electronics

MDPI

Article

From Conventional to State-of-the-Art IoT Access Control Models

Ahmad Kamran Malik [1,*], Naina Emmanuel [1], Sidra Zafar [2], Hasan Ali Khattak [3], Basit Raza [1], Sarmadullah Khan [4], Ali H. Al-Bayatti [4], Madini O. Alassafi [5], Ahmed S. Alfakeeh [5] and Mohammad A. Alqarni [6]

[1] Department of Computer Science, COMSATS University Islamabad, Islamabad Campus, Islamabad 45000, Pakistan; nemmanuel1992@gmail.com (N.E.); basit.raza@comsats.edu.pk (B.R.)

[2] Department of Computer Science, Lahore College for Women University, Lahore 54000, Pakistan; sidzafar.88@gmail.com

[3] School of Electrical Engineering and Computer Science (SEECS), National University of Sciences & Technology (NUST), Islamabad 44000, Pakistan; hasan.alikhattak@gmail.com

[4] School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester LE1 9BH, UK; sarmadullah.khan@dmu.ac.uk (S.K.); alihmohd@dmu.ac.uk (A.H.A.-B.)

[5] Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah 21589, Saudi Arabia; malasafi@kau.edu.sa (M.O.A.); asalfakeeh@kau.edu.sa (A.S.A.)

[6] College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia; maaalqarni8@uj.edu.sa

* Correspondence: ahmad.kamran@comsats.edu.pk

Received: 23 July 2020; Accepted: 1 October 2020; Published: 15 October 2020

check for updates

Abstract: The advent in Online Social Networks (OSN) and Internet of Things (IoT) has created a new world of collaboration and communication between people and devices. The domain of internet of things uses billions of devices (ranging from tiny sensors to macro scale devices) that continuously produce and exchange huge amounts of data with people and applications. Similarly, more than a billion people are connected through social networking sites to collaborate and share their knowledge. The applications of IoT such as smart health, smart city, social networking, video surveillance and vehicular communication are quickly evolving people's daily lives. These applications provide accurate, information-rich and personalized services to the users. However, providing personalized information comes at the cost of accessing private information of users such as their location, social relationship details, health information and daily activities. When the information is accessible online, there is always a chance that it can be used maliciously by unauthorized entities. Therefore, an effective access control mechanism must be employed to ensure the security and privacy of entities using OSN and IoT services. Access control refers to a process which can restrict user's access to data and resources. It enforces access rules to grant authorized users an access to resources and prevent others. This survey examines the increasing literature on access control for traditional models in general, and for OSN and IoT in specific. Challenges and problems related to access control mechanisms are explored to facilitate the adoption of access control solutions in OSN and IoT scenarios. The survey provides a review of the requirements for access control enforcement, discusses several security issues in access control, and elaborates underlying principles and limitations of famous access control models. We evaluate the feasibility of current access control models for OSN and IoT and provide the future development direction of access control for the same.

Keywords: access control models; security; privacy; social network security; Internet of Things

1. Introduction

Access control provides security measures for regulating the access of the subject to the object. Therefore, it includes the identification, authorization, and authentication for making up an access control mechanism. In the identification phase, the subject/user can use credentials and get authenticated. After providing legitimate credentials, the user becomes authorized for accessing only those resources that are granted by an admin (or owner of the resource) through access control permissions/rules. Since the beginning of the distributed systems access control is being widely used. In today's integrated on-demand data-driven world, security is a major concern and access control is the solution [1]. To develop a data protection system for an organization that protects its data from malicious activities and unauthorized access while making sure of its availability at the same time, some information management system is needed to guarantee that only authorized users can access the data. For the development of such an access control system, regulations and rules are required, according to which access can be controlled. The development of the access control system is done in different phases and these phases depend on some security measures [2]. These phases include (i) Policies: Security policies are a set of rules that define conditions under which one gets access or is denied. (ii) Models: Access control policies are implemented through security models. These models are designed according to the scenarios and industry's needs. Models are formal representations of security policies. (iii) Mechanisms: Security controls (imposed by the policies) are implemented by the low-level functions (hardware and software), these low-level functions are security mechanisms. These three concepts stated above provide the conceptual separation between the abstraction and design levels while providing multi-phase software development. This conceptual separation presents independence between enforcement of policies on one side and mechanisms on the other side [3]. In the digital world of access control, a subject (defined as a computer system, a process, or a user) performs some operations (defined as delete, add, search, read, write, etc.) on an object (defined as a resource) according to the policy. Allowing a user to Carry out operations on object is known as permission. Policies are made according to the access control models. Informally, access control tells "who can access what", and it is the fundamental part of the information security [4]. Basic risks in the security of information include Confidentiality, Integrity, and Availability (CIA). Confidentiality is making sure that data/resources have not been accessed or viewed by any unauthorized party. Integrity makes sure that data/resources are in its original form and are not changed intentionally or accidentally. During the system development phase, some techniques only provide confidentiality but not integrity; this approach is not as good as the adversary can manipulate data without having its knowledge. The availability of resources is making sure that resources/data are accessible and ready to use. After compromising the system resources, the adversary tries to remove the availability of the data/resources. The CIA cycle is illustrated in Figure 1.

The main purpose of access control mechanism is to preserve all three CIA security traits. It controls access through permissions to sensitive data and resources. Access controls protect the resources from internal and external attacks. Real world scenarios have complex situations and consequently complex policies. Access control system development needs to ensure the integrity, availability, and confidentiality of the resources. A comprehensive survey on Access Control Models has not been dealt yet; existing literature surveys either provide a review of some famous models (with their extensions) like MAC (Mandatory Access Control), DAC (Discretionary Access Control), and RBAC (Role-Based Access Control) models or only cover latest trends like Cloud and IoT models. This paper includes a detailed review of literature from 1970 to 2020 covering significant conventional access control models as well as state-of-the-art OSN and IoT models to put things in perspective.

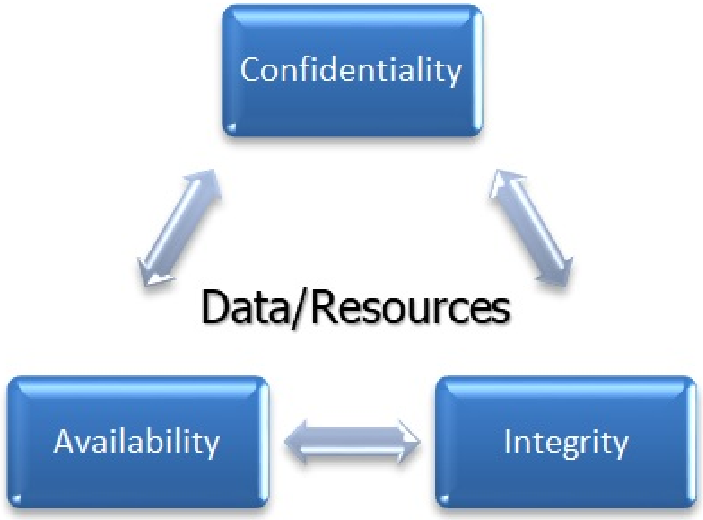


Figure 1. The CIA model.

Comparison with Other Surveys

This survey is focused on access control in conventional, OSN, and IoT models. It presents models, protocols, and framework solutions in a comprehensive manner. The following are a few existing surveys on the similar topic; however, they have tried to address access control issues related to any one of the paradigms or in a specific context.

Sicari et al. [5] provide a comprehensive survey of the main security challenges and issues in IoT. It also discusses possible privacy, security, and trust-based solutions and future directions for IoT. This paper, however, does not discuss in detail conventional access control or OSN-based models extensively as its focus is only on IoT [6].

Ouaddah et al. [7] provides an extensive review of the state-of-the-art access control models for IoT. It uses a methodology for a survey that it named Objectives, Models, Architecture, and Mechanisms (OM-AM). Privacy as well as security requirements for the state-of-the-art IoT applications such as smart homes, e-government, enterprise, and industry are analyzed in detail. The feasibility of traditional as well as recent access control models is highlighted from the IoT perspective. This paper also presents a comprehensive evaluation of the access control project relevant to IoT that represent research and commercial solutions during the period 2011–2016.

Bertin et al. [8] provide a brief survey on conventional access control models (e.g., DAC, MAC, RBAC, ABAC) and access control architectures and protocols (e.g., XACML, SAML, OAuth, ACE, UMA, LMW2M, AllJoyn). This paper does not cover the recent access control models like CapBAC, OrBAC, LBAC, and extensions of traditional access control models.

Zhang et al. [9] present a short overview of a few existing works on trust computing, access control models and systems in IoT. This paper provides a literature review of existing models for IoT-based access control. However, it does not discuss their comparisons or feasibility of those access control models through any evaluation metrics.

Ravidas et al. [10] investigate access control solutions related to IoT and perform a detailed analysis of existing access control frameworks. They also provide elicitation of the requirements that IoT-based authorization frameworks should provide along with criteria for evaluation. This work provides is an extensive review of access control models discussing the security of each layer in the IoT architecture.

Most of the recent access control surveys are related to specific domains like IoT and Cloud. However, our survey provides a general view of the access control models focusing on conventional, OSN, and IoT models. It is specifically created for the interest of those researchers who want to learn access control models in general, later they can go into details of a specific domain.

The rest of the paper is arranged as follows. Section 2 discusses access control requirements and security issues. Section 3 deals with conventional access control models along with their extensions. Section 4 provides a discussion on access control models for online social networks. Section 5 describes IoT-based access control models. Section 6 presents the analysis and discussion of the conventional and IoT-based models. Section 7 concludes the survey.

2. Access Control Requirements and Challenges

This section describes access control requirements on modeling and deployment. It also highlights the main security issues and challenges for access control.

2.1. Requirements of Access Control Models

Decisions are made in such a way that within a system, the accessibility of the objects is managed, and the nature of the environment is expressed [11]. Access control requirements are being summarized as follows.

- Generic access control models are encouraged so that access right needs can be met for a variety of enterprise models [12,13].
- For collaboration, access controls need scalability in terms of operations' quantity because it serves best in a collaborative environment than a single user system.
- Access control models are required to enable transparent access for legitimate users and heavy segregation of unauthorized users.
- High level rules/conditions of access rights must be allowed by the access control models for better management of increased complexity [11].
- Access control models should be dynamic; it should be able to modify the policies at runtime according to the requirements [14].
- Cost and performance of the resources should be under acceptable bounds.
- Access control models are required to design in such a way that each corporation must have the freedom of enforcement and design of their security policies [15].
- Access control policies' management should be easy to maintain the trust and usability in the system.
- To ensure the availability of the systems and overruling "need-to-know" requirements of data access in an emergency [15].
- The application and enforcement of access control should also include distributed level security.
- Access control must be accessible in a fine-grained format with the protection of sensitive assets [16].
- Access control should be interoperable between different resources. Ideally, relationship groups and access policies given by the user must 'follow the user' instead of redevelopment for each resource.
- Policies in an access control should follow the data of the object to which they are applied [16].

Along with the requirements mentioned above, other access control necessities like access administration and meta access control are also relevant. Meta access control can be assimilated either as a basic model or as a separate model. It is pointless to try to count practically useful requirements because we have multiple variations and possibilities [11]. It is recommended to follow the access controls that are simple yet rigorous. These requirements are useful in identifying the strengths and weak points of the existing access control models.

2.2. Security Issues and Challenges in Access Control

In the era of mainframes, access control was just about physical security. The notion of users and resources came with the idea of operating systems. ACLs were established to make the relationship between resources and their users while OS's job was to mediate the user's request to access resources. Now databases and operating systems have embedded access controls in them. Because of the distributed systems, we have simulated back towards access control models 'if one can reach the application, one can run it'. Each model has different security requirements. As much as capabilities get inherited, so are the risks and security issues in access control models [17–21]. Each model has significant trade-offs in terms of complexity, extensibility, integrated features, and security. In the cloud's perspective, security is maintained by the service providers while consumers become liable for managing and implementing security capabilities [17,22,23]. Access controls security is dependent on access control types. The access control model can be categorized into the following types.

- Preventive: It keeps unwanted events from happening.
- Detective: Recognize unauthorized events.
- Corrective: Correct the undesirable events that happen.
- Deterrent: Prevent security violations from happening.
- Recovery: After security violation, it restores the capabilities and resources.
- Compensation: Provides control alternatives.

Besides being useful, the access control mechanism has many risks and security issues as well, some of them are listed here:

- Providing fine-grained access is one of the key issues in the access control models while accessing data.
- The searching cost gets increased when user requests for data access and the server must search the entire system for making data available [24,25].
- To access data from outside the server, users must get register their domain [7,24].
- Access control mechanism should be efficient enough to make difference between sensitive and common data, to prevent common data from public access.
- High possibility of data leakage by the malevolent user.
- Scalability is one of the key features in access control models. Performance attribute must be maintained by the mechanism as the number of users, roles, attributes, or resources increase.
- Fairness in resource offers and consumption.
- Resource management capabilities should be provided such as delegation, management, addition, deletion of roles, resources, and operations [26].
- Semantic-grouping of information is the basic need in access controls [26].

3. Conventional Access Control Models

Access control models are concerned with the rules/permissions or obligations/conditions which determine how a subject/user can be allowed to manipulate the resource/object and how can it be determined as a potential danger for the resource. Access control models provide the framework as well as the mode of implementation for ensuring the integrity, availability, and confidentiality of the resource. Initially Access Control List (ACL) and Access Control Matrix techniques were used to specify which user can access which file. The most common and oldest access control models are MAC, DAC, and RBAC. In this paper, we will discuss each one of them in detail along with other access control models with their advantages and limitations [27]. We begin with a review of existing access control models with their evolution and propose a taxonomy of conventional access control models in Figure 2.

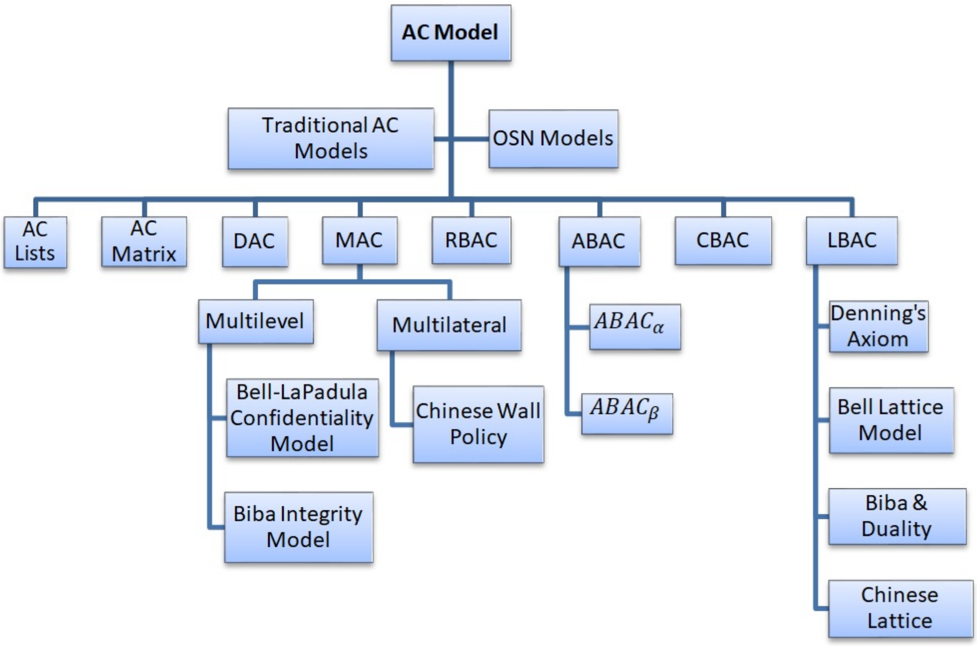


Figure 2. Taxonomy of AC Models in Conventional Systems.

3.1. Access Control Lists (ACL)

Access control lists are used to implement access control matrices [28–30]. Figure 3 depicts the access control list for the access control matrix mentioned in Table 1 representing each object with its access control list. The early form to implement the access control is access control lists (ACL) that were used in the UNIX OS. ACL is defined as a list of mappings associated with the resources where mappings are between a set of entities that request to have access to the resources and several actions that can be taken on the resources [31]. For instance, when the user tries to access the file, before granting access operating system checks the ACLs to determines if the permission is granted or rejected. ACL's along with OS can be used in a network context, relational database management, etc. [1]. ACLs are even predominant across all modern OS, every organization that uses operating systems certainly has an implementation of ACLs by default, and ACLs are implemented at the application level [32–34]. In the scenarios where ACLs of hundreds of thousands of users need to be managed then databases are used to store ACL data. ACLs contain much information and they consume much space, so researchers are working on ACLs compression [35–38].

Table 1. Access Control Matrix.

	File 1	**File 2**	**File 3**
User1	RWO	RWX	WX
User2	RWX	WX	RWX
User3	R	RWO	RWO

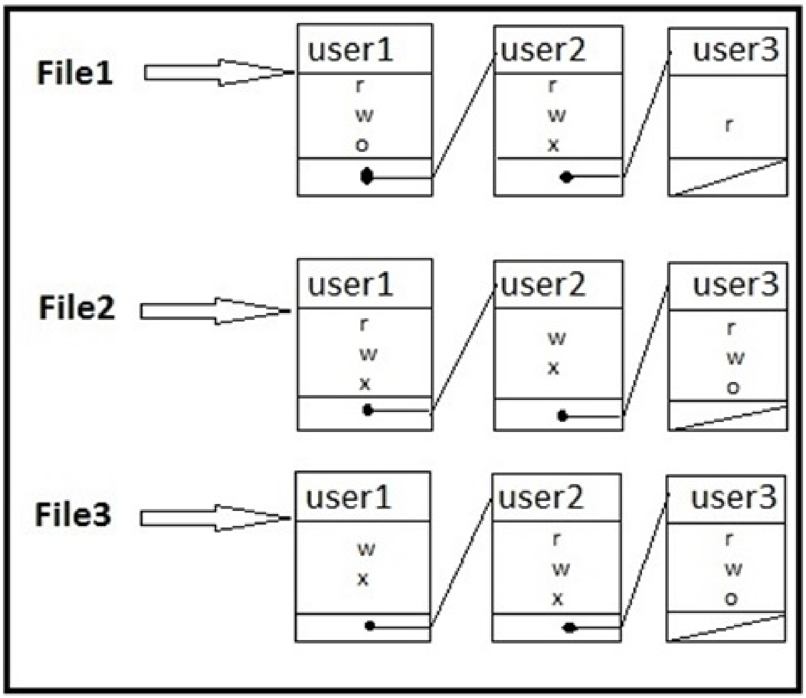


Figure 3. Access Control List.

3.2. Access Control Matrix

Several abstractions have been defined so far while dealing with access control. The resources can be characterized as files (stored data) also known as objects. A subject that accesses the resource can be referred to as a program (on the user's behalf) or as a user. The access control matrix is referred to as a digital file or record that consists of 'objects' and 'subjects' with the details similar to what action a user can perform or what permissions are associated with which user. In simple words, the matrix permits certain users for certain information. Subjects and objects are written along the axes in the matrix [28].

The purpose of the access control matrix is to protect unauthorized access and making sure the adherence to confidentiality, integrity, and availability of resources/data. Access Control Matrices list the processes and files in a matrix, users (subjects) are identified as rows and files (objects) are identified as columns. Table 1 depicts the access control matrix, where w stands for write, r stands for reading, x stands for executing, and o for owns. It is used as a model of static access permissions in control systems.

3.3. Mandatory Access Control (MAC)

MAC is a security model that limits the accessibility of the resource where the resource owner has the right to grant or deny the permissions for the manipulating resource [1,39]. MAC policies are defined by a system administrator and enforced by the Operating System (OS). In MAC, the policies are unalterable by the users. Users are not authorized to override the policies and policies are strictly controlled by the policy administrator. MAC is the system-wide policy that provides permission to the users [40]. Operating systems that support MAC policies are SELinux, Trusted Solaris, and TrustedBSD, etc. [12,27,41] MAC is deployed in government agencies and military facilities. It is also known as labeled systems and can be divided into the following two types.

- Multilevel Security
- Multilateral Security

Multilevel Security

In multilevel security, the users and information they access are divided into different levels. Levels are assigned according to the sensitivity of the information and are classified as top secret, secret, confidential, etc. These levels are defined as classification level, security level, and clearance level. Classification: Classification level gives the level of sensitivity to some recourse/data. The level of sensitivity is defined as: for instance, how much the military information is sensitive and if it gets leaked to any enemy or gets compromised then what degree of damage it would be for the country. Clearance: Clearance level identifies the user rights with some clearance. These rights or trust specifies the highest level of information managed by the subject/user [1]. Security: it is used for both the clearance and classification level. The following are some well-known access control models that are based on multilevel security.

Bell–LaPadula Confidentiality Model: Bell security model was proposed in 1973 by David Bell and Len Lapadula as a formal state transition model. This model was used for providing security to time-sharing mainframe systems. It is also known as Multilevel Security (MLS) model for dealing with confidentiality [42]. Its access control rules use security labels on objects and clearances for subjects. To provide confidentiality, it uses two security properties Simple Security Property and *-property to limit the flow of information from high to low-security level [27].

Simple Security Property: A subject is not allowed to access/read an object at a higher security level than itself (no read up).

*-Property: A subject is not allowed to write any object at a lower security level than itself (no write down).

Property defined as tranquility property is used to improve the above-mentioned properties. This property is further classified into strong and weak tranquility property. Strong tranquility expresses that while the system is performing operations, security levels cannot be changed and weak tranquility tells that security levels should never be changed in such a way to violate the defined security policies [27,43].

Biba Integrity Model: The Biba model was developed for ensuring information integrity. It is a reverse of the Bell–Lapadula model as it adheres to the principles of reading writing for integrity. It labels the data and subjects from low to high levels of integrity. It also uses simple security property and star property (*-Property); however, they are reverse of the Bell model and use no read down and no write up [44].

Multilateral Security: In multilateral security, the lateral flow of information is controlled instead of up or downflow. For example, data access from competing organizations or medical records. It is also called compartmentation, with competing compartments that also have some shared data. Chinese Wall model and British Medical Association (BMA) model are the well-known multilateral security models.

Chinese wall policy: In 1989 Nash and Brewerin proposed a Chinese wall policy to address the conflicts of interest [45,46]. It deals with confidentiality but not with integrity. This policy model uses three-level of abstractions to build security policies.

Objects: The lowest level consists of objects which contain information regarding a single company.

Company Groups: Intermediate level describes the collection of the entire objects associated with one company.

Conflict classes: At the highest level, clusters of objects related to contending companies are described, e.g., Microsoft, Google, Linux is one conflict class [47,48].

In Chinese wall policy, a subject can access the object if and only if he has not accessed any object before from the group of conflict classes. For example, the subject who has accessed the Google object cannot access the Microsoft object; however, it can access another object from other conflict groups. Formally, the policy is assigned according to the following properties:

Simple Security Rule: This property tells that object can be read by a subject only if: The object was already accessed or belongs to another conflict class.

*-property: permission for write access is granted only if: the subject cannot read from any conflicting class.

Regarding secure cloud-related operations, the solution is being provided by the Chinese wall policy [46].

3.4. Discretionary Access Control (DAC)

In 1985, Discretionary Access Controls (DAC) was established by US Department of Defense (DoD). DAC is used where subjects having legitimate legal rights can specify resource sharing rules with other subjects [49,50]. Access restriction in DAC is based on the identity of the user to which an object belongs. Access is granted by the resource owner, therefore, an owner can accidentally or maliciously grant to unauthorized users. Many operating systems like Window or UNIX have DAC implemented in them [51,52].

DAC and MAC are not mutually exclusive, if permission for the upper bound access is given then MAC also behaves as DAC [51,52] otherwise they are not mutually exclusive. The permissions which are decided by the administrator are upper bound permissions. DAC does not need state information but it needs access right confirmation. An add-on can be installed to modify the security rules because the DAC given by OS is not sufficient for organizations. DAC model's enforcement merely requires access right's verification for single user operations and does not need state information. DAC security models given by operating systems are not fully sufficient for organizational needs. An add-on product can offer substitute security model by rule's modifications.

ACM files are listed in a matrix, subjects in the row and objects in the columns, the point where they intersect are mapped to the permissions the subject has on an object. In DAC action by subject is performed based on its identity and discretionary policies. Access control is defined by these policies. In DAC according to the administrative policy rights are given to the other users by some user who owns those rights [1].

DAC uses access control matrix where subjects are placed in rows and objects in columns [1]. The entries in the matrix grow O(n^2) in size of matrix if O(n) is the growth of subject and objects. In practice, these matrices are thin as some of the subject does not have any access permissions and some of the object is not accessible by some subject. But if access controls must be placed in these matrices then large quantity of memory would be required and lookups would be expensive [27].

This right discretion in DAC model makes it vulnerable to Trojan horses. Administratively maintaining the systems is very problematic as resources are owned by the users themselves and they control the access. Giving rights of the resources to other users violates the safety as file/data can be copied from one location and can be placed at another. DAC is seen as Access control matrix that includes ownership relation, permitting subjects to relax policies for their resources. This mechanism performs granting or revocation of rights to the user's discretion, evading system administrator controls. DAC are widely spread models but still, they suffer from numerous issues including: In Linux system, insecure rights can be settled. For example, "chmod 777" allows any rights to any user. Transitive read access: For example, if user1 is permitted to read user2's file, she can copy the file content and give access to another user to read. In DAC model the right discretion makes it defenseless against Trojan horses. System maintenance is very difficult as the users own the resources and access are controlled by them. If the rights are given to other users it violates the security. DAC is an ACM which contains relation between owners, allowing a subject to reduce policies regarding their resources. DAC is very popular and mostly used but facing the number of issues which are as follows:

Insecure rights could be settled in Linux Systems. E.g., "chmod 777" will allow any right to any user. Transitive read access: it can give access to the contents of one user to another and the other user can give access to the contents of the first user to third without having its consent. Thus, it provides undesirable security in access control matrix. As one cannot claim that initial secure access rights would remain secure. The use of these access controls is now limited to noncritical structures [53]. In the untrusted environment, where the system can be compromised. DAC provides the security with the risk of serious leakage or damage. This model is not being used by cyber terrorism's potential target i.e., governments, biological or war industries.

3.5. Role-Based Access Control (RBAC)

RBAC has been used for the past 25 years and is the most implemented access control model. It emerged as a full-fledged model about a decade ago [54] with the maturity level as MAC or DAC had. RBAC is even being recommended as a generalized approach to access control. In the 1970s, the initial idea of Role-based access control came with multi-application and multi-user (online) systems. The first RBAC model is proposed in 1996 [55] and is standardized by NIST in 2001 [54]. The main idea of RBAC is that roles are assigned to permissions and users are assigned to roles. Permissions management becomes simple in RBAC [55–57]. Roles are created according to the job function and users are given roles according to their responsibilities. In understanding the RBAC model, it is important to understand the difference between group and role. Groups are not the collection of permissions but the collection of users while roles are both the collection of users and the collection of permissions, being users at one side and permissions at another side. Roles bring these two collections together [54,58]. Figure 4 explains the concept of RBAC model.

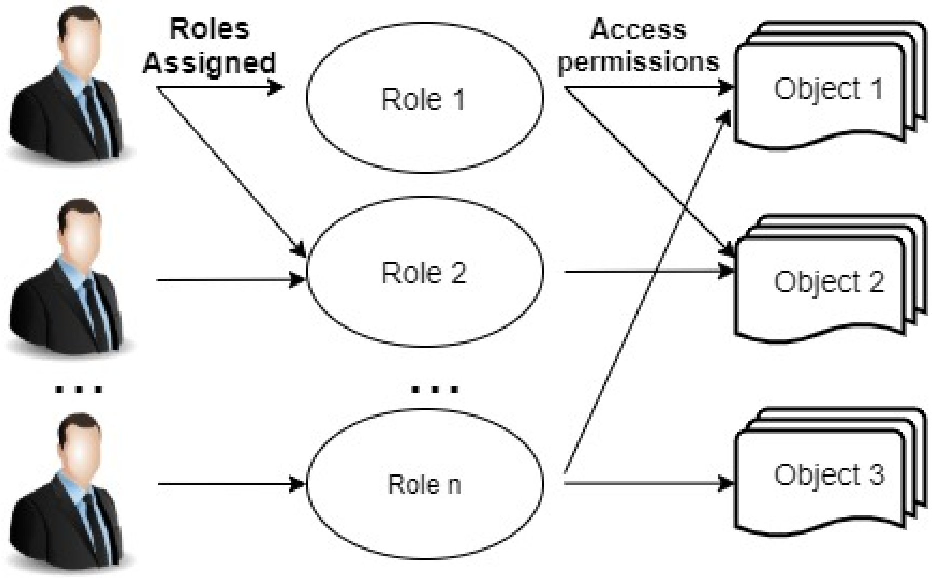


Figure 4. Basic concept of Role-Based Access Control.

In 2001, NIST proposed the standard RBAC model that is arranged into two components: Reference model and Functional specification. The reference model provides a definition of the RBAC model. It also provides the terms used in the RBAC model and features' scope in the standard [54,59]. It has four model components: Core-RBAC, Hierarchical-RBAC, Static Separation of Duty (SSD)-RBAC, and Dynamic Separation of Duty (DSD)-RBAC. Core-RBAC contains the main aspects of RBAC. The RBAC model defines that users are allocated to roles, permissions are given to roles and users get the permissions associated with that role. The association between user-role and permission-role is many-to-many. One user is allowed to be assigned to many roles and one role can be assigned to many users, the same in the case with role and permissions [60,61]. Core-RBAC also has user sessions that define which role can be activated by the user. The RBAC model is shown in Figure 5 representing four model components of the NIST standard. OBS are objects and OPS represents operations. THE hierarchical RBAC model is for role hierarchies. The hierarchy can be defined as seniority relation of roles; whereby the senior role obtains permissions of the junior role while the junior role obtains the users of the senior role. Overlapping capabilities are present between roles; that is users from distinct roles may have some common permissions. There are two types of hierarchies:

General Hierarchy: In a general hierarchy, roles hierarchy is supported. It includes the multiple inheritances and membership of users among roles. role hierarchy is supported in it; permissions, inheritance, and user membership among roles are included,

Limited Hierarchy: It represents the role hierarchy restrictions. Hierarchies are limited to structures (tree or inverted tress). A number of commercial products support limited hierarchies.it shows role hierarchy boundaries. Hierarchies are restricted to structures.

Conflict of interest policies is handled with separation of duties relations. Conflicts in the RBAC model occur when users gain permissions from conflicting roles. This scenario can be prevented by using SSD to impose limitations on user assignment to roles. For instance, one user is the manager of the bank and is a cashier; in this case, he can request the expenses and get them approved by himself. Organizations want to prohibit such cases in which the same user performs such a conflict of interest functions. SSD is implemented in both presence and absence of role hierarchies. In absence of role hierarchy, constraints are placed on the user to role assignments [61]. In presence of role hierarchy, both assigned roles and inherited roles are considered. DSD puts constraints on available permissions to users by limiting the role activation within or across the user sessions. Constraints are defined as a pair (role set, n) where n $\geq$ 2 showing that the user cannot activate n number of roles at the same time from assigned roles set [54]. Due to its simplicity in rights management, the RBAC model is widely adopted and implemented in the industry as well as in research. There are numerous extensions of the RBAC model, every researcher extended the basic RBAC model for its own application requirements. Recent work on the Intelligent Role-Based Access Control (I-RBAC) model [62] proposes semantic business roles for multi-domain collaborations.

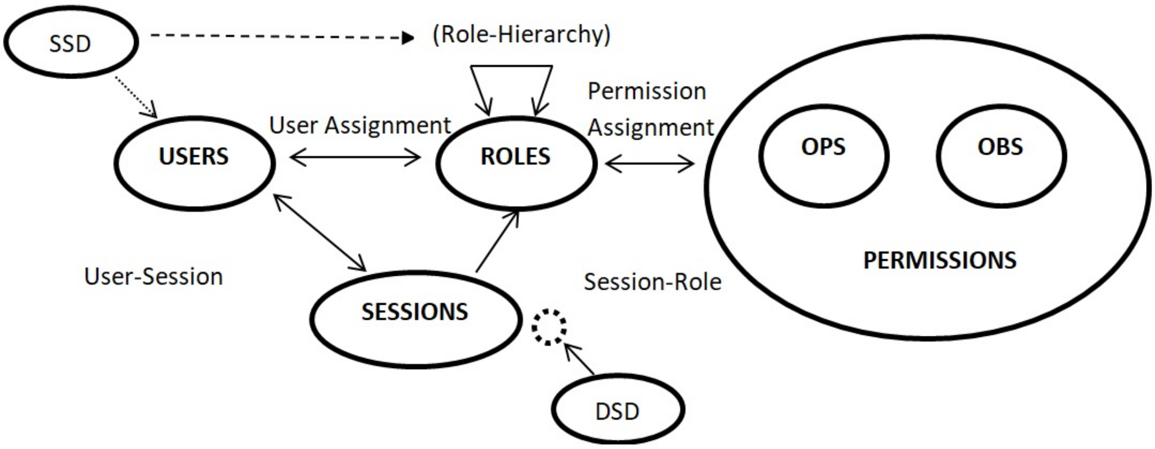


Figure 5. Role-Based Access Control (RBAC) model.

3.6. Context-Based Access Control

Context-Based Access Control (CBAC) models are built on context-centric information sharing. CBAC models are usually applied on top of the RBAC model. In CBAC the permissions are assigned, and tasks are performed based on context conditions. Many real-life applications use context-based access control models such as tour guides, hospital information systems, smart environments, and tour guides [63,64]. In literature, context can be thought of as "characterization of conditions for performing appropriate operations for its desired behaviors". A user's context is its location, activities, connected device, or network, in some cases, temporal attributes (time and duration of occurrence) can be referred to as context. The situation of an entity and the world which operates the entity can be characterized by the context [65]. This entity can be location, time, or the user itself. In the healthcare example [66], context-aware authentication can be performed via the location of the patient who stays at home and health services provided by the PDA's. In the network environment, CBAC provides four features: Traffic filtration, traffic inspection, intrusion detection, and alerts and audit generations.

CBAC also performs deep packet inspection and terms as an IOS firewall. In the smart environment (mobile applications), the context can be referred to as physical and virtual components. The physical components include location, date, time, and type of device used. All these contexts are used for enabling granting access permissions. In Context-Sensitive Access Control [67], the Access Controller is the main part involved which grants or denies the permissions of a Subject to perform Operation based on the Access Policy. The permissions are given to the user based on context. The Subject ID can be a user pseudonym and the token can be its context information. Access Controller performs the user's authentication and authorizations:

Authentication: Authentication is performed on subject ID, Token information, etc.

Authorization: Authorization is performed by determining the subject permissions associated with it.

For authentication, contextual verification can be performed in several ways: The source (trusted party or broker) providing the context can be checked, context-based signatures are in use for the integrity of the context, proximity is the main concern in the case of the context location and comparisons can be made with some authentic objects [67]. Context-aware access controls are widely being used in wireless sensor networks (WSNs). A context-aware RBAC (CA-RBAC) [68] is proposed for WSNs which is based on modular context. These models provide context-awareness for user's safety assurance in sensor networks. In [69], authors show that RBAC is not good for use in WSN, as policies and roles are predefined in traditional RBAC. In the CA-RBAC model, decisions are made based on three modular contexts: emergency, critical and normal conditions. These situations will allow different access rights to sensed data [68]. Decisions are made based on context information i.e., time, location, and policies of above-mentioned three modular situations. In Wireless Medical Sensor Network (WMSN), sensors get attached to the human body and checks for the body's health for healthcare services [31]. In the case of the normal situation, the authorized doctor accesses the EHR (Electronic Health Record) based on the role/s assigned to him but the nurse will not have the privileges as the doctor has. But in emergency or critical cases both can access and perform any action.

3.7. Attribute-Based Access Control (ABAC)

Access to the resource through the Attribute-Based Access Control by verifying access policies, these policies are designed by the combinations attributes related to users. This mechanism basically refines resource access. It motivates the need 'Principle of least privilege' that ensures the prevention of sensitive information and resources of the system. An example of ABAC can be related to the company that offers data to the employees who have completed their 2 days of training. Attribute-Based Access Control is known to be a logical model that evaluates attributes (subjects or objects), operations, and the request related environment [70–72]. Access policies or access rules are created without the relationships between each subject and object. In the enterprise model, users could not evaluate the advantages and challenges of the model. For addressing this problem NIST has provided the definitions and considerations which serve 2-fold purposes: First, it gives a definition of ABAC and describes its functional components. Second, it defines design, implementation, planning, and operational considerations for deploying Attribute-Based Access Control within the enterprise. ABAC is potentially secure in e-commerce and IOTs [70]. In ABAC attributes can be associated with:

Subject Attributes: Attributes associated with the subject can be (user, process, or application) that describes subject characteristics. These attributes can be a role, job, title, ID, name, etc.

Resource Attributes: Attributes associated with resources i.e., data, functions, or services.

Environment Attributes: These attributes define the situational, technical, or operational environment or context that causes the information access occurrence i.e., current date, current time or threat levels, etc.

ABAC is not new it was first used in the 1990s as X.509 identity certificates; X.509 attributes certificates and X.500 directory [73,74]. Attributes in ABAC can be associated with actions, users, subjects, objects, context, or policy. Attribute values can be possibly chained or complex data structures. These attributes are preserved by security administrators, users, or trust mechanisms. ABAC model needs identification of PCPs (Policy Configuration Points) and their formalisms and language. ABAC can be configured as DAC, MAC, and RBAC. In the future relationships and provenances are needed along with attributes. Some hieratical ABAC has also been proposed for cloud environment [75–77] and IoT [78].

ABAC$_a$: ABAC can be configured to do MAC, DAC, and RBAC. This 'just sufficient' model is known as ABAC$_a$. It is one of the members of the ABAC family models. Mutual attributes, connection attributes, and environmental attributes are further enhancements beyond the ABAC$_a$ [79]. At this stage ABAC$_a$ is premature to be thought of as core-ABAC, because ABAC$_a$ provides the deployment of three classical models (MAC, DAC, and RBAC) along with dynamic access control. ABAC$_a$ model will eventually be deployed as an authoritative member of ABAC family models. To understand the ABAC$_a$, it is important to understand the DAC access control lists, MAC lattice-based access control, and hierarchical RBAC. ABAC$_a$ model can be seen in Figure 6 [79]. Components of ABAC$_a$ are U (Users), S (Subjects), O (Objects), UA (User Attributes), SA (Subject Attributes), OA (Objects Attributes), P (Permissions), constraints, and authorized policies.

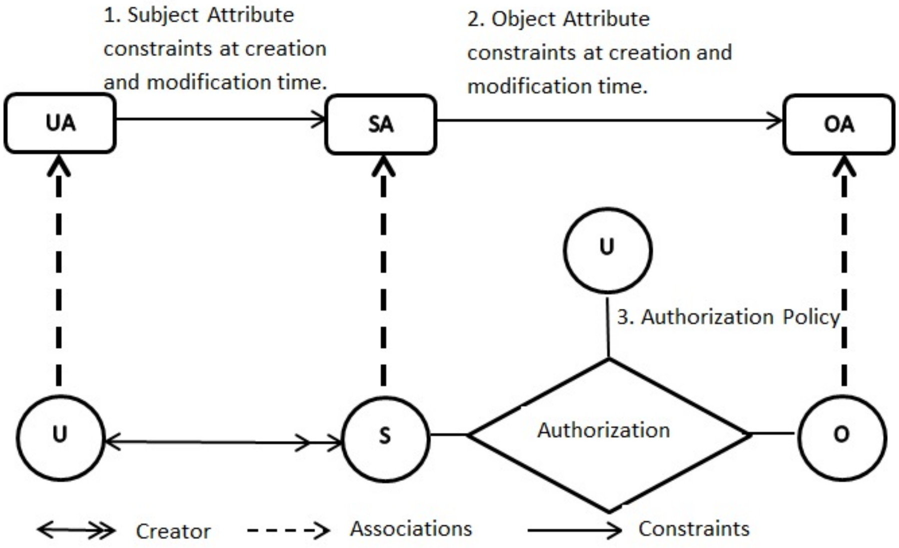

1. Subject Attribute constraints at creation and modification time.
2. Object Attribute constraints at creation and modification time.
UA
SA
OA
U
3. Authorization Policy
U
S
Authorization
O
Creator
Associations
Constraints

Figure 6. ABAC$_a$.

ABAC$_b$: This Model is similar to ABAC$_a$ model; however, ABAC$_b$ contains another feature of the constraint attribute. Figure 7 depicts the whole ABAC$_b$ [73]. Constraints can be specified on authorization rules that are helpful in making constraint-based access control decisions.

3.7.1. Lattice-Based Access Control (LBAC)

Lattice-based access control models are very useful in environments where circumstances have critical information flow [80]. Lattice models have become computer security's key components. For dealing with information flow in computer systems, Bell and LaPadula established Lattice-Based Access Control models, and along with bell and Lapadula, Biba and denning made a significant search in this area in the 1970s. Since then these models have been used in multiple organizations and especially in the US defense sector and allies. The commercial sector has the main concern in information flow so these models are of their need. The following are the main components and models of Lattice-Based Access Control.

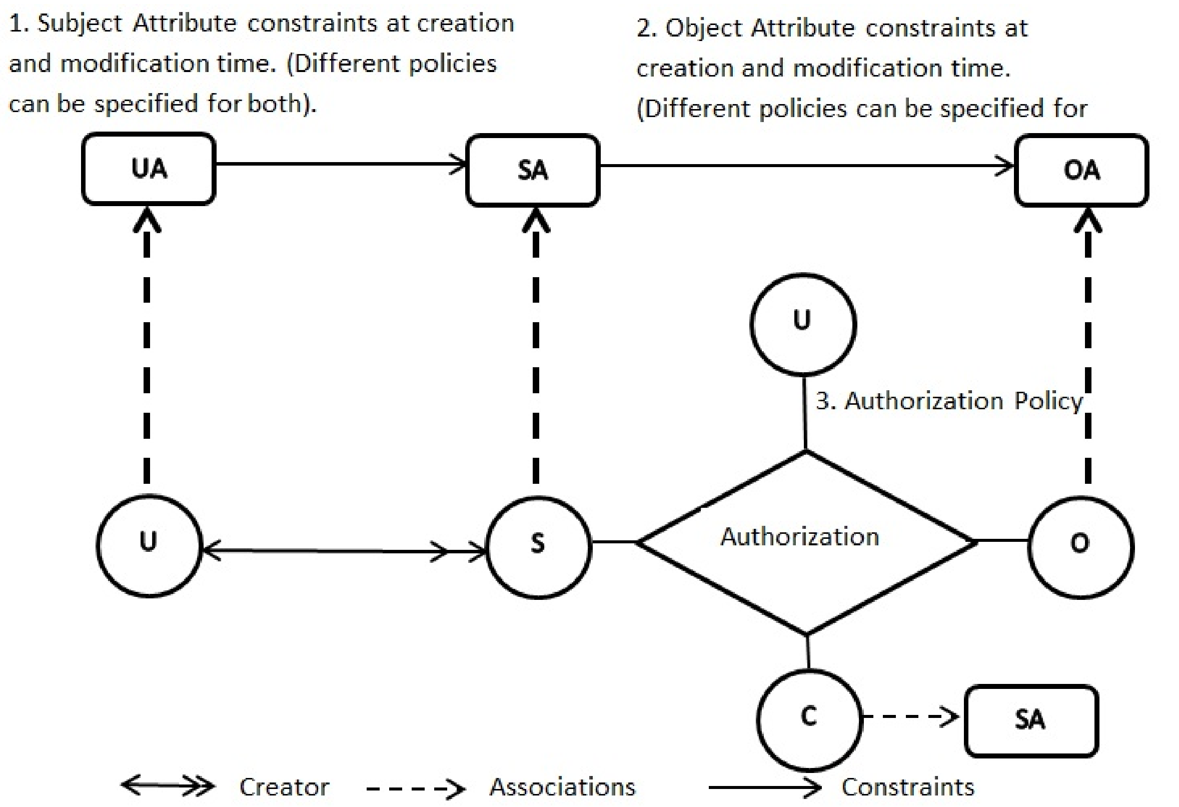

1. Subject Attribute constraints at creation and modification time. (Different policies can be specified for both).
2. Object Attribute constraints at creation and modification time. (Different policies can be specified for
UA
SA
OA
U
3. Authorization Policy
U
S
Authorization
O
C
SA
Creator
Associations
Constraints

Figure 7. ABAC$_b$.

Denning's axioms: Denning showed that an information flow policy can form finite lattice but under certain assumptions. Following are the main points of denning are axioms:
Set of the security classes (SC) is finite
The partial order on SC is a → (can-flow relation)
SC contains lower bound regarding →
The join operator ⋈ is the least bound operator.
Denning's axioms are as follows:

Denning's axiom 1: The first axiom states that the security classes set should be finite and requires little justification. Axioms are not applied to the object in the system but to the security classes. Objects can be created and destroyed dynamically using denning's axioms, with no limit on several objects to create.

Denning's axiom 2: The second axiom states → represents partial order on SC. A partial order can be defined as a transitive, reflexive, and anti-symmetry binary function. Reflexivity: A → A for all A ∈ SC. The Transitivity: if A → B and B → C, then A → C i.e., indirect flow is possible from A to C through B, there should be direct flow from A to C. There are multiple situations in which indirect information flow should not suggest direct flow [80]. These scenarios are handled as exceptions which are outside the Lattice Framework of flow. These concepts can be enforced using Type enforcement and assured Pipeline concepts.

Anti-symmetry entails A → B and B → A then $A = B$. If transitive and reflexive requirements are given, anti-symmetry removes redundant SC. If objects are restricted for having the same information flow with these labels, then there is no need for different security labels.

Denning's axiom 3: Denning's third axiom recognizes public information in the systems. L represents the lower security bound of security classes i.e., L →A for all A ∈ SC. Public information permits for needed features (public bulletin boards and databases). One can argue that constant objects should be labeled with L. Version information of the operating system is the best example of constant. For certain programs, this constant information is very necessary and publicly available.

Denning's axiom 4: Denning's fourth axiom is known as the subtlest. The fourth axiom consists of two parts: First, define the joint operation, i.e., A $\bowtie$ B for each pair of security classes that belong to SC. This gives the labeled output from the information taken from two security classes.

3.7.2. Bell–LaPadula Lattice Model

The Bell–LaPadula model (BLP) is the formalization of the MAC concept [80]. The BLP model contains all vital access control properties. The main idea in BLP is to supplement DAC with MAC for enforcing information flow policies. BLP uses two steps method. First, using discretionary access matrix D, the subject can modify the contents. Authorizations in matrix D are not enough for carrying operations. Second, the operations are carried out for accessing objects after authorization by the MAC policy where users have no control over the administration. MAC works with security labels attached to the subjects and the objects. Object labels are also known as security classification and user labels are known as security clearance. Subjects running the same program on the behalf of a user, having different labels represents different privileges.

The 'λ' is used for security labels of the objects and the subjects. Mandatory access BLP rules are as follow:

Simple-security property: Subject s can read object o iff λ(s)$\geq$ λ(o).

*-property (star-property): Subject s can write to object o iff λ(s) $\leq$ λ(o).

3.7.3. Biba Model and Duality

Biba's model concept is that low-integrity information is not allowed to flow from low to high-integrity objects while the opposite is acceptable. Biba uses mandatory controls for integrity, the best known is called strict integrity. In Biba formulation, at the top of the lattice, high integrity is placed and low integrity at the bottom. Permitted flow is from top to the bottom. Biba's model is opposite to the Bell model and Denning's axioms. This thing leads the Biba model for proposing following mandatory controls (ω represents integrity labels of objects and subjects):

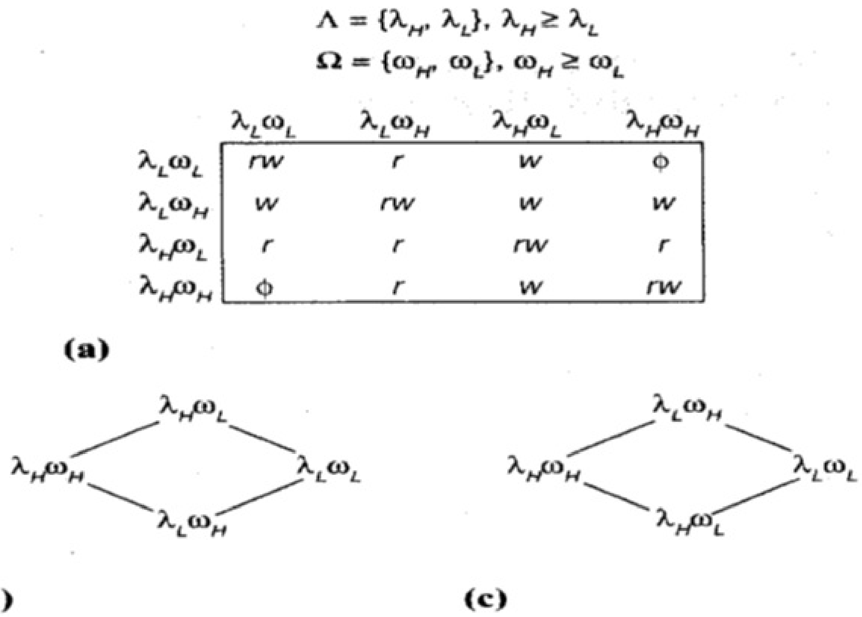
Simple-integrity property: Subject s can read object o iff ω(s) $\leq$ ω(o).

Integrity *-property: Subject s can write object o iff ω(s) $\geq$ ω(o).

These properties are known as duals properties in BLP. There is nothing intrinsic in the Biba model for placing high-integrity labels at top of the lattice model. Biba model's information flow can be brought in line regarding BLP model by placing low integrity at the top of the lattice and high-integrity at the bottom of the lattice model. With this point of view, mandatory controls can be used for enforcing the flow of information needed by the Biba model, the situation named symmetrical. In the same way, Denning's (BLP) lattice can be inverted by placing low confidentiality at the top and high confidentiality at the bottom and mandatory controls for enforcing information flows.

Considering more useful situations where high integrity and high confidentiality is placed and top of the lattice, where λ represents the confidentiality label and ω as integrity label. Let λ be the lattice of confidentiality given by λ = λ_1,...,λ_p and ω is lattice of integrity given as ω = ω_1,...ω_q. The combined mandatory controls become: Subject s can read object o iff λ(s)$\geq$$\lambda$(o) and $\omega(s) \geq \omega(o)$.

Subject s can write object o iff $\lambda(s) \leq \lambda(o)$ and $\omega(s) \leq \omega(o)$. This composite model has many implementations in many areas like operating systems, databases, and networks. The product of two lattices, which is considered to be one lattice, has been shown in Figure 8 [80].



$\Lambda = \{\lambda_H, \lambda_L\}, \lambda_H \geq \lambda_L$

$\Omega = \{\omega_H, \omega_L\}, \omega_H \geq \omega_L$

	$\lambda_L\omega_L$	$\lambda_L\omega_H$	$\lambda_H\omega_L$	$\lambda_H\omega_H$
$\lambda_L\omega_L$	rw	r	w	φ
$\lambda_L\omega_H$	w	rw	w	w
$\lambda_H\omega_L$	r	r	rw	r
$\lambda_H\omega_H$	φ	r	w	rw

Figure 8. (**a**) Composite model (**b**) Equivalent BLP lattice (**c**) Equivalent Biba Lattice.

3.7.4. Chinese Wall Lattice Model

Chinese wall was discovered by Nash and Brewer and was first presented as a Lattice-based access control model in 1992 for the enforcement of the Chinese wall policy [81]. Conflict of interest in information flow is prevented by this policy. Let us take the scenario in which consultants are dealing with confidential information of their clients, but a consultant cannot have access to the same company said two oil companies or two banks because of conflict of interests. Insider information from the same type of companies, offers the potential for personal benefits to consultants, using this knowledge. Here comes the dynamic aspect of the Chinese wall policy, consultants face no restrictions (mandatory) on access rights. It is beneficial to differentiate public information and company information. Public information includes electronic mails, public databases, bulletin boards should have no mandatory restrictions and they can have DACs restricting the read access to public items. Policy for writing information either of public or company is derived from the concept of its result on providing read access that is conflicting MAC read access. Assume, with n classes of conflict of interest: $COI_1, \ldots COI_n$, each class with m_i companies, so $COI_i = 1, \ldots m_i$ where $i = 1 \ldots n$. Suppose that oil companies and banks are of different conflict of interest. Then, labels Bank A, Bank B, Oil Company are differing from the Chinese wall policy. Such labels have been restricted in Chinese wall lattice by introducing the security label (n-element vector $[i_1, \ldots, i_n]$) where each $i_k \in COI_k$ and i_k can be a number or $i_k = \perp$ for $k = 1 \ldots n$. The symbol $\perp$ represents null. Chinese wall lattice is shown in Figure 9 [80].

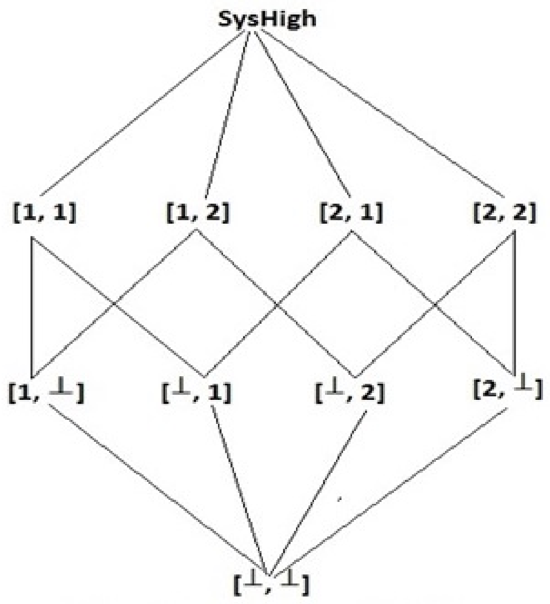


Figure 9. Chinese Lattice Wall.

3.8. Identity-Based Access Control (IBAC)

In security systems, identity is one of the critical aspects. IBAC is a coarse-grained digital security mechanism that determines user authentication. Access control models identify user's credentials supplied by trusted authorized parties for granting access to sensitive resources. Username and password are the most common identities for authentication systems. Identifications can be divided into passphrases, biological measurements, and physical tokens, etc. Combinations of individual factors are employed for increasing the complexity of security. Multiple factors provide more security than an individual (single) factor. Three main types of authentication factors are as follows:

Type1: Something that you know i.e., pin, password, etc.
Type2: Something that you have i.e., tokens, smart-cards, keys, etc.
Type3: Something which you are i.e., biometrics (fingerprints, iris, face/voice recognition), etc.

Most of today's access controls policies are 'Identity-centric'. The term is used for accessor specified policies. The questions like "who?", "who can do what?", "who is accessing?" etc. are answered by the policy. The information security industry is encouraging Identity-based access for the last two decades. Identity-based mechanisms provide the user's authentication based on their identities or password information they have [82,83]. This mechanism ensures the identification of the user's existence. Group identity is one of the variations that perform access control for the whole user group to some resources like databases. Wi-Fi network's secure access is the best example of identity-based access control. An identity-based scheme looks like a mail system [84]. If you want to send someone a message, you need to know his name and address so that only the intended recipient can read. This thing can be verified by the signatures that only he could have generated [85]. There is a tradeoff between ease of use and complexity in the identity-based systems. Electronic identity is "something verifiable and difficult to reproduce". Identity should be easy to use. Password with account ID provides an example of an ineffective identity as they are easy to use but easy to reproduce as well. Easily guessed information does not provide high Identity probability (IP). On the other hand, identity effectiveness is a solution that provides the 100% probability of the subject's identity but is unusable. For example, for accessing financial information, a combination of the token, certificate, passwords, and voice prints is a wastage of resources. The verification process's complexity and cost for identity should mirror associated risk with unauthorized access.

Roles get attached to identities, as roles do not get authenticated but the identities get authenticated. If identities get authenticated, then roles are authorized. Roles are the extension of identities. For example, the admin has the role of 'administration' the privileges of the standard users are different from an administrator. It is the capability of identity with multiple roles, so the administrator can have rights of administrator and standard user as well. Passwords are also tied to identities [82], so the password gets authenticated against the identity. If the access control system does not have a username field, then the server will check all the passwords for password validation associated with every user. Identity-Based Signatures (IBS) are the cryptographic primitives that provide strong authentication. IBS scheme generates the signatures based on the secret key of the user who is signing, so it becomes quite hard for the unauthorized user to sign the message to generate the signatures. Signature verification methods detect any illegal change, invalid messages, or signatures which do not permit the verification. An attacker can never triumph to falsify these systems. IBS is used in cryptographic operations. Reusable IBS schemes are available that get replaced with new improved, more secure IBS schemes for better performance and securities [86].

There are many more access control models based on different systems or applications. Team-based access control models [87,88] are used to grant access to the users working together in a collaborative environment like teams. All members (users) of the team may get the same access permissions in general and a few others (admins etc) may have more permissions. Collaborative access control systems are mostly the extensions of the RBAC model and are usually implemented using DAC or hybrid techniques where users grant access rights on their objects to other users. Usually working in teams, users must perform one or more tasks. Task-based access control models are developed [89,90] to grant access based on user's participation in the task.

4. Access Control Models for Online Social Network (OSN)

Access Control models for OSN are mainly based on patterns of relationship and structure of the community. OSN models have different policy specification languages, architectures, and rules. Access control models for OSN can be categorized into the following models: Relationship-Based Access Control, Community Structure, User-Centric Access Control, and Attribute-Based Access Control. Relationship-Based Access Control Model is further divided into sub-categories. But the most important access control for OSN is Relationship-Based, as the whole social network is based on relations of the users. A survey on SN privacy is presented in [91] and a detailed survey on access control for SN is presented in [92]. In this survey, we are discussing Relationship-Based Access Control in detail.

Relationship-Based Access Control (ReBAC)

This model is based on the user-to-user relationships in OSN. Users can have different types of relationships when connecting to other users in the social network. Social network relationships are plotted in graphs that are analyzed using different Social Network Analysis (SNA)-based techniques and algorithms for finding hidden patterns in these graphs. These patterns help in implementing access controls in OSN. Relationship-Type-based access control models are based on the type of relationships users have with other users such as close-friend, friend-of-friend, etc. In a friend-of-friend relationship, a "friend" of the owner does not have that much access to a resource as a "close-friend" has. Relationship type of the owner becomes the base for access control. In [93], the importance of access control policies for personal data sharing in OSN's applications (Social Bit-Torrent, Social Firewalls, and Google Calendar) is described. The concept of social attestation and social access control lists has been introduced for social-networking-based access control. Social attestation is to verify the relationship with other users and the social access control list has three concepts: the public key of users who can access the information, the owner's public key, and the relationship between owner and requester. For accessing an object, a user needs its public key which is already listed in social ACL or in another way the user will have to demonstrate attestation given by the owner of the object and that attestation is verified through the relationship type. Different views of the user's calendar can be enforced through social attestation. This model shows the user-to-user relationships into the OSN. In the social network when users are connected they have different types of relationship types and statuses. Social Network Analysis algorithms and techniques are used to analyze social network graphs which are plotted based on SN relationship and hidden patterns are found in these graphs. Such findings help implement OSN's access controls. Relationship-Type Access Control models are mainly based on the user-to-user relationships like friend-of-friend, close-friends, etc. In a friend-of-friends relationship, the owner friend does not have too much access to the resources as a close-friend has.

The base of the access control is the Relationship type of the owner. In [93] the personal data sharing the importance of access control policies in OSN's applications (Social Firewalls, Social Bit-Torrent, and Google Calendar) has been explained. The concept of social access control lists and social attestation is introduced in social-networking-based access control. Social attestation is the process of verifying the relationship to the other users and there are three concepts of social access control list: access of the information is based on the public key, relationship, and owner's public key. To access objects user requires its public key that is listed in social ACL or on the other hand the user will prove attestation which is given by the object's owner and verification of attestation is done through the relationship type. The user's calendar has different views that are shown with the help of social attestation. The Social attestation to bypass the firewall in Different views is proposed in this study.

Social ACL concept has also been used in [94–96]. Social ACLs have two fields: relationship type and authorized user identifiers. Authorization is applied through the relationship certificate approach. Relationship information of users is recorded by getting their identifiers and relationship type placed in social ACL. A user-to-user Relationship-Based access control model for OSN is proposed in [97]. Different notations are used for different relations like in [94–96] the concept of Social ACLs has been used. There are two fields of Social ACLs: authorized user identifiers and relationship type. The relationship certificate approach is used to apply Authorization. The user's Relationship information is recorded by getting their relationship type and identifiers sited in social ACL. The OSN's AC model for user-to-user Relationship-Based is proposed in the [97]. Different types of notations are used for to show different type relations like $\sum$ has been used for the setting of bi-directional relationship types, for active action "action" and for passive action is used to set bi-directional relationship, to show active action the term "action" and to show passive action the term "action^{-1}" is used. This model has five components: Accessing user, Target user, Access request, Policy, and Target. Policies in this model are either user-specified or system-specified. System-specified policies are implemented by the OSN system and user-specified policies belong to resources and users. Based on regular expressions policy language is presented in [97,98]. It contains an evaluation procedure algorithm that extracts policies from the system when the user requests a target. An access control policy is dependent on graph rule and requested action. For traversing the graph this algorithm uses a depth-first search. All path spec (path, hop count) are combined for getting the result of the policy. The path represents a relationship path among users and max no. of edges is limited by hop count in the algorithm. System policies are designed to handle multi-user conflict; however, it does not consider node repetition for deterrence of redundant iterations. There are five components of the proposed model: Access request, Accessing user, Target, and the Policy. This model has the policies in the form of either system-specified or user-specified. The policies that are system-specified can be implemented by the OSN's system and the user-specified policies comprise the users and resources.

The regular expressions policy-based language is presented in [97,98] for the first time. It contains the algorithm for evaluation in which policies are extracted from the system based on the user request made for a target. Access control policy depends on the requested action and the graph rule. To traverse the graph the depth-first search is used in this algorithm. All the path specifications like path and hop counts are combined to get the required result for the policy. The path: max no is used to show the relationship path between users of edges that is limited by an algorithm for hop count. The multi-user conflicts are handled with the help of system policies, but the proposed method ignores node repetition for iteration redundancy in deterrence.

The user-to-resource and resource-to-resource-based relationship access control model is proposed in [99,100]. This model is an extension of the model discussed in [97]. This model discusses the administrative activities and the user-to-user policy is extended to user-to-resource and resource-to-resource policies. Users, resources, sessions, policies, and social graphs are components of the model. Policies defined in this model are either user-defined or system-defined. The system-defined policies are either conflict resolution or authorization policies while user-defined policies are divided into target user policy, accessing user policy, object policy, session policy, and policy for policy. Policy language has also been proposed for this model where accessing session and accessing user policies consist of pair (graph rule, act) while target session policy, target user policy, object policy, system policy, policy for policy consists of pair Relationship access control model which is based on resource-to-resource and user-to-resource is proposed in the [99,100]. The proposed model is an improvement made in the model stated in [97]. The administrative activities are discussed in the proposed model; user-to-user, user-to-resource, and resource-to-resource are extended to make the policy based on a regular expression. There are six components of the model: resources, users, sessions, social graphs, and policies. Policies in this model can be either system-defined or user-defined. System-defined policies can be either authorization policies or conflict resolution while the user-defined policies are categorized into object policy, target user policy, session policy, access user policy, and the policy for policy. This model also proposed policy language in which accessing user policies and accessing session has the pair (rule, graph act) while the target user policy, target session policy, system policy, object policy, policy for a policy can have the pair (rule, graph rule, act^{-1}). The System policy for the resource has the pair (rule, graph rule, o.type, act^{-1} 0. type).

For conflict resolution, three approaches disjunctive approach, conjunctive approach, and prioritized approach are suggested in this model. Another Relation-Based Access Control is proposed in [101]. This model works with the collaboration of users, system administrators, and system designers and can be used as a group-based or user-centered. In a user-centered approach, while a user makes an access request, her friends, followers, and the following information is sent to the system. However, in a group-centered approach, information of the group (group creator, etc) is sent to the system. Alloy Analyzer is used to demonstrate how potential misconfigurations and conflicts can be detected automatically for OSN access control [102]. Access Control for Facebook is proposed in [103]. This model focuses on public information of the user in OSN along with user relationships. Public information graph and user graph concepts are proposed in this model. To resolve conflict, there are 3 approaches: conjunctive approach, prioritized approach, and disjunctive approach that are suggested in the proposed model. In [101] a Relation-Based Access Control model is also proposed. The model works based on the collaboration of system administrators, users, and system designers, and the access control is either user-centered or group. In the user-centered approach when a user wants to access any website then the followers, friends, and the following information are first sent to the system. On the other hand in a group-centered approach, if a user wants to access any website the information of entire groups (this site or web pages are created by which group) is directed to a system.

The OSN's access control model and its formal specification are proposed by the authors in [102]. They demonstrated that conflicts and potential misconfigurations can be automatically detected by using Alloy Analyzer. This model also contains the same existing policies used in OSN. The Facebook Access Control is proposed for the popular social site Facebook in [103]. The OSN's public information is the main focus of this model that is the user and user relationships. It consists of three categories of information: public information, user relationships and connections of users, user linkage, and public information. This model also proposed concepts of using graphs and public information graph.

An Extended-ReBAC Administrative Model is proposed in [104] that can be applied beyond OSN where administrative authorization and edges dependencies exist. This model also deals with the relationship graph's integrity constraints and cascading revocation. This model has been designed to provide administrative capabilities in the multi-tenant collaborative cloud system. A Relationship Strength-Based Access Control model is proposed in [105]. This mechanism is based on closeness and intimacy degree regarding a user's friend as the user wants to give access to his content. Profile similarities and activities are used to calculate reliable intimacy. The user can create an access control policy based on a range of intimacy degree and only users with an acceptable range of intimacy degree are allowed to access. Brokerage and community aspects are important in SN research. A community-centric brokerage-aware access control model is formally described in [106].

5. Access Control for IoT

Internet of Things (IoT) is an evolution which is reshaping the routine errands of individual, governments, and industries [107]. Applications of IoT are categorized into three broad groups by [7] that include Personal and Home, Government and Utilities, and Enterprise and industries. Through IoT, physical everyday activities are closely connected to the cyber world with the help of tiny data-collecting sensors that send collected data to third parties like a cloud through the Internet. On one hand, IoT is making our lives smarter by applications like smart cities, smart grid, and smart health while on the other hand, it is entering our personal and intimate spaces. A recent study conducted by Orange reveals that 78% of customers are reluctant to share their private data due to security and privacy concerns.

Access Control is one of the major security and privacy-preserving mechanisms for any networking paradigm. In the context of IoT, access control not only means performing operations on the data source but also actuating the physical IoT object [8]. In this work, we explore access control models specifically related to IoT and its application. A comprehensive review of the access control models like RBAC, AABC, UCON, CapBAC, and OrBAC is performed and their suitability in IoT is evaluated through Security and Privacy-Preserving (S&PP) objectives presented in [7]. A survey on access control for specifically IoT networks is presented in [108].

5.1. Access Control Models for IoT Using RBAC

In this section, we provide the access control models for IoT that are based on the RBAC model. The domRBAC model [109] is an access control model proposed for grid computing-based collaborative systems. It is an extended RBAC model for collaborative systems that are based on ANSI INCITS 359-2004. The basic elements of domRBAC are users, roles, sessions, operations, objects, and containers. The domRBAC essentially receives all the features of RBAC such as ease of management, and separation of duty relationships yet al.so being supported in multiple domains. The domRBAC provides real-time checking of violations by providing usage management in a role-based approach. The performance of domRBAC is evaluated by implementing a simulator that is capable of enforcing a multi-domain access control policy. According to evaluation results, domBRBAC is better than other proposals but has lower interoperability.

Digital watermarking and contextualization techniques are combined to propose a role-based data obfuscation technique [110]. Digital watermarking is generally used to secure multimedia content where additional information is embedded within the digital content in a way that does not affect the original content. Digital watermarking is combined with a highly scalable contextualization technique ConTaaS [111]. ConTaaS is an optimization technique that overlooks the irrelevant data, which reduces the data volume thus reducing the computation time and increasing performance and scalability of privacy-preserving mechanisms. The proposed data obfuscation technique employs the bottom-up principle of data access according to the domination of roles. An experimental testbed has been developed on AmazonEC2 to evaluate the proposed technique. Their results reveal that the computational time taken by the proposed technique is modest.

An extended RBAC model for IoT applications is proposed in [112] by adding context-aware information like time, location environment parameters of physical IoT devices, to make access decisions. In this model service-oriented approach is used where IoT devices offer functionality as services. The extended context-aware RBAC model is demonstrated by the help of use cases by authors. This proposal seems to be more suitable for web-based services as they have only considered IoT users rather than devices. Another model [113] uses the Web of Things (WoT) approach and proposes an RBAC model that integrates with Social Network Services (SNS). This enables users to define policies under their user profiles and social links. The standard components of RBAC i.e., a user (U), permission (P), and role (R) have been redefined after a comprehensive analysis of SNS, user data, and abstraction of RESTful web service application interface (API). Sharing IoT devices through SNS enables the device owners to make user-friendly access policies considering the context information like user profiles (age, gender, location, etc.) and social links (friends, family, etc.). Integration of SNS with RBAC supports usability on one hand while on the other hand, it increases the dependence of resource owners and requestors on SNS thus introducing the SNS providers as a trusted third party.

An RBAC-based access control policy for WoT has been defined in [114] that provides a mapping between RBAC and WoT components. This proposal addresses two main issues of access control WoT, i.e., use of reference monitor and user proliferation through role parameterization technique developed in [115]. The proposed model is based on an Access Decision Facility (ADF) and end devices (sensors, actuators) are not considered to be information providers. This proposal does not provide a lightweight solution, which is not suitable for constrained devices of IoT. An access control security protocol using ECC (Elliptic Curve Cryptosystem) is presented in [116], which provides user anonymity, mutual authentication, and secure session key establishment. An OpenID identity layer on top of OAuth authentication is provided in [117]. IoT-based RBAC system for handling emergencies is proposed in [118]. It uses dynamic context-aware roles to provides access in time-constrained situations. An interoperable access control [119] is presented that uses OAuth authentication and roles for diverse IoT platforms.

5.2. Access Control Models for IoT Using ABAC

An ABAC-based access control architecture [120] is proposed for home IoT using NIST Next Generation Access Control (NGAC). The NIST NGAC provides a unified access control view to multiple operating systems with different types of access control views. NGAC implementation examines the flow of packets and enforces access policy in conjunction with suitable switching devices like the firewall of Software Defined Network (SDN). The attributes of entities in home IoT are enumerated in detail and then categories of policies suitable for home IoT are described. This proposal supports scalability as it has the policy of trust zones for new arriving devices in the network. The trust zone process is incremental and if the newly entered device is found malicious, the access grant is revoked.

A lightweight ECC for authentication and ABAC access control model [121] is proposed for the authorization process of the perception layer of IoT. A secure key session is established in the proposal for mutual authentication between users and sensor nodes. Mutual authentication is a simple authentication process that is suitable for resource constraint environments such as IoT. The authors believe that data access based on user attribute certificates in access control authority can achieve flexible fine-grained access control. Theoretical results are presented after evaluating the computational overhead of user nodes.

5.3. Access Control Models for IoT Using UCON

A state-of-the-art research of UCON models concerning the Internet of things is presented in [122]. The components of the UCON model are mapped on the entities of IoT. The subject (S) of the UCON model corresponds to Device (D) in IoT. The subject attribute in UCON is Device attribute Att (Device) in IoT which contains attributes related to IoT devices. The Object (O) of the UCON model is a Service (S) is IoT which lies in the application layer and is requested to be accessed by IoT Devices. The object attributes of UCON correspond to service attributes Att(Service) in IoT which are digital attributes of service. The Condition (C) is the limitations and constraints of underlying wireless sensor networks concerning IoT application. The oBligation(B) depends on the needs and requirements of IoT applications and they can be decided before or during the usage. Authorization (A) is decided according to the functional predicated of usage policies for Devices (D) and Services (S). The assessment model is based on the fuzzy theory. Several use case examples are given to verify the expression of UCON concerning IoT; however, the practical feasibility of this approach is not demonstrated.

A proposal on usage control for smart cities application is presented [123]. A formal conceptual data usage model DUPO is developed that captures the diversity of obligations and constraints resulting from the usage control requirements for smart cities. Furthermore, a rule language is formally defined by applying the defeasibility approach on DUPO along with practical expression. Accountability of the policy enforcement and traceability of data usage are the main goals that are addressed.

5.4. Access Control Models for IoT Using CapBAC

The original concept of Capability-based access control (CapBAC) for IoT applications has some drawbacks like capability propagation and revocation. However, extensions to CapBAC are found in the literature that suits IoT applications. A capability-based access model for IoT Identity-based Capability System (ICAP) is presented in [84] in which IoT user uses the capability to access a device or resource. The ICAP structure and how capability is used for access control is represented as ICAP = (ID, AR, Rnd) where ID presents the device identifier, AR the set of access rights for the device with device identifier ID, and Rnd the random number to prevent forgery and it is a result of one way hash function. The proposal does not consider context information while making access decisions.

An Identity Authentication and Capability-based Access Control (IACAC) model for access control and authentication in IoT applications is presented in [124]. IACAC uses a two-step process, first capabilities are made for the devices that need to communicate with each other through Capability-based Access Control (CAC) and then authentication is performed to check if the requesting device can communicate with the requested object. The IACAC model is evaluated for the following parameters: scalability, granularity delegation, and efficiency. The performance of the tool is presented concerning computational times. The issue of interoperability is not addressed in this proposal.

Another proposal Capability-based Context-Aware Access Control (CCAAC) model [125] extends ICAP model [84] designed for federated IoT. This model is a special UCON case where capabilities can be disseminated through a mutable attribute. As the model considers context-aware information, therefore, additional field Contexts (C) have been added to the traditional ICAP model which contains context information. These works lack a mutually trusted entity that supports the security requirements of federated IoT. A part of project IoT@Work [126] has been extracted in [18] that uses capability-based access control; however, this model is not lightweight and hence cannot be applied to resource-constrained devices in IoT. However, similar work in [127] presents a model for resource contained devices. The authors in [128] have presented a distributed access control DCapBAC model based on Elliptic Curve Cryptography (ECC) that supports the management of certificates, authentication, and authorization processes. This work provides end-to-end access control through traceability of the access, authentication chains to extend scalability and support of standard certificates. The DCapBAC model does not consider granularity and context awareness. An extension Trust-aware Access Control for IoT (TACIoT) is presented in [129]. It considers four parameters, i.e., quality of service, reputation, security aspects, and social relationships to compute trust values about IoT devices. The feasibility of the model has been evaluated on real testbed scenarios that reveal efficient computation time. This model lacks a definition of formal trust negotiation language to support interoperability within IoT. Another work uses a capability-based access control equipped with ECC-based key management for the M2M local cloud platform [130]. The capability-based component and key management are implemented in the security manager and feasibility is tested by evaluating their performance by a series of experiments.

5.5. Access Control Models for IoT Using OrBAC

The basic OrBAC model cannot cover the distribution, heterogeneity, collaboration, and interoperability needs of IoT applications. Therefore, the extension of OrBAC in the context of IoT is presented in [131,132] where the SmartOrBAC model is proposed to deal with constrained IoT devices. Security enforcing policies using context-aware information are defined for individual organizations as well as interactions between them. SmartORBAC is specifically designed for WoT and to reduce the bulk of interactions RESTful web services technology is used.

6. Analysis and Discussion

This paper covers many access control models. This section gives a comparison of the conventional models with evaluation characteristics that are given in Table 1.

6.1. Evaluation Criteria for Conventional Access Control Models

The following characteristics are used to discuss Access control models:
Complexity: It defines the access control model's nature. More complex models do not have implementations and lead to unexpected problems. There is a tradeoff between the complexity and the functionality of the models.
Understandability: It defines the underlying principles of the models and their transparency. The significance of the change in access privileges and manipulation should be clear for the proper usage of the system.
Ease of use: It indicates the usage of the access model from the standpoint of end-users that how simple the models are for them. If the models are difficult to use, then they will not be appreciated by the users—nonetheless, security brings complexity. The simpler the model is, the more popular it would be.
Applicability: It defines the signs of the access control model's practicality. Theoretical models may have some benefits. There should be an infrastructure for the deployment of the model.
User's group: Access control environment suggests a common task commenced by the user's group. Changes, specifications, and manipulations made for the user's group should be represented by the access control models.
Policy Enforcement: it should be ensured that the access control model enforces the policies and constraints correctly.
Flexibility: It is defined as the flexible formation of access control policies, giving supple control over access control operations. In this way, it will provide better interoperability through administrative boundaries
Policy specifications: The basis of access control models are the representation and specification of the policies. The model must have support for appropriate syntax, specifying policies and language for modification and extension transparently and simply. It helps in the scalability of the access control system.
Fine-Grained Control: An access control model should provide fine-grained control over a situation where a user needs some set of permissions on the occurrence of an object at a specific point without the complexities or compromises into the system.
Resistance: It is defined as the security of the system that how to secure the access control model. It is designed to tackle the deliberate attacks or fend off situations, which restrict the users from a large consumption of resources.

In Table 2, the access control models discussed in this survey are being evaluated against the stated criteria. The terminologies used in the table are comparative degrees like high, low, and med (medium), descriptive terminologies like yes (O), and no (X) for criteria characterization. High, low and med (medium) categories describe the degree such as low complexity means the model's nature is simple and high understandability means it is easy to understand. Low in the user's group specifies primitive support for the respective feature. Enablement and lack of enablement have been indicated as Yes or No. Where presence along with degree is concerned high, low and the med (medium) are used.

Table 2. Comparison between AC Models for the Internet of Things.

Criteria	Matrix	MAC	DAC	RBAC	CBAC	ABAC	Lattice	Identity	ReBAC
Ease of use	Med	Med	Med	High	High	High	Low	High	High
Understandability	High	High	High	High	Med	Med	Low	Med	Med
Complexity	Low	High	Med	Med	High	Med	High	Med	Med
Applicability	Med	High	Med	High	Med	High	Low	Med	High
User's Group	O	O	O	O	O	O	O	O	O
Flexibility	X	Low	O	Low	O	High	Low	O	O
Policy enforcement	Low	High	Low	O	O	O	High	Low	O
Policy specification	Low	High	O	O	O	O	High	O	Low
Fine-Grained control	X	High	X	Low	O	High	O	O	High
Resistance	X	High	Low	Low	Low	High	Low	High	Med

Access control models aim to provide security and privacy. Research on access control helps in finding expressive models to investigate evolving trends in context-aware, temporal, attribute-based, and latest computing models/architectures. MAC is one of the oldest access control models and is not without limitations. It over-classifies data through the principle of high-water mark, thus productivity gets hurt by limiting labeled information transformation between systems and confining user control over data [27]. System maintenance and security principle verification are hard for DAC systems. DAC also lacks in constraints of copy privileges. Considering RBAC, some of the aspects have been explored much and some have not achieved community consensus. Authorization for administration was the main omission in NIST standard RBAC [54]. Most studies for RBAC are related to a single organization. Moreover, ARBAC97 [133] addresses RBAC administrative paradigm. Recently, new models are studied concerning the concepts of personalization and delegation, which are not part of the standard NIST model. In workflow management systems, different applications of RBAC have been investigated. RBAC has remained a rich area for future research. Though ABAC is a good supplement to RBAC and provides an instinctive way to express conditions for security administrators. Lattice models are applicable in every environment where information flow is concerned. They are the key ingredient of security-related information systems, though they are not the comprehensive solution for issues related to information flow.

A study related to the general perspective of access control is a major concern for users as well as researchers. There is a need for multi-party access controls for OSN. Relationship-Based Access Control describes user-to-user, user-to-resource, and resource-to-resource relationships but currently, there is a need to manage authorization in OSN for U2U and R2R relationships. Few studies [99,103] provide the mechanism for these relationships, though relationship-based models do not emphasize history-based access models (in which permissions are granted based on user's history). Semantic web technologies are the solution and trend to extract information about difficult relationships. In ReBAC model [104], the focus is on user-to-user relations, although some models have also given user-to-resource and resource-to-resource relationships. However, user-independent object-to-object (or resource-to-resource) relations are being discussed for decades in privacy systems. Object-to-Object ReBAC (OOReBAC) has been introduced in [134] which uses relationships of objects for governing access to objects.

Here, we are considering distinct aspects of access control models that need more research. Some have been already sightseen, some have not achieved much consensus despite being mature. In the future, RBAC applications to Business-to-Consumer and Business-to-Business electronic consumers are being considered [135]. IDM365_product for enforcement and design of rules based on business environment and attributes is the future approach for bridging the gap between ABAC and RBAC.

Proactive Dynamic Secure Data Scheme (P2DS) resolves the issues like customer's information privacy and the financial industry using ABAC and data self-deterministic scheme, designed to prevent unauthorized parties to get to private data [136]. A hybrid of both schemes provides more flexible and adaptable access control. As time goes, ABAC is going to be accepted for businesses as the authorization model. Approval of ABAC would lead to its next evolution i.e., context-based access control to be accepted as well. ABAC is in use in most enterprises in the form of static groups; this makes ABAC a reality.

In social networks, the main problem is with blockage of SNS's potential for accessing networked people and content online. The proposed solution in [137] is to build semantic social networking for performing the operation and linking on the varied person and object-related data gathered from SN sites. Capability-Based Access Control models are the future of IoT (Internet of Things). In [125], Capability-Based Context-Aware Access Control (CCAAC) is proposed for federated machine-to-machine IoT networks. The main idea of this proposed mechanism is the realization of the capability propagation mechanism. This model uses identity-based control and secure federated IoT provides flexibility, scalability, and authority delegation. RBAC and ABAC are not suitable for distributed systems like IoT, as they do not deliver scalable, efficient, and manageable mechanism [18]. As more end-users are added in device usage, then more scalable, manageable, and understandable mechanisms are needed. Most of the discussed techniques and access control models either the general or for OSN are based on and have characteristics debated in this survey.

We need to focus on the security aspects of access control models to protect the sensitive information of users that could be disclosed either by the intruder or some malicious activity. Each model discussed here has its pros and cons and different functionalities, so we must consider all facilities provided. This research aspect is of excessive importance because access controls may have security flaws because of their poor configurations or administrative mistakes. An organization that wants to protect itself from cyber-attacks must define security policies and mainly the enforcement of these policies through access control mechanisms and implementation of these policies should be verified.

6.2. Evaluation of Access Control Models for IoT

The Internet of Things paradigm has different security and privacy-preserving objectives as compared to other networking systems. A comprehensive list of Security and Privacy-Preserving (S&PP) objectives for IoT is presented in [7]. In this work following objectives are selected for analysis of IoT access control proposals available in the literature.

Scalability: IoT is a dynamic paradigm and requires the addition of new resources and users frequently. Therefore, access control solution should be extensible in the size and structure of policies [10].

Usability: IoT is becoming part of everyday life and users with different levels of expertise need to implicate in the authorization of IoT devices. Access control policies should be developed considering the ease of use for end-users in related to management and modifications of policies.

Interoperability: Access control mechanisms defined for IoT must be able to operate seamlessly in heterogeneous domains.

Context awareness: IoT devices continuously produce raw data according to the environmental conditions. This raw data is the contextual information that must be taken into account while developing access control policies.

Lightweight: The IoT devices are constrained in terms of size, computation, and communication power and memory. Lightweight security solutions are ideal for constrained IoT environments to reduce computational overhead on the device.

User-driven: Personal and home applications of IoT require direct involvement of users in the authorization process and the user is the master of their data. Therefore, access control mechanisms must be user-driven.

Granularity: The grammar in which access control policies are written should be more verbose and must contain context information to ensure fine-grained access control.

Delegation: The dynamic nature of IoT requires the addition of users and resources frequently. The access control policy must be flexible enough so that subjects can delegate access decisions to new subjects. The evaluation of access control models according to S&PP objectives are presented in Table 3.

Table 3. Evaluation of IoT-based access control models according to S&PP (High = H, Medium = M and Low = L).

Model	Ref.	Scalability	Usability	Interope-Rability	Context Awareness	Light Weight	User-Driven	Granul-Arity	Delegation
RBAC	107	L	H	L	H	M	M	M	L
	109	M	M	H	M	L	M	M	L
	110	M	H	H	L	L	H	M	No
	111	M	M	H	L	L	M	M	No
ABAC	115	L	H	L	H	M	M	H	H
	116	M	L	M	H	L	M	M	No
UCON	117	L	M	L	H	No	M	H	No
CAPBAC	121	H	M	L	H	L	M	M	H
	58	H	M	L	L	L	M	L	M
	120	H	M	L	L	H	M	L	H
	124	H	M	L	L	H	M	M	H
	127	H	H	H	M	M	L	H	L

The comprehensive literature survey on RBAC models for access control in IoT has revealed that the RBAC model is less suitable for the distributive and heterogeneous environment of IoT due to its static nature. The definition of "roles" in different platforms, applications and enterprise is a real issue. Subjects in RBAC model do not have the right to grant access to other subjects, i.e., delegation is not supported in RBAC. Due to the huge number of IoT users and dynamicity, the RBAC models cannot assign permissions to roles in advance. IoT applications require self-configuring access control policies to emulate dynamicity. Although using RBAC models, scalability is not supported as it requires a redefinition of roles. The RBAC does not support interoperability when roles are to be shared among different platforms, domains, and enterprises. The ABAC appears to be more suitable collaborative and distributive systems like IoT, since access decisions are made on the basic attributes of the requestor, and attributes are the basic elements in ABAC model [138].

ABAC supports interoperability and is fine-grained access as it makes use of subject and object attributes for making access decisions. ABAC is usually written in XACML which requires semantic interpretation and expressing attribute-based authorization. XACML is itself complex which increases the complexity of ABAC models. For some applications, like medical and wearable IoT, this complexity is acceptable where medication in policies is not easy. However, in applications like smart home, this complexity is not acceptable as it forces naïve users to learn XACML for making trivial modifications. The ABAC for smart home [116] is user-driven and highly supports delegation.

UCON-based access control is found to be suitable for the dynamic environment of IoT. It supports mutability, flexibility, scalability, fine-grained access, and uses context-aware information for access decisions. However, UCON models for IoT proposed in the literature are complex and not lightweight. Moreover, they are not user-driven and do not support delegation. Capability-based access control models for IoT have fulfilled most of the S&PP objectives and are found most suitable for IoT applications. These models are easy to use, user-driven, flexible, support revocation and delegation, and have high usability.

7. Conclusions

In this paper, a broad survey of conventional, OSN and IoT-based access control models is presented from their functionality point of view. It covers most of the material regarding access control including its requirements, and major security issues. The comparison of access control models highlights the different capabilities available in these models. Each model has different functionalities and can be used according to the requirements of an environment. Regarding conventional access control models, there is a need to focus on attribute-based access control due to the heterogeneity of nodes. Regarding IoT, existing access control models for internet security are web-based and are not compatible with the constrained environment of IoT. There are two approaches found in the literature to define security protocols for IoT. The first one suggests adapting the existing security mechanisms and re-profiling them in the context of IoT. The second approach suggests rethinking and rebooting new security protocols for IoT. No approach is better than the other; it just depends on the requirements of IoT application for which security protocols need to be defined. Due to the variety of environments and applications, it is not possible to have a general model that fulfils all requirements. Every model has its advantages and disadvantages that are discussed in the survey. A model should be selected according to the requirements of the context and application.

Author Contributions: Conceptualization, A.K.M. and H.A.K.; Methodology, A.K.M. and B.R.; Software, H.A.K. and S.K.; Validation, A.K.M., N.E. and S.Z.; Formal Analysis, B.R.; Investigation, A.K.M., N.E., and S.Z.; Resources, M.O.A., A.S.A., and M.A.A.; Data Curation, A.K.M. and A.H.A.-B.; Writing—Original Draft Preparation, A.K.M., N.E., S.Z. and H.A.K.; Writing—Review & Editing, A.K.M., B.R., N.E., B.R. and S.Z.; Visualization, A.K.M., H.A.K. and S.K.; Supervision, A.H.A.-B., M.O.A.; Project Administration, M.O.A., A.S.A. and M.A.A.; Funding Acquisition, A.H.A.-B., M.O.A., A.S.A. and M.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia under Grant No. (KEP-19-611-38).

Acknowledgments: The authors acknowledge with thanks Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia for technical and financial support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bokefode, J.D.; Ubale, S.A.; Apte, S.S.; Modani, D.G. Analysis of DAC MAC RBAC Access Control based Models for Security. *Int. J. Comput. Appl.* **2014**, *104*, 6–13.
2. Aho, A.; Hoperoft, J.; Ullman, J. *The Design and Analysis of Computer Algorithms*; Addison-Wesley: Boston, MA, USA, 1974.
3. Damianou, N.; Bandara, A.; Sloman, M.; Lupu, E. *A Survey of Policy Specification Approaches*; Department of Computing, Imperial College of Science Technology and Medicine: London, UK, 2002; Volume 3, pp. 142–156.
4. Emmanuel, N.; Anjum, A.; Shafiq, S.; Adam, M. Current State of Art in Security of Data Aggregator in Smart Grids. *Preprints* **2016**, 2016070077. [CrossRef]
5. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
6. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. *Futur. Gener. Comput. Syst.* **2019**, *100*, 144–164. [CrossRef]
7. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in The Internet of Things: Big challenges and new opportunities. *Comput. Netw.* **2017**, *112*, 237–262. [CrossRef]
8. Bertin, E.; Hussein, D.; Sengul, C.; Frey, V. Access control in the Internet of Things: A survey of existing approaches and open research questions. *Ann. Telecommun.* **2019**, *74*, 375–388. [CrossRef]
9. Zhang, Y.; Wu, X. Access control in internet of things: A survey. *arXiv* **2016**, arXiv:1610.01065.
10. Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. *J. Netw. Comput. Appl.* **2019**, *144*, 79–101. [CrossRef]
11. Tolone, W.; Ahn, G.-J.; Pai, T.; Hong, S.-P. Access control in collaborative systems. *ACM Comput. Surv.* **2005**, *37*, 29–41. [CrossRef]

12. Kirrane, S.; Mileo, A.; Decker, S. Access control and the resource description framework: A survey. *Semantic Web* **2017**, *8*, 311–352. [CrossRef]
13. Peón, P.G.; Uhlemann, E.; Steiner, W.; Björkman, M. Medium access control for wireless networks with diverse time and safety real-time requirements. In Proceedings of the IECON 2016—42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 23–26 October 2016.
14. Ventura, D.; Gómez-Goiri, A.; Catania, V.; López-De-Ipiña, D.; Naranjo, J.; Casado, L.G. Security analysis and resource requirements of group-oriented user access control for hardware-constrained wireless network services. *Log. J. IGPL* **2015**, *24*, 80–91. [CrossRef]
15. Alhaqbani, B.; Fidge, C. Access control requirements for processing electronic health records. In *International Conference on Business Process Management*; Springer: Berlin/Heidelberg, Germany, 2007.
16. Gates, C. *Access Control Requirements for Web 2.0 Security and Privacy*; IEEE Web 2.0; CA Labs: Islandia, NY, USA, 2007.
17. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11. [CrossRef]
18. Gusmeroli, S.; Piccione, S.; Rotondi, D. A capability-based security approach to manage access control in the internet of things. *Math. Comput. Model.* **2013**, *58*, 1189–1205. [CrossRef]
19. Choi, C.; Choi, J.; Kim, P. Ontology-based access control model for security policy reasoning in cloud computing. *J. Supercomput.* **2014**, *67*, 711–722. [CrossRef]
20. Singhal, M.; Chandrasekhar, S.; Ge, T.; Sandhu, R.; Krishnan, R.; Ahn, Ga.; Bertino, E. Collaboration in multi-cloud computing environments: Framework and security issues. *Computer* **2013**, *46*, 76–84.
21. Malik, A.K. (Ed.) *Innovative Solutions for Access Control Management*; IGI Global: Hershey, PA, USA, 2016.
22. Small, A.; Wainwright, D. Privacy and Security of Electronic Patient Records–Tailoring Multimethodology to Explore the Socio-Political Problems Associated with Role Based Access Control Systems. *Eur. J. Oper Res.* **2017**, *265*, 344–360. [CrossRef]
23. Rexer, P.; Patil, A. Security Enhancement through Application Access Control. U.S. Patent No. 9,691,051, 27 June 2017.
24. Majumder, A.; Namasudra, S.; Nath, S. Taxonomy and classification of access control models for cloud environments. In *Continued Rise of the Cloud*; Springer: London, UK, 2014; pp. 23–53.
25. Singh, A.; Chatterjee, K. Cloud security issues and challenges: A survey. *J. Netw. Comput. Appl.* **2017**, *79*, 88–115. [CrossRef]
26. Androutsellis-Theotokis, S.; Spinellis, D. A survey of peer-to-peer content distribution technologies. *ACM Comput. Surv.* **2004**, *36*, 335–371. [CrossRef]
27. Ryan, A. *Methods for Access Control: Advances and Limitations*; Harvey Mudd College: Claremont, CA, USA, 2013; Volume 301, p. 20. Available online: https://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/ryan.pdf (accessed on 12 October 2020.)
28. Sandhu, R.S.; Samarati, P. Access control: Principle and practice. *IEEE Commun. Mag.* **1994**, *32*, 40–48. [CrossRef]
29. Barkley, J. Comparing simple role-based access control models and access control lists. In Proceedings of the Second ACM Workshop on Role-Based Access Control, Fairfax, VA, USA, 6–7 November 1997.
30. Tang, P.; Diep, T.; Hlasnik, W. Access Control Management System Utilizing Network and Application Layer Access Control Lists. U.S. Patent No. 7,054,944, 30 May 2006.
31. Maw, H.A.; Xiao, H.; Christianson, B.; Malcolm, J. A survey of access control models in wireless sensor networks. *J. Sens. Actuator Netw.* **2014**, *3*, 150–180. [CrossRef]
32. Adams, R.; Puthenkulam, J.P. Control of Access Control Lists Based on Social Networks. U.S. Patent No. 7,467,212, 16 December 2008.
33. Shalabi, S.M.; Doll, C.L.; Reilly, J.D.; Shore, M.B. Access Control List. U.S. Patent Application No. 13/311,278, 6 June 2013.
34. Nelson, K.C.; Noronha, M.A. Facilitating Ownership of Access Control Lists by Users or Groups. U.S. Patent No. 9,697,373, 4 July 2017.
35. Daly, J.; Liu, A.X.; Torng, E. A difference resolution approach to compressing access control lists. *IEEE/ACM Trans. Netw.* **2016**, *24*, 610–623. [CrossRef]
36. Cankaya, H.C. Access control lists. In *Encyclopedia of Cryptography and Security*; Springer: NewYork, NY, USA, 2011; pp. 9–12.

37. Abadi, M.; Goldstein, A.C.; Lampson, B.W. Compound Principals in Access Control Lists. U.S. Patent No. 5,315,657, 24 May 1994.
38. Gai, S.; McCloghrie, K.; Kanekar, B.M. Method and Apparatus for Organizing, Storing and Evaluating Access Control Lists. U.S. Patent No. 6,651,096, 18 November 2003.
39. Bacis, E.; Mutti, S.; Rosa, M.; Paraboschi, S. Improving Android security by widening the role of Mandatory Access Control. *TinyToCS* **2016**, *4*, 1.
40. Na, J.s.; Kim, D.-Y.; Pak, W.; Choi, Y.-J. Mandatory Access Control for Android Application Security. *J. KIISE* **2016**, *43*, 275–288. [CrossRef]
41. Mell, P.; Shook, J.; Harang, R.; Gavrila, S. Linear Time Algorithms to Restrict Insider Access using Multi-Policy Access Control Systems. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2017**, *8*, 4–25. [PubMed]
42. Shu, Z.; Ji, X.; Lin, Y. A hybrid security model for virtual machines in cloud environment. *Int. J. Auton. Adapt. Commun. Syst.* **2017**, *10*, 236–246. [CrossRef]
43. Brocardo, M.L.; Rolt, C.R.D.; Dias, J.D.S.; Custodio, R.F.; Traore I. Privacy information in a positive credit system. *Int. J. Grid Utility Comput.* **2017**, *8*, 61–69. [CrossRef]
44. Liu, G.; Song, H.; Wang, C.; Zhang, R.; Wang, Q.; Ji, S. BTG-BIBA: A Flexibility-Enhanced Biba Model Using BTG Strategies for Operating System. *World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng.* **2017**, *11*, 706–712.
45. Brewer, D.F.C.; Nash, M.J. The Chinese wall security policy. In Proceedings of the 1989 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1–3 May 1989.
46. Basu, S.; Sengupta, A.; Mazumdar, C. Modelling operations and security of cloud systems using Z-notation and Chinese Wall security policy. *Enterp. Inf. Syst.* **2016**, *10*, 1024–1046. [CrossRef]
47. Sandhu, R.S. A lattice interpretation of the Chinese Wall policy. In Proceedings of the 15th NIST-NCSC National Computer Security Conference, Baltimore, MA, USA, 13–16 October 1992.
48. Fehis, S.; Nouali, O.; Kechadi, M.-T. A New Distributed Chinese Wall Security Policy Model. *J. Digit. Forensics, Secur. Law* **2016**, *11*, 11. [CrossRef]
49. Moffett, J.D. Specification of management policies and discretionary access control. *Net. Distrib. Syst. Manag.* **1994**, 455–480.
50. Savage, C.; Petro, C.; Goldsmith, S. System for Providing Session-Based Network Privacy, Private, Persistent Storage, and Discretionary Access Control for Sharing Private Data. U.S. Patent No. 9,619,632, 11 April 2017.
51. Tirosh, O.; Werner, E. Method and System for Implementing Mandatory File Access Control in Native Discretionary Access Control Environments. U.S. Patent No. 9,350,760, 24 May 2016.
52. Han, D.-J.; Gong, L.; Qin, F. A Dynamic Access Control Policy Based on Hierarchical Description. In Proceedings of the 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chengdu, China, 13–15 October 2016.
53. Thion, R. *Access Control Models. Cyber Warfare and Cyber Terrorism*; IGI Global: Hershey, PA, USA, 2008; pp. 318–326.
54. Ferraiolo, D.F.; Sandhu, R.; Gavrila, S.; Kuhn, D.R.; Chandramouli, R. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.* **2001**, *4*, 224–274. [CrossRef]
55. Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E. Role-based access control models. *IEEE Comput.* **1996**, *29*, 38–47. [CrossRef]
56. Nakamura, S.; Duolikun, D.; Enokido, T.; Takizawa, M. A read-write abortion protocol to prevent illegal information flow in role-based access control systems. *Int. J. Space-Based Situated Comput.* **2016**, *6*, 43–53. [CrossRef]
57. Ferraiolo, D.; Cugini, J.; Kuhn, D.R. Role-based access control (RBAC): Features and motivations. In Proceedings of the 11th Annual Computer Security Application Conference, New Orleans, LA, USA, 13–15 December 1995.
58. Mishra, A.; Ghodke, A.; Mohanty, S.; Bagul, Y. Access Control and Recovery Model in Cloud. *Imperial J. Interdiscip. Res.* **2017**, *3*, 678–681.
59. Liu, Q.; Zhang, H.; Wan, J.; Chen, X. An Access Control Model for Resource Sharing based on the Role-Based Access Control Intended for Multi-domain Manufacturing Internet of Things. *IEEE Access* **2017**, *5*, 7001–7011. [CrossRef]

60. PV, R.; Sandhu, R.POSTER: Security Enhanced Administrative Role Based Access Control Models. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016.
61. Ferraiolo, D.; Kuhn, D.R.; Chandramouli, R. *Role-Based Access Control*; Artech House: Norwood, MA, USA, 2003.
62. Ghazal, R.; Malik, A.K.; Qadeer, N.; Raza, B.; Shahid, A.R.; Alquhayz, H. Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments. *IEEE Access* **2020**, *8*, 12253–12267. [CrossRef]
63. Kulkarni, D.; Tripathi, A. Context-aware role-based access control in pervasive computing systems. In Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, Estes Park, CO, USA, 11–13 June 2008.
64. Corrad, A.; Montanari, R.; Tibaldi, D. Context-based access control management in ubiquitous environments. In Proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA 2004), Cambridge, MA, USA, 1 September 2004.
65. Feng, F.; Lin, C.; Peng, D.; Li, J. A trust and context-based access control model for distributed systems. In Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, 25–27 September 2008.
66. Jih, W.-R.; Cheng, S.-Y.; Hsu, J.Y.-J.; Tsai, T.-M. Context-Aware Access Control in Pervasive Healthcare. 2005. Available online: https://scholars.lib.ntu.edu.tw/bitstream/123456789/115216/1/mam05.pdf (accessed on 12 October 2020).
67. Hulsebosch, R.J.; Salden, A.H.; Bargh, M.S.; Ebben, P.W.; Reitsma, J. Context sensitive access control. In Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies ACM, Stockholm, Sweden, 1–3 June 2005.
68. Garcia-Morchon, O.; Wehrle, K. Modular context-aware access control for medical sensor networks. In Proceedings of the 15th ACM Symposium on Access Control Models and Technologies (SACMAT '10), Pittsburgh, PA, USA, 9–11 June 2010; pp. 129–138.
69. Morchon, O.G.; Wehrle, K. Efficient and context-aware access control for pervasive medical sensor networks. In Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and CommunicationsWorkshops (PERCOMWorkshops), Mannheim, Germany, 29 March–2 April 2010.
70. Yuan, E.; Tong, J. Attributed based access control (ABAC) for web services. In Proceedings of the IEEE International Conference on Web Services (ICWS'05), Orlando, FL, USA, 11–15 July 2005.
71. Hu, V.C.; Kuhn, D.R.; Ferraiolo, D.F. Attribute-Based Access Control. *IEEE Comput.* **2015**, *48*, 85–88. [CrossRef]
72. Servos, D.; Osborn, S.L. Current Research and Open Problems in Attribute-Based Access Control. *ACM Comput. Surv.* **2017**, *49*, 65. [CrossRef]
73. Sandhu, R. Attribute-Based Access Control Models and Beyond. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security - ASIA CCS Association for Computing Machinery (ACM), Singapore, 10 April 2015.
74. Crampton, J.; Williams, C. Attribute Expressions, Policy Tables and Attribute-Based Access Control. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 21–23 June 2017.
75. Abo-Alian, A.; Badr, N.L.; Tolba, M.F. Hierarchical attribute-role based access control for cloud computing. In Proceedings of the 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), Beni Suef, Egypt, 28–30 November 2015.
76. Liu, J.K.; Au, M.H.; Huang, X.; Lu, R.; Li, J. Fine-grained two-factor access control for web-based cloud computing services. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 484–497. [CrossRef]
77. Tu, S.-s.; Niu, S.-z.; Li, H. A fine-grained access control and revocation scheme on clouds. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 1697–1714. [CrossRef]
78. Lim, L.; Marie, P.; Conan, D.; Chabridon, S.; Desprats, T.; Manzoor, A. Enhancing context data distribution for the internet of things using qoc-awareness and attribute-based access control. *Ann. Telecommun.* **2015**, *71*, 121–132. [CrossRef]

79. Jin, X.; Krishnan, R.; Sandhu, R. A unified attribute-based access control model covering DAC, MAC, and RBAC. In *IFIP Annual Conference on Data and Applications Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2012.
80. Sandhu, R.S. Lattice-based access control models. *Computer* **1993**, *26*, 9–19. [CrossRef]
81. Sandhu, R. Role hierarchies and constraints for lattice-based access control. In *European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 1996.
82. Saxena, N.; Tsudik, G.; Yi, J.H. Identity-based access control for ad hoc groups. In *International Conference on Information Security and Cryptology*; Springer: Berlin/Heidelberg, Germany, 2004.
83. Kunzinger, C.A. Integrated System for Network Layer Security and Fine-Grained Identity-Based Access Control. U.S. Patent No. 6,986,061, 10 January 2006.
84. Gong, L. A secure identity-based capability system. In Proceedings of the 1989 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1–3 May 1989.
85. Shamir, A. Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1984.
86. Al-Mahmud, A.; Morogan, M.C. Identity-based authentication and access control in wireless sensor network. *Int. J. Comput. Appl.* **2012**, *41*, 18–24. [CrossRef]
87. Thomas, R.K. Team-based access control (TMAC) a primitive for applying role-based access controls in collaborative environments. In Proceedings of the Second ACM Workshop on Role-Based Access Control, Fairfax, VA, USA, 6–7 November 1997; pp. 13–19.
88. Malik, A.K.; Truong, H.L.; Dustdar, S. DySCon: Dynamic sharing control for distributed team collaboration in networked enterprises. In Proceedings of the 2009 IEEE Conference on Commerce and Enterprise Computing, Vienna, Austria, 20–23 July 2009; pp. 279–284.
89. Oh, S.; Park, S. Task–role-based access control model. *Inf. Syst.* **2003**, *28*, 533–562. [CrossRef]
90. Malik, A.K.; Dustdar, S. Enhanced sharing and privacy in distributed information sharing environments. In Proceedings of the 2011 7th International Conference on Information Assurance and Security (IAS), Melaka, Malaysia, 5–8 December 2011; pp. 286–291.
91. Ali, A.; Malik, A.K.; Ahmed, M.; Raza, B.; Ilyas, M. Privacy Concerns in Online Social Networks: A Users' Perspective. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 10. [CrossRef]
92. Asim, Y.; Malik, A.K. A survey on access control techniques for social networks. In *Innovative Solutions for Access Control Management*; IGI Global: Hershey, PA, USA, 2020; pp. 1–32.
93. Gollu, K.K.; Saroiu, S.; Wolman, A. A Social Networking-Based Access Control Scheme for Personal Content. In Proceedings of the 21st ACM Symposium on Operating Systems Principles, Skamania Lodge Stevenson, WA, USA, 14–17 October 2017.
94. Tootoonchian, A.; Ganjali, Y.; Saroiu, S.; Wolman, A. Lockr: Better privacy for social networks. In Proceedings of the 5th ACM International Conference on emerging Networking Experiments and Technologies, Rome, Italy, 1–4 December 2009; pp. 169–180.
95. Tootoonchian, A.; Gollu, K.K.; Saroiu, S.; Ganjali, Y.; Wolman, A. Lockr: Social access Control for web 2.0. In Proceedings of the WOSN'08, Seattle, WA, USA, 17–22 August 2008; pp. 43–48.
96. Rizvi, S.Z.R.; Fong, P.W.L. Interoperability of relationship-and role-based access control. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, 9–11 March 2016.
97. Cheng, Y.; Park, J.; Sandhu, R. A User-to-User Relationship-based Access Control Model for Online Social Networks. *Data Appl. Secur. Privacy* **2012**, *26*, 8–24.
98. Bui, T.; Stoller, S.D.; Li, J. Mining Relationship-Based Access Control Policies. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 21–23 June 2017.
99. Cheng, Y.; Park, J.; Sandhu, R. Relationship-based Access Control for Online Social Networks: Beyond User-to-User Relationships. In Proceedings of the InInternational Conference on Social Computing, Privacy, Security, Risk, and Trust, Amsterdam, The Netherlands, 3–5 September 2012; pp. 646–655. [CrossRef]
100. Ahmed, T.; Sandhu, R.; Park, J. Classifying and Comparing Attribute-Based and Relationship-Based Access Control. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, Scottsdale, AZ, USA, 22–24 March 2017.
101. Du, Z.; Liu, Y.; Wang, Y. Relation Based Access Control in Campus Social Network System. *Procedia Comput. Sci.* **2013**, *17*, 14–20. [CrossRef]

102. Bennett, P.; Ray, I.; France, R. Analysis of a relationship based access control model. In Proceedings of the Eighth International C* Conference on Computer Science & Software Engineering, Yokohama, Japan, 13–15 July 2015.
103. Pang, J.; Zhang, Y. A new access controls scheme for Facebook-style social networks. In Proceedings of the Availability, Reliability and Security, Fribourg, Switzerland, 8–12 September 2014; pp. 1–10.
104. Cheng, Y.; Bijon, K.; Sandhu, R. Extended ReBAC Administrative Models with Cascading Revocation and Provenance Support. In Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies, Shanghai, China, 5–8 June 2016.
105. Kumar, A.; Rathore, N.C. *Relationship Strength Based Access Control in Online Social Networks*; Springer International Publishing: Berlin, Germany, 2016.
106. Asim, Y.; Malik, A.K.; Raza, B.; Naeem, W.; Rathore, S. Community-centric brokerage-aware access control for online social networks. *Futur. Gen. Comput. Syst.* **2018**, *109*, 469–478. [CrossRef]
107. Manzoor, A.; Shah, M.A.; Khattak, H.A.; Din, I.U.; Khan, M.K.; Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. *Int. J. Commun. Syst.* **2019**, e4033. [CrossRef]
108. Gabillon, A.; Gallier, R.; Bruno, E. Access Controls for IoT Networks. *SN Comput. Sci.* **2020**, *1*, 24. [CrossRef]
109. Gouglidis, A.; Mavridis, I. domRBAC: An Access Control Model for Modern Collaborative Systems. *Comput. Secur.* **2012**, *31*, 540–556. [CrossRef]
110. Yavari, A.; Panah, A.S.; Georgakopoulos, D. Scalable Role-based Data Disclosure Control for the Internet of Things. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017.
111. Yavari, A.; Jayaraman, P.P.; Georgakopoulos, D.; Nepal, S. ConTaaS: An Approach to Internet-Scale Contextualisation for Developing Efficient Internet of Things Applications. In Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS), Hilton Waikoloa Village, HI, USA, 4–7 January 2017; pp. 5932–5940.
112. Zhang, G.; Tian, J. An extended role based access control model for the Internet of Things. In Proceedings of the 2010 International Conference on Information, Networking and Automation (ICINA), Kunming, China, 17–19 October 2010; p. V1-319.
113. Jindou, J.; Xiaofeng, Q.; Cheng, C. Access Control Method for Web of Things Based on Role and SNS. In Proceedings of the 2012 IEEE 12th International Conference on Computer and Information Technology, Chengdu, China, 20–22 October 2012; pp. 316–321.
114. Barka, E.; Mathew, S.S.; Atif, Y. Securing the Web of Things with Role-Based Access Control. In Proceedings of the International Conference on Codes, Cryptology, and Information Security, Rabat, Morocco, 18–19 July 2015; pp. 14–26.
115. Soni, A.; Keoh, S.L.; Kumar, S.S.; Garcia-Morchon, O. HADA: Hybrid Access Decision Architecture for Building Automation and Control Systems. In Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research 2013, Leicester, UK, 16–17 September 2013; pp. 1–11.
116. Liu, J.; Xiao, Y.; Chen, C.L.P. Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing SystemsWorkshops; Institute of Electrical and Electronics Engineers (IEEE), Macau, China, 18–21 June 2012; pp. 588–592.
117. Sakimura, N.; Bradley, J.; Jones, M.; Jay, E. *OpenID Connect Discovery 1.0 Incorporating Errata set 1*; OpenID Foundation: San Ramon, CA, USA, 2014. Available online: https://openid.net/specs/openid-connect-discovery-1_0.html (accessed on 14 October 2020).
118. Kayes, A.S.M.; Rahayu, W.; Dillon, T. Critical situation management utilizing IoT-based data resources through dynamic contextual role modeling and activation. *Computing* **2019**, *101*, 743–772. [CrossRef]
119. Oh, S.R.; Kim, Y.G.; Cho, S. An Interoperable Access Control Framework for Diverse IoT Platforms Based on OAuth and Role. *Sensors* **2019**, *19*, 1884. [CrossRef] [PubMed]
120. Bezawada, B.; Haefner, K.; Ray, I. Securing Home IoT Environments with Attribute-Based Access Control. In Proceedings of the Third ACM Workshop on Mobile Cloud Computing and Services—MCS Tempe, AZ, USA, 21 March 2018; pp. 43–53.
121. Ye, N.; Zhu, Y.; Wang, R.-C.; Malekian, R.; Qiao-Min, L. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. *Appl. Math. Inf. Sci.* **2014**, *8*, 1617–1624. [CrossRef]
122. Guoping, Z.; Wentao, G. The research of access control based on UCON in the internet of things. *J. Softw.* **2011**, *6*, 724–731.

123. Quyet, H.C.; Giyyarpuram, M.; Reza, F.; Noel, C. Usage control for data handling in smart cities. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2016; pp. 1–6.
124. Mahalle, P.; Anggorojati, B.; Prasad, N.R.; Rangistty, N.D. Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *J. Cyber Secur. Mobil.* **2013**, *1*, 309–348.
125. Anggorojati, B.; Mahalle, P.N.; Prasad, N.R.; Prasad, R. Capability-based access control delegation model on the federated IoT network. In Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, 24–27 September 2012; pp. 604–608.
126. Green, J. The Internet of Things Reference Model. In Proceedings of the Internet of Things World Forum 2014, Chicago, IL, USA, 14–16 October 2014; pp. 1–12.
127. Hernández-Ramos, J.L.; Jara, A.J.; Marín, L.; Gómez, A.F.S DCapBAC: Embedding authorization logic into smart things through ECC optimizations. *Int. J. Comput. Math.* **2016**, *93*, 345–366. [CrossRef]
128. Hernández-Ramos, J.; Jara, A. Distributed Capability-based Access Control for the Internet of Things. *J. Internet Serv. Inf. Secur.* **2013**, *3*, 1–16.
129. Bernabe, J.B.; Ramos, J.L.H.; Gomez, A.F.S. TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Comput.* **2016**, *20*, 1763–1779. [CrossRef]
130. Anggorojati, B.; Prasad, N.R.; Prasad, R. Capability-Based Access Control with ECC Key Management for the M2M Local Cloud Platform. *Wirel. Pers. Commun.* **2018**, *100*, 519–538. [CrossRef]
131. Ouaddah, A.; Bouij-Pasquier, I.; Elkalam, A.A.; Ouahman, A.A. Security analysis and proposal of new access control model in the Internet of Thing. In Proceedings of the 2015 International Conference on Electrical and Information Technologies (ICEIT), Marrakech, Morocco, 25–27 March 2015; pp. 30–35.
132. Bouij-Pasquier, I.; El, A.A.K.; Ouahman, A.A.; Montfort, M.D. A Security Framework for Internet of Things. In Proceedings of the International Conference on Cryptology and Network Security, Marrakesh, Morocco, 10–12 December 2015; Volume 1, pp. 19–31.
133. Sandhu, R.; Bhamidipati, V.; Munawer, Q. The ARBAC97 Model for Role-Based Administration of Roles. *ACM Trans. Inf. Syst. Secur.* **1999**, *2*, 105–135. [CrossRef]
134. Ahmed, T.; Patwa, F.; Sandhu, R. Object-to-Object Relationship-Based Access Control: Model and Multi-Cloud Demonstration. In Proceedings of the 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), Pittsburgh, PA, USA, 28–30 July 2016.
135. Sandhu, R. Future directions in role-based access control models. In *International Workshop on Mathematical Methods, Models, and Architectures for Network Security*; Springer: Berlin/Heidelberg, Germany, 2001.
136. Qiu, M.; Gai, K.; Thuraisingham, B.; Tao, L.; Zhao, H. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in the financial industry. *Futur. Gen. Comput. Syst.* **2016**, *80*, 421–429. [CrossRef]
137. Breslin, J.; Decker, S. The future of social networks on the internet: The need for semantics. *IEEE Internet Comput.* **2007**, *11*, 86–90. [CrossRef]
138. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.