with organizational goals. In summary, despite the updates in the modern approach to access control, RBAC remains a relevant structure that ensures the organization's assets are protected in a structured and safe manner.

REFERENCES

[1]. E. Sturrus and O. Kulikova, “Identity and Access Management,” pp. 396–405, May 2016, https://doi.org/10.1002/9781118821930.ch33

[2]. L. Martin, “Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management,” Information Systems Security, vol. 16, no. 1, pp. 9–14, Mar. 2007, https://doi.org/10.1080/10658980601051268

[3]. M. V. Thomas and K. Chandrasekaran, “Identity and Access Management in the Cloud Computing Environments,” in Advances in systems analysis, software engineering, and high-performance computing book series, 2016, pp. 61–90. https://doi.org/10.4018/978-1-5225-0153-4.ch003

[4]. M. A. Thakur and R. Gaikwad, "User Identity and Access Management trends in IT infrastructure- an overview," Jan. 2015, https://doi.org/10.1109/pervasive.2015.7086972

[5]. A. M. Lonea, H. Tianfield, and D. E. Popescu, “Identity Management for Cloud Computing,” in Studies in Computational Intelligence, 2013, pp. 175–199. https://doi.org/10.1007/978-3-642-28959-0_11

[6]. O. Alsaadoun, “A Cybersecurity Prospective on Industry 4.0: Enabler Role of Identity and Access Management,” Mar. 2019, https://doi.org/10.2523/iptc-19072-ms

[7]. S. Chung, S. Moon, and B. Endicott-Popovsky, “Architecture-Driven Penetration Testing against an Identity Access Management (IAM) System,” Sep. 2016, https://doi.org/10.1145/2978178.2978183

[8]. N. Naik and P. Jenkins, “A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards,” Mar. 2016, https://doi.org/10.1109/mobilecloud.2016.22

[9]. M. Hummer, M. Kunz, M. Netter, L. Fuchs, and G. Pernul, “Adaptive identity and access management—contextual data-based policies,” EURASIP Journal on Multimedia and Information Security, vol. 2016, no. 1, Aug. 2016, https://doi.org/10.1186/s13635-016-0043-2

[10]. J. Xiong et al., "PRIAM: Privacy-Preserving Identity and Access Management Scheme in Cloud," Transactions on Internet and Information Systems, vol. 8, no. 1, pp. 282–304, Jan. 2014, https://doi.org/10.3837/tiis.2014.01.017

[11]. F. Schell, J. Dinger, and H. Hartenstein, "Performance Evaluation of Identity and Access Management Systems in Federated Environments," in Springer eBooks, 2009, pp. 90–107. https://doi.org/10.1007/978-3-642-10485-5_7

[12]. N. A. P, P. N. Railkar, and P. N. Mahalle, "Proposed Identity and Access Management in Future Internet (IAMFI): A Behavioral Modeling Approach," Journal of ICT Standardisation, vol. 2, no. 1, pp. 1–36, Jan. 2014, https://doi.org/10.13052/jicts2245-800x.211

[13]. [13] F. Damon and M. Coetzee, "Towards a generic Identity and Access Assurance model by component analysis - A conceptual review," Nov. 2013, https://doi.org/10.1109/es.2013.6690086

[14]. S. N. Dhanabagyam and G. R. Karpagam, "Identity and access management as a service in the e-healthcare cloud," International Journal of Biomedical Engineering and Technology, vol. 26, no. 3/4, p. 250, Jan. 2018, https://doi.org/10.1504/ijbet.2018.089955

[15]. M. T. Banday and S. Mehraj, "Directory services for identity and access management in cloud computing," Dec. 2017, https://doi.org/10.1109/icatcct.2017.8389157