



Minor Research Project: Best Practices and Technique in Access Control System Adopted by Private Security Organization:

Submitted By
Vrunda Joshi

Guided by
Mr. Sagar Kumar Ghodasara
Assistant Professor (SISSP)

Submitted to
Rashtriya Raksha University, Lavad – Gandhinagar
(An Institution of National Importance)

1.Introduction:

In today's digital age, “databases are the lifeblood of organizations.” as important stores of extremely private data like financial documents, Personal data, intellectual property, and other data. Consequently, this has made protecting these vital resources a priority. The problem of protection is one of the top priorities, especially for private security providers to protect both persons and property. Physical and electronic resources. Identity and Access Management (IAM) is an important part of This is meant to cover the policies, processes and technologies developed to ensure that, Specific resources are limited to access by only authorized persons; the Information systems confidentiality, integrity and availability.

An Access Control System is a security measure that controls access to certain. Any type of resource that can be physically or virtually accessed in an organization. It guarantees that only authorized clubs are allowed to use it. Users can be granted access according to predefined policies. In private security organisations, This access control is utilized to safeguard information systems, restricted areas, as well as buildings. and other key assets. Access Control is a type of security measure that limits the visibility, Access and use of resources in a computing environment. This assures that access to Only authorized users are allowed to access information and systems, as part of cyber security. This Makes access control a key element in the protection of sensitive data, as well as critical systems. is protected against unauthorized access to ensure that it doesn't become the victim of a data breach and face the consequences. Loss of its

integrity or credibility. AI-powered protection on Singularity's platform. To ensure access is well managed and enforced.

A basic structure that underlies access control systems is the Authentication, Authorization, and Accountability (AAA) model. Authentication is the process of identifying the identity of the users who are accessing the system. With a password, biometrics or tokens etc. Gives access to membership according to roles and responsibilities Accountability, This will allow user activity to be monitored and tracked through auditing and monitoring to ensure this is achieved. Recorded, which will help organizations identify and counteract suspicious activity. Together, These are the elements of a structured method of accessing sensitive information: systems.

Access control is used to manage by private security organizations in several different ways. permissions effectively. The traditional methods like Discretionary Access Control (DAC) are the methods that we are familiar with. There is a mandatory access control (MAC) and role based access control (RBAC). widely adopted due to their structured and scalable nature. Nevertheless, as the clouds have risen, More dynamic models like computing, mobile technologies, and the Internet of Things (IoT), There are two types of these: Attribute Based Access Control (ABAC) and Relationship Based Access Control (RBAC). 5 (ReBAC) have emerged. These modern techniques allows context-aware and real-time access: They are ideal for complex and distributed security environments due to their ability to make decisions. Although all these progressions have been made, the access control systems still have tremendous difficulties, mainly. Despite the challenges of insider threats and what are increasingly becoming cyber risks, they are still conquering them. When the unauthorized access is due to mis-use. There is a significant concern for of legitimate credentials, particularly in places where users are involved in. Already have system privileges. Furthermore, the recent rise in BYOD usage means that many teachers are now having to implement this new technology and adapt to its implications. A new vulnerability has been added to the policies (BYOD), since most devices don't have the same security as you expect. standardized security controls. These are all reasons why perimeter based security strategies are weak. To tackle these challenges, the following best practices have been adopted: Least Privilege (PoLP) and Zero Trust Architecture (ZTA) have become more popular. The Principle of Least Privilege: Users are given just enough access to do the job. Had to carry out their jobs, which will minimise the risk of improper use. Zero Trust Architecture Further enhances security with ongoing user and device verification, Whether they are in or out of the network. Moreover, organizations must comply with regulatory standards to ensure data protection and privacy

The future of the business will witness new technology, including blockchain, artificial intelligence, and others, that will continue to shape the industry. machine learning are transforming access control systems. These technologies enable Decentralized management, real-time behavioural analysis, proactively detecting threats, Playing a part in the development of more resilient and adaptive security frameworks. As security threats continue For achieving strong, to evolve, such innovations are turning into essential for maintaining robust. access control mechanisms.

Access control is an important part of information technology (IT) and cyber security. It is a way of controlling who or what can see, use, or access a certain resource computing environment. That the security risks are minimized, and that only those who should be able to access the computer system are allowed. Authorized users, systems or services have access to resources they need.

Access control is more than just the granting and denying of access. It involves identifying an the individual or system verifying identity, authorizing access and/or privilege to the resource, and monitoring their usage habits. This process will help in reducing the risk of unauthorised access, protecting sensitive information and systems. This is in line with approaches like Next, NIST SP 800-53 specifies controls for authentication, authorization, and access management. Then, NIST SP 800-53 outlines controls to manage authentication, authorization and access management. The access auditing of complex IT systems.

Modern IT infrastructure and work patterns are creating new access control challenges. Trends like the use of cloud computing, the growing use of mobile devices in the workplace, and the transition to remote work, mean that the number of access points to an organization is growing exponentially. New technologies

like identity and access management (IAM) and approaches like zero trust are helping manage this complexity and prevent unauthorized access.

Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. A given information technology (IT) infrastructure can implement access control systems in many places and at different levels. Operating systems use access control to protect files and directories. Database management systems DBMS apply access control to regulate access to tables and views. Most commercially available application systems implement access control, often independent of the operating systems and/or DBMSs on which they are installed.

The objectives of an access control system are often described in terms of protecting system resources against inappropriate or undesired user access. From a business perspective, this objective could just as well be described in terms of the optimal sharing of information. After all, the main objective of IT is to make information available to users and applications. A greater degree of sharing may get in the way of resource protection; in reality, a well-managed and effective access control system actually facilitates sharing. A sufficiently fine-grained access control mechanism can enable selective sharing of information where in its absence, sharing may be considered too risky altogether [FKC03]. The access-matrix model directly manipulates access rights in that granting or revoking access to a resource explicitly refers to a particular permission. This approach yields a fine-grain level of control where each access type and its required permissions are related by a mapping that can be one-to-one at the finest level. For example, the read J permission clearly means one can view the information contained in a resource but not modify it or add to it. To allow for updates, a new access right such as write or append is needed. Although this approach offers the advantage of fine-tuning an access control policy to accommodate any level of access needed, it can be costly to manage. The inherent cost factor becomes apparent with the increase in the number of managed users and resources. Furthermore, the effects from resources removed or added to the system as well as users leaving and joining an organization or simply changing job functions adds up to the complexity and overhead of maintaining such policy. For example, assigning an employee to a new function may require revoking his or her access rights to a large number of resources that are no longer needed for the tasks required by the new position. Similarly, functions of the new job may require access to various new resources. In this scenario, explicit revocation of access rights as well as the granting of new ones needs to span every old and new resource that is or used to be accessible to the user. The notion of user groups was introduced to alleviate some of these issues. Users sharing similar access to the same resources become members of a single group. The group as a single entity is then granted or denied access to the managed resources. Access decisions take into account the fact that a user is a member of one group or another. Grouping users is certainly one important aspect in addressing the scale of manageability in access-control systems but alone is not sufficient. In addition to user groups, another important dimension in the manageability of access controls is the grouping of access rights. Following on the concept of managing users that share similar access capabilities as a unit, role-based access control evolves around the idea of grouping access rights pertinent to a particular functionality into a role abstraction. management as such is performed at a coarse-grain level than that of individual privileges. In our previous example of a person moving to a new function, he or she is simply assigned to the new role and removed from the old one when a role-based access control (RBAC) mechanism is in place. RBAC policies provide a natural and powerful way for an administrator to specify the privileges required by various job functions and efficiently manage user to role associations. The appeal of RBAC is its inherent representation of real-world access control processes. In many situations, people perform day-to-day functions based on the role in the organizations to which they belong, within a community of people, or in society at large. A role is a higher-level concept that can be better understood as opposed to individual access rights or operations. Roles are compatible with the hierarchical organizations found in real, such as those in an enterprise. Roles can be easily mapped onto an already hierarchical structure of an organization. Higher-level roles are automatically granted the roles associated with lowerlevel organizational entities. It is for these reasons RBAC is being touted as the generalized form of access-control models. The underlying RBAC foundations are Permissions are assigned to roles, Users are assigned to roles, and Access decisions are based on users being members of applicable roles. The premise of ease in managing an RBAC policy is based on the fact that user assignments to roles tend to change over time, while permission assignments to roles are relatively stable. The privileges associated with a particular role may remain unchanged over a long period of time due to the fixed semantics

of the functions assigned to that role. Users can be easily reassigned to new roles as the need arises. Basing security administration on roles rather than on permissions provides simplicity, is easier to understand, and enables better scalability. Roles support the data-abstraction principle in systems design and can be viewed as higher-level encapsulations of lower-level privileges and permissions. Roles have been adopted in many environments and contexts, at times with varying semantics.

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

Access control (AC) is one of the best approaches that is used to secure the information from inside and outside attacks of the organization and decisions of granting and revoking access to any user. The access control gives access to those who are authorized to organizations, i.e., persons, processes, and systems. The access control models define its mechanisms and security policies first, and then, these models are implemented in organizations according to goals and objectives. There are several traditional and hybrid access control models that have various pros and cons.

The traditional access control models are discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC). In the DAC model, the owner of the object has the authority to give and deny access to others without a system administrator mechanism. The DAC model is divided into two types: strict DAC and liberal DAC. In the strict DAC model, only the owner has the authority to permit and deny access to created resources, but in the liberal DAC model, the authority of the owner can be transferred to another individual who will be able to permit and deny the access. In the MAC model, the centralized mechanism is used to permit and deny the access of resources to users. The MAC model is more secure, flexible, and efficient for commercial and military use due to its centralized behaviour. The RBAC model is prominent due to the least privilege and tight security that makes it more powerful than all other models. The ABAC model has dynamic behaviour that is the most suitable model for changing environments. There are some disadvantages of both RBAC and ABAC models. So, researchers proposed some hybrid models as an extension of RBAC and ABAC.

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

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

Access control is critical in the protection of organizational assets, which include data, systems, and networks. The system ensures that the level of access is ideal to prevent unauthorized actions against the integrity, confidentiality, and availability of information. Enterprises, therefore, need robust access control

measures not only at a security level but also for compliance with industry-set regulatory standards like GDPR, HIPAA, and PCI DSS, among others.

Access control works by identifying and regulating the policies for accessing particular resources and the exact activities that users can perform within those resources. This is done by the process of authentication, which is the process of establishing the identity of the user, and the process of authorization, which is the process of determining what the authorized user is capable of doing. It can occur at various levels, such as network level, application level, and physical level, in relation to buildings and other structures. Access Control System (ACS) a security mechanism organized through which access to different parts of a facility or network will be negotiated. This is achieved using hardware and software to support and manage monitoring, surveillance, and access control of different resources. In a cybersecurity context, ACS can manage access to digital resources, such as files and applications, as well as physical access to locations. access control technique identifies users, authenticates the credentials of a user recognized, and then ensures that access is either granted or refused according to already-set standards. All sorts of authentication methods may be used; most methods are based upon user authentication, methods for which are based on the use of secret information, biometric scans, and smart cards. Once the authenticity of the user has been determined, it checks in an access control policy in order to permit the user access to a particular resource .Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. A given information technology (IT) infrastructure can implement access control systems in many places and at different levels. Operating systems use access control to protect files and directories. Database management systems DBMS apply access control to regulate access to tables and views. Most commercially available application systems implement access control, often independent of the operating systems and/or DBMSs on which they are installed. The objectives of an access control system are often described in terms of protecting system resources against inappropriate or undesired user access. From a business perspective, this objective could just as well be described in terms of the optimal sharing of information. After all, the main objective of IT is to make information available to users and applications. A greater degree of sharing may get in the way of resource protection; in reality, a well-managed and effective access control system actually facilitates sharing. A sufficiently fine-grained access control mechanism can enable selective sharing of information where in its absence, sharing may be considered too risky altogether Policies, Models, and Mechanisms When planning an access control system, three abstractions of controls should be considered: access control policies, models, and mechanisms. Access control policies are high-level requirements that specify how access is managed and who, under what circumstances, may access what information. While access control policies can be application-specific and thus taken into consideration by the application vendor, policies are just as likely to pertain to user actions within the context of an organizational unit or across organizational boundaries. For instance, policies may pertain to resource usage within or across organizational units or may be based on need-to-know, competence, authority, obligation, or conflict-of-interest factors. Such policies may span multiple computing platforms and applications. 4 NISTIR 7316 Assessment of Access Control Systems At a high level, access control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. There are a wide variety of structures; for example, a simple table lookup can be performed to grant or deny access. Although no well-accepted standard yet exists for determining their policy support, some access control mechanisms are direct implementations of formal access control policy concepts.

Rather than attempting to evaluate and analyze access control systems exclusively at the mechanism level, security models are usually written to describe the security properties of an access control system. A model is a formal presentation of the security policy enforced by the system and is useful for proving theoretical limitations of a system. Access control models are of general interest to both users and vendors. They bridge the rather wide gap in abstraction between policy and mechanism. Access control mechanisms can be designed to adhere to the properties of the model. Users see an access control model as an unambiguous and precise expression of requirements. Vendors and system developers see access control models as design and implementation requirements. On one extreme, an access control model may be rigid in its implementation of a single policy. On the other extreme, a security model will allow for the expression and enforcement of a wide variety of policies and policy classes.

As stated previously, the focus of this document is on the practical side of the access control system; detailed descriptions of access control models are not included in this publication. This section provides additional information on access control policies and gives examples of several types of policies. introduces the concept of role-based access control. Finally, Section discusses the type and use of temporal constraints in access control policies. Generating a list of access control policies is of limited value, since business objectives, tolerance for risk, corporate culture, and the regulatory responsibilities that influence policy differ from enterprise to enterprise, and even from organizational unit to organizational unit. The access control policies within a hospital may pertain to privacy and competency (e.g., only doctors and nurse practitioners may prescribe medication), and hospital policies will differ greatly from those of a military system or a financial institution. Even within a specific business domain, policy will differ from institution to institution. Furthermore, access control policies are dynamic in nature, in that they are likely to change over time in reflection of ever-evolving business factors, government regulations, and environmental conditions. There are several wellknown access control policies, which can be categorized as discretionary or non-discretionary. Typically, discretionary access control policies are associated with identity-based access control, and non-discretionary access controls are associated with rule-based controls.

Access control is a crucial component of information technology (IT) and cybersecurity. It is a mechanism that regulates who or what can view, use, or access a particular resource in a computing environment. The primary goal is to minimize security risks by ensuring only authorized users, systems, or services have access to the resources they need.

Access control is not just about allowing or denying access. It involves identifying an individual or system, authenticating their identity, authorizing them to access the resource, and auditing their access patterns. Implementing these measures is an important step in preventing unwanted access to your data and computers. This is similar to measures outlined by NIST SP 800 53 that describe controls necessary for the proper authentication, authorization, and access auditing of computers, networks, and data on IT environments.

The new IT infrastructure and “world of work” are creating new access control issues. The number of access points to an organisation is growing exponentially with the advent of cloud computing, mobile users and the “move to remove work” from the office. However, new technology such as identity and access management (IAM) and organisational strategies like zero trust are helping to control access to physical and information assets within the organisation and preventing unwanted access.

Access control is an proactive security measure designed to prevent, detect and deter unwanted activity by restricting access to resources, data and services to only those with the proper authorization. Implementing an access control strategy is an important step in securing resources against external and insider threats. Access control also plays a crucial role in ensuring that an organization meets its access control regulatory requirements. Rules such as those outlined by the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) mandate the enforcement of robust access control strategies to protect sensitive information. Non-compliance can be costly to an organization and detrimental to brand.

What are Access Control Security Best Practices?

Implementing multi-factor authentication

MFA requires users to provide two or more verification factors to gain access to a resource. This could be something they know (like a password), something they have (like a smart card), or something they are (like a fingerprint).

By implementing MFA, you add an extra layer of security. Even if a malicious actor manages to get hold of one factor, they will still be unable to gain access without the other factors. MFA is especially useful in protecting against phishing attacks, where attackers trick users into revealing their passwords.

Implement Strong Password Policies and Consider Going Passwordless

Passwords are often the first line of defense in security. However, weak passwords can easily be guessed or cracked by attackers. Implementing strong password policies is a must. These policies should enforce the use of long, complex passwords and regular password changes.

Strong passwords are just the beginning. You might have a killer password strategy in place, but it still has the potential to go horribly wrong – e.g. your users could lose or misremember their login credentials, or an enterprising hacker might correctly guess them. For these reasons, many organizations are ditching the password altogether in favor of “password less” authentication strategies, which employ social login, magic links, and biometric data (e.g. fingerprint or facial recognition info) to grant users access to apps and services.

No Shared Accounts

Many attacks occur through shared accounts. Allowing multiple individuals or programs to access a single account can make it difficult to keep track of who is doing what, and create an atmosphere of rampant misbehavior, since no one wants to be held accountable for another person’s actions. In the event of an incident, it becomes extremely difficult to determine responsibility.

Instead of sharing a single account, individual user accounts should be assigned to each person. This makes it easier to follow a user's actions, and creates a sense of responsibility, because whatever you do will be traced back to you.

Although shared accounts might be unavoidable in certain scenarios, that doesn’t mean that your exposure has to be limitless. For example, you can also employ a privileged access management system to monitor sessions and log activity, and use that information to provide better visibility into who is responsible for particular actions, as well as to investigate and respond to incidents as needed.

Implement the Principle of Least Privilege

The principle of least privilege (PoLP) means enabling users to perform no more action than is necessary to fulfill their role or responsibilities. By enforcing the principle of least privilege, organizations can be assured that a user’s actions cannot lead to malicious intent because they do not have access to information, systems, and resources that could be abused.

Least privilege is not a one-time operation, it is an on-going process. Firstly an audit must be conducted to look at users and the privileges that have been granted. Secondly those privileges that are unnecessary for employees to perform their job functions should be removed. Thirdly on an ongoing basis the system administrator must review and modify user permissions to make sure that individuals have the proper level of access on an ongoing basis

Implementing the principle of least privilege is only half the battle, since users over time may inadvertently accumulate more access privileges and have those privileges exceed the necessary level to perform their jobs, a phenomenon commonly known as privilege creep. Auditing and managing these permissions and roles must be an ongoing process to mitigate such threats.

Access control is an important security feature that regulates whether entities (users, applications etc.) can take specific actions on resources, such as data, networks, physical locations, operational functions, IT system parameters, business documents, heritage objects, artifacts, information objects, or knowledge base entries. Access control enables organizations to control who should access what. It is a critical aspect of IT security and physical security; the consequences of a failed access control policy can be severe.

Access control systems play a critical role in the overall security of your site. Many aspects of a business require access protection such as high value items, sensitive information, proprietary data, restricted areas and valuable company assets. However, access control systems are not just about security; they also offer convenience and management benefits.

Access control systems provide numerous benefits and one of the primary benefits is keyless entry. Traditional keys have the potential to cause damage, can be misplaced, copied by unauthorized individuals,

and left in unsecure locations. Access control systems on the other hand utilize digital authentication methods and provide robust security with streamlined system management.

The access control system does not only lock and unlock doors but it also monitors and records the activities of users who are accessing through the access points. Each event of access such as an entry or an exit is logged and recorded with relevant details including identity of the user, time of access and location of access. The log of access events can be used for security audits, attendance tracking, crime investigation and for compliance to various health and safety policies.

An access control system checks if a person is who they claim to be and if that person has permission to access a particular area, room, object or access various resources such as information, computers, networks, systems or databases. Access control can be physical i.e. access to a building, room or door, or logical i.e. access to computer resources such as information, database, network or system.

Access control is based on two key elements: authentication and authorization. Authentication verifies the identity of a user, whereas authorization establishes the specific access rights that the verified user has. Various approaches and technologies are currently used to authenticate users, for example, by entering passwords, PIN codes, using smart cards, fingerprint recognition, facial recognition, and access control based on mobile phones.

1. Ease of use: The software ought to be simple to configure and easy to manage.

2.Support scalability: Handle increasing volumes of users and resources across the organisation as it grows, handling millions of users.

3.Integration: Interoperate with customer/enterprise systems and security infrastructure as well as other cybersecurity tools.

4. Customization: Ability to customize the product so that the resulting access policy meets your very specific and stringent security requirements.

1. **Conformance:** Ensure that the product allows you to meet all industry standards and government regulatory requirements.

2. **Support and maintenance:** Choose a tool that has reliable support and that frequently provides updates to be able to deal with emergent security threats.

1.1 Benefits of Effective Access Control Systems

1. Security is really important. Access control systems help keep information safe. They stop people from getting in when they are not supposed to. Reduce the risk of someone getting into the system or the building when they should not be there.

2. There are a lot of rules that companies have to follow when it comes to keeping data safe and controlling who can get in. Access control systems help companies follow these rules so they do not get in trouble or have to pay fines.

3. Access control systems also make things easier for the people, in charge of security. They can give people permission to get in or take it away quickly and easily which saves a lot of time and means the security team has work to do.

4. Audit and Accountability Access control systems maintain detailed logs of who accessed which areas and when.

1.2 The factors shaping new and future security technology

In 2026, several broader forces are shaping the adoption of security technologies, including new hardware and software, as well as workforce changes in general. Key drivers of security trends include:

- **Work environment shifts:** The growth of remote and hybrid work continues and more critical assets are accessed remotely from myriad endpoints.
- **AI & automation:** The cybersecurity arms race is increasingly AI-driven, both for defenders and adversaries, due to the costs for businesses being estimated at 20 trillion.
- **Cloud migration and sovereignty concerns:** More workloads going to the cloud, including security camera footage; geopolitical tensions raise data-sovereignty and governance issues.
- **Sensor proliferation and smart spaces:** IoT, advanced sensors, edge computing, smart buildings and cities are becoming common, meaning physical security tech is more connected and data-rich.
- **Regulatory and trust pressures:** Studies show organizations expect regulations, digital trust and risk governance to be major focus areas in 2026.
- **Threat escalation and complexity:** Threat actors are using more advanced techniques (deepfakes, agentic AI, etc.), forcing a shift in how security tech must operate.

1.3 The top security technology trends in 2026

From recent innovations in AI-powered security software and machine learning algorithms to novel information technology security systems and emerging cloud security developments, below are eight top security technology trends to consider in 2026.

1. Pre-emptive cybersecurity and AI security platforms

In 2026, organizations are less willing to simply react to breaches; they're moving towards predictive, pre-emptive defence. A notable example is when AI security platforms govern and monitor both defenders and attackers to detect anomalies, misuse or malicious agents. Others include automated denial and deception software that proactive misdirects attackers.

Intelligent AI programs and machine learning algorithms will continue to revolutionize business security. Modern integrations are designed to improve the operation of digital and physical security technologies, primarily through automated incident detection and response functions.

For example, AI software solutions are now commonly integrated alongside existing business security cameras to optimize core security operations. AI video analytics imbued with the latest machine and deep learning capabilities can be deployed to continuously search for anomalous events. This removes the need for security teams to constantly monitor camera feeds, with instant alerts sent to staff remotely via the cloud.

With support from machine learning algorithms, modern AI software solutions can understand how security and physical spaces are used under normal conditions, alerting staff instantly to the occurrence of anomalous events. This is what it could look like in life: if a lot of people start gathering in a place that is usually empty, the system will let the people, in charge, know. It will also send a message if the camera sees something moving around when the office is closed.

Companies can use these messages from the AI camera system to help the security people make better choices and pay attention to what really matters. This is the way security systems will work in the future. They will be able to change and react to things that happen. They will help keep people safe.

2. Digital provenance, geopatiation and cloud sovereignty

Since security is increasingly distributed and global, verifying the origin, integrity and lifecycle of software and data is essential. Digital provenance refers to knowing where a data set, software component or AI model came from, its chain of custody and whether or not it's been tampered with. With the rise of AI-generation media and deepfakes, digital provenance has become critical for maintaining trust and authentication online. In the context of video security,

Geopatiation and cloud sovereignty refer to moving or governing data so that it resides under favorable regulatory jurisdictions and handling compliance and localization issues. As nations implement stricter data protection regulations, many are reassessing where their data is stored, processed and backed up. This has led to a rise in:

- Localized data centers and sovereign cloud infrastructures
- Geo-fencing for digital assets
- Cross-border compliance controls that ensure sensitive data doesn't leave its legal jurisdiction

Geopatiation also has implications for critical infrastructure and defence sectors. For example, a smart city that captures facial recognition data may be required to store and process that information within national borders, preventing foreign entities from accessing or exploiting it.

In 2026 and beyond, as security ecosystems become more cloud-based and AI-driven, these principles underpin ethical AI governance, cybersecurity and international compliance.

3. Advanced sensors, edge AI and physical AI

The line between physical security and IT security is blurring. Advanced sensors, edge-AI processing and integrated platforms are becoming increasingly common. Smart occupancy sensors, environmental sensors, video analytics, acoustic sensing and more. Edge computing ensures real-time detection and response closer to the source of a problem rather than relying solely on the cloud. Physical AI, referring to machines or devices that detect and act.

A notable example are sensors supporting real-time detection and data-driven decision-making efforts. Vape detection sensors help improve air quality and ensure compliance with no-smoking policies. They leverage specialized hardware and software tools to detect the presence of vape aerosols and provide real-time alerts for prompt action.

Some smart sensors, such as the Halo Smart Sensor, offer a wide range of functionalities beyond vape detection, including noise detection and keyword recognition, enabling these security technologies to function as a smart panic alert. Air quality sensors can also monitor pollutants, humidity and heat levels to help facilitate healthier indoor environments.

Some advanced smart sensors contain dedicated panic buttons. This provides an immediate means for individuals to warn other people in the building of emergencies and request aid from local authorities, helping to mitigate damage and enhance overall security outcomes.

The data collected by sensor technology and security can not only be leveraged to promote occupant safety and well-being but also to optimize building management operations. Insights can help inform the operation of HVAC and lighting to reduce energy waste, suggesting the future of physical security may lie in multi-functional hardware.

4. Mobile credentials, touchless access and integrated physical-digital access

Touchless and mobile-credential access will continue to advance, but in 2026, the emphasis is on integration with broader security like video, sensors, cloud and analytics.

The primary benefits of the adoption of mobile credentials include a lowered risk of lost or stolen credentials leading to serious security breaches, reduced expenses related to the cost of replacing physical credentials and convenience and hygiene benefits for users. Thanks to an entirely touchless access process secured behind emerging cybersecurity technology solutions, users can manage property access safely and securely at all times.

The development of mobile access control also allows businesses to implement additional policies and wider integrations to further improve on-site security. Credentials stored within smartphones can be secured behind the MFA protections already present in modern devices, and access control can be linked to existing digital scheduling programs. Most mobile access

apps are developed alongside cloud-based management platforms, allowing security teams to create bespoke integrations between access devices. This is what it means when we talk about security. We can use security cameras like the ones that turn all the way around and alarms to keep an eye on things. These security cameras and alarms can be set up to go off automatically if someone tries to get in who should not be there. The people in charge can watch what is happening on their phones or computers from else.

We use our phones or watches to get into places. This is called credentials. We do not need to carry cards or remember codes. We can just use our phones to unlock doors or get into systems. Our phones store these credentials in apps and we can use them with things like Bluetooth or special codes.

The good thing about credentials is that they are easy to use. We always have our phones with us so we do not need to carry anything. The people in charge can also easily give us access. Take it away from us if we need it. If we lose our phone they can stop it from working away which makes things more secure..

Mobile credentials are also very safe. We can use our phone and other things like our fingerprint or face to get into places. This makes it very hard, for someone who should not be there to get in. Mobile credentials can do this by using ways to check who we are like looking at our phone and our fingerprint and checking with the cloud.

5. Data-informed occupancy management

Companies are using data to figure out how to make the most of their security teams. They want to know where to put their time and money. To do this they are putting sensors in places to see how people are using their buildings. These sensors give them information about what is going on.

They can then use technology to look at this information and understand what it means. This helps the people in charge know what areas need security.

For example they might find out that people are often walking through areas where there are no security cameras.

This information can help security teams make plans for emergencies. They can see which areas get really busy and use that to plan how to get people out of the building

This makes it a lot harder, for someone to get into the building who should not be there.

Occupancy management sensors are often integrated into scheduling and amenity booking to help optimize core operations. For instance, if certain facilities are used more frequently during specific times, leaders may look to expand those services during future renovations or adjust internal schedules to optimize operational efficiencies.

6. Biometric technology for high-security applications

Biometric access control integrations are becoming increasingly popular as an additional form of verification to protect high-security locations and sensitive company data. Though it's rare to find biometric access deployed to secure all areas of a commercial property, the extra protections biometrics provide for high-security assets have seen their use increase.

Installing biometric access readers to secure high-risk locations like server rooms, inventory storage facilities and cash vaults helps ensure that even if token-based credentials become compromised, intruders cannot access valuable assets.

Examples of popularly deployed biometric options include:

- Voice recognition
- Facial recognition
- Fingerprint scans
- Retina/iris scans
- Gesture recognition
- Gait analysis
-

Considering the increasing number of significant data breaches that have impacted businesses in recent years, more companies that traditionally secured behind password protections are expected to gradually move toward biometric authentication. As most smart devices already contain biometric scanners, transitions toward this form of verification may also be easily adopted by end-users.

New security technology developments are leading to promising innovations in biometrics, with novel processes like post-quantum cryptography and multi-model biometrics increasing the accuracy of scans beyond current limitations, potentially impacting future security industry trends.

7. Increasing adoption of behavioral analytics

Behavioral analytics programs are really good at helping us with security. These new security technologies are getting popular with people who work on cybersecurity. This new technology helps us look at a lot of data quickly and get the information. It gives us insights that can help our security systems work better. Behavioral analytics programs are useful, for making our security systems stronger.

Utilizing AI and machine learning tools, these futuristic security technology solutions help professionals better understand user behaviors, leveraging insights to identify suspicious cybercrime-related activity. AI-

informed behavioral analytics software is commonly used to spot warning signs of sophisticated threats like DDoS attacks and data exfiltration activities, enabling security teams to program automatic responses triggered by predetermined criteria.

Behavioral analytics programs share particular synergies with converged and cloud-based security, enabling organizations to frequently test and assess all aspects of active security networks, including web applications, cloud-based servers, management platforms and physical security technologies.

By deploying new cybersecurity technologies, admins can better understand how employees typically use them to help optimize existing processes and improve their ability to accurately detect emerging cyber threats.

8. License plate recognition (LPR)

The use of License Plate Recognition technology is growing fast. It will keep getting bigger in 2026 as a trend in security.

License Plate Recognition technology uses cameras and software to read license plates on moving cars.

This helps with access control and parking management.

License Plate Recognition technology is really important for controlling who can get into places like offices and government buildings and neighborhoods.

It does this by looking at license plates and keeping track of them.

The License Plate Recognition technology can let people in. Keep them out based on who they really are.

This really helps to cut down on the risks of people getting into these places when they are not supposed to.

License Plate Recognition technology is very good at stopping people from getting in when they should not be there.

License Plate Recognition technology works with other security things like video security and access control and alarms.

This helps to make a security system.

When License Plate Recognition technology is used with these security things it's easy to look at information about vehicles and see if it matches anything in security databases.

This means that teams can quickly do something about problems or weird things that happen with vehicles.

License Plate Recognition technology is very useful for keeping people and places safe.

In parking management License Plate Recognition technology helps with using parking spaces and making it easier for people to get verified by automating the process of giving out tickets and getting payments.

As License Plate Recognition technology and security get better the equipment and computer programs will probably become more accurate and affordable which will help with working with systems that can shape what security looks like in the future.

License Plate Recognition systems usually have a mix of equipment and computer programs.

The equipment has high-quality cameras lights that help see at night and units that process information.

The computer programs use ways of looking at pictures and artificial intelligence to find the part of the picture with the license plate make the picture look better and read the characters correctly.

Today many systems use kinds of computer programs called machine learning and deep learning to make sure they can read license plates correctly even when it is hard to see, like when it's dark the car is moving fast or the license plate is dirty.

License Plate Recognition technology is getting better and better.

It is helping with parking management and security and License Plate Recognition technology will keep playing a role in making parking management more efficient.

License Plate Recognition is really useful in vehicle access control systems. For example in areas, office buildings and industrial zones License Plate Recognition is used to open gates, for authorized vehicles. This means that people do not need to use cards or wait for someone to verify who they are. It is more convenient saves time and makes the place more secure because only vehicles that are registered can get in.

License Plate Recognition is also used a lot in parking management systems. When a vehicle enters a parking place the system takes a picture of its license plate. Notes the time it arrived. When the vehicle leaves the system figures out how much the parking fee is based on how the vehicle was there. This means that people do not have to buy tickets and it makes the whole process work better. License Plate Recognition makes things easier and more efficient.

1.4 Implementing physical and cybersecurity technology trends

While remaining informed about the latest technology in cybersecurity, physical security and cloud computing will help businesses better understand how new innovations may shape the future of security technology, not all emerging technologies are well-suited to all applications.

In many cases, leaders and security personnel will make better use of available resources by prioritizing a smaller selection of new security technologies suited to their core operations.

Often, it's not practical or financially feasible to continuously update all active security solutions according to the latest security trends. Therefore, stakeholders must work together to identify key security technologies that will likely have the most significant positive impacts.

Perform detailed risk assessments

Before choosing what to upgrade, teams must combine their knowledge to perform detailed physical security risk assessments to identify the organization's five most prominent threats. For example, businesses with high numbers of remote staff may prioritize cloud security improvements, while retail security may benefit from access control upgrades.

Develop risk mitigation strategies

With all major security threats identified and discussed, teams should develop risk mitigation strategies. This can be achieved by assessing existing IT security technology and physical security hardware, alongside relevant organizational policies and then considering how specific new security technologies may be leveraged to improve them.

For some teams, this could mean investing in AI software integrations positioned to enhance video security and IP cameras, rather than taking on the cost of replacing current hardware. For others, planned new security processes may not be achievable using existing security tools, requiring full-scale infrastructure updates as a long-term investment.

Consider scalability and future upgrades

Any investments into emerging security technologies must be made with future scalability, upgrades and maintenance in mind. For instance, if teams have decided that mobile access will be beneficial to the business, they must also ensure that installing new readers, developing wider integrations and upgrading software can be reasonably achieved.

Evaluate installation and integration costs

New security technology and high-tech security devices will need to be installed by professional teams trained to integrate these with existing tools without exposing significant vulnerabilities. Business leaders must consider whether structural work will be required and how labor-intensive the work will be, as these factors could dramatically increase overall costs.

1.4 Benefits of Implementing an Access Control System in Security System

Access control systems are really important for keeping people and things safe in lots of places like offices, factories, schools and homes. These systems help decide who can go into areas use certain things or get to certain information. They are a way to keep things safe than just using locks and keys. Access control systems make it harder for the wrong people to get in. They help organizations run more smoothly and safely.

One of the things about access control systems is that they make everything more secure. Old locks and keys are not very good at keeping people out because they can be stolen or copied. Access control systems use things like cards, secret codes and ways to check who you are like looking at your fingerprint or face to make sure you are who you say you are. This means that only the right people can get into areas. Places that have things like computers, money or secret information can be kept safer with access control systems.

Using things like fingerprint scanning and face recognition makes it even harder for the wrong people to get in because nobody else has your fingerprint or face. Another good thing about access control systems is that they can watch what people are doing and keep a record of it. Every time someone tries to get in the system writes it down including who they're when they tried to get in and where they were. This helps organizations keep an eye on their employees and figure out if someone is doing something they should not be doing.

In workplaces access control systems are also used to keep track of when employees are working. This means that the organization does not have to use much paper to keep track of things and it makes things easier to manage. Access control systems are a help, to organizations because they make everything safer and more efficient. They are a part of keeping people and things safe in lots of different places. Access control systems are used to protect access control systems and the people who use them.

suspicious activities, and investigate security incidents when necessary. In many workplaces, access control systems are also integrated with attendance management systems, allowing organizations to track employee working hours automatically. This reduces manual paperwork and improves administrative efficiency.

Access control systems get rid of a lot of problems that come with using keys. When you lose a key it can be a security risk because someone who should not have access might find the key or make a copy. Replacing locks and giving out keys can take a long time and cost a lot of money.. With modern access control systems

you can quickly turn off and replace digital things like access cards or mobile permissions without changing the whole locking system. This makes things more convenient. Reduces costs and security risks.

Remote management is another benefit of modern access control systems. Systems that use the cloud and networks let administrators watch and control access from anywhere using computers or mobile devices. Security managers can. Take away access permissions right away lock or unlock doors from far away and get notifications in real time about suspicious activities or emergencies. This is especially useful for organizations with branches or big facilities where they need to manage everything from one place. Being able to manage access from away helps security personnel respond quickly to potential threats or things that need to be done.

Access control systems are also very convenient. Users do not need to carry keys for different rooms or departments. Instead one access card, fingerprint or smartphone application can let them into places. Automated entry systems reduce waiting times. Make it easier to move around buildings especially in big offices, hospitals, universities and industrial facilities. In homes smart access systems let homeowners get into their homes without keys and control their home security features from away.

Modern access control systems can also work with security technologies to create a big security network. They often work with CCTV surveillance systems, alarm systems, fire detection systems and visitor management software. For example if someone tries to get in who should not the system can automatically trigger alarms. Turn on nearby cameras to record what is happening. During emergencies like fires, access control systems can unlock emergency exits automatically so people can get out safely. This makes the whole security system work better together and helps emergency response procedures work effectively.

Using access control systems makes things work efficiently. Automated systems reduce the need for security personnel to check things manually manage keys and keep track of visitors on paper. Security personnel can focus more on watching and managing emergencies of doing routine tasks. Organizations can also give levels of access to employees based on their jobs and what they are responsible for. For instance administrative staff can get into office areas while IT personnel can get into server rooms. This way of giving access based on roles makes sure that the organization has control over its resources and information.

- * Access control systems are very helpful
- * They make things more convenient. Reduce costs
- * They help security personnel respond quickly to threats
- * They work well with security technologies
- * They make things work efficiently

Access control systems are very useful for many organizations. They can be used in different places, such, as offices, hospitals and homes. Access control systems are a way to keep people and things safe. Access control systems are the way to go for people who want to keep their things safe.

.Scalability and flexibility make access control systems suitable for organizations of all sizes. When businesses grow they can easily add users, doors and security features without replacing the entire access control system. They can modify permissions easily according to changing needs. This adaptability allows organizations to maintain access control management even as their operations expand.

Cloud-based access control solutions further simplify scalability because updates and new features can often be implemented through software without hardware changes.

Access control systems also contribute to improved safety and regulatory compliance.

Many industries, such as healthcare, banking, government and information technology are required to follow security standards and maintain detailed records of access activities.

Access control systems provide logs and reports that help organizations comply with legal and regulatory requirements.

These records are valuable during audits, investigations and compliance assessments.

In addition by restricting access to sensitive areas, access control systems help reduce workplace accidents and ensure employee safety.

An access control system may involve installation and maintenance costs but the long-term benefits often outweigh these expenses.

Organizations experience reduced losses from theft improved operational efficiency, lower administrative workload and enhanced protection of assets and confidential information.

Technological advancements in biometrics, artificial intelligence, cloud computing and mobile integration continue to make access control systems more intelligent, reliable and user-friendly.

Implementing an access control system provides advantages that strengthen security improve convenience and support efficient management.

Access control systems protect people, property and information by ensuring that authorized individuals can access restricted areas and resources.

Features such as real-time monitoring, remote management, system integration and automated reporting make access control systems a component of modern security infrastructure.

As security challenges continue to evolve access control technologies will remain a solution, for creating safe, secure and well-managed environments.

In today's evolving security landscape businesses need robust solutions to protect their premises and assets.

One such solution is an access control system, which offers benefits in terms of security, control and peace of mind.

In this blog post we will explore the 6 benefits of implementing an access control system in your security system.



1. Better Security

When you use an access control system you can make your place a lot safer. Access control helps you decide who can come in and who cannot. This means that only the people you want to let in can get in and you can stop others from getting in and causing trouble.

2. Control Who Gets In

An access control system lets you choose who can go into areas of your place and when they can go in. You can say who can go where based on what they do so only the right people can get into areas.

3. Keep Your Stuff Safe

If you have an access control system you can protect the things that're important to you like equipment, computers or secret information. By letting the right people in you can stop bad things from happening, like theft or vandalism.

4. Watch Who Comes and Goes

Access control systems can show you who is coming and going in time. This means you can keep a record of who went where and when which can be really helpful if you need to look into something or follow the rules.

5. Make Your Place Safer

Access control systems can help make your place safer by adding a layer of protection. You can use things like keys or passwords to make sure only the right people can get in which can stop people from pretending to be someone they are not.

6. Make Things Easier

Access control systems can make things easier by automating some tasks like letting people in or managing who can go where. You can also get messages if something goes wrong. You can schedule reports. This can save you time and money. Let your security and IT teams focus on other important things.

An Access Control System is a way to control who can get into areas or use certain things. It makes sure that only the people who are supposed to be let in can get in based on the rules you set. Access control systems are used in security companies to protect buildings, important areas, computers and other important things. Access control is a way to keep people from getting into things they should not be getting into. It helps keep important information and systems safe from people who should not be using them. This is really important for keeping your information and systems safe, from people who might try to hurt them which could damage your reputation or credibility. Access control systems are a part of keeping your important things safe and they help make sure that only the right people can get into them. The AAA Framework is really important for keeping our stuff safe. It is made up of three parts: Authentication, Authorization and Accountability.

* The Authentication part checks to see if you are who you say you are. It does this by using things like passwords, biometric things like fingerprints or tokens.

* The Authorization part figures out what you can. Cannot do. It does this by looking at what your job's what you are supposed to be doing.

* The Accountability part keeps track of what you do. It does this by watching what you do and writing it down so if something bad happens the people, in charge can see what went wrong and fix it.

The AAA Framework, which includes the Authentication part and the Authorization part and the Accountability part helps us keep our data and systems safe.

1.5 Evolution of Access Control Models

Private security organizations use ways to control who can do what. They have been using methods like Discretionary Access Control and Mandatory Access Control and Role-Based Access Control for a long time. Role-Based Access Control is very popular because it works with how businesses actually work. It gives people permissions based on their job than who they are.

Private security organizations like Role-Based Access Control because it is simple and easy to manage. However with all the technology like cloud computing and mobile devices and the Internet of Things private security organizations need new ways to control access. So now they are using things like Attribute-Based Access Control and Relationship-Based Access Control. These new methods are better because they can make decisions based on the situation and they can do it away. This makes them very good, for security organizations that have to deal with a lot of complex security issues. Private security organizations use Attribute-Based Access Control and Relationship-Based Access Control to control access in a way.

We have a lot of technology these days but our systems still have big problems with people who work inside the company and cyber risks that are always changing. When people who work for the company do things with the access they are given that is a major issue. This is especially true in places where people already have a lot of power to do things on the system.

Also more and more companies are letting people use their devices for work, which is called Bring Your Own Device or BYOD for short. This is a problem because peoples own devices do not always have the security as the companys devices.

To deal with these problems companies are starting to use some practices. One of these is called the Principle of Least Privilege or PoLP for short. This means that people who work for the company are only given the access they need to do their job, which helps stop people from doing things. Another best practice is called Zero Trust Architecture or ZTA for short. Zero Trust Architecture makes the system more secure, by checking who people are and what device they are using no matter where they are.



Future Trends: AI, Biometrics and Blockchain

Looking at what's coming in 2026 new technologies like AI and Machine Learning are changing the way we think about keeping things safe. AI programs are really smart now. Can figure out how people usually move around in a space. They can tell staff away if something weird is happening, like a big crowd in a place that is usually empty or someone moving around when they should not be.

Biometric technology, like recognition is being used more and more for really secure places like server rooms and cash vaults. This technology can also look at how people walk and scan their eyes.

Blockchain technology is also being used to make sure logs of who is coming and going are safe and honest.

Access control systems are very important for keeping things safe today. They help control who can get into a building or a room. They also help control who can get to information. These systems are used in lots of places like offices, schools and hospitals. They are even used in apartments and commercial buildings.

They are much better, than using keys to lock and unlock doors. Access control systems are a way to keep people and things safe. They are also more reliable and easier to use than locks and keys.

Access control systems help people feel safer. They also help things run more smoothly.

Access control was mainly about security like using locks and keys. These systems were simple and lots of people used them in their homes, offices and small institutions. If you had the key you could get in.. These systems had some big problems, like people making extra keys losing keys and no way to keep track of who was coming and going. You could not even tell who went into a place or when they went in which made it bad for places that needed to be really secure.

Then computers came along. Access control started to change from physical security to digital security. One of the new models was called Discretionary Access Control or DAC for short. With DAC the person who owned something got to decide who could use it. This system was pretty flexible and easy to use especially when people were sharing files on their computers.. It also had some security problems because people could share important information with the wrong people either on purpose or by accident.

To fix the problems with DAC people came up with Mandatory Access Control or MAC. MAC was a system where a central authority controlled who could access things. People were given security clearances and important information was labeled as sensitive. This system made things a lot more secure. It was used by the military and the government. Access control like MAC was good, for keeping information safe. Mandatory Access Control and Discretionary Access Control are both types of access control that people use to keep their information safe.

As companies got bigger and more complicated they needed a way to manage who can access what. This led to the creation of Role-Based Access Control or RBAC for short. Role-Based Access Control is a system where people are given permissions based on their job title, not who they're. For instance employees, managers and administrators all have levels of access because they have different jobs. Role-Based Access Control made it easier for companies to grow and it reduced the amount of work administrators had to do so it became very popular in companies.

When the internet and cloud computing became widely used the way companies controlled access to information changed too. New systems like policy-based and attribute-based access control were developed. Attribute-Based Access Control or ABAC is a system that decides who can access what based on different things like what job someone has where they are, what time it is what kind of device they are using and how sensitive the information is. This makes Attribute-Based Access Control more flexible and precise, than systems.

Access control has changed much in the last few years. It is now about systems that are smart and can understand the situation. These new systems use information and artificial intelligence and machine learning to figure out if someone's a risk and make good decisions about who can access what. For example if a user is trying to log in from a place or a different device they may have to do some extra things to prove who they are. This change has really helped to make things more secure when it comes to cloud computing and mobile apps and Internet of Things devices.

Another big change in access control is that it now works with identity and access management systems. These systems combine access control so organizations can manage who gets to do what and how they get access from one place. This is really helpful in workplaces where people need to use different systems but they can use the same identity for all of them. Access control and identity and access management systems are working together to make things easier and more secure.

Access control systems are really useful because they can work with CCTV cameras and alarm systems to keep everything. When something bad happens these systems can open doors automatically. Send messages to the people who take care of security. This way the security team does not have to do paperwork, which makes their job easier. Access control has changed a lot over the years to make sure organizations and businesses are safe. A time ago people just used locks and keys to keep others out. These old methods were okay. They were not very flexible and it was hard to keep track of everything.

As computers and digital systems became common new access control systems were made to improve security and make it easier to manage resources. Access control systems have really improved. Now they can do a lot to help keep people and things safe. Access control systems are a part of keeping organizations and businesses secure. The first generation of access control was about security. It used locks and manual checks. You got access if you had a key or if security personnel said it was okay. This worked for places but it got really hard to manage in big organizations. Keys could get lost, copied or taken. There was no way to keep track of what users were doing.

Access control systems today use technology like biometrics and cloud computing and artificial intelligence. They also use something called two-factor authentication. These modern systems let you monitor things in time manage from far away and analyze security smartly. Access control systems have changed a lot. They show that we need more flexible security for both physical and digital places. Access control is really important. Access control systems keep getting better. They help keep our places safe. Access control is a part of security.

The way we control who gets into a place or a system has changed a lot over time. We used to have locks and keys. Now we have really advanced computer systems that help keep us safe. Each time we made a change we found ways to protect things manage the people who use them and make sure only the right people get in. As computers and technology get better the way we control access will also get better so we can deal with security problems. Make sure our future homes and workplaces are safe.

The way we control access has really changed from using systems to using new smart systems that can think and work on their own. Each time we made a system we fixed the problems with the one and added new things to help with security. Now we have systems that use technology like special body scanners, computers that can be accessed from anywhere, artificial intelligence and phones to prove who we are. This makes it really safe and easy to control who gets into a place or a computer system whether it is a place or a digital one. Access control systems, like these are making our lives safer and more secure. Access control is a part of our daily lives.

1.6 Old Access Control Technologies VS New / Modern Access Control Technologies

Feature / Aspect	Old Access Control Technologies	New / Modern Access Control Technologies
Identification Method	Basic to moderate security	High-level, multi-factor authentication (MFA)
Security Level	Keys, swipe cards, passwords	Fingerprint, iris scan, smartphone credentials, cloud identity
Credential Type	Manual record keeping	Centralized digital management
User Management	Usually not available	Full remote monitoring and control
Scalability	Difficult to expand	Easily scalable through cloud platforms
Data Storage	Local storage only	Cloud-based and encrypted storage
Examples	Mechanical locks, RFID cards, keypad entry	Smart locks, biometric scanners, mobile-based access
Cost Structure	Lower initial cost, higher maintenance	Higher setup cost, lower long-term operational cost

1.7 Types of Access Control:



Access control has changed a lot over time. It used to be very basic. Now it is very advanced. Access control is used to protect information in complicated systems like the Internet of Things and cloud computing. These systems control how people or computers interact with information by using specific security rules.

Access control is a way to control who can access things like buildings, computers or information. It is very important for keeping things secret information and company resources safe from people who should not have access. Because security is a concern now different types of access control have been made to provide different levels of protection and flexibility.

The main goal of access control is to make sure only the right people can do things based on what they are allowed to do. Access control systems are used in places, like offices, schools, hospitals, banks and technology companies to keep everything safe and running smoothly.

There are types of access control and each one is designed to meet the needs of different companies and organizations. Some types of access control are very strict while others give users freedom to control who can access things. New access control systems also use technology like biometrics, cloud computing, artificial intelligence and multi-factor authentication to make things more secure and convenient.

Some common types of access control are Discretionary Access Control, Mandatory Access Control, Role-Based Access Control and Attribute-Based Access Control. Each type of access control is unique. Has its own advantages and uses depending on how much security is needed. It is important to understand these types of access control to make sure systems are safe and work well in companies and digital systems. Access control is crucial, for protecting access control systems and keeping them running. Access control systems are used to manage access control and make sure everything is safe.

1. Traditional Access Control Models

Traditional Access Control Models are the security rules that help manage who can access physical and digital things in a system. These models make sure that only people who are allowed can get to information, systems or areas. They are used in security systems in organizations, operating systems and databases.

These models mainly focus on fixed rules and permissions that are set ahead of time. This means that decisions about who can access something are based on these rules not on what's happening in real time or how

people are behaving. These models are commonly used in places where security needs are well understood and do not change often.

One of the Traditional Access Control Models is Discretionary Access Control or DAC for short. In DAC the person who owns something like a file or folder gets to decide who can access it and what they can do with it. For example the owner of a file can let other people read, write or run the file. DAC is easy to use and flexible. It has some security problems because people can share permissions by mistake or on purpose, which can cause security issues.

Another important Traditional Access Control Model is Mandatory Access Control or MAC. In MAC a central authority controls who can access things and makes decisions based on security levels. People are given security clearances and things they can access are labeled as secret or top secret. People cannot change permissions on their own, which makes MAC very secure but less flexible. It is often used in government systems where secrecy is very important.

Role-Based Access Control or RBAC is another Traditional Access Control Model that is widely used. In RBAC people are given permissions based on their job not who they're. For example employees, managers and administrators have levels of access based on what they do. This model makes it easier to manage access and is better for organizations. RBAC is one of the commonly used access control models in modern companies because it balances security and usability.

Traditional Access Control Models are based on three things: users, permissions and resources. Users are people or systems that want to access things permissions are what they are allowed to do and resources are the things they want to access. Access control rules are set ahead of time. Enforced by the system.

However Traditional Access Control Models have some limitations. They are not very flexible compared to access control systems because they do not consider things like how people behave, where they are or what device they use. They also need to be updated when the organization or security needs change, which can take a lot of time. They might not be suitable for cloud-based or constantly changing environments.

Traditional Access Control Models were designed for environments where things do not change often. There are models, like MAC, DAC, RBAC and ABAC each with its good and bad points. Traditional Access Control Models can be divided into two groups: DAC and non-DAC. The non-DAC group includes MAC, RBAC and ABAC. These models are compared based on things like the principle of privilege how they behave, safety, separation of duties, capability delegation, flexibility and auditing.

- * Traditional Access Control Models are used to manage access to digital resources.
- * They are based on fixed rules and permissions.
- * They have limitations, such as being less flexible and not considering factors.
- * There are models, including MAC, DAC, RBAC and ABAC.
- * Each model has its pros and cons.
- * They are compared based on criteria, such, as the principle of least privilege and safety.

Comparison of traditional access control models.

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

Discretionary Access Control: This is a way that the person who owns something like a file or a database gets to decide who can use it and what they can do with it. It is very flexible. Gives the owner a lot of power but it can also be a security problem because the owner might give someone too much access without realizing it. With Discretionary Access Control the owner is in charge of saying who can use their stuff. They do not need an administrator to help them decide. There are two kinds of Discretionary Access Control: one that's more open and one that is more strict. The open kind lets the owner give access to people so they can also be in charge. The strict kind only lets the owner be in charge. Discretionary Access Control works because the owner gets to choose what happens. There are three things that are considered when deciding who gets access: who owns the thing, who the users are and who gets to give access to others. Discretionary Access Control is not great for organizations like companies or governments because it can cause problems. For example someone might give access to the person and that can cause big security issues. On the hand Discretionary Access Control is popular because it works well with different types of computer systems. Discretionary Access Control is a way that the owner of something like a file gets to decide who can use it and what they can do with it like read it change it or delete it.

• Discretionary Access Control is talked about in the "Trusted Computer System Evaluation Criteria" which is also called the Orange Book. Because users can share things easily Discretionary Access Control systems are thought of flexible. However this also means that they can be used in the way either on purpose or, by accident.

Benefits of DAC

When you want to control who can access something Discretionary Access Control solutions are a choice. There are good reasons to use Discretionary Access Control. The good things about Discretionary Access Control systems are:

- * **Flexibility:** with Discretionary Access Control users can decide who can access each thing. The person who owns the thing can make groups of users and control who can access it. This is something you cannot do with kinds of access control systems.
- * **Speed and efficiency:** Discretionary Access Control makes it easy for information to move around. Users can give someone access to something quickly. You do not have to make a profile for each new person.

* Low administrative burdens: with Discretionary Access Control, the person who owns the thing gets to control who can access it. The people in charge do not have to keep track of who can access what. Instead users can access the information they need when they need it. Discretionary Access Control solutions make things easier, for everyone. Discretionary Access Control is a way to go because it is simple and easy to use.

Simple policy management: all admins need to do is assign object access privileges to users. With the right ACL management systems, discretionary access technology is extremely simple to use.

Challenges of DAC

Discretionary access control has some benefits. It also has some problems. Here are the main issues to think about.

* Security: the main thing to remember is that discretionary access control is not as secure as access control. With access control bad people can put bad software on the systems they want to attack. This is because users can give themselves much access over time. Users might also give access to many people.. They might not really understand what they are agreeing to when they give access to someone. Discretionary access control is just not as safe as types of access control.

* Lack of visibility: when you have access control it can be hard to keep track of everything. This is because each person is in charge of their access control. Security teams need to know who is looking at information.. With discretionary access control it is hard for them to do that. This can lead to security problems and issues with following the rules. Discretionary access control can be very confusing.

* Maintenance: the people who own the systems are responsible for keeping the access control lists up to date. As the lists get bigger and the networks get bigger it gets harder to do that. For example an access control list might still have the name of someone who used to work at the company.. It might not get updated when someone gets a new job. This can cause problems.

* Poor data protection: companies should use controls to protect their most sensitive information. Discretionary access control systems just cannot give companies the protection they need for data, like health or financial information. Discretionary access control is not the way to protect this kind of data.

Discretionary Access control

DAC is a common feature of everyday life and private network management. Most of us encounter discretionary access systems without even realizing it. Important use cases include:

Social media

Facebook groups are managed via a form of discretionary access control. Group owners can determine who has access to content hosted on each group. Group members generally have a restricted ability to transfer content and share it outside the Facebook platform.

Smartphone apps

When you allow apps to access your smartphone, you are using discretionary access systems. The smartphone owner determines which applications can access functions like the contacts directory or GPS. Users decide when to allow potentially insecure operations.

File system management

Most operating system technologies use a form of DAC to manage files. For example, UNIX file mode allows object owners to set read, view, and write privileges. The same applies to Windows or

DOS. Discretionary file controls govern whether users can transfer or edit files. They can hide file attributes such as size or path. And they can deny access privileges without proper authentication.

Collaboration platforms

Productivity tools like Dropbox or Google Docs use DAC to set user access to files. For example, the owner of a Google Document could create an ACL including relevant employees. Some members of the group are given write functions, while others may only be able to view the file. And the owner retains the power to delete the document or close the project.

Crypto wallets

DAC allows access to crypto wallets, providing the user has both private and public keys. But users can also transfer cryptocurrency via the public key. This allows owners to guard their assets and make transactions securely.

Role-Based Access Control (RBAC) Meaning & Definition

As the global economy continues to drive digitalization, mass amounts of personal and financial data are being stored. According to one recent study, the total amount of data created, consumed, copied, and captured globally grew from 33 zettabytes (ZB) to almost 60ZB in just two years. Estimates project it to rise to 175ZB by 2025. Google, Microsoft, Facebook, and Amazon alone store at least 1,200 petabytes of information.

Growing in parallel to this surge in data storage is the frequency and cost of data breaches and other cyberattacks. The number of data breaches as of September 2021 is up by 17% from 2020, and data compromises are up 27%. A 2021 report by IBM and the Ponemon Institute estimates that a single data breach can cost an organization over \$4 million. And what is the chief cause of such breaches? Compromised credentials.

Why is access control important (RBAC)?

The key to data and network protection is access control, the managing of permissions and access to sensitive data, system components, cloud services, web applications, and other accounts. Role-based access control (RBAC), or role-based security, is an industry-leading solution with multiple benefits. It is a feature of network access control (NAC) and assigns permissions and grants access based on a user's role within an organization.

How does RBAC work?

RBAC is an efficient way to manage access and protect sensitive data and can be illustrated this way:

Imagine a hotel with doors that are accessed by a keycard. A guest is given a keycard that accesses a single room, a maid is given a card that accesses any room on an assigned floor, and a maintenance worker is given a card that accesses all doors in the building. All are given cards, but the extent of access is determined by their role.

Large organizations can further streamline RBAC by creating groups. The roles are assigned to the group, so while personnel can be moved around within the organization, their access depends on the group they have been assigned to.

Essential building blocks of RBAC

The key building blocks of Role-Based Access Control (RBAC) include users and roles, permissions, operations, resources (or objects), and sessions.

- **Users and roles:** They are individuals, services, or systems that require access. Access is granted through assigned roles, which are collections of permissions. RBAC assigns roles based on characteristics, such as job function, location, or device used, rather than assigning permissions to users directly.
- **Permissions and resources:** This reflects what operations a role can perform on specific resources. Resources or objects can include files, databases, or applications.
- **Operations:** These are things that the system does like taking in information doing something with it sending it out storing it and controlling it. For example changing how the system works is something that only administrators can usually do.
- **Sessions:** This is the time when a user is using something. We keep track of what happens during this time like what the user does and what device they use so we can look back, at it later.
- **With Role Based Access Control** what people can do depends on their role, not who they're. So companies first decide what roles there are and then they give those roles the permission

Access control involves three key areas: viewing resources, modifying content (with approvals if needed), and sharing or downloading. For instance, only specific roles may be able to see, edit, or share specific documents or data based on defined rules.

Foundational principles of role-based access control

With role-based access control, permissions are assigned strictly based on roles. This makes administration more efficient than traditional methods. When a user's position changes or if they leave the organization, administrators only need to update the user's role. The associated permissions will then adjust automatically. RBAC also allows users to be assigned multiple roles when necessary.

- **User role assignment** links a user to specific access rights or permissions according to their role or task.
- **User role authorization** verifies that the user has been granted approval for the assigned role and is permitted to carry out its related functions.
- **User role permission** and access rights determine exactly what actions a user is allowed or not allowed to perform within the system.

Key benefits of Role-Based Access Control (RBAC)

1. **Better security:** RBAC can dramatically reduce the effect of human vulnerabilities because many access privileges that could be exploited are eliminated. As a role-based access control example, say someone from marketing falls victim to a phishing attack. If they do not have access to the sensitive database the hacker is after, then the damage is minimized.

2. Streamlined compliance: Compliance requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), dictate who should be allowed access to specific types of information. Using RBAC, it is easy to prevent noncompliant access.
3. Less work for admins: With role-based access control, an admin can easily change access privileges for either individuals or teams of people all at once. This saves time while ensuring employees have on-demand access to an area of the network they need.

Mandatory Access Control (MAC)

MAC is a strict, policy-driven model commonly used in military and government systems. Both users and data are assigned security labels (e.g., “Secret,” “Top Secret”). For instance, User A with a “secret” security clearance can access resources with “secret” asset labels but cannot access documents and resources with “top secret” classifications. In MAC models, systems administrators implement and maintain controls based on a uniform policy. Especially in dynamic and changing environments, implementing mandatory access control can be challenging and difficult. Mandatory Access Control (MAC) is a security framework used to manage access to system resources by enforcing policies that are centrally defined and strictly applied. Mandatory Access Control is a system where users do not get to decide who can see what. Instead Mandatory Access Control uses rules and security labels to control access. These rules are set by an administrator or a security policy.

In places like government offices or big companies with a lot of rules Mandatory Access Control is very important. It makes sure that only people who are supposed to see certain information can see it. This way Mandatory Access Control keeps everything

Mandatory Access Control can also cause problems. It can slow things down in places where people need to get access to things quickly. In these cases it is often the developers who have to figure out how to make it work.

Mandatory Access Control is a secure way to control access to information. It uses rules that are set by an authority to decide who can see what. Users cannot change these rules on their own. Only the system administrator can do that. Mandatory Access Control is used in places like the military, government offices and laboratories where information's very sensitive.

The idea of Mandatory Access Control was created to fix problems with systems. In the past users could share information easily which was not safe. Mandatory Access Control fixes this by having one set of rules that everyone must follow.

In Mandatory Access Control, every user and every piece of information gets a label. Users get a label based on what they're allowed to see and information gets a label based on how sensitive it is. There are different labels and they help make sure that only the right people can see the right information.

Some common labels include:

- * levels of security clearance
- * labels for how sensitive information is
- * labels for what users are allowed to do

Mandatory Access Control is very good at keeping information safe. It is used in places where security is very important. Mandatory Access Control makes sure that users can only see what they are supposed to see and that is what keeps everything safe.

For example in a government office Mandatory Access Control would make sure that only people who are supposed to see certain documents can see them. This way Mandatory Access Control helps prevent secrets from being leaked.

Mandatory Access Control is also used in research laboratories. In these places there is often sensitive information that not everyone should see. Mandatory Access Control helps keep this information safe by allowing certain people to see it.

Overall Mandatory Access Control is an important tool, for keeping information safe. It is used in places where security is very important and it helps prevent secrets from being leaked.

Top Secret

- Secret
- Confidential
- Restricted
- Public or Unclassified

When we talk about access decisions we are looking at the users clearance level and the classification level of the resource. The users clearance level has to be high enough to access the information they want. If the user has a level of security clearance they can see the information. For instance someone with a "Confidential" clearance level cannot see "Secret" or "Top Secret" information. This is because we have a hierarchy in place. The hierarchy is important because it helps prevent people from seeing data when they are not supposed to. The security clearance system is like a ladder. The user has to be, on a high enough rung to access the information they need. We make access decisions based on the users clearance level and the classification level of the resource to keep everything.

Pros and cons of MAC

Pros

- security: The MAC system has very strong control and strict rules so it really cuts down on people getting in who should not be there. This is because it follows the idea that people should only have access to what they need to do their job.
- Compliance-This system is great for places like the government, finance, healthcare and defence where they have to follow a lot of rules.
- Reduces insider risk: People who use the system cannot just share access. Change the rules because everything is controlled by the main system policy.
- Cons
- Rigid and inflexible: The MAC system can be very slow to change when the business needs something. Every time someone needs access the main people in charge have to make the change.
- friction: The people who make things like developers do not get to decide on the MAC system rules but they are often the ones who have to figure out what is going wrong when there are access problems, with the MAC system.

Content and Relationship-Centric Models

As data formats changed and environments got more interactive models that focus on attributes and connections started to appear.

- Attribute-Based Access Control (ABAC) is often considered the best model for IoT and cloud. ABAC makes access decisions based on a combination of user, resource and environment details like location, time or device status. This approach provides detail and awareness of context but needs more advanced infrastructure and processing power. ABAC helps to make sure that access is given based on conditions.
- Relationship-Based Access Control (ReBAC) decides access based on connections between people or things. ReBAC works well for networks or healthcare systems where permissions depend on personal or professional relationships between users. Relationship-Based Access Control helps to make sure that access is given based on relationships.
- Task-Based Access Control (TBAC) gives permissions based on tasks or workflows not user identity. This approach ensures access is only available for the duration of a responsibility. Task-Based Access Control helps to make sure that access is given based on tasks.
- One main idea behind content- access control is that access permissions are determined by the actual content of the resource. For example a document may contain keywords like "confidential" or "medical record " and access can be granted or denied based on these attributes. This approach is useful in environments with data like emails or social media posts. Centric access control helps to protect sensitive information.
- On the hand relationship-centric access control focuses on the connection between users and resources or between users. In this model access is granted based on how a user is connected to a resource or another user. For example in a network a user may view another user's private posts if they are friends. Relationship-centric access control helps to make sure that access is given based on relationships.
- This relationship-based approach is widely used in environments where teamwork is essential. It provides a way of managing access compared to traditional role-based systems. By considering relationships organizations can create dynamic access policies that adapt to changing interactions. Relationship-Based Access Control helps to make sure that access is given based on relationships.
- Content and relationship-centric models are flexible. They can adapt to evolving environments where traditional access control methods may not work. They allow organizations to define access rules based on real-time conditions and user behavior. Content and relationship-centric models help to make sure that access is given based on conditions.
- Another benefit of these models is improved precision in access control decisions. Since they consider information like content attributes and user relationships they can make accurate decisions about who should access what data. This reduces the risk of granting much or too little access. Content and relationship-centric models help to make sure that access is given based on conditions.
- Content and relationship-centric models also support context-aware security policies. Access decisions can change based on factors like location or device type. For example a user may access files only during working hours. Content and relationship-centric models help to make sure that access is given based on conditions.
- However these models also present challenges. One main challenge is complexity, in implementation and management. Defining content-based rules and relationship-based policies requires system design and continuous monitoring. As data and users increase managing these rules can become difficult.

4. Modern and Context-Aware Models

Modern models are designed for the "information without boundaries" concept, utilizing real-time data to adjust security postures.

Modern and Context-Aware Access Control Models are advanced security approaches designed to provide dynamic, intelligent, and flexible access decisions based on real-time conditions. Unlike traditional models such as MAC, DAC, or RBAC, which rely mainly on fixed rules and predefined permissions, context-aware models consider the situation or environment in which an access request is made. This makes them highly suitable for today's cloud computing systems, mobile applications, IoT environments, and enterprise networks where users access resources from different locations, devices, and conditions.

The main idea of context aware access control is that access to a system should not just depend on who the user's. It should also depend on when the user's trying to access the system and where they are. The system should consider how the user is trying to access it and under what conditions they are trying to access it. This way of doing things makes the system a lot more secure. The system is more secure because it makes decisions based on what's happening at that moment. It does not just make the decisions all the time.

For example a user may be allowed to access the system when they're at the office and it is during working hours.. If the user tries to access the system from a device that is not recognized or from a place that is not familiar they may not be allowed to access it.

One of the important things about context aware models today is that they use information about what is happening right now. This includes things like where the user's what time it is what kind of device they are using how secure the network is and what the user normally does. The system can even consider things like what's happening around the user. By looking at all these things the system can make decisions, about who should be allowed to access it. For example if a user always logs in from Ahmedabad but then they try to log in from a place the system will notice that something is different.

Risk-Based Access Control or RAdAC for short is something a lot of people use to keep their stuff safe. So when someone wants to get into the system it checks how much of a risk that's. If the risk is not very high it is easy to get in.. If the risk is high the system will make them do some extra things to prove who they are like use a special code or something or it might not let them in at all. This way of doing things, which is called Risk-Based Access Control makes everything more secure and easier to use because it finds a balance, between keeping things safe and making things easy to do with Risk-Based Access Control.

Zero Trust Access Control is a model that works on the idea that no one and nothing should be trusted. It always checks who you are and what device you are using. Zero Trust Access Control also divides the network into parts. Only allows access based on rules. This way Zero Trust Access Control makes sure that everything is safe.

- Risk-Based Access Control is a model that checks how risky it is to give someone access to something. It looks at things like who the person's how sensitive the information is. Risk-Based Access Control also checks if they have done anything before. This helps keep your data safe by allowing access if it seems okay.

- Usage-Based Access Control is a model that keeps an eye on how you're using the system. It checks before during and after you access something to make sure you are following the rules. For example Usage-Based Access Control can limit how data you can download.

- Behavior-Based Access Control is a model that watches how you behave when using the system. It looks for anything. This helps catch people who might be trying to cause trouble from the inside. Behavior-Based Access Control is always on the lookout for something that does not seem right.

- Many modern systems use intelligence and machine learning to keep your data safe. These technologies look at how you behave and catch anything that does not seem normal. For example if you suddenly start doing something like downloading a lot of data at night the system can stop you. These systems get better at keeping you safe over time as they learn more about your behavior. Zero Trust Access Control and other models like Risk-Based Access Control and Usage-Based Access Control use these technologies to keep your data safe.

One of the advantages of context-aware models like Zero Trust Access Control and Risk-Based Access Control is that they provide enhanced security through adaptability. Since access decisions are based on real-time conditions it becomes much harder for attackers to misuse stolen credentials. Even if a password is compromised access may still be denied if the login attempt does not match expected behavior or trusted conditions. This significantly reduces the risk of access and cyberattacks. Context-aware models like Usage-Based Access Control and Behavior-Based Access Control are very good at keeping your data safe.

- Another good thing about these systems like Zero Trust Access Control and Behavior-Based Access Control is that they make things easier for users. When the system knows what is going on it can skip some of the security steps when it does not think there is a problem. Legitimate users can get access faster. It is smoother. At the time context-aware systems like Risk-Based Access Control and Usage-Based Access Control increase security checks when they see something suspicious. This balance between keeping things safe and making things easy to use is one of the strengths of access control systems, like context-aware systems.

- Context-aware systems are used in a lot of places, such as cloud services, mobile banking applications, enterprise systems and smart devices. For example online banking systems may only let you do transactions from devices or locations that they trust. Similarly corporate networks may not let you see files unless you are connected through a secure VPN. Context-aware systems are used in these cloud services and mobile banking applications to keep things safe.

- Context-aware systems have some issues. One major issue is that they require a lot of information because these systems have to gather and examine what is happening around them. This makes people concerned about their privacy and who is safeguarding their information.

Context-aware systems are also complicated because they need equipment and skilled people to design and manage the rules.

Context-aware systems need power to process everything immediately and make decisions, which can be a challenge for context-aware systems. Context-aware systems have to be able to do all of this which's a big task, for context-aware systems.

in real time and make decisions, which can be a challenge, for context-aware systems.

2.1 Review of Literature

1. The Protection of Information in Computer Systems

- The paper called The Protection of Information in Computer Systems by Jerome H. Saltzer and Michael D. Schroeder from 1975 is really important for computer security. This paper talks about eight ideas like least privilege and separation of privilege that are still used today to make sure computer systems are secure. The authors think that simple systems are better because they are less likely to have problems. They also think that systems should not let anyone access something unless they are specifically allowed to. The Protection of Information in Computer Systems says that every time someone wants to use a resource the system should check if they are allowed to. The authors of The Protection of Information in Computer Systems also believe in being open about how systems are designed so security does not rely on keeping secrets. They want security to be easy for people to use, which is what they mean by acceptability.

The Protection of Information in Computer Systems has been referenced times in research about access control models and operating systems and cybersecurity frameworks. Many modern standards and best practices, including how to develop software are based on the ideas from The Protection of Information in Computer Systems. Overall The Protection of Information in Computer Systems is an important paper that has shaped how people think about information security, both in theory and, in practice.

2. Role-Based Access Controls

The paper Role-Based Access Controls by David F. Ferraiolo and D. Richard Kuhn, which was published in October 1992 is very important for access control research.

It talks about Role-Based Access Control or Role-Based Access Control for short as a way to control access that is more organized than the old ways like DAC.

The people who wrote the paper think that decisions about who can access something should be based on the roles people have in an organization, not who they're as individuals.

This makes it easier to manage in big organizations with many levels.

Role-Based Access Control is good because it gives people the permissions they need to do their jobs, which is called the principle of least privilege.

The paper also shows how Role-Based Access Control works with the way businesses actually work and the rules they have to follow.

It makes things more secure by controlling who can do what which reduces the risk of someone getting access to something they should not have.

Role-Based Access Control allows roles to be stacked on top of each other so people can get the permissions they need without having to be given each one which makes the system work better and be more flexible.

There are also rules to prevent people from having much power, which helps prevent problems.

So the paper made Role-Based Access Control a leading idea in research and, in world systems used by companies.



3. Access Control: Principles and Practice

The paper Access Control: Principles and Practice that was written in September 1994 by Ravi Sandhu and Pierangela Samarati is really important. It gives us an idea of how access control mechanisms work. The authors talk about models like Discretionary Access Control and Mandatory Access Control. They also explain access matrix frameworks.

Access Control is a part of this paper. The authors look at the bad things about each model when it comes to keeping things secure. They think the access matrix is a way to show how subjects and objects can work together. The paper also talks about how hard it can be to make Discretionary Access Control and Mandatory Access Control work in systems.

The authors say we need models like Role-Based Access Control that're more flexible. Access Control is what they focus on. They help us understand how the ideas they talk about can actually be used in life. Their work makes it clear how different access control policies can be enforced. This paper is special because it compares new ways of doing Access Control in a structured way.

Overall Access Control is a part of what this paper is, about. It helps us understand how Access Control frameworks have changed over time.

4. 2010 Economic Analysis of Role-Based Access Control

The paper called 2010 Economic Analysis of Role-Based Access Control from December 2010 by Alan C. O'Connor and Ross J. Loomis takes a look at how Role-Based Access Control affects the money and work of organizations.

Role-Based Access Control is what the authors are focusing on to see how it helps with costs and managing systems.

They found that Role-Based Access Control really helps cut down on work by making it easier to add or remove users from the system.

This is because Role-Based Access Control makes it easy for the people in charge to give permissions to people based on their roles in the organization.

The people in charge do not have to do the tasks over and over because Role-Based Access Control helps them.

The study also shows that Role-Based Access Control helps with following rules and checking who has access to what in the organization.

This is because Role-Based Access Control has structured rules for who can access what in the organization.

The paper says that Role-Based Access Control helps people get to work and do their jobs better because they get the access quickly and correctly with Role-Based Access Control.

The money saved is looked at in terms of mistakes and less time spent on maintenance with Role-Based Access Control.

The research shows that Role-Based Access Control works well in companies with a lot of users and that Role-Based Access Control is good for security.

It also helps the organization with Role-Based Access Control.

Overall the study gives proof that Role-Based Access Control helps organizations work better and be more efficient, with Role-Based Access Control.

5. Guide to Attribute Based Access Control (ABAC) Definition and Considerations

The guide to Attribute Based Access Control, which was written by Vincent C. Hu and his colleagues is really important. This guide was published by the National Institute of Standards and Technology in 2014. It tells us what Attribute Based Access Control is and how it works. Attribute Based Access Control is a system that decides who can access something based on the attributes of the user the resource and the environment.

The guide says that Attribute Based Access Control is better than the ways of doing things like Role Based Access Control. This is because Attribute Based Access Control can make detailed decisions about who can access something. It does this by using rules that look at attributes at the same time. The people who wrote the guide think that Attribute Based Access Control is very flexible and can be used in complicated systems.

People also discuss some of the problems with using Attribute Based Access Control like getting systems to work together. The guide provides some tips on how to use Attribute Based Access Control, including how to manage rules and integrate systems. One of the things about Attribute Based Access Control is that it can make decisions based on the situation, which makes it more secure.

The guide to Attribute Based Access Control is used by people in universities and companies. It helps them build systems, for controlling who can access what. Overall Attribute Based Access Control is a way to control access and it lets us create more detailed and flexible security rules. Attribute Based Access Control is a tool that helps us keep our systems and data safe.

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations

The NIST Special Publication 800-53 Revision 4 is an important guide. It was published in January 2015 by the Joint Task Force Transformation Initiative. This guide helps people in charge of Federal Information Systems and Organizations manage security and privacy risks.

The National Institute of Standards and Technology published it. It has a list of controls that help with things like access control and incident response.

There are controls for system integrity and risk assessment too. The NIST Special Publication 800-53 Revision 4 organizes these controls into families. This makes it easy for organizations to pick the safeguards.

The NIST Special Publication 800-53 Revision 4 has baseline controls for levels of risk. These levels are low, moderate and high. The publication tells organizations to think about the risks they face.

Then they can choose the controls that're right for them. The NIST Special Publication 800-53 Revision 4 also thinks about privacy. It does not just focus on security.

It helps organizations keep an eye on their system security all the time. The NIST Special Publication 800-53 Revision 4 is used by organizations.

It is not just used by systems. It helps set cybersecurity standards and best practices.

The new version of the NIST Special Publication 800-53 Revision 4 has guidance, on advanced threats. It also talks about cyber risks that are evolving.

7."Assessment of Access Control Systems"

The paper Assessment of Access Control Systems from 2016 by Vincent C. Hu, David F. Ferraiolo and D. Rick Kuhn gives us a way to look at how well access control systems are working. It says that making sure we have security is a big part of what managers of organizations have to do it is not just something for the technical people to worry about.

The authors discuss three parts of access control: access control policies, access control models and access control mechanisms. Access control policies are the rules that determine what we want to achieve with security. Access control models are the plans that help us see if these rules are actually working. Access control mechanisms are the things that enforce these rules when it comes to deciding who can access what.

The paper explains that it is really important for these three parts to work well together so we can have security. If there are gaps between what the access control policies say and what the access control models and access control mechanisms do it can cause problems. The study shows us how to check access control sys-

tems in the world. It reminds us that we need to look at our security practices and make them better all the time.

The work helps us understand that we need to put what we know about access control in theory and what we know about access control, in practice to really protect our systems. The authors of the paper Assessment of Access Control Systems are saying that access control is very important and we need to make sure that access control policies and access control models and access control mechanisms all work together. They want us to know that access control is crucial and we need to get access control policies and access control models and access control mechanisms right so we can have security.

8. Systematic Review of Identity Access Management in Information Security

The paper Systematic Review of Identity Access Management in Information Security by Ishaq Azhar Mohammed is really helpful. It gives us an idea of what Identity and Access Management's all about in today's computers. Identity and Access Management practices are very important because they help keep our information safe.

The paper looks at the Identity and Access Management tools and frameworks that companies use to manage people's digital identities. It talks about how important Identity and Access Management is when we use cloud and mobile devices. This is because the old ways of keeping things secure do not work well in these environments.

Identity and Access Management systems are very good at stopping people from accessing things they should not. They do this by checking who people are and what they can do and by managing their accounts. The study compares ways of doing Identity and Access Management and the technology used. It says what is good and bad about each one.

For example some Identity and Access Management systems are better at handling a lot of people while others are better at working with systems. People are also worried about their privacy when it comes to Identity and Access Management. The paper says that Identity and Access Management is very important for following security rules.

It also looks at ideas like federated identity and single sign-on which're types of Identity and Access Management. The main thing it finds is that if we do Identity and Access Management correctly our computers and information will be much safer. So this study is very useful for understanding why Identity and Access Management is so important for protecting our information. Identity and Access Management is critical, for keeping our identities safe.



9. Security and Privacy Frameworks for Access Control Big Data Systems

The paper Security and Privacy Frameworks for Access Control Big Data Systems by Paolina Centonze looks at the problems we face when we try to control access to Big Data systems. Big Data systems are getting bigger and more complicated. The old ways of controlling access do not work well in these systems. This is because they have to handle a lot of data and they are spread out over computers.

The study looks at the security and privacy risks that come with storing and sharing amounts of data. Paolina Centonze compares frameworks that can help control access to data in systems like Hadoop. The author says we need access control systems that can adapt to situations and scale up to handle large amounts of data.

When we process data across computers it gets harder to keep the data private. The paper talks about using cryptography and rules-based controls to keep the data safe. However this can slow down the system. The study shows that we have to make a choice between keeping the data safe and making the system run quickly.

The paper also says that we need to be able to make decisions about access in systems that are always changing. Security and Privacy Frameworks for Access Control Big Data Systems helps us understand how we need to change the way we control access to Big Data systems. Big Data systems are getting more complex. We need to find new ways to control access to them. This is important for Big Data systems, like Hadoop.

10. A Survey on Empirical Security Analysis of Access-control Systems: A Real-world Perspective

The paper called A Survey on Empirical Security Analysis of Access-control Systems: A Real-world Perspective from December 2022 by Simon Parkinson and Saad Khan gives us a look at how access-control systems are actually used. This paper is about how people evaluate access-control systems.

It looks at the ways people check access-control systems for security problems like when someone has many permissions or when the rules do not make sense. The authors talk about access control models like RBAC, DAC, MAC and ABAC and they show how each one can have different kinds of mistakes. They think it is very important to use data and measurements to check access-control systems rather than just using theories.

The paper also talks about tools and methods that look at logs, policy sets and how systems behave to find security weaknesses. It discusses how hard it is to keep access policies in big systems, where users and roles are always changing and this can lead to people getting too many privileges over time. The survey finds security problems like giving people too many permissions or having rules that conflict with each other. It also looks at how automation and machine learning're used to find strange things in access control configurations.

The authors believe that access policies should be checked all the time not once. They also point out that there is a difference between the way access control models are supposed to work and how they really work in real systems. Overall the paper gives a look at access control security using real evidence and it helps to bridge the gap between what access control models say and how systems really behave. The paper A Survey on Empirical Security Analysis of Access-control Systems: A Real-world Perspective is, about access-control systems. How they are evaluated. The authors Simon Parkinson and Saad Khan wrote this paper to help us understand access-control systems better.

11. Surveys traditional (DAC, MAC) and novel (ABAC, RBAC, PBAC) techniques. It explores adoption in Cloud, Blockchain, IoT

The 2022 survey by Lewis Golightly, Paolo Modesti and Victor Chang gives us a picture of access control models. Access control models are what we use to control who can do what with our data and systems. This survey looks at new ways of doing access control. It talks about Discretionary Access Control and Mandatory Access Control which're old ways of doing things. Then it looks at ways like Role-Based Access Control, Attribute-Based Access Control and Policy-Based Access Control.

These old ways of doing access control were good for a time but they have some problems. They are not very good at handling systems that are always changing. Role-Based Access Control is better because it gives people permissions based on their job. Attribute-Based Access Control and Policy-Based Access Control are more flexible because they look at the situation and make decisions based on that. The people who wrote the survey say that we need access control that can adapt to situations.

The survey also looks at how these access control models work with technologies like Cloud Computing, Blockchain and the Internet of Things. Cloud Computing works with Attribute-Based Access Control because it can make decisions quickly. Blockchain is different because it is decentralized so we need special access control designs. The Internet of Things needs access control that's simple and can understand the context because the devices are all different and do not have a lot of power.

The survey also talks about some problems we have with access control like getting all the models to work together. Sometimes access control can slow down the system. It can be hard to make policies that work for

everyone.. The survey says that people are starting to use a combination of different access control models to solve these problems. So the survey gives us an idea of how access control has changed over time and how it will keep changing as our systems get more complicated. Access control models, like Discretionary Access Control, Mandatory Access Control, Role-Based Access Control, Attribute-Based Access Control and Policy-Based Access Control are all important. We need to understand how they work together.

12. A Systematic Review of Access Control Models: Background, Existing Research, and Challenges"

The 2023 systematic review A Systematic Review of Access Control Models: Background, Existing Research and Challenges by Jose Barata gives us a picture of how access control has changed over time in different areas. It starts by saying that the information a company has is very important so we need to have access control to keep it safe and make sure the company keeps running smoothly.

This study looks at access control models like DAC, MAC and RBAC. It talks about why they were important in the past and how they helped create the ideas we use for access control today. The study also looks at models like ABAC and other ways of combining different models to work with modern systems that are spread out over many places. The author says that as systems get more complicated we need access control that can change and understand the context of what's happening.

One of the things about this paper is that it looks at access control from many different viewpoints, including cloud computing, IoT, big data and systems used by companies. It finds that many studies only look at one type of access control model at a time which means we do not have an understanding of how they all work together. This review fills that gap by comparing the bad points of different models and how well they work in different situations. The review of access control models, by Jose Barata helps us understand access control better by looking at how different access control models work in areas.

13. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions

The 2023 survey Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions by Kaushik takes a look at access control mechanisms for Internet of Things (IoT) environments. This survey checks out existing Internet of Things authorization architectures. It shows how traditional models do not work well in settings that are very spread out and have resources.

The study says it is important to have policies for access control. This means access decisions can change based on things like the state of the device, where it's the network conditions. The study looks at models like Role-Based Access Control and Attribute-Based Access Control. It says these models are used for Internet of Things. They still have problems with scalability and responding in real time. The paper says the big difference in Internet of Things devices is a problem. This is because systems have to deal with everything from sensors to complicated edge devices.

Internet of Things devices have some limitations. They have limited power to process information they need to be energy efficient. They are not always connected to the internet. All these things make it hard to enforce access control policies. The survey says we need access control frameworks that're simple and can adapt to changing situations. These frameworks must work well in environments with resources. The survey also talks about ways of doing things, such as enforcing policies in a decentralized way and using machine learning to make decisions about access control, for Internet of Things.

14. A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond

The 2023 review A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control and Beyond by Habeeb Omotunde and Maryam Ahmed is really about looking at how database systems keep our information safe. This review checks out how database systems use layers of security to protect important information from people who should not have access to it and from attacks.

The study looks at things like how people log in to database systems. It talks about how we do not use simple passwords anymore. Now we use things like -factor authentication and adaptive identity verification to make sure only the right people get in. The study also looks at how database systems control who can do what. It explains how things like RBAC and ABAC work. These are like rules that say who can do what in the database system.

The authors of the review also spent a lot of time talking about how encryption keeps our data safe. Encryption is like a code that keeps our data safe when it is sitting still and when it is moving around. The authors say that encryption is important because even if someone gets into the database system who should not be there the data will still be safe because it is encrypted. The review also talks about challenges that come up when we use cloud and distributed systems. In these systems data is often in places at the same time. This makes it harder to keep the data safe. The 2023 review, by Habeeb Omotunde and Maryam Ahmed looks at how database systems deal with these challenges.

15. From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational

The 2024 study From Theory to Practice: Implementing Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Settings by Yewande Alice Marquis looks at how Role-Based Access Control works in the real world. It checks how Role-Based Access Control does in keeping organizations safe from people inside the organization who might cause problems.

This paper talks about the difference between what Role-Based Access Control should be and how it is actually used in organizations. It says that in organizations with good security there is still a big risk from insiders who might misuse their privileges get into data they should not have or abuse their credentials. The study looks at Role-Based Access Control as a way to limit these risks by making sure people only have access to what they need to do their jobs.

The author of the study looked at different types of organizations and found that Role-Based Access Control really does help stop people from getting into things they should not. It also helps stop data breaches. The study says that to make Role-Based Access Control work organizations need to have rules about what each role can do check what people have access to on a regular basis and make sure that no one person has too much power. This makes Role-Based Access Control a way to keep organizations safe, from insider threats.

16. A systematic review on blockchain-based access control systems in cloud environment

The 2024 study A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environment by Aarti Punia and colleagues looks at how blockchain technology's being used in access control for cloud computing systems.

This study looks at a lot of existing research. Finds twelve major ways that blockchain is being used for access control. These methods try to make things more secure by spreading out the decisions about who can access what and making it clearer who has access to what. One good thing about these methods is that they get rid of points of failure, which can be a problem with traditional access control systems that are controlled from one place.

The paper explains how the blockchain ledger, which cannot be changed can be used to keep track of who's accessing what so we can see what is happening and make sure everything is working correctly in cloud environments. It also talks about contracts, which can automatically enforce the rules about who can access what without needing a central authority. This helps build trust among the people and systems involved in cloud computing especially when there are clouds and hybrid clouds involved.

The study also finds some problems, like the fact that blockchain can be slow and use a lot of computer power and it can take a long time to verify permissions. It can also be hard to integrate blockchain with existing cloud systems. The authors say that while blockchain is good for making things more transparent and trustworthy it might not be the choice for making quick decisions about access in big systems that need to happen in real time because blockchain technology may not be efficient enough for real time access decisions, in large-scale cloud computing systems and blockchain technology is still being developed.

17. Security Practices in Database Access: A Technical Review

The 2025 technical review Security Practices in Database Access by Madhusudana Naidu Gundapaneni looks at ways to keep database systems safe in big companies. It talks about how new threats are making companies use better and more complicated security systems.

One important thing the paper looks at is controlling who can access the database. This means setting up rules for parts of the database so that only people who need to see certain information can see it. This helps keep information safe by making sure people can only see what they need to do their job.

The study also looks at ways to encrypt data like Always On Encryption. This means that data is always encrypted, whether it is being used or just stored without anyone having to do anything. This keeps the data secret. Reduces the risk of it being stolen or lost when it is being used or stored.

Madhusudana Naidu Gundapaneni says that using access control and encryption together makes the database more secure. The paper also talks about the problems that can happen like it slowing down the system making it hard to manage keys and working with systems. Security Practices in Database Access is about keeping database systems safe and secure.

The Security Practices in Database Access review is important because it helps companies keep their database systems safe. Database systems are very important for companies so they need to be kept safe from threats. The Security Practices, in Database Access review helps companies do this by showing them ways to keep their database systems secure.

18. Least Privilege and Access Control Principles in Enterprise Network Security: A Comparative Analysis of the United States and Global Practices

The 2025 study Least Privilege and Access Control Principles in Enterprise Network Security: A Comparative Analysis of the United States and Global Practices by Taiwo Justice Olorunlana compares how companies in the United States and other countries follow the Principle of Least Privilege. This principle is about giving users and systems the permissions they need to do their jobs.

* It is a security rule.

* The study looks at company security systems, especially those that follow Zero Trust rules.

The study explains that the Principle of Least Privilege helps keep companies by limiting what users and systems can do. This makes it harder for attackers to cause damage. The study finds that while many companies around the world know about this principle some are better at following it than others.

The study also looks at how the Principle of Least Privilege works with Zero Trust systems. In these systems nothing is. Everything is checked all the time. The author says that Zero Trust systems make it harder for attackers to get in by checking who is trying to get in and what they want to do.

The study compares how companies in the United States and other countries follow the Principle of Least Privilege.

* Companies in the United States are better at using automated systems to control who can get in and monitoring what is happening.

* Some companies in countries have trouble, with old systems, inconsistent policies and not enough automation.

The Principle of Least Privilege is helpful.

The Principle of Least Privilege helps companies.

Companies use the Principle of Least Privilege.

19. High Availability for Identity Access Management (IAM)

The authors, Srinivasulu Harshavardhan Kendyala, Archit Joshi, Indra Reddy Mallela, Dr. Satendra Pal Singh, Shalu Jain and Om Goel talk about this in the literature. The paper was published around 2023. The title of the paper is High Availability Strategies For Identity Access Management Systems In Large Enterprises.

This source says that Identity Access Management systems need to be available all the time so people can keep using them without any problems. The authors discuss some techniques like having extra servers and data centers in different places balancing the load so the system does not get too busy and having a plan, in place to quickly recover when something goes wrong.

The authors of High Availability Strategies For Identity Access Management Systems In Large Enterprises think that using layers to keep the system available makes it more secure. This means that even if something unexpected happens people can still access what they need. High Availability Strategies For Identity Access Management Systems In Large Enterprises also looks at how Artificial Intelligence and machine learning can help predict when something might go wrong and make sure the load is spread out evenly to keep the system running.

20. Intelligent RBAC in Multi-Domain Environments

• Authors: Rubina Ghazal, Ahmad Kamran Malik, Nauman Qadeer, Basit Raza, Ahmad Raza Shahid and Hani Alquhayz.

• Published Date: January 9 2020.

• Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in -Domain Environments.

• Review: This paper talks about the problems with the way of doing Role-Based Access Control. Role-Based Access Control has a time working in environments with many different parts, like the cloud. The authors of this paper Rubina Ghazal, Ahmad Kamran Malik, Nauman Qadeer, Basit Raza, Ahmad Raza Shahid and Hani Alquhayz suggest a way of doing Role-Based Access Control called Intelligent Role-Based Access Control. Intelligent Role-Based Access Control uses business roles and intelligent agents. One of the things about Intelligent Role-Based Access Control is that it uses special words to find important roles in big texts. It uses something called WordNet and deep neural networks to do this. This helps people work together in business environments because it can automatically assign roles and update rules. The Intelligent Role-Based Access Control model is really good for environments, with different parts.

21. Intelligent Attribute-Based Access Control (ABAC) for IaaS

- Author: Shadha Mohamed Sulaiyam Al-Amri.
- Published Date: September 18 2017.
- IaaS-cloud Security Enhancement: An Intelligent Attribute-Based Access Control Model and Implementation (Doctoral Thesis).
- Review: This study looks at how to make IaaS cloud platforms more secure. It uses an Attribute-Based Access Control model called ABACsh. What is different about ABACsh is that it knows about the context and follows the Separation of Duty security rule. The study uses a kind of logic to figure out who can access what and when. It also shows how this can be done using agents on the OpenStack platform. The results show that Attribute-Based Access Control is better for environments that are always changing because it is more flexible and can handle more users than Role-Based Access Control. IaaS cloud platforms need a security system, like Attribute-Based Access Control to keep user data safe.

22. Blockchain-Based Access Control for IoT

- Authors are Peng Zhai, Jingsha He and Nafei Zhu.
- The paper was published on April 6 2022.
- The title of the paper is Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing.
- This paper is about using blockchain technology with something called ABAC to make the Internet of Things or Internet of Things secure in smart factories. The Internet of Things is made safer by using blockchain technology because it does not have a point of failure like other systems do. The people who wrote this paper used something called contracts on Hyperledger Fabric to make decisions about who can access the Internet of Things. This way of doing things gives us a lot of control over what's happening and it is very secure. The Internet of Things devices can be controlled in a detailed way and all of the interactions are recorded, which makes the data in the factory safer. This is, about the Internet of Things and how blockchain technology can help make it more secure

23. Security Policies and Techniques in BYOD Environments

- The authors of this paper are Aljuaid Turkea Ayedh M, Ainuddin Wahid Abdul Wahab and Mohd Yamani Idna Idris.
- This paper was published on July 10 2023.
- The title of this paper is Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions.
- This review talks about BYOD security policies and it breaks them down into three parts: the first part is about how to get devices ready to use at work the second part is about how to keep information safe and private and the third part's about managing risks.

The review looks at techniques to see how well they meet seven important requirements for keeping information private such as keeping information secret making sure it is correct making sure it is available when needed and detecting attacks.

The review also talks about technologies like Software-Defined Networking using body features to verify identity and using machine learning to detect threats.

It points out that many techniques do a job of verifying identities and keeping information secret but there is a need for more research, on ways to make sure that information cannot be denied or altered and to protect peoples privacy specifically in BYOD security policies and BYOD environment.

24. Physical Access Control Using RFID and ALPR

- Authors: M. Mohandes, M. Deriche H. Ahmadi, M. Kousa and A. Balghonaim.
- Published Date: April 16 2016.
- An Intelligent System for Vehicle Access Control using RFID and ALPR Technologies.
- Review: This paper is about a system that helps control vehicle access. It is made for crowded areas like Makkah during Hajj. The system uses RFID technology for vehicles that are allowed to enter. It also uses Automatic License Plate Recognition to find vehicles that are not allowed. Vehicles that are allowed have a RFID tag with their schedule and route. If a vehicle does not have this tag cameras take a picture of the license plate. The system reads the Arabic characters. The Vehicle Access Control system is a way to manage a lot of vehicles in crowded areas. It is also cost-effective. The Vehicle Access Control system is very useful, for events. The RFID and ALPR Technologies work together to make the Vehicle Access Control system work well.

25. Semantic Role Mining for Smart City Applications

- Authors: Rubina Ghazal, Ahmad Kamran Malik, Basit Raza, Nauman Qadeer, Nafees Qamar, and Sajal Bhatia.
- Published Date: June 22, 2021.
- Title: Agent-Based Semantic Role Mining for Intelligent Access Control in Multi-Domain Collaborative Applications of Smart Cities.
- Review: This work focuses on the challenge of collaborative access control in smart cities, where users frequently move between multiple domains. Building on the I-RBAC model, it introduces an agent-based semantic role mining technique. It uses word embedding and bidirectional LSTM neural networks to automatically derive organizational ontologies from textual policies. This allow agents to identify unified business roles and permissions intelligently, ensuring that security policies are aligned with actual organizational needs and changing contexts in a smart city environment

3. Research Objectives:

The main goal of this research is to figure out the ways for private security companies to control who has access to important information. We want to make sure that this information is safe, private and available when it is needed. To do this we will look at what other researchers have found and what the industry thinks is best. Here are the specific things we want to do:

1. Find and Group Security Threats: We need to make a list of all the security threats that private companies face threats from inside the company. We know that about half of the times when someone misuses their access it is someone who works for the company.
2. Look at and Compare Access Control Models: We will compare the ways of controlling access, like Role-Based Access Control and Discretionary Access Control with new ways like Attribute-Based Access Control and using Blockchain.

3. Look at the Challenges of Implementing Access Control: We want to know what problems companies have when they try to put these systems in place. For example Role-Based Access Control can get very complicated. Attribute-Based Access Control can be expensive to run.

4. See How Access Control Affects the Bottom Line: We need to find out if using advanced access control systems is cost-effective. We will look at how these systems can make it easier to give people access to what they need reduce costs and make the company more productive.

5. Create a Plan for Best Practices: Based on the idea that people should only have access to what they need and that we should not trust anyone completely we will come up with a set of recommendations for private security companies to follow. These recommendations will be tailored to the needs and rules of the private security sector and to access control systems and we will focus on access control systems throughout this process because access control systems are what this research is all, about and we want to make sure that access control systems are used in the best way possible.

4.Research Gaps

There are studies on information security but information security still has some big problems that this research wants to fix.

- Information security lacks real world testing: A lot of the research on ways to control access, especially in the Internet of Things and Blockchain areas is still just ideas or designs. There are not studies that use real world data to see how things really work instead of just using made up examples.
- Information security does not do enough to stop threats from inside: Even though access control systems are supposed to stop people from getting in without permission there is not research on how to use role based access control and attribute based access control to stop threats from inside the system.
- Information security needs a way to work with different systems: The problem is that there is no one way to control access that works for all the different systems, like the Internet of Things. Researchers often do not provide a way to combine models so they can work together.
- Information security lacks tests: There is no standard way to test information security systems and it is often hard to get the data and techniques used in tests so we can compare them.
- Information security often forgets about people: Researchers often focus on making systems strong. They forget about how easy they are to use for the people who have to run them and the people who use them. This can lead to mistakes that make the system not secure.
- Information security needs to look at policies in a way: Other studies have not looked at how to keep security and privacy safe by using a system with three levels of policies especially, for mobile devices and when people use their own devices for work

5.Research Methodology

To make sure the results are reliable and accurate this research uses an organized method that combines qualitative and quantitative approaches.

1. Systematic Literature Review (SLR)

The base of the project is a review of existing scholarly articles, conference papers and federal guidelines like NIST SP 800-53.

* Search Strategy: We use databases like IEEE Xplore, Scopus, ACM Digital Library and Google Scholar with Boolean operators like "Access Control" AND "Private Organization".

* Inclusion/Exclusion Criteria: We only consider peer-reviewed publications from the 10-20 years to include recent technological advancements like Machine Learning and Blockchain.

* Data Synthesis: We organize the data we find to identify themes like adaptive security and context-awareness.

2. Quantitative Empirical Analysis

When it is applicable the study uses methods to measure how well access control strategies work:

* Survey Instrument: We give a structured questionnaire to identity management professionals like IT managers and security architects to get data on business drivers and implementation challenges.

* Statistical Validation: The research uses Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM) to analyze the relationships between the effectiveness of Access Control Systems and the reduction of insider threats.

* Performance Metrics: We evaluate the effectiveness of technologies using established benchmarks like response time, throughput and detection rates for activities.

3. Qualitative Comparative Analysis (QCA)

We look at governance frameworks across areas with a qualitative approach:

* Document Analysis: We carefully analyze requirements from first-order sources like the GDPR, HIPAA and ISO/IEC 27001.

* Thematic Synthesis: We code the findings into themes like "identity as the perimeter" and "privacy-driven access limitations" to identify patterns of similarity and difference in global best practices.

4. Economic Impact Modeling

Following the RTI International approach the research may include a benefit-cost analysis to calculate the savings from switching from manual Access Control Lists to automated role-based systems. This involves calculating the time and money saved for administrators and reducing downtime, for employees by using Access Control Systems.



7 Conclusion

The security situation we are in today is changing fast because of how much we are using digital stuff and physical spaces and this is happening because of things like moving to the cloud using Internet of Things devices and working from home. As companies rely more on databases and important information managing who can access what also known as Identity and Access Management has become super important for keeping our assets safe and secure.

One big thing we found out is that the way we control access to things is changing. The old ways of doing it like Discretionary Access Control and Mandatory Access Control were good back in the day. They do not work well with the way we do things now because they are not flexible or scalable. Then we got Role-Based Access Control, which's better because it gives people access based on their job not who they are and this makes things easier to manage.. Even this way of doing things has problems like having too many roles and not being able to handle really specific situations in real-time especially with Internet of Things and cloud systems.

So what is going to happen in the future is that we will be using Attribute-Based Access Control and Zero Trust Architecture. Attribute-Based Access Control is good because it looks at a lot of things like the user, the resource and the environment to decide who can access what. And Zero Trust is like having a rule that

says we never trust anyone so we always check who they are, no matter if they are inside or outside our network. Also using Artificial Intelligence and Machine Learning is making these systems better at finding problems and stopping threats in real-time.

In the end our research says that for companies that want to be really secure the best way to do it is to use a system that has layers, like Role-Based Access Control for the organization Attribute-Based Access Control for its flexibility and Zero Trust Architecture, for its strict verification and always following the Principle of Least Privilege, which means giving people only the access they need to do their job.

Recommendations.

1. We need to use a Zero Trust Architecture: this means we do not trust anyone to access our network without checking who they are first. We need to check every single access request all the time. We also need to use micro-segmentation to stop people from moving around the network once they're in.
2. We have to be very strict about who can do what: every user and every system should only be able to do the things that they need to do to get their job done. This way we can reduce the risk of someone doing something on purpose or by accident.
3. We need to use ways to check who people are: we should not just use passwords anymore. We should use things like codes on our phones or biometrics like fingerprints or face recognition. These are much harder to fake.
4. We should use computers to watch what people are doing: we can use computer programs to look at what people are doing on the network and catch anyone who is doing something strange. This can help us stop people from getting in.
5. We need to check who can do what on a basis: we should look at what everyone can do on the network and make sure they still need to be able to do those things. If someone changes jobs or leaves the company we need to take their access right away.
6. We need to make sure our systems can grow: when we get hardware or software we need to make sure it can work with what we already have. We also need to make sure it can handle people and devices in the future like special sensors or cloud computers.

The research says that the best way for private security companies to keep their networks safe is to use a combination of methods. We need to use Role-Based Access Control to organize our company, Attribute-Based Access Control to make decisions. Zero Trust Architecture to always check who people are.. We need to always follow the Principle of Least Privilege to make sure people can only do what they need to do. Zero Trust and the Principle of Least Privilege are very important, for security organizations.

8.Suggestions for Future Implementation

Testing with Real-Life Examples: Future studies should test models like Blockchain-based access control using real-life data instead of just theory. This will help understand how they work in practice.

- Blockchain for Access Control: Using Blockchain and Smart Contracts can help manage access and authorization. This approach removes points of failure and provides a permanent record of all actions.
- Easy-to-Use Design: We need to make access control systems easier to use without compromising security. This means finding ways to reduce the workload on administrators and users making it less likely for mistakes to happen.
- Edge Computing for Faster Access: Research how Edge AI can help make access decisions by processing them closer to where they are needed such as with smart cameras or sensors. This can reduce the need for connectivity.

- Combining Access Control Methods: Develop frameworks that combine access control methods like RBAC for organizations and ABAC, for detailed control. This can create a solution that offers the best of both worlds.

9. References

1. Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. (Design principles: Least privilege, separation of privilege).
2. Ferraiolo, D. F., & Kuhn, D. R. (1992). Role-Based Access Controls. (Introduction of RBAC).
3. Sandhu, R., & Samarati, P. (1994). Access Control: Principles and Practice. (Theoretical foundation of DAC, MAC, and Access Matrix).
4. O'Connor, A. C., & Loomis, R. J. (2010). Economic Analysis of Role-Based Access Control. (Financial benefits of RBAC).
5. Hu, V. C., et al. (2014). Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (NIST SP 800-162).
6. National Institute of Standards and Technology. (2015). NIST Special Publication 800-53 Revision 4. (Security and privacy controls).
7. Hu, V. C., Ferraiolo, D. F., & Kuhn, D. R. (2016). Assessment of Access Control Systems. (Policy, model, and mechanism layers).
8. Mohammed, I. A. (2017). Systematic Review of Identity Access Management in Information Security..
9. Centonze, P. (2019). Security and Privacy Frameworks for Access Control Big Data Systems..
10. Parkinson, S., & Khan, S. (2022). A Survey on Empirical Security Analysis of Access-control Systems..
11. Golightly, L., Modesti, P., & Chang, V. (2022). Survey on traditional (DAC, MAC) and novel (ABAC, RBAC, PBAC) techniques..
12. Barata, J. (2023). A Systematic Review of Access Control Models: Background, Existing Research, and Challenges..
13. Kaushik. (2023). Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions..
14. Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems..
15. Marquis, Y. A. (2024). From Theory to Practice: Implementing Effective RBAC Strategies to Mitigate Insider Risks..
16. Punia, A., et al. (2024). A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environment..
17. Gundapaneni, M. N. (2025). Security Practices in Database Access: A Technical Review..
18. Olorunlana, T. J. (2025). Least Privilege and Access Control Principles in Enterprise Network Security..
19. Kendyala, S. H., et al. (c. 2023). High Availability Strategies For Identity Access Management Systems In Large Enterprises..
20. Ghazal, R., et al. (2020). Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles..

21. Al-Amri, S. M. S. (2017). IaaS-cloud Security Enhancement: An Intelligent Attribute-Based Access Control Model..
22. Zhai, P., He, J., & Zhu, N. (2022). Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing..
23. Aljuaid, T. A. M., et al. (2023). Systematic Literature Review on Security Access Control Policies in a BYOD Environment..
24. Mohandes, M., et al. (2016). An Intelligent System for Vehicle Access Control using RFID and ALPR Technologies..
25. Ghazal, R., et al. (2021). Agent-Based Semantic Role Mining for Intelligent Access Control in Smart Cities.
26. <https://scholar.google.com/>
27. <https://www.researchgate.net/>
28. <https://notebooklm.google.com/notebook/a3142d94-87b7-4f45-916a-4b6de36e9632>
29. <https://scholar.google.com/intl/en/scholar/publishers.html>

