









Review Article

Traditional and Hybrid Access Control Models: A Detailed Survey

Muhammad Umar Aftab ^{1,2}, Ali Hamza ¹, Ariyo Oluwasanmi ³, Xuyun Nie ^{2,3},
Muhammad Shahzad Sarfraz ¹, Danish Shehzad ¹, Zhiguang Qin ^{2,3},
and Ammar Rafiq ⁴

¹Department of Computer Science, National University of Computer and Emerging Sciences, Islamabad, Chiniot-Faisalabad Campus, Chiniot 35400, Pakistan

²Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu, China

³School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

⁴Department of Computer Science, NFC Institute of Engineering and Fertilizer Research, Faisalabad, Pakistan

Correspondence should be addressed to Xuyun Nie; xynie@uestc.edu.cn and Zhiguang Qin; qinzg@uestc.edu.cn

Received 21 October 2021; Revised 11 December 2021; Accepted 30 December 2021; Published 7 February 2022

Academic Editor: Thippa Reddy G

Copyright © 2022 Muhammad Umar Aftab et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Access control mechanisms define the level of access to the resources among specified users. It distinguishes the users as authorized or unauthorized based on appropriate policies. Several traditional and hybrid access control models have been proposed in previous researches over the last few decades. In this study, we provide a detailed survey of access control models and compare the traditional and hybrid access control models based on their access control criteria. This survey focuses on the growing literature of access control models and summarizes it through comparative analysis, identifying limitations and illustrating the advantages of both traditional and hybrid models. This study will help the researchers to get a deep understanding of the traditional and hybrid access control models.

1. Introduction

Information is the most important asset of any organization that must be secure. The security of information can be ensured with the help of confidentiality, integrity, and availability [1, 2]. Furthermore, an organization's information can be secured with different approaches or technologies such as intrusion detection, steganography, cryptography, and access control [3–5]. These approaches are used according to the goal and objective of the information and organization.

Access control (AC) is one of the best approaches that is used to secure the information from inside and outside attacks of the organization and decisions of granting and revoking access to any user [6]. The access control gives access to those who are authorized to organizations, i.e.,

persons, processes, and systems. The access control models define its mechanisms and security policies first, and then, these models are implemented in organizations according to goals and objectives [7]. There are several traditional and hybrid access control models that have various pros and cons.

The traditional access control models are discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC). In the DAC model, the owner of the object has the authority to give and deny access to others without a system administrator mechanism [5]. The DAC model is divided into two types: strict DAC and liberal DAC. In the strict DAC model, only the owner has the authority to permit and deny access to created resources, but in the liberal DAC model, the authority of the owner can be

transferred to another individual who will be able to permit and deny the access. In the MAC model, the centralized mechanism is used to permit and deny the access of resources to users [8]. The MAC model is more secure, flexible, and efficient for commercial and military use due to its centralized behaviour. The RBAC model is prominent due to the least privilege and tight security that makes it more powerful than all other models [9]. The ABAC model has dynamic behaviour that is the most suitable model for changing environments [10]. There are some disadvantages of both RBAC and ABAC models. So, researchers proposed some hybrid models as an extension of RBAC and ABAC.

The existing surveys on access control provide a review of basic access control models, i.e., MAC, DAC, RBAC, and ABAC, or focus on access control trends, i.e., IoT, cloud, and fog computing, but there is no comprehensive survey that explains advanced access control models with their framework and applications along with pros and cons. So, this study presents access control models and advanced hybrid access control models with their framework and applications in a comprehensive manner. The access control models are used in small and large organizations according to the pros and cons of the model and the requirements of the organization. This survey encourages the researchers to propose new hybrid access control models according to the problem.

There are some existing survey studies on access control models that tried to explain access control policies with few models in specific contexts, i.e., IoT, cloud, and fog computing. Bertin et al. [11] conduct a survey paper that explains the basic access control model in detail, but this study does not include advanced hybrid access control models. The studies [12, 13] conduct surveys that focus on IoT security and challenges, and they proposed solutions based on a trust-based access control model. Zhang et al. [14] present a survey paper that explains some access control models and trusted system computing in the IoT domain. The author proposed a novel method for IoT that includes access control, network attack, and trusted computing, but this study does not explain the applications, limitations, pros, and cons of each model.

The rest of the study is organized as follows and also described in Figure 1. The second section describes the access control and its traditional and hybrid models. The third section makes comparisons of the access control models, and the fourth section concludes the study.

2. Access Control

The access control (AC) mechanism is used to permit or deny the access of resources within the organization to secure the data [6]. The AC permits the access of resources only to authorized personnel of the organization and denies the access of resources to unauthorized and other users. The access control is normally consisting of identification, authentication, and authorization. The access control grants access to authorized users according to user privilege level after authentication [15]. The access control is classified into traditional and hybrid models as shown in Figure 2. The traditional access control is further divided into four types:

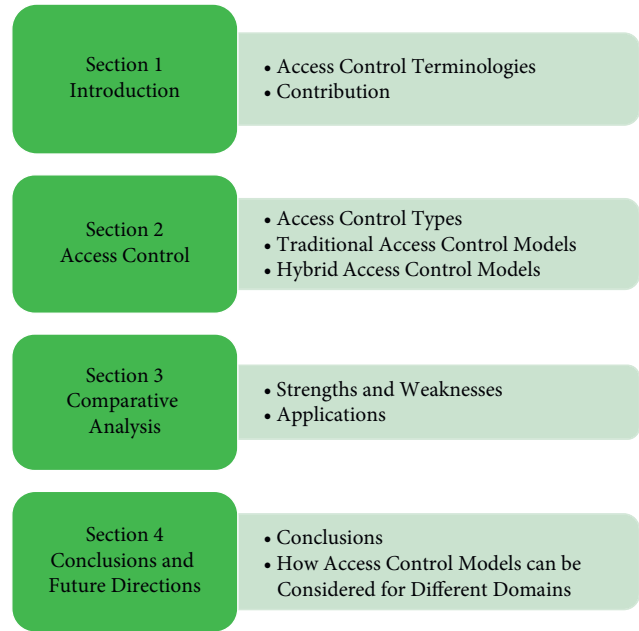


FIGURE 1: Organization of the work.

MAC, DAC, RBAC, and ABAC. The hybrid access control has also several types. Each traditional and hybrid access control model has its pros and cons. So, organizations use access control models according to their objectives and goals.

2.1. Traditional Access Control Models. There are different traditional models of access control, i.e., MAC, DAC, RBAC, and ABAC. Each model has its pros and cons. The traditional access control models are classified into two categories: DAC and non-DAC. The non-DAC is further divided into MAC, RBAC, and ABAC [16]. The traditional access control models are also compared with each other based on criteria; the principle of least privilege, dynamic behaviour, safety of models, separation of duties, capability delegation, configuration flexibility, and auditing as shown in Table 1.

2.1.1. Discretionary Access Control (DAC). The DAC is a model that allows owner-based access where the owner is the creator of a resource or object. The owner of the object decides the access granting or revoking policy for the subjects or users as shown in Figure 3. In this manner, there is no need for the administrator to provide its services regarding access rights. DAC is divided into two different types: liberal and strict DAC. According to the liberal DAC, the owner can transfer the access rights or ownership to other individuals so that they can also work as an owner of the resource. On the contrary, the access rights are limited to the owner of the resource, and ownership is restricted for that individual, in the strict DAC [17, 18]. It can be assumed that the DAC model works according to the choice or discretion of the owner. The enforcement of access control policies is made on three different categories: resource

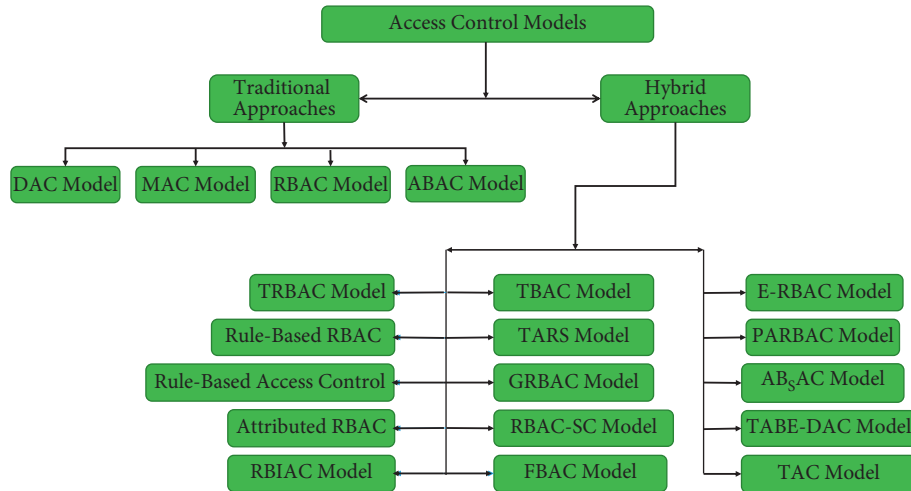


FIGURE 2: Types of traditional and hybrid access control.

TABLE 1: Comparison of traditional access control models.

Criteria	DAC	MAC	RBAC	ABAC
Principle of least privilege	X	X	✓	✓
Dynamic behaviour	X	X	X	✓
Safety of models	X	✓	✓	✓
Separation of duties	X	X	✓	✓
Capability delegation	✓	X	X	X
Configuration flexibility	✓	X	✓	X
Auditing	✓	✓	✓	✓

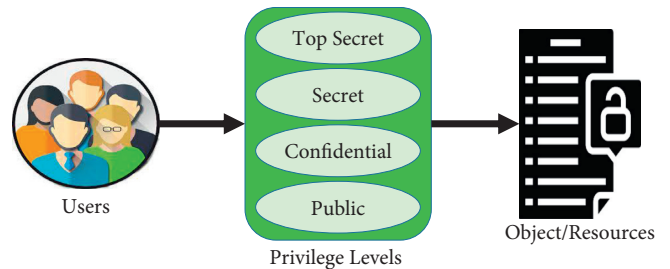


FIGURE 4: Abstract view of mandatory access control (MAC).

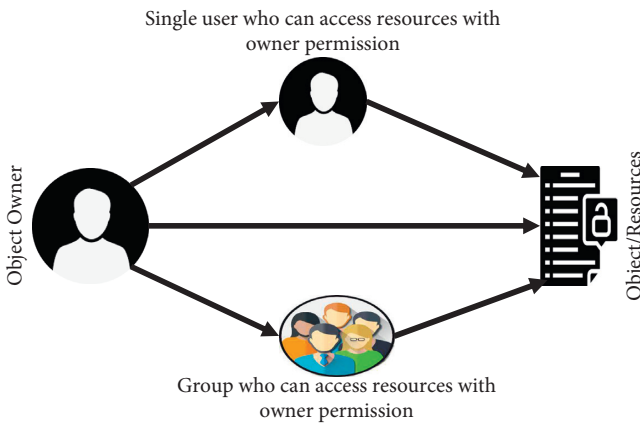


FIGURE 3: Abstract view of discretionary access control (DAC).

ownership, user identities, and permission delegation. DAC is not an appropriate model for commercial and government organizations due to the deficiencies or limitations because it allows the users to set or deploy the access rights that might lead it towards Trojan horse attacks [19]. Moreover, DAC is popular due to its integration quality with different types of computer systems.

2.1.2. Mandatory Access Control (MAC). MAC works on the basis of security labels that can be either taken as a hierarchy model. It controls the access rights of users or processes against the resources of the system. The users are assigned to various

security levels, while the objects are assigned to security labels as shown in Figure 4. The user access is affiliated with the security levels of resources that are equal or lower than their hierarchy [20]. The access control rights are strictly controlled by the administrator, who can also set the permissions in the access control. MAC is effectively used for military and commercial systems due to its high-level security [21,22]. There are some limitations of MAC such as difficult to manage the MAC systems because the system puts all burden on the administrator to set permissions, manage configurations, and future maintenance. This complexity may increase as the size of the system increases [23]. Furthermore, the MAC operating systems are costly to set up and hard to operate due to the dependence on the trusted parts [24].

2.1.3. Role-Based Access Control (RBAC). The RBAC model made a revolutionary change in the field of access control due to its strictness and tight security. This model is based on five different entities: objects, actions, permissions, roles, and users, as shown in Figure 5. Objects are considered as the resources such as directories, files, or folders. In addition, actions are the tasks or operations that can be performed on the objects. The examples of the actions are write, edit, and delete. The permissions are the combined form of an object and action; such one permission can be considered as “Edit (action) and File.doc (object).” Any change in the action or object will be considered as new permission. The intermediate and one of the key entity of RBAC is the role that connects users and permissions. The

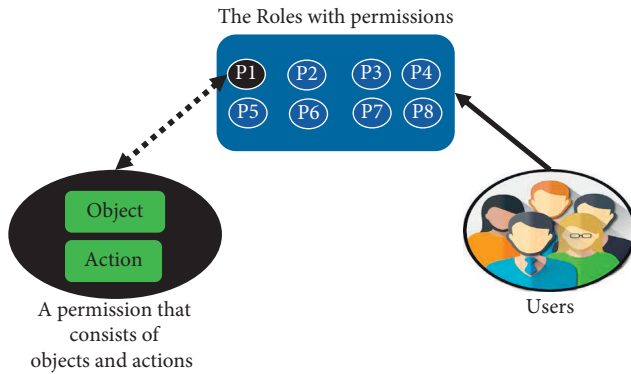


FIGURE 5: Abstract view of role-based access control (RBAC).

roles are the containers that have various permissions. For example, a role named “deputy manager” contains all necessary permissions to fulfil or perform the tasks of the deputy manager. Furthermore, the roles are assigned to users according to their designated positions. After assigning the roles, the permissions inside every role are automatically assigned to users [25]. RBAC provides the least privilege with the usage of roles that is the central entity between users and permissions. In this way, RBAC is not allowing users to deal with the permissions directly and it eradicates the ownership rights. So, it behaves significantly better as compared to DAC because the ownership rights of a resource owner may lead to a Trojan horse attack [26]. RBAC implements the least privileges using the concept of roles because a user can only access those permissions that are assigned to the role, not more than that. This is one of the reasons that makes it popular. On the contrary, RBAC puts a lot of burden on the administrator by managing all the tasks related to permission creation, permission and user assignment to roles, role designing, etc. As the size of the organization increases, the workload of the administrator will also increase [27]. RBAC also violates the rules of separation of duties provided in the NIST standard [25]. The violations are discussed in detail by some researchers [9, 26, 28].

(1) *RBAC Model Components.* The RBAC model is most suitable for healthcare centers and especially for the hospital to make sure the security features of all the records and information details of a patient [29]. Interestingly, RBAC is implemented in the dialysis department for kidney disease due to flexibility and security. The sessions are used to connect users. A user may have more than one session at one time. The RBAC model is classified into three components or modules: core RBAC, hierarchical RBAC, and constrained RBAC. The constrained component of the RBAC model is further divided into two parts: dynamic separation of duty (DSD) and static separation of duty (SSD). The main reason behind this tight security is the implementation of dynamic and static separation of duty [25].

(i) *Core RBAC.* The core RBAC is an essential and fundamental component of the RBAC model that is implemented first in any organization, and then, advanced components of the RBAC model are considered to implement [30]. A user is described as a person, and the role of user denotes functionality and authority. The permission represents a permit

to do any operation on more than one object. The permission can be read and write. The object is anything that is holding some information or receiving information. The object can be a row, table, directory, view, or file. Also, the object might be CPU cycles, printer, or disk storage space.

The main concern of the core RBAC model is to assign users and permissions to roles in many-to-many fashions. It is possible to assign one role to one or more users and vice versa. It is also possible to assign permission to one or more roles and vice versa. There is a lack of research on permission, roles, and their relation. Some authors proposed the symmetric RBAC model that applies constraints on permissions using role hierarchies and separation of duty (SOD) [25].

(ii) *Hierarchical RBAC.* The hierarchical RBAC is the second component of the RBAC model that is constructed on the basis of core RBAC component [30]. The roles are implemented using the role hierarchy (RH) concept that is based on the firm’s authoritative structure [31]. In RBAC, the roles faced some common standard permission again and again, which is not a better choice. The RH is used to link the same permission so that the security admin can face the same permission in few roles. Hence, every role will contribute common permissions and will lie in RH [32]. There are some roles that standalone separately with the RH approach.

In role inheritance (RI), all permissions of juniors can be assigned to senior roles and junior roles cannot have permission as having senior roles. The system cannot manage the situation when junior needs to access the permissions of senior role. The security admin has to permit and deny the same permissions again and again without RI that is a very hard job. This thing needs to be a hierarchy feature in the form of a tree with respect to different categories such as a senior, junior, junior-most, and senior-most. The role inheritance is the best choice for such type of situation; from one side, a role may inherit some permission, and on the other side, another role can inherit some permission [33].

(iii) *Constrained RBAC.* The constrained RBAC has some specific constraints along separation of duty (SOD) to implement. These constraints can be either location-based or time-based. The main theme of these types of constraints is to grant access based on specific time slots and locations. The RBAC constraints enable RBAC with the implementation of information security, which protects the whole system from both external and internal threats. Same as RBAC, the safety conditions are confirmed for access control models [34].

2.1.4. *Attribute-Based Access Control (ABAC).* ABAC is a model that is capable to provide fine-grained access control, flexibility, and dynamicity. The main story revolves around

the attributes allocated by the attribute authorities. The Boolean formula is used to define an access control policy using the set of attributes so that an authorized and valid access can happen. There is no need to create and assign numerous roles. Moreover, there is no need to make or design access control lists for everyone in the organization [35, 36].

The attributes provide the facility to automatically perform access control decisions. Examples of attributes are citizenship, IP address, identity, location, and user-name. ABAC works on the evaluation rules of the attributed entities such as objects and subjects, environment related to a request, and operations. If the attributes, as well as attribute values, match, then the access is granted to a user; otherwise, access is denied [37, 38]. The benefit of this facility is the dynamic behaviour as shown in Figure 6. In this manner, any change in the attribute values or user identities will be dynamically detected and the decision has been made. Previously, the RBAC model was unable to deal with this issue. On the other hand, the ABAC model has complexity issues. If the number of the attributes increases, then the complexity of the system will also increase [27, 28].

Figure 6 shows that each subject and object has its own attribute. The attribute-based access control allows the subject to access objects by checking attributes. In Figure 6, *desig*, *locat*, *categ*, and *AR* stand for designation, location, category, and access rules, respectively.

The user of system will define as subject by the administrator to access the file management system. The characteristics of user will capture as subject attributes. The attributes of subject can be name, designation, organizational affiliation, gender, age, nationality, or security clearance. The identity information of subject is maintained by administrator or authorities in file management system. The proper management and assignment of subject attributes on a regular basis are required as member leave or joins the organization on a regular term [39].

The required functionality of ABAC is based on device policy, documents, or procedural rules on which a business operates. The object may have a policy or rule on which it allows access to the subject. For example, only physician is permitted to access the patient record or information for treatment and prescription in a medical emergency setup. The nonmedical person is not allowed to access the information recorded in the file of a patient. This case also defines access privileges for a specific subject [40].

The ABAC protects the objects as object, subject, attributes, and policies are defined. The access control method gathers information related to the subject, object, and policy to render the logical decision for the execution of the requested operation. Access control mechanism (ACM) must be smart enough to recognize information, policy, attributes, and their chronology and source along with necessary computations for decision-making [41].

The policies related to ABAC depend upon the richness of computational languages and the degree to which attributes are available. The system is flexible when subjects can access more objects. A subject can have

maximum access to maximum objects and can perform a number of operations on the object under the established policies or rules. It is not required to create a new additional role in the system with new members because a new member shares the same attributes that are already defined. For example, a nurse wants to access patient information in medical emergency, and there is no need to set a new rule set or policy as it shares the same attributes defined earlier.

The four basic access control models are compared with each other on the basis of parameters, i.e., least privilege, dynamic behaviour, safety, separation of duties, capability delegation, configuration flexibility, and auditing as shown in Table 1. The principle of least privilege means that the user should have access to only the necessary resources when needed to do a specific operation or task. The dynamic behaviour means that the operations and tasks should be performed automatically using different access rules rather than manual instructions. The safety of models means preventing permission leakage of access control models from unauthorized users. The separation of duties means permitting the access of resources only to authorize users and denying the access request of unauthorized users. The capability delegation means the ability of a user to revoke their own features to other users that have already been granted. Configuration flexibility means providing an easy way to users for installation and uninstallation like the wizard menu. Auditing means monitoring the access control model by recording requests from users.

2.2. Hybrid Access Control Models. In this section, we explained various hybrid models that are extensions of traditional AC models.

2.2.1. Temporal Role-Based Access Control (TRBAC). The TRBAC [42] is an advanced form of the RBAC model that eliminates non-permanent limitations on the on/off switching of roles. The TRBAC braces up seasonal role enabling and disabling and transitive dependencies on those types of activities. Those forms of dependencies that are stated using role triggers can also be utilized to limit the series of roles that a specific user can make operative at a particular period. The release of a trigger can lead to the switching on or off of a role that can happen instantly or after a specified period of time. The enabling and disabling activities can be assigned for resolving disputes, for instance, the constant switching on and off of a role. In this case, the activity that has the highest assigned priority will always be performed [43].

To enhance the capacity of the security officer (SO) to react in emergency circumstances, the authors give the access to manipulate the state of role and the series of users that have the control to perform that specific role by giving run time requests [44]. The run time requests are those requests that are not attached with other events or the validation of stated conditions. For example, a run time request can be used to temporarily delay the user from making a role operative. This is useful, especially when a user

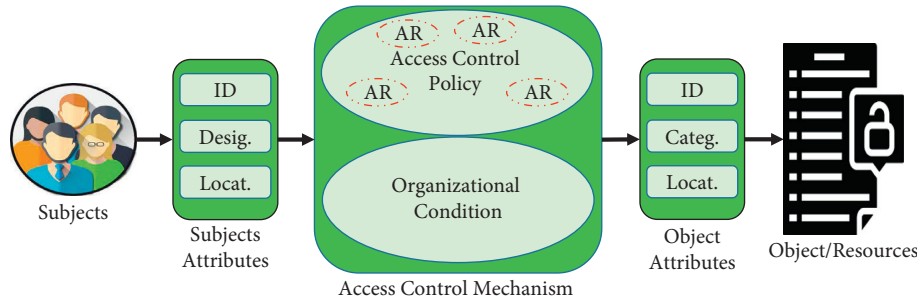


FIGURE 6: Abstract view of attribute-based access control (ABAC).

utilizes a specific role to execute an activity that could be detrimental to the system. In this situation, the SO can react by releasing a run time request that will cause a temporary denial for the user and prevent him from executing the role. Just like triggers, run time requests can be performed immediately or after a specified period of time.

2.2.2. Rule-Based RBAC. The rule-based RBAC is basically a modification in RBAC. Kahtani and Sandhu [45] proposed a model that works like the traditional RBAC model. They made a different set of rules for the enterprise to define its access policy. The rules are activated automatically for the assignment of users to roles. The permission creation and assignment of the permissions to roles are working the same as the traditional RBAC model. The modification was done in between user role assignments. The authors made the user role assignment portion dynamic. The system will verify the attributes of the users with attributes of roles. If attributes on both ends match with their attribute values, then the assignment will be done automatically, otherwise not. For example, a user from country of India, with age of 19, can view the adult sites. It means a user should qualify the attributes of age and country, with the values of their attributes; then, he/she can access those particular roles with the same access rule. The working of rule-based RBAC model is very good because it decreased a load of an administrator by automating the concept of user role assignment. The efficiency of the model can be increased by giving the idea of a fully dynamic RBAC model that can make reliability and ease of management [46].

2.2.3. Rule-Based Access Control. The rule-based access control model is used for Web-based social network (WBSN). It permits access to resources that are located online. In this framework, authorized subjects are expressed based on the relationship form, depth, and degree of trust that exist among the network users with attribute-based RBAC. Access to resources is given based on distinct access rules. In rule-based models, protocols are given by resource owners and they indicate the profile of authorized users by one or more access conditions. The access conditions include limitations on the type, depth, and trust level of their associations with other network users. The access control needs a particular object that can be clearly stated by a series of conditions [47].

For instance, for an object created by v_o (node that has a relationship with requester), the series of access conditions applicable to the object is given by an access rule that is determined by v_o . This type of concept is usually described as follows: the access rule is always in the form of (oid, cset), where oid represents the identifier of the object and cset represents a series of conditions (cond1..., condn). For instance, assume that Tom is the one who created an object that is associated with the identifier obj1 and he wants users who are his direct pals and whose trust level is up to 0.5 to have access to his object. Also, he wishes to give access to all his direct friends that are his colleagues provided that their trust level is up to 0.5.

2.2.4. Attributed RBAC. The RBAC model is famous due to its strictness in terms of security, and the ABAC model is famous due to its dynamic behaviour [27, 48]. Some studies proposed a hybrid model that used basic entities of RBAC such as actions, objects, permissions, roles, and users. They introduced the concept of attributes for the creation of permissions, permission assignment to roles, and role assignment to users. This sort of addition makes the RBAC model a dynamic model. Most of the work in the hybrid model is done automatically, which made it different from the existing models and covered some of the deficiencies of the RBAC and ABAC. All the objects of the system have some attributes such as time, IP address, and location. These attributes of objects are automatically granted to permissions after the creation permissions.

This model also creates permissions automatically with the merger of object containers and action-level containers. So, this kind of merger creates more than one permission at a time and creates it automatically. After that, the permission is assigned to roles by matching their attributes. If the attributes of roles and permissions are matched, the permissions will be added to those roles automatically. In last, the user's attributes are matched with roles and automatic role assignment will be done with the help of attributes. If a user's time, location, and IP address matched with the role's same attributes, then that user can access that particular role. If one of the attributes does not match, then the user cannot access that role. The model idea was good, but it only supports the basic working of RBAC. If the administrator wants to do the whole access control working through this model, then the model is not useful. The reason is that this model does not support conflicts

of interest, separation of duty, and role hierarchy concepts [49]. So, these are some limitations of attributed RBAC model. Some authors proposed various models to resolve this issue by extending this work. The proposed techniques are capable to support separation of duty in various ways. Furthermore, the hybrid models proposed different methods to generate permissions [26, 28].

2.2.5. Role-Based Integrated Access Control (RBIAC). Reliability and security are the most important concerns in multi-domain service-based systems, where data are used to flow from one domain to another domain. There are many access control models. The data provenance methods are developed for service-based systems. On the other hand, there was not a single mechanism that provides an integrated model with data provenance and access control. The role-based data provenance scheme was developed to track originator's and contributor's roles. Moreover, data reliability can be evaluated using the information of data objects from the roles. The proposed [50] model is better for the applications of multi-domain services with respect to reliability and security. This model provided a new way in the field of integrated or hybrid models. In addition, RBAC is used for the evaluation of data security and reliability. Moreover, the extended version of typical RBAC is used to control data usage and flow of information in multi-domain systems. The developed model is also capable of using information about newly added roles and implementing data quality derivation [51].

2.2.6. Trust-Based Access Control (TBAC). The threat level is comparatively more when users interact with online social networks (OSN). Several users download and upload data from the OSN that may lead to different data security risks and access control. The trust-based access control was proposed as a solution or strategy for users and their friends for restricting them through a proper trust rule in accessing the data from OSN. The proposed [52] model works on the concept of roles such as the owner, contributor, and stakeholder. These roles are associated with users to play during the usage of OSN. There are different security levels introduced with the help of different roles. The concept of a multi-role environment is also introduced. In this way, more than one security parameter can be applied by the users. The user and his friends can make the decision of access grant or revoke for the other users on the OSN. So, policy conflicts do not occur between various users. The model was proposed for the OSN, but it is not suitable for other fields such as wireless sensor networks, IoT, and cloud computing. Moreover, the access decision is placed between users and their friends, but there is no role of the administrator that can make sure security issues. If the administrator wants to delete some unethical photographs or material, then how can an administrator remove it? Even the role of the administrator is not discussed, and this is a question or research gap in this model [53].

2.2.7. Trust-Aware RBAC. During the communication process, there are certain threats in breaching the security from the malicious users. The reason behind the threat is the absence of some access control mechanism. The trust-aware RBAC system (TARAS) [54] model was proposed to solve the security issues in IoT devices communication. The users with similar roles are considered to respond in the same manner so that a trust level can be established between IoT and smart devices, and users. The TARAS is capable of detecting unauthorized and malicious users. Moreover, TARAS performed dynamic trust estimation and increased the integrity of data. The TARAS also increased the availability, detection of accuracy, robustness, and provided better performance under high attack density. The model is specifically designed for IoT, but the model can be implemented only for wireless sensor networks and cloud computing devices. In addition, some researches are proposed regarding the privacy of IoT environments for cloud and blockchain [55, 56].

2.2.8. Garbled RBAC. Data outsourcing originates different security issues in the cloud and IoT environment. Moreover, security threats and privacy risks are leading problems in the fields of military, health care, and intelligent organizations that are associated with the task assignment. As a solution to the problems, the garbled RBAC (GRBAC) [57] model was proposed. The model is a fine-grained security model that adopted a garbled function. The proposed model is specifically designed for those organizations where roles are not disclosed with the servers and for the users. Moreover, the main contributions of the model are that a user cannot activate more than one garbled role set. The data of organization is secret from everyone, but the algorithm is not secret. The model can be implemented in the IoT environment as an extension. On the other hand, the model is not flexible. Moreover, one more disadvantage is restricting the server from the user's roles. In this way, the server is unable to keep the record of roles and the server cannot make the necessary steps for controlling the access control system.

2.2.9. RBAC Using Smart Contract. The open blockchain platform Ethereum provides flexibility, adaptability, and security. In this model, smart contract is used with the typical RBAC model. The RBAC smart contract (RBAC-SC) [58] model is proposed to verify users' role ownership in small organizations. In this model, RBAC-SC is deployed on Ethereum's testnet blockchain and the design of RBAC-SC is also provided with performance analysis. The proposed model is efficient, secure, and minimizes the costs, but it is only suitable for small organizations. In this way, we cannot consider this model for large organizations. This is the drawback and limitation of the model; that is, it is restricted to small organizations only. Some other authors also proposed a lightweight technique for blockchain-based systems for the authentication process [59].

2.2.10. Feasible Fuzzy-Extended ABAC (FBAC). The ABAC model is becoming a mature model day by day, and it is famous due to the dynamic authorization technique. The ABAC model can even dynamically perform in complex environments, but it is unable to provide flexible, exceptional approval. The limitation of ABAC model is that it is unable to perform efficiently resource usability and business timeliness. The proposed FBAC [60] model is comparatively efficient and flexible for granting exceptional critical authorization. The FBAC model is better by increasing the utilization of resources and business suitability. The FBAC is also tested for the audit mechanism and the credit system at high-risk requests. Moreover, the proposed model is analysed for risks, usability, and evaluated for its effectiveness by different experiments. The FBAC model is comparatively better than the traditional ABAC model due to its time efficiency and flexibility. On the other hand, the model is the extended version of ABAC, and it is unable to provide tight security and least privilege.

2.2.11. Emergency Role-Based Access Control (E-RBAC). Nazerian [61] proposed the emergency role-based access control (E-RBAC) model to increase the flexibility of RBAC model in emergency situations. Because the RBAC model is failed to achieve better results in emergency situations. The proposed E-RBAC model is based on break the glass (BTG) policy and separation of duty (SOD) constraint. The BTG policy was proposed to override access control and give maximum responsibility to users, and SOD constraints are used to restrict the users. The proposed E-RBAC model can achieve better results in normal, emergency, and exception situations. The normal situation is the same as RBAC in which the access of user is known. In the emergency situation, the events are predictable except their time and access are not given to users due to privilege contradicts. In an exceptional situation, the user access is unknown and policies are not predefined. This model improves the flexibility of RBAC model in normal, emergency, and exception situations.

2.2.12. Priority-Attribute-Based RBAC (PARBAC). Thakare [62] proposed a priority-attribute-based RBAC (PARBAC) model for medical based on authentication mechanism to increase the consistency and flexibility of RBAC model. Because the RBAC model is failed to handle large number of requests from user in large organizations that cause overloading on the cloud server, the proposed PARBAC works in seven steps. In the first step, the users get token that consists of individual's details. In the second step, user calls to API. In the third step, the Azure resource manager (ARM) accepts or denies assignments of users based on priority. In the fourth step, ARM

advises to user based on role assignment. In the fifth step, ARM verifies the activity and privileges of users. In the sixth step, logging is not allowed to user if he has no role with activity. In the last step, access is blocked if a denial assignment is applied. This PARBAC model is able to handle problems in large organizations with dynamic scenarios.

2.2.13. Attribute-Based Access Control Model Supporting Anonymous Access (ABSAC). Zhang [63] proposed attribute-based access control model supporting anonymous access (AB_sAC) model that is used to protect user data for Internet of things (IoT) in small cities. The models of attribute-based access control (ABAC) are not protected and efficient to work in large organizations properly. According to researcher, anonymous access is able to protect user data and it is not stored in authentic place. This proposed model is more secure for the transaction of user data in public place with minimum risk factors.

2.2.14. Traceable Attribute-Based Encryption Scheme with Dynamic Access Control (TABE-DAC). Guo [64] proposed an efficient traceable attribute-based encryption scheme with dynamic access control (TABE-DAC) model to share secret data on cloud servers based on blockchain technology. The confidentiality of secret data can be protected using attribute-based encryption (ABE), but the ABE scheme is not flexible and efficient to fulfil access control policies. The TABE-DAC model can control illegal sharing of secret data on cloud by tracing malicious users using accountability method. This model provides flexibility to data owners to modify access control policy. The proposed TABE-DAC model is efficient and flexible to share secret data on cloud without illegal sharing.

2.2.15. Time-Based Access Control. Wang [65] proposed time-based access control (TAC) model to secure user data in Internet of things (IoT). The user data are divided into two directional subspaces that represent attribute and time generation of data. Access control and privacy are achieved by sending encrypted data before transmission. The data owner or data source has authority to give access to anyone using sub-key. The TAC model is able to generate sub-key of data within minimum time and memory space for each subspace. The proposed TAC model is efficient and flexible to share secret data on IoT.

3. Comparative Analysis of Traditional and Hybrid Access Control Models

This section contains a summarized comparison and information of traditional and hybrid AC models in tabular form as shown in Table 2.

TABLE 2: Comparative analysis of traditional and hybrid access control models.

Model name	Strengths	Weaknesses
DAC [18]	Flexible to implement, customize access policies, and read/write access for users	Lack of security, no dynamicity, access management is not centralized and inefficient for government use
MAC [24]	Confidentiality, data protection, suitable for military use, and strictly enforced by OS	No dynamic alteration in policies, not user-friendly, load on administrator, maintainability, and scalability
RBAC [25]	Easy administration, least privileges, best for local domains, and tight security	Mobility problem, no flexibility, role explosion, and no dynamic behaviour
ABAC [37]	Flexible for big systems, dynamic behaviour, and global agreement of attributes	Complex implementation and maintenance, time constraints to define attributes, and difficult policy specification
TRBAC [42]	Periodic role enable/disable and temporal dependencies for actions	No dynamic behaviour, role explosion, and limited specification language
Rule RBAC [45]	Dynamicity, less load on administrator, and induced role hierarchy	Not consistent for conflicts of interest and policy specification complexity
Rule BAC [47]	Use certificates for authenticity, good for social networks, and dynamic environment	Only useful for WSBNs and difficult to manage
Attributed RBAC [49]	Dynamic behaviour, tight security, and decrease load of administrator	Limited features of RBAC, role explosion, and complexity in designing access policy
RBIAC [50]	Enhanced data security, trustworthiness, and data provenance for multi-domain service applications	Execution time overhead due to the addition of various elements of data provenance.
TBAC [52]	Automated access control model designed for multi-role implementation	Reliability and scalability problems, and not secure because users also decide access rights
TARAS [54]	Enhanced detection accuracy, robustness, and service availability against malicious users	Designed for smart objects and not suitable for military and government organization due to unknown users' run time access
GRBAC [57]	Enhanced security, flexibility, and user's identity and task information is secret	SOD is implemented on the level of roles
RBAC-SC [58]	Efficient and secure for the verification of user's ownership for role	Specification language is not provided and is limited to basic functionalities
FBAC [60]	Enhanced business timeliness and resource usability for unpredictable scenarios	Hard to manage access control policies and security risks
E-RBAC [61]	Efficient and flexible for large systems, effective behaviour for normal, emergency, and exception situations	SOD violations can occur, limit the user access according to situations
PARBAC [62]	Secure, consistent, flexible, and efficient to handle dynamic scenario problems in large organizations	Denial-of-service occurrence, high system execution, and third-party reliance
AB_sAC [63]	Efficient, secure, minimum risk factor, and support to anonymous access	Increase in number of policies will affect the execution time, third-party reliance
TABE-DAC [64]	Protect to illegal data sharing, trace to malicious users by accountability method	The authorities can be dishonest, no dynamic access policies
TAC [65]	Protect data using encryption in IoT, different sub-keys of each subspace	The sub-keys are not secure and the data owner cannot manage its privacy

TABLE 3: Applications of traditional and hybrid access control models.

Model name	Applications
DAC [18]	The most appropriate applications of DAC are Web applications and operating systems such as Unix and Linux
MAC [24]	MAC is used in operating systems and database management systems. Furthermore, it is used in the organizations such as government departments and military
RBAC [25]	The applications of RBAC are banking and education systems
ABAC [37]	The application of ABAC is for companies such as telecommunications, insurance, and airlines
TRBAC [42]	The TRBAC is an extension of the RBAC model to achieve dynamic behaviour for activation and deactivation of role
Rule RBAC [45]	The rule RBAC model is an extension of the RBAC model to achieve dynamic behaviour of user role assignment
Rule BAC [47]	The application of rule BAC is Web-based social networks
Attributed RBAC [49]	The attributed RBAC model is a hybrid model of RBAC and ABAC to achieve strict security and dynamic behaviour
RBIAC [50]	The RBIA model is extension of the RBAC model to provide integrity of user data
TBAC [52]	The applications of TBAC are online social networks (OSN) and websites
TARAS [54]	The application of TARAS is communication of IoT devices
GRBAC [57]	The application of GRBAC is IoT environment where roles are not disclosed
RBAC-SC [58]	The application of RBAC-SC is blockchain-based smart contract
FBAC [60]	The applications of FBAC are auditing, business environment
E-RBAC [61]	The E-RBAC is an extension of the RBAC model to work in emergency situations
PARBAC [62]	The application of PARBAC is cloud server-based authentication mechanism for medical domain
AB _s AC [63]	The application of AB _s AC is IoT-based user data protection
TABE-DAC [64]	The application of TABE-DAC is sharing of secret data on cloud servers based on blockchain and also control illegal sharing of secret data
TAC [65]	The application of TAC is IoT-based user data protection

3.1. Applications of Traditional and Hybrid Access Control Models. The access control models are classified into traditional and hybrid models. The basic traditional access control models are DAC, MAC, RBAC, and ABAC. The hybrid access control models are proposed as extension of traditional access control models on the basis of pros and cons. Each traditional and hybrid access control model has its own application as described in Table 3.

4. Conclusions and Future Directions

The access control (AC) mechanism is used to control the access level of resources among legitimate users. The main purpose of access control mechanism is to ensure the security of data by limiting the access of data to only authorized users. The access control is classified into traditional and hybrid models. Due to several limitations of traditional access control models, hybrid access control models were proposed as an extension of traditional access control models. The hybrid access control models are more efficient, flexible, scalable, and secure. The hybrid access control models are used generally in both small and large organizations according to the objective of the organization.

In the future, the access control models also can be designed using fog computing instead of cloud computing. The fog computing stores data over the fog in the form of chunks. Suppose user wants to update the stored data, then user will download only specific chunk of data for modification instead of downloading whole data. The access control model can be made more secure using fog computing due to data chunk mechanism. Moreover, the access control models also can be designed using artificial intelligence (AI) to achieve some key characteristics such as detecting malicious code in resources, identifying illegal sharing of resources, and distinguishing unauthorized users. AI will also be used to

permit and deny the access of resources among users and will limit the users so that they can perform tasks up to the specified role. In short, the access control models can be fully automated with the help of artificial intelligence.

Data Availability

All the data used to support the findings of this study are available in this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was funded by a Faculty Research Support Grant (FRSG-21) of FAST-NUCES, Pakistan, under Project ID “11-71/NU-R/20” and by International Scientific and Technological Innovation Cooperation Project in Sichuan Province (Project ID 2020YFH0062).

References

- [1] H. Huang, F. Shang, J. Liu, and H. Du, “Handling least privilege problem and role mining in RBAC,” *Journal of Combinatorial Optimization*, vol. 30, no. 1, pp. 63–86, 2015.
- [2] J. Hassan, D. Shehzad, I. Ullah et al., “A lightweight proxy Re-encryption approach with certificate-based and incremental cryptography for fog-enabled E-healthcare,” *Security and Communication Networks*, vol. 202117 pages, 2021.
- [3] S. Latif, Z. E. Huma, S. S. Jamal et al., “Intrusion detection framework for the internet of things using a dense random neural network,” *IEEE Transactions on Industrial Informatics*, vol. 99, p. 10, 2021.

- [4] A. Hamza, D. Shehzad, M. S. Sarfraz, U. Habib, and N. Shafi, "Novel secure hybrid image steganography technique based on pattern matching," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 3, pp. 1051–1077, 2021.
- [5] N. W. Hundera, C. Jin, D. M. Geressu, M. U. Aftab, O. A. Olanrewaju, and H. Xiong, "Proxy-based public-key cryptosystem for secure and efficient IoT-based cloud data sharing in the smart city," *Multimedia Tools and Applications*, 2021.
- [6] H. Zhang, J. Wang, and J. Chang, "An access control model for multi-level security in multi-domain networking environments," in *Proceedings of the in 2017 ninth International Conference On Modelling, Identification and Control (ICMIC)*, pp. 809–814, Kunming, China, July 2017.
- [7] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Applied Sciences*, vol. 10, no. 2, Article ID 488, 2020.
- [8] S. Kausar, A. Rahman, A. M. Khan, and T. Ahmad, "Attribute-based Access Control in Web Applications," in *Applications Of Artificial Intelligence Techniques In Engineering*, Springer, New York City, NY, USA, pp. 385–393, 2019.
- [9] M. A. Habib, N. Mahmood, M. Shahid, M. U. Aftab, U. Ahmad, and C. M. N. Faisal, "Permission based implementation of dynamic separation of duty (DSD) in role based access control (RBAC)," in *Proceedings of the 2014 eighth International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–10, Gold Coast, QLD, Australia, December. 2014.
- [10] M. Liu, C. Yang, H. Li, and Y. Zhang, "An efficient attribute-based access control (ABAC) policy retrieval method based on attribute and value levels in multimedia networks," *Sensors*, vol. 20, no. 6, p. 1741, 2020.
- [11] E. Bertin, D. Hussein, C. Sengul, and V. Frey, "Access control in the Internet of Things: a survey of existing approaches and open research questions," *Annals of Telecommunications*, vol. 74, no. 7-8, pp. 375–388, 2019.
- [12] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
- [13] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.
- [14] Y. Zhang and X. Wu, "Access control in internet of things: a survey," 2016, <http://arxiv.org/abs/1610.01065>.
- [15] P. Samarati and S. C. de Vimercati, "Access control: policies, models, and mechanisms," *Foundations of Security Analysis and Design FOSAD 2000 LNCS*, Springer, vol. 2171, pp. 137–196, Bertinoro, Italy, 2001.
- [16] M. A. Habib, *Secure RBAC with Dynamic, Efficient & Usable DSD*, Johannes Kepler University Linz, Linz, Austria, Ph.D, 2011.
- [17] J. Moffett, M. Sloman, and K. Twidle, "Specifying discretionary access control policy for distributed systems," *Computer Communications*, vol. 13, no. 9, pp. 571–580, 1990.
- [18] R. S. Sandhu, "Role-based access control," *Advances in Computers*, vol. 46, pp. 237–286, 1998.
- [19] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-based Access Control*, Artech House, NY, USA, 2003.
- [20] L. Bo, C. ShuhuiB, and D. Jinsheng, "Survey of bell-LaPadula model," *Application Research of Computers*, vol. 30, pp. 656–660, 2013.
- [21] R. R. Jueneman, "Integrity controls for military and commercial applications," in *Proceedings of the 1988 Fourth Aerospace Computer Security Applications*, pp. 298–322, Orlando, FL, USA, September 1988.
- [22] D. D. Clark and D. R. Wilson, "A comparison of commercial and military computer security policies," in *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, pp. 184–194, Oakland, CA, USA, April 1987.
- [23] D. Rountree, "Chapter 2—what Is Federated Identity?" *D. B. T.-F. I. P. Rountree*, Syngress, Rockland, MA, USA, pp. 13–36, 2013.
- [24] E.-B. Choi and S.-J. Lee, "Access control mechanism based on MAC for cloud convergence," *Journal of the Korea Convergence Society*, vol. 7, no. 1, pp. 1–8, 2016.
- [25] American National Standard for Information Technology, *ANSI INCITS 359-2004*, American National Standards Institute, Washington, D.C, USA, 2004.
- [26] M. U. Aftab, Z. Qin, N. W. Hundera et al., "Permission-based separation of duty in dynamic role-based access control model," *Symmetry*, vol. 11, no. 5, Article ID 669, 2019.
- [27] M. U. Aftab, A. Oluwasanmi, A. Alharbi et al., "Secure and dynamic access control for the Internet of Things (IoT) based traffic system," *PeerJ Computer Science*, vol. 7, Article ID e471, 2021.
- [28] M. U. Aftab, Y. Munir, A. Oluwasanmi et al., "A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles," *IEEE Access*, vol. 8, pp. 24196–24208, 2020.
- [29] K. Z. Bijon, R. Krishnan, and R. Sandhu, "A Framework for Risk-Aware Role Based Access Control," in *Proceedings of the in 2013 IEEE Conference on Communications and Network Security (CNS)*, pp. 462–469, National Harbor, MD, USA, October 2013.
- [30] A. Anderson, *Core and Hierarchical Role Based Access Control (RBAC) Profile of XACML V2. 0*, OASIS Stand, 2005.
- [31] C.-J. Moon, D.-H. Park, S.-J. Park, and D.-K. Baik, "Symmetric RBAC model that takes the separation of duty and role hierarchies into consideration," *Computers and Security*, vol. 23, no. 2, pp. 126–136, 2004.
- [32] N. Solanki, Y. Huang, I.-L. Yen, F. Bastani, and Y. Zhang, "Resource and role hierarchy based access control for resourceful systems," *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, pp. 480–486, 2018.
- [33] R. Ghazal, A. K. Malik, N. Qadeer, B. Raza, A. R. Shahid, and H. Alquhayz, "Intelligent role-based access control model and framework using semantic business roles in multi-domain environments," *IEEE Access*, vol. 8, pp. 12253–12267, 2020.
- [34] T. Jaeger and J. E. Tidswell, "Practical safety in flexible access control models," *ACM Transactions on Information and System Security*, vol. 4, no. 2, pp. 158–190, 2001.
- [35] M. K. Hedayati, A. Abdipour, R. Sarraf Shirazi et al., "Challenges in on-chip antenna design and integration with RF receiver front-end circuitry in nanoscale CMOS for 5G communication systems," *IEEE Access*, vol. 7, Article ID 43190, 2019.
- [36] S. Jha, S. Sural, V. Atluri, and J. Vaidya, "Enforcing Separation of Duty in Attribute Based Access Control Systems," *Information Systems Security. ICISS 2015. Lecture Notes in Computer Science*, Springer, Cham, Switzerland, 2015.
- [37] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.
- [38] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

- [39] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: taxonomy and open issues," *Future Generation Computer Systems*, vol. 72, pp. 273–287, 2017.
- [40] V. C. Hu, D. Ferraiolo, R. Kuhn et al., *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2014.
- [41] C.-W. Liu, W.-F. Hsien, C. C. Yang, and M.-S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal on Network Security*, vol. 18, no. 5, pp. 900–916, 2016.
- [42] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: a temporal role-based access control model," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 191–233, 2001.
- [43] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A generalized temporal role-based access control model," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 1, pp. 4–23, 2005.
- [44] E. Uzun, V. Atluri, S. Sural, and J. Vaidya, "Analyzing temporal role based access control models," in *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies*, pp. 177–186, New Jersey, NJ, USA, June 2012.
- [45] M. A. Al-Kahtani and R. Sandhu, "Induced role hierarchies with attribute-based RBAC," in *Proceedings of the eighth ACM symposium on Access control models and technologies - SACMAT '03*, pp. 142–148, Como, Italy, June 2003.
- [46] A. Rashid, I. K. Kim, and O. A. Khan, "Providing authorization interoperability using rule based HL7 RBAC for CDR (Clinical Data Repository) framework," in *Proceedings of the 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 343–348, Islamabad, Pakistan, January 2015.
- [47] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops," in *Proceedings of the in OTM Confederated International Conferences On the Move to Meaningful Internet Systems, LNCS*, vol. 4278, pp. 1734–1744, Montpellier, France, November 2006.
- [48] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, and M. Irfan, "Attributed role based access control model," in *Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS)*, pp. 83–89, Rawalpindi, Pakistan, Dec 2015.
- [49] J. Yong, E. Bertino, and M. T. D. Roberts, "Extended RBAC with role attributes," *PACIS 2006 Proc.* vol. 8, 2006.
- [50] W. She, W. Zhu, I.-L. Yen, F. Bastani, and B. Thuraisingham, "Role-based integrated access control and data provenance for SOA based net-centric systems," *IEEE Transactions on Services Computing*, vol. 9, no. 6, pp. 940–953, 2016.
- [51] Q. M. Rajpoot, C. D. Jensen, and R. Krishnan, "Integrating attributes into role-based access control," in *Proceedings of the in IFIP Annual Conference On Data And Applications Security And Privacy*, pp. 242–249, Fairfax, VA, USA, July 2015.
- [52] V. Takalkar and P. N. Mahalle, "Trust-based access control in multi-role environment of online social networks," *Wireless Personal Communications*, vol. 100, no. 2, pp. 391–399, 2018.
- [53] O. Folorunso and O. A. Mustapha, "A fuzzy expert system to Trust-Based Access Control in crowdsourcing environments," *Applied Computing and Informatics*, vol. 11, no. 2, pp. 116–129, 2015.
- [54] B. Gwak, J.-H. Cho, D. Lee, and H. Son, "TARAS: trust-aware role-based access control system in public internet-of-things," in *Proceedings of the 2018 Seventeenth IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 74–85, New York, NY, USA, September 2018.
- [55] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, 2021.
- [56] T. Wang, Y. Quan, X. S. Shen, T. R. Gadekallu, W. Wang, and K. Dev, "A privacy-enhanced retrieval technology for the cloud-assisted Internet of Things," *IEEE Transactions on Industrial Informatics*, 2021.
- [57] M. Alam, N. Emmanuel, T. Khan, Y. Xiang, and H. Hassan, "Garbled role-based access control in the cloud," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1153–1166, 2018.
- [58] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240–12251, 2018.
- [59] W. Wang, C. Qiu, Z. Yin et al., "Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks," *IEEE Internet Things J*, 2021.
- [60] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "A feasible fuzzy-extended attribute-based access control technique," *Security and Communication Networks*, vol. 201811 pages, 2018.
- [61] F. Nazerian, H. Motameni, and H. Nematzadeh, "Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy," *Journal of Information Security and Applications*, vol. 45, pp. 131–142, 2019.
- [62] A. Thakare, E. Lee, A. Kumar, V. B. Nikam, and Y.-G. Kim, "PARBAC: priority-attribute-based RBAC model for azure IoT cloud," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2890–2900, 2020.
- [63] R. Zhang, G. Liu, S. Li, Y. Wei, and Q. Wang, "ABSAC: attribute-based access control model supporting anonymous access for smart cities," *Security and Communication Networks*, vol. 2021, pp. 1–11, 2021.
- [64] L. Guo, X. Yang, and W.-C. Yau, "TABE-DAC: efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain," *IEEE Access*, vol. 9, pp. 8479–8490, 2021.
- [65] B. Wang, W. Li, and N. N. Xiong, "Time-based access control for multi-attribute data in internet of things," *Mobile Networks and Applications*, vol. 26, no. 2, pp. 797–807, 2021.