

Original Article

A Novel Framework for Dynamic Access Control in Computer Networks: Analysis and Implementation

Alshawwa Izzeddin A O¹, Nor Adnan Bin Yahaya², Ahmed Y. Mahmoud³

^{1,2}University Malaysia of Computer Science and Engineering (UNIMY), Malaysia

³Faculty of Engineering and Information Technology, Al-Azhar University, Gaza, Palestine

³Corresponding Author : ahmed@alazhar.edu.ps

Received: 03 February 2026

Revised: 22 June 2026

Accepted: 21 August 2026

Published: 30 September 2026

Abstract - The proliferation of distributed environments and remote computing has shown the urgent need for secure and dependable access control for computer networks. This paper proposes a novel security model and develops a framework to prevent unauthorized data access. The framework leverages the access control principles of the Bell-LaPadula model and fortifies data confidentiality using the Advanced Encryption Standard (AES) algorithm. The proposed model determines the structured access control according to the organization's roles and enforces it through a policy-based security mechanism. The experiment was performed on an emulated institutional network where the user privileges were dynamically managed. The findings show that the model provides robust protection against unauthorized access and guarantees secure data flow between networked systems.

Keywords - Access control, Bell-LaPadula, AES, Network security, Authentication, Remote access.

1. Introduction

Access control policies play a critical role in ensuring that modern computer networks and distributed systems are secure. These policies govern user privileges, separate the duties and mitigate the chances of unauthorized access [1]. In legacy systems like industrial systems, there has been a long history of restricting access to various systems because of the complexity of operations and critical dependencies on infrastructure [2]. Nevertheless, the fast development of digital systems has posed new challenges, which are not limited to fixed and isolated environments.

Access control policies play a critical role in ensuring that modern computer networks and distributed systems are secure. These policies govern user privileges, enforce the separation of duties, and mitigate the risk of unauthorized access [1]. In legacy systems, such as industrial environments, there is a long history of restricting access due to operational complexity and critical infrastructure dependencies [2]. Nevertheless, the rapid development of digital systems has posed new challenges that extend beyond fixed and isolated environments.

Advanced technologies, including the Internet of Things and artificial intelligence, have been introduced into the old infrastructures, resulting in a significant complexity of the systems. These mixed environments are made up of legacy systems with the new distributed components, which causes

interoperability issues and increased attack surfaces [3]. This has led to the fact that traditional, non-dynamically controlled access control measures are inadequate to cope with the dynamism of the current networks [4, 5].

Simultaneously, the extensive use of IoT in different areas like healthcare, smart cities, and industrial automation has brought a very heterogeneous ecosystem of devices. These devices vary in terms of functionality, security level, and communication. This variety gives rise to a living and frequently not foreseeable network environment where the customary models of authentication and authorisation cannot perform suitably. Thus, insider threats, data breaches, and unauthorized access are now more difficult to detect and prevent [6, 7].

These issues have been attempted to be addressed by available access control schemes such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). RBAC is simple to manage as it distributes permissions basing on the defined roles; however, it lacks flexibility in a dynamic environment [8, 9]. ABAC brings in the flexibility but introduces more contextual qualities; however, it introduces more complexity and performance load to systems, especially real-time systems [10]. In addition, the majority of the current strategies consider access control and data protection in isolation, and this has created a security loophole that can be exploited [11].



Despite all these innovations, the current structures have major weaknesses regarding dynamic, context-sensitive and security-sensitive environments. The integrated solutions that combine hierarchical access control, contextual validation and strong data protection in a single model are absent. Specifically, the available systems tend not to have a tall enough decision-making process in place to allow a combination of user clearance, device identity and a time limit to be enforced simultaneously, and offer confidentiality of data through the use of encryption.

To overcome these shortcomings, the current paper suggests a cohesive and context-sensitive access control model that combines the Bell-LaPadula security model with Advanced Encryption Standard (AES) encryption and dynamic context validation. The proposed model will use the access decisions based on user role, security clearance, device identity, and access time restrictions. It also includes multi-factor authentication that involves both the use of biometrics and credentials to enhance the verification of identities.

The framework is rolled out and tested in a simulated enterprise environment to assess the efficacy of the proposed framework in preventing unauthorised access, secure flow of data, and improving accuracy in enforcing policies. The results show that a hierarchical security model that is combined with encryption and contextual constraints can significantly enhance the resistance and flexibility of access control mechanisms in today's network systems.

2. Related Work

One of the key elements of securing computer networks and distributed systems of modern times is access control. It has grown in importance with the growth of cloud computing, remote access, and Internet of Things (IoT) environments. Several models of access control have been created: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). These are just some of the reasons why an initial implementation, such as DAC and MAC, is limited in its own scalability and adaptability in dynamic and context-aware environments [12]. This has led to the development of more flexible access control systems, which could be applied in modern distributed systems. Role-Based Access Control (RBAC), owing to its high ability to grant access permissions according to the predefined roles, has gained a lot of popularity in enterprise systems because it can simplify the aspect of access control [13]. The administration of this model is less complex, and it promotes scalability in a structured environment. RBAC is, however, not scalable to a dynamic system where the decision on access has to be determined in the light of several contextual factors that involve time, identity of the device and user behaviour. As a result, it will not be as effective in an environment where real-time and dynamic implementation of policies is needed.

To overcome these deficiencies, a more context-sensitive and flexible model known as the Attribute-Based Access Control (ABAC) was suggested. The decision-making in ABAC is determined based on some of the features, including the identity of the user, the type of device, location and time of access [14]. This design is flexible and supports fine-grained access control, particularly in large-scale and distributed applications such as IoT systems. However, ABAC further complicates policy definition and evaluation and may introduce performance overhead and difficulties in implementing policies in real-time.

More recent researchers have examined how machine learning techniques can be used together with access control systems to enable adaptive and behaviour-sensitive decisions. These strategies are used to examine the user activity patterns and system interactions to identify anomalies and dynamically change access permissions. Experiment in [15] demonstrates that the standard access control system can be enhanced with the help of behaviour-based analytics to identify the suspicious behaviours and reduce the risk of insider attacks.

On a similar note, Shawa [3] introduced a behaviour-aware RBAC model that takes advantage of supervised learning to categorise users according to their interaction patterns in IoT settings. The model enables the access permissions to be dynamically tied in during the running of the system to optimize the system to counter any abnormal behaviour and potential privilege escalation attacks. This combination of machine learning and access control is a major leap towards intelligent and responsive security systems.

Although these are the benefits, access control models based on machine learning have a number of challenges. They include a high level of computation, the need for large and high-quality data, and interpretability of the decision-making process. Besides, they can be degraded during live scenarios where decisions on accessing data in real-time are required.

In contemporary distributed systems, encryption is essential in ensuring data access security. Conventional access control systems specify access to resources, yet do not necessarily ensure the integrity of data transmitted or stored. To overcome this drawback, several studies have combined encryption methods and access control policies to implement secure data sharing. As an illustration, hierarchical encryption algorithms together with Advanced Encryption Standard (AES) have been employed to tie user roles to decryption keys so that only a given user can decrypt confidential data [16].

Moreover, policy-based encryptions have been suggested to ensure effective data transfer in IoT settings. These techniques provide cryptographic access control where access keys are linked to access policies and, therefore, enhance the confidentiality and integrity of communication across untrusted networks [17].

In spite of these developments, encryption-based access control models tend to be independent of contextual and behavioural factors. They are not necessarily dynamic conditions, which are essential in the nowadays adaptive systems, such as the device identity, access time, or user behaviour. Consequently, the use of encryption mechanisms alone is not enough to have context-aware and comprehensive access control.

The idea behind Zero Trust Architecture is a relatively new one with respect to the access control of decentralization and cloud-computing systems. The model does not consider the implicit trust concept, but continuously questions users, devices and access requests regardless of their location inside or outside the network perimeter [18]. Dynamic assessment of access decisions based on identity, device posture and contextual information in Zero Trust systems enhances security in very dynamic environments.

All the challenges of Zero Trust come with practical challenges. Continuous verification implies that verifying and evaluating policy should be carried out continuously, which can increase computational burden and can affect system performance. In addition, many changes to existing infrastructure and access control policies will be required to implement Zero Trust architectures, making it more difficult to adopt Zero Trust in a legacy infrastructure or resource-limited environments.

Recently, Blockchain technology has been considered as an access control mechanism in decentralized distributed systems that is decentralized. Using smart contracts, access control models based on blockchain can be used to apply access policies in a transparent and tamper-proof manner, without the use of a central authority. Such systems could be applied to both the IoT and cloud environments, as they enhance the trust, auditability and integrity of the data, and thus play a crucial role in the overall enhancement of trust, auditability, and data integrity [19].

However, there are also certain limitations when it comes to the implementation of blockchain solutions. These are high computation incurred, longer latency with the use of consensus mechanisms, and scalability in large-scale deployments. Therefore, their real-time and resource-constrained applicability is still restricted.

The development of authentication has contributed greatly to access control systems. This multi-factor authentication has been used more and more to replace the traditional password-based authentication, which is based on knowledge, token and biometric authentication. The practices are used to increase the security of the system and reduce the possibility of illegal access to the system, particularly in mobile and distributed systems, where devices are vulnerable to physical and network attacks, as shown in Figure 2 [20].

Along with the enhancement of authentication, recent studies have paid attention to the device-aware access control mechanisms. These approaches rely on the identity of the device, its network activity and other physical characteristics such as MAC addresses, and issue permissions based on those attributes. A hybrid model can enhance security because it can detect and quarantine unknown or suspicious devices in a distributed system [21].

In addition, the complexity of cyber threats has given rise to complex access control systems that have the capability to identify misconfigurations and policy violations. Most recent publications have proposed dynamic and encryption-sensitive models that track how access is made in real time and find that deviations from the access rules are anomalies in the policy implementation. These approaches can be used for proactive defense against access intrusion and improve the security setup stability [22].

Reading the literature, there is a clear trend towards integrating multiple security aspects like authentication, behavioral analysis, encryption and device-aware policies. Nevertheless, the current strategies and strategies tend to deal with them separately and not in the context of a single system. This constraint has resulted in an integrated model that integrates such mechanisms to offer adaptive and comprehensive access control in modern network environments.

Although research has been done extensively on access control mechanisms, there are still a number of limitations that are apparent in existing mechanisms. Traditional approaches such as RBAC and ABAC provide a structured, flexible policy solution, but fail to support the dynamic and context-dependent decision-making requirements of the modern distributed world. The newest features that include machine learning, encryption and device-aware features have yielded greater flexibility and security, but these are generally used separately as standalone features rather than as a cohesive solution.

Additionally, new paradigms like Zero Trust and blockchain-based access control have even stronger security assurances, such as continuous verification and decentralized policy enforcement. Although these advantages, these models have practical limitations in terms of complexity, scalability and overhead of performance, limiting their use to real-time and resource-limited systems.

Moreover, most current solutions fail to combine the various dimensions of security, such as hierarchical access control, contextual constraints, such as device identity and access time, behavioral analysis and data confidentiality in one coherent model. The result of this disintegration is a lack of uniformity in the implementation of security and the potential for inconsistent policies and for unauthorised access

to occur. This is why an integrated and context-sensitive control system based on the combination of hierarchical security policies, dynamic contextual checks, and strong

encryption systems is obviously needed. A framework needs to be robust, scalable, efficient and provide real-time decision making in today's network environment.

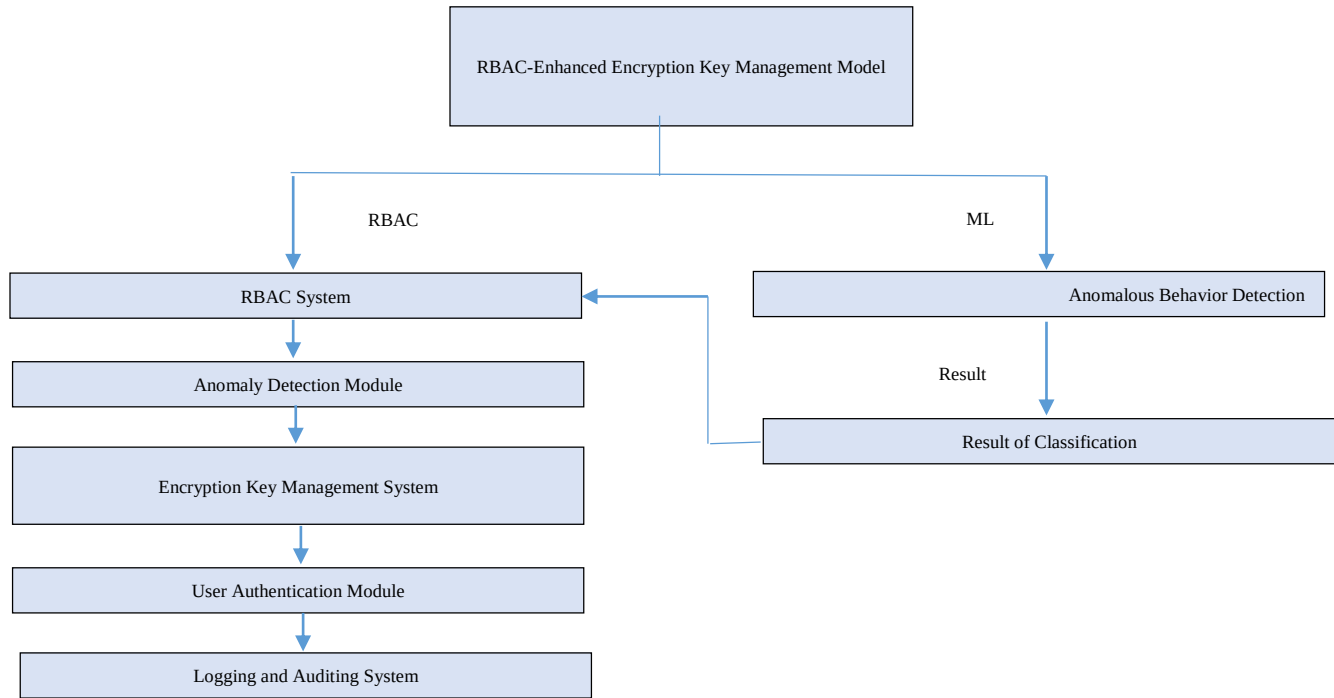


Fig. 1 RBAC-enhanced encryption

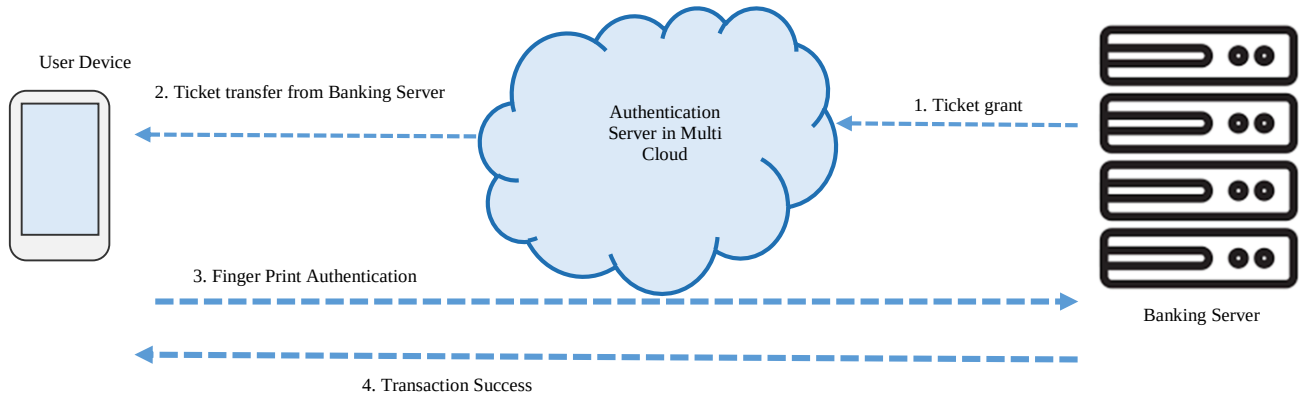


Fig. 2 Message flow diagram- shielded transaction phase [19]

3. Proposed Access Control Framework

The design and implementation of the proposed access control framework are presented in this section. The model aims to allow for secure and dynamic access control in a distributed environment by integrating hierarchical security policies, contextual validation and encryption. The model is a combination of the Bell-LaPadula model of multi-level access control and the Advanced Encryption Standard (AES) of data confidentiality. The system architecture is such that it is able to support many layers of security levels, such as user authentication, role-based authorization, device identification

and contextual limits like access time. All these elements work in unison such that access decisions are not merely made on the basis of predefined roles but also on the on-the-fly environmental conditions. The model is used in the authentication process by the use of biometric and credentials, for access to the model in a flexible and safe way.

The suggested framework is a well-organized decision-making framework where access requests are considered according to the level of user clearance, device validity, and time limitations. Only under the condition of all security requirements being met, access can be provided, which makes

it difficult to evade the policy and avoid unauthorized access. Encryption mechanisms have also been incorporated in the system to ensure that sensitive data is not accessed after it has been granted access.

3.1. System Architecture

The suggested system architecture will impose safe and context-based access control by incorporating various security elements. The framework is composed of four key layers, as shown in Figure 3, which are authentication, access control, contextual validation, and data protection. The authentication layer will be doing the user identity verification based on biometric authentication or credential-based authentication. This is a two-way method of ensuring security and usability. After the user has been authenticated, the system lands on the access control layer, where the role-based permissions are considered based on predefined security levels based on the Bell-LaPadula (BLP) model.

The contextual validation layer adds further security as it checks the environmental conditions related to each access request. This involves verifying the identity of a device by verifying the MAC address and making sure that it is accessed within the permitted timeframes. These contextual checks will ensure that unknown devices or those that are not supposed to be operating at a given time are not able to access it.

The last layer is concerned with the protection of data with the Advanced Encryption Standard (AES). Encrypted data can only be accessed by users who are appropriately secured and have the relevant security clearance and decryption privileges. This guarantees the confidentiality of the data even after the access control decisions have been implemented. The communication between these layers creates a progressive decision-making process where each access request has to go through all validation processes before it is allowed to access. In case of failure of any condition, the request is denied. This hierarchical architecture adds more security to the system because the identity checks, policy enforcement, contextual awareness and encryption are built into a single architecture.

3.2. Dynamic Access Control

The suggested access control model uses a systematic approach to each decision-making in access control to assess every access request, as shown in Figure 4. It is a process that incorporates authentication, authorization, contextual validation, and data protection to guarantee secure and consistent policy enforcement.

First, authentication is done with the user, and the system can be authenticated either with biometric authentication or username and password. To avoid the failure of the biometric authentication or its inability, the system will automatically revert to credential-based authentication. In case of failure of the authentication step, access is denied.

Upon authentication of the user identity, it compares the level of security clearance assigned to the user with the predefined roles. The model uses the multi-level classification system (Confidential, Secret and Top Secret) based on Bell-LaPadula (BLP) security principles. The levels stipulate the degree of available information and authorized actions. The system conducts contextual validation after role verification. This step involves validation of the MAC address of the device accessing it and verifying if the request to access is within the authorized time frame. These restrictions also help in making sure that only authorized devices have access to it, and at their authorized operational times.

When everything is checked, the system will give access to the respective data module depending on the level of clearance of the user. Basic data access is allowed to the confidential users, intermediate-level access is allowed to the Secret users, and extended access to critical data in the system is allowed to the Top-Secret users.

Simultaneously, all the sensitive data is encrypted by AES. Decryption can only be provided once the user has the right clearance level in place, and this makes access control policies closely intertwined with data confidentiality. In case of failure in any of the validation steps, the system aborts the request and sends back. This flow of decisions, as shown in Figure 4, will be used to guarantee that access policies are strictly followed and limit the chances of unauthorized access or privilege escalation.

3.3. Security Model and Policy Integration

The proposed framework consists of the Bell-LaPadula (BLP) model and the Advanced Encryption Standard (AES) for access control and data confidentiality, respectively, in one security framework. This integration provides some uniformity in terms of the level of the security clearance of the user, the rights that are granted and the visibility of the data.

Enforcing hierarchical access control is done using the BLP model with two main rules: no read up and no write down. It is these rules that ensure that at higher level security and control, users are unable to access the data at lower levels and that sensitive information does not flow towards the lower level. The mechanism ensures that the data access control is in strict compliance with the security classification specified by the data security levels defined, such as Confidential, Secret and Top Secret.

To supplement the access control enforcement, the AES encryption is employed to encrypt sensitive data on the storage and transmission levels. Individual data objects are encrypted, and only when the user meets the necessary security clearance can they be decrypted. This establishes a direct dependency between access control policies and cryptographic operations, so that even in cases where there is a bypass of system-level protection, unauthorized users are not able to access data. By

using BLP in conjunction with AES, a dual-level security model can be provided to both access decisions and protection mechanisms. BLP has logical access controls, while AES ensures the confidentiality of the data and prevents exposure to unauthorized parties. Such a hybrid solution can help improve the security of systems by minimizing the chances of data leakage, privilege escalation, and unauthorized access in the distributed environment.

3.4. System Realization and Implementation

The suggested access control structure was implemented in a web-based and mobile-supported structure to replicate a real-life distributed environment. The back-end system was created based on the Laravel PHP framework that offers a secure and structured space to carry out the logic of authentication, authorization and access control. MySQL was the main database where the user credentials, access policies and encrypted data were stored.

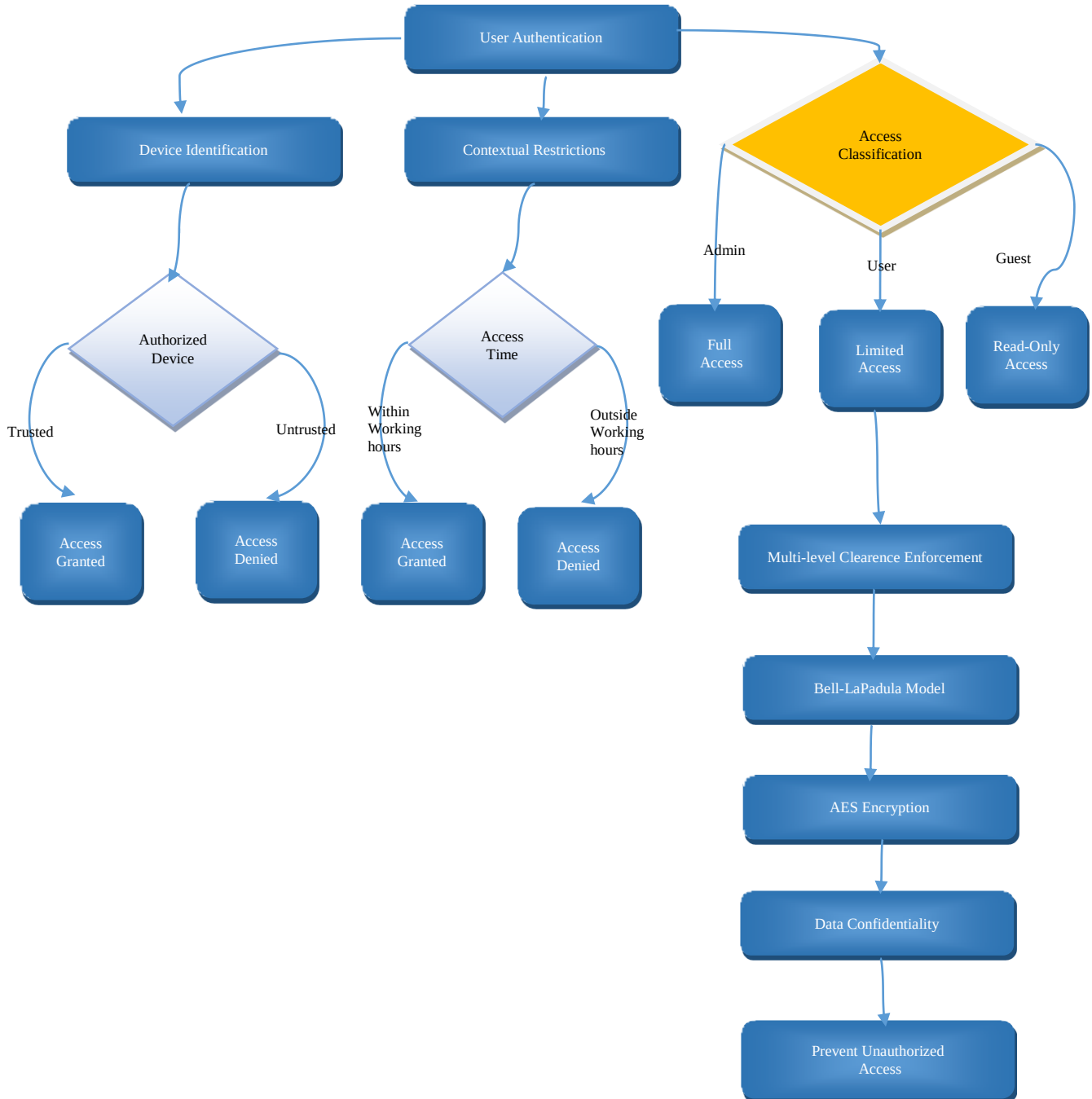


Fig. 3 Proposed model

The system has both administrative and user-level interfaces. The administration interface enables the system managers to create the roles, grant permissions, track user activities, and create temporary key access. The user interface is created in such a way that the employees can authenticate and have access to the system resources depending on their roles and authorization.

A mobile Android and iOS app was created to improve the usability and accessibility. The app will allow users to authenticate with biometric verification or with the help of login credentials and control the system remotely. This arrangement is representative of the real-life situations when users are connected to the organizational systems, not only in various locations but also using diverse devices.

The environment in which the implementation is done has various security measures, such as biometric authentication, credential verification, MAC address verification, and time-based access control. These elements are embedded into the workflow of the system that implements strict policies on access and is used to make sure that only authorized users working under valid conditions can access protected resources.

The system was implemented in a simulated system that is a medium-sized organizational network. This environment was utilized to assess the effectiveness and performance of the proposed model in different access conditions, such as authorized and unauthorized access attempts.

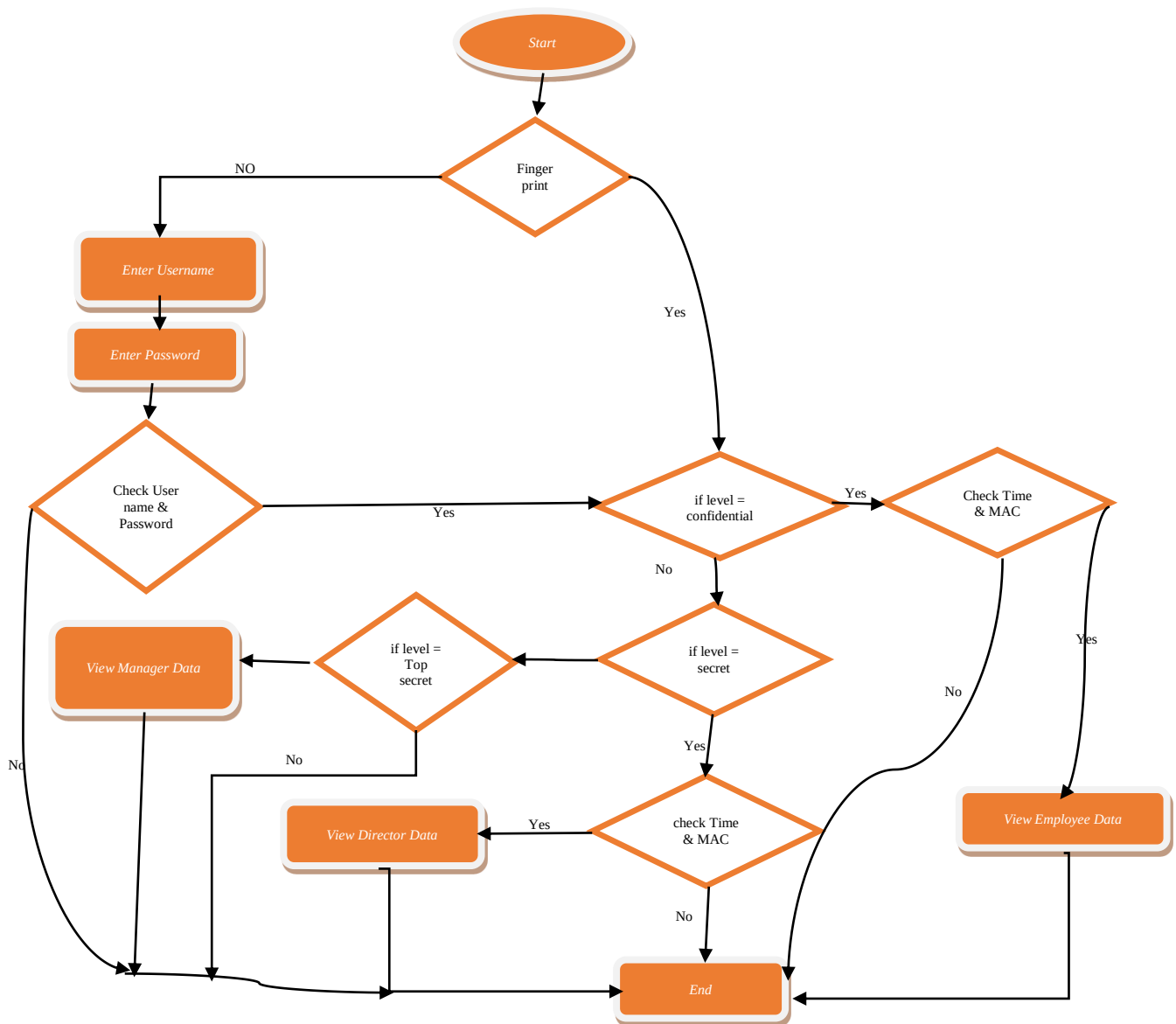


Fig. 4 Work flow of the proposed model

4. Implementations

The following section gives the implementation of the proposed access control framework in practice. The system was designed to investigate the feasibility of hierarchical access control, contextual validation and encryption in a single environment. The implementation is aimed at demonstrating the proposed model and to be not only a theoretical design but also practical for real life.

The environment is based around two main user interfaces, one for the staff and one for the system managers. The employee end has secure password logon, and the admin end has real-time user activity monitoring, user profile management/creation or deletion of access authorisations, and maintenance of emergency override back-doors with randomly generated short-term keys.

4.1. Login to System

The login component is the main point of access to the system, and it is supposed to facilitate secure user authentication by both credential-based and biometric authentication. After accessing the application, a login box appears, enabling users to be authenticated using their fingerprints or a username and password. In case of biometric checking failure or no availability, the system will automatically log in with credential-based authentication.

Once the authentication is successful, further security checks are made to implement contextual validation. The system compares the MAC address of a device with records that are registered to be sure that an authorised device has requested access. Simultaneously, the system will check whether the attempted login process is within the allowed access time that the user is supposed to have. The access is granted under the condition of the fulfilment of both conditions; otherwise, the request is denied.

The mechanism of user authentication in the proposed framework is a simple and effective user authentication mechanism, as shown in Figure 5, which implements the security limitations of the proposed framework.

This element depicts the combination of multi-factor authentication and contextual validation, whereby identity validation is merged with environment conditions before access is granted.

4.2. Administrator Dashboard

The system management interface is the administrator interface. See what the employees are doing in real time at home, in their offices or on leave. This is represented graphically in segments in the form of "progress indicators", which are circular, giving management a snapshot of their staff's progress.

The overview on the main dashboard is illustrated in Figure 6. It shows administrative simple functions such as adding new members, assigning roles, etc., below the upper part where it shows the visual statistics. At the bottom of the page, some icons are provided with immediate links to the main page, employee directory, the scheduling of tasks, the message centre and the emergency key generation panel. The use of colour grades and iconography adds emphasis, and also helps make the site accessible and usable.



Fig. 5 System login

4.3. Permission Assignment

The permission assignment component will allocate all access rights to the system based on the users' roles and enforce them. When the user has registered, the administrator assigns permissions according to the role of the user and according to the tasks he/she has to fulfil, so that each user receives access to the things he/she needs in order to perform his/her duties, as illustrated in Figure 6.

Such permissions regulate access to system features like access to remote systems, organizational data, changes to assigned tasks, and communication with connected systems. The process of assignment adheres to the principle of least privilege, wherein users can only have a restricted set of permissions based on their role.

This element is a direct representation of the role-based access control mechanism presented in the proposed framework, wherein the access decisions are organized based on the predefined roles and the corresponding privileges. The system will provide uniform administration of access policies by centralizing permissions and minimizing the chances of unauthorized operation.

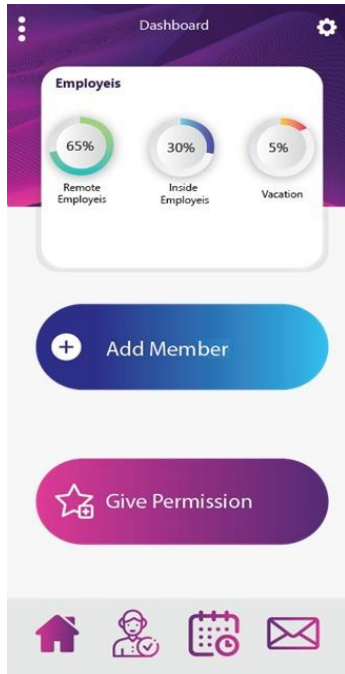


Fig. 6 Admin dashboard

4.4. Adding a New Member

The user registration module allows administrators to add new users safely and in a controlled manner with respect to set access control policies. In the process of registration, the user is given a unique identity, in the form of a username and email and a system-generated password that is changed upon the first log-in. Moreover, the administrator assigns the role and access rights of the user as per organizational policies.

The registration interface enables the administrator to add user characteristics and also give role types like employee or director, as shown in Figure 7. These roles define the amount of access allowed in the system and regulate the number of available resources. Top positions can be linked with more access privileges, whereas the lower positions are more limited.

There are also contextual constraints in the registration phase of the system. These involve connecting the user account to a particular machine based on its MAC address and stipulate authorized time frames. This will ensure that only approved devices can access it, and that only approved timeframes are working on it, further ensuring the security of the whole system.

Furthermore, a special permission configuration interface controls the permission configuration, as shown in Figure 8. This interface allows administrators to give or limit certain system functions to each user. The principle of least privilege is used in the permission assignment process, where a user is only allowed to have the minimum level of access needed to carry out his work.

This component integrates identity management, role assignment and contextual constraints in a single procedure, ensuring that the access control policies are always enforced, while greatly reducing the risk of unauthorized access.

The 'Add Member' form has a purple header with a back arrow and the title 'Add Member'. It features a circular profile picture of a worker. Below the picture are input fields for 'Username', 'Email', 'Password', 'Allowed Time', and 'MAC Address'. A 'Category' section has radio buttons for 'Director' and 'Employee'. At the bottom is a purple 'Done' button.

Fig. 7 Add member

The 'Give Permission' form has a purple header with a back arrow and the title 'Give Permission'. It displays the user's name 'Izzeddin'. Below are four toggle switches for permissions: 'Allow Remote Access', 'Allow View his Department', 'Allow Make Edit', and 'Allow Control Camera', all currently turned on. A purple 'Confirm' button is at the bottom, and a red 'Remove Member' link is at the very bottom.

Fig. 8 Give permission

4.5. Time-Limited Entry Key Generation

The system offers a system of giving users temporary privileges to access the system under controlled circumstances. This aspect enables administrators to create time-based access keys for users who need to access resources that are not in their assigned roles over a given period.

In the process, the administrator will select the target user and specify the validity of the access key, including the expiration time and the start time. The key, once created, allows temporary access to the restricted resources but is still subject to a set of security policies and monitoring.

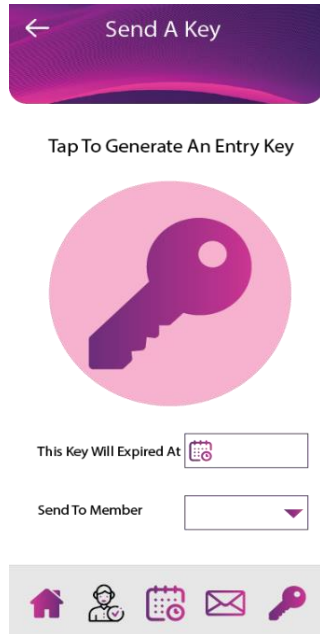


Fig. 9 Generate an entry key

As shown in Figure 9, the interface would allow administrators to organize and administer temporary access requests in an organized fashion. This feature enables privileged escalation to be controlled and all temporary privileges to be time-limited and traceable.

This component makes the access control structure more flexible to dynamically modify the user privileges without permanently changing the role allocations. Meanwhile, there are no time restrictions and system logs that make the use of higher access rights accountable and not abused.

In general, the application illustrates how the suggested framework can be effective to include authentication, role-based authorization, contextual validation, and dynamic access controls in a single system. This validates the practicability of implementing secure and adaptable access control guidelines within practical distributed settings.

4.6. Real-World Case Study

A practical case study of how the suggested access control framework can be applied in the organizational setting is presented in this section.

The system is designed to help in managing access control in institutions where access to sensitive resources should be restricted, and the system is deployed in a distributed and

remote environment. When the employees of an enterprise network can access internal systems from desktops and mobile gadgets, the framework can be applied to the enterprise network. The different roles are assigned to each user based on his/her job function, and access is granted based on the defined policies. The verification of identity is done by biometric verification, or the use of credentials to log in, and this is to guarantee secure identity validation.

Other constraints of context are enforced in the system to provide improved security. Access requests are checked; access time periods are granted if they are registered with the device identifiers before the access is enabled. This makes sure that only the approved devices and within the authorized time limits can access the system by the user.

Use of temporary access control mechanisms is also brought out in the case study. An example would be where a manager can provide a staff member with limited such as time access to a particular job that he/she is not allowed to do. This privilege is automatically revoked once the specified time period is up, allowing for the gradual escalation of privileges without compromising the security of the system.

The provided framework can be applied in various contexts, including corporate structures, educational institutions, and IoT-based architectures. Its stacked architecture enables it to be used in centralized as well as distributed systems, both cloud-based and hybrid.

The proposed model was tested to be valid in a simulated setting, but the case study demonstrates the applicability of the proposed model in practice. The final stages of the work will involve the implementation of the system in the real-world scenario of the large-scale enterprise to assess the scalability, interoperability, and sustainability of the system in real-world use.

5. Results and Evaluation

In this part, the effectiveness and performance of the suggested access control scheme are investigated under a simulated distributed setting. The test focuses on the accuracy of policy enforcement, the responsiveness of a system and usefulness in different modes of operation.

A range of 30 controlled access scenarios was used to test the system to try to simulate real-world usage. These tests included both authorized and unauthorised attempts with various parameters, such as valid and invalid device identities, access time granted and denied, and user clearance levels, among others. There were three security levels of users: Confidential, Secret and Top Secret.

The results of the experiment indicate that the proposed model was always able to apply access control policies. 20 of

30 access attempts were successfully authenticated and authorized, while 10 were denied correctly due to policy violations. These breaches were in the form of five invalid device identity cases and five cases of access attempts that were not within the authorized time ranges.

Since the system was effective in detecting the authorized and unauthorized access requests, as demonstrated in Figure 10, it was concluded that the system was effective. Device validation and time constraints helped to enhance the quality of access decisions and enabled security policies to be strictly adhered to.

Conventional classification measures that were considered were taken into account to have a quantitative evaluation. The model was also very accurate in access decision enforcement, with all test cases being properly classified.

Time to process authentication and administration operations was used to measure system responsiveness. Biometric authentication took an average time of 1.4 (± 0.09) seconds to respond, and credential-based authentication took an average time of 2.1 (± 0.1) seconds. For the permission assignment, which is done by administrative action, the mean response time was approximately 0.9 seconds.

Biometric authentication has the lowest response time, as shown in Figure 11, then permission execution, and lastly, the longest processing time was credential-based login. The results in Table 1 demonstrate the feasibility of achieving an efficient performance, and a set of layers of security is enforced by the suggested system.

Table 1. System performance metrics

Operation	Average Time (seconds)
Biometric Authentication	1.4
Credential-based Login	2.1
Permission Assignment	0.9

A comparison with the conventional Role-Based Access Control (RBAC) systems was implemented for further evaluation of the proposed framework. In contrast to traditional RBAC systems, based on a fixed set of roles assigned to users, the suggested framework includes contextual validation (identity and access time of a device), as well as encryption-based protection. This enables the correct access decision to be made and helps to reduce the risk of unauthorized access in dynamic scenarios.

The combination of various security measures, such as authentication, contextual constraints, and encryption, offers improved protection as opposed to conventional methods. This results in increased robustness and flexibility in access environments in which access conditions are often changing.

The other part of the evaluation in the areas of performance and usability was the user satisfaction study, which was done on ten staff members and five administrators. The respondents evaluated the system according to the following aspects; Usability, simplicity and responsiveness. The results indicated that the system gained a rating of 4.6 from the administrators and 4.2 from the employees, showing that the system was well accepted by the users.

Despite the positive findings in the controlled environment, further trials and evaluations are required using more varied data sets and across larger systems to verify and validate the scalability and generalization.

5.1. Threat Model and Security Analysis

In this portion, the threat model is considered in the framework proposed, and how the system deals with the possible security problem in the distributed environments is discussed.

The threat model presupposes the existence of external and internal enemies trying to achieve unauthorized access to the resources of the system. Outside attackers might seek to take advantage of poor authentication procedures, spoofing device identities, or use the system beyond authorized periods. Internal threats can include legitimate users trying to gain privilege escalation/unauthorized access to elevated-level data.

These threats are mitigated by the proposed framework in several layers of security. First, biometric verification and credential-based login are features of multi-factor authentication, which minimize the chances of identity spoofing and unauthorized access. Second, the validation of devices via MAC address validation will ensure that only registered devices make access requests, which will reduce the chances of unauthorized access to a device.

Time-based access control also limits access to the system to scheduled operation timeframes, so that unauthorized access by an individual outside the valid time frames is prevented. Moreover, the role-based access control and the Bell-LaPadula (BLP) model imply the strict hierarchical rules of access, which do not allow users to access the higher-level data or reveal the information of lower levels.

The AES encryption will add another level of protection as sensitive data will be encrypted when stored and transferred. Unauthorized users do not have access to the encrypted data without the proper level of clearance, even after access control mechanisms have been bypassed.

It also contains the risks of privilege escalation by restricting the assignment of permissions and the use of time-limited access keys. The access privileges are temporary and limited by time, and are audited to ensure accountability and

to prevent abuse. In general, the suggested framework offers a layered defense approach that comprises authentication, authorization, contextual validation, and encryption. This multi-layered solution would greatly lower the attack surface and increase the capacity of the system to deter unauthorized access, data leakage and policy breaches.

5.2. Limitations and Assumptions

Although the given framework was efficient, a few limitations can be thought of.

The system requires the biometric hardware to be available to the user devices, and this may not be feasible in resource-restricted or legacy systems. In addition, sensors and environmental factors can impact the accuracy of biometric authentication and usability of the authentication method when inputs are of poor quality, resulting in a possible false rejection. While MAC binding can be used as a device validation method, it has some security concerns, as it can be spoofed using only a single device validation method.

This scenario shows the importance of more powerful schemes to identify devices in future applications uniquely. The present testing was done in a medium-scale, controlled simulated scenario. Consequently, the performance of the system with large-scale deployments or during high workloads has not been well tested. Further testing of system performance is required in a real-world enterprise environment.

Furthermore, the architecture assumes that all networks are connected all the time as a way to authenticate and enforce the policies. This assumption might not be valid in situations where there is intermittent or offline access, which might impact system usability.

Research in the future will focus on solving the drawbacks by incorporating advanced device recognition techniques, increasing the scalability of the system using distributed systems, and improving the robustness and reliability of systems in low-connectivity scenarios.

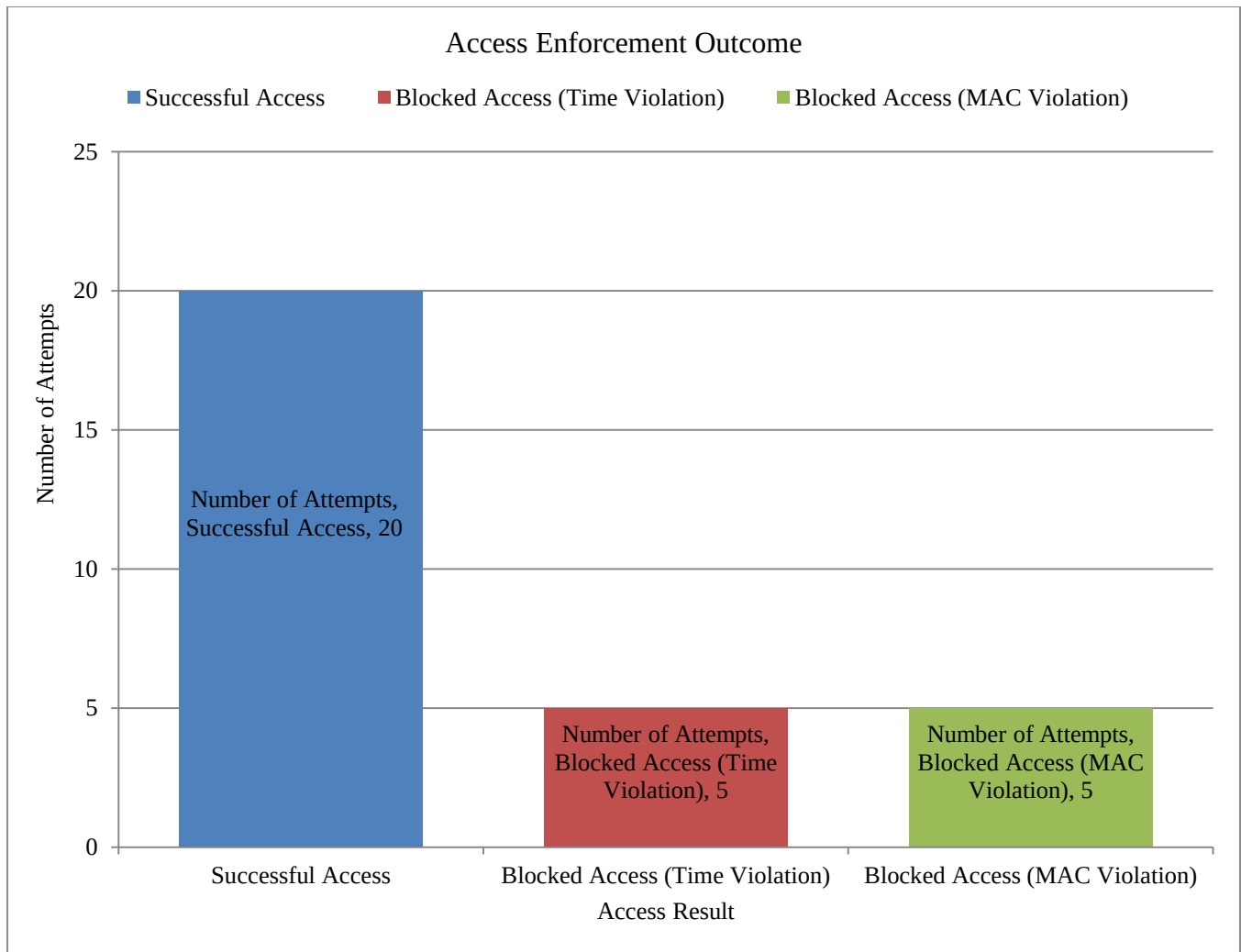


Fig. 10 The number of successful and blocked login attempts during testing

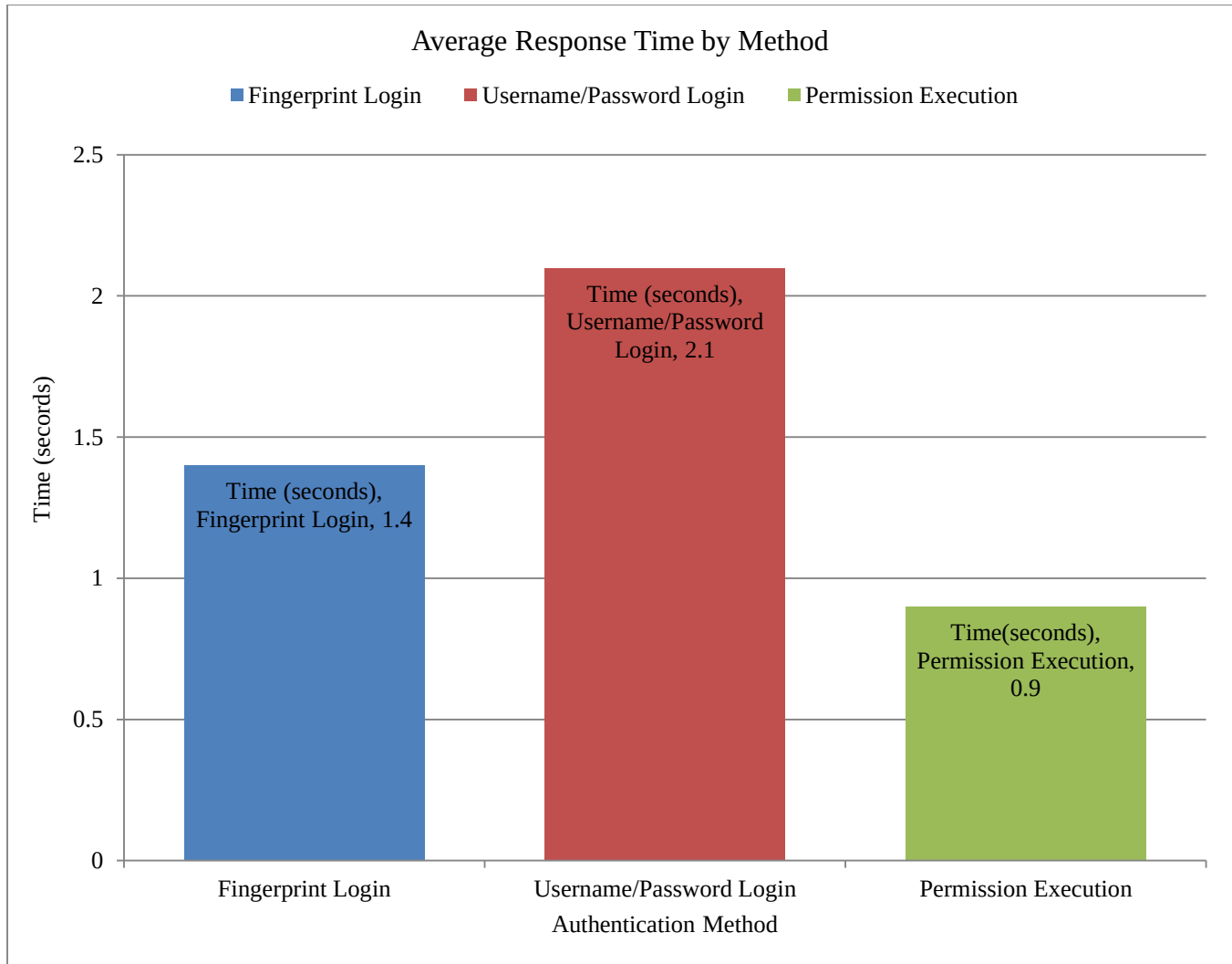


Fig. 11 Average response times of key operations in the system

6. Ethical, Legal, and Privacy Considerations

The access control framework proposed implies processing sensitive user data, such as biometric information, device identifiers, and access activity logs. Hence, ethical, legal, and privacy issues should be well-tuned to provide the responsible deployment of the system.

Privacy-wise, biometric information like fingerprint data should be kept safely, and it should not be accessed by unauthorized persons. Whenever possible, the system must not store raw biometric data but should make use of encrypted templates or hash representations. This minimizes the chances of data exposure in case of system compromise.

The list of device identifiers, including MAC addresses, and user activity logs, also brings up further concerns about privacy. These are the data elements that may be utilized in tracking user behavior. In order to reduce this risk, data collection must be restricted to that which is necessary to

enforce access controls by the principle of data minimization. The system should be compliant with relevant data protection laws, such as the General Data Protection Regulation (GDPR) and other local privacy policies, in line with legal requirements. This involves seeking user consent to the collection of data, transparency of how data is handled, and offering the user ways of accessing or removing personal data.

The ethical factors also require that the system be established in such a way that it does not discriminate or treat unjustly. An example is that biometric authentication systems should be tested to ensure that they can sustain the same level of performance across different groups of users. In addition, access control decisions should be auditable and exploratory in order to be accountable. Lastly, any access logs and administrative activity should be logged in a secure manner to assist in auditing and investigating an incident. Logging also increases the transparency of the system and assists the organization to identify and remedy on possible security breaches.

7. Conclusion

The issue of secure access control continues to be a significant problem in the contemporary computer network, especially in settings that require sensitive information and distributed functions. The growing use of cloud computing and IoT systems has generated the necessity of dynamic and context-sensitive security models that are not based on the usual fixed methods. The paper introduced a consistent access control system that combines role-based access control, contextual validation and an encryption system. The new model integrates the Bell-LaPadula (BLP) security model of hierarchical access control with the Advanced Encryption Standard (AES) to provide confidentiality of data. Moreover, the framework includes the use of multi-factor authentication, verification of the devices, and time-based access restrictions to assist in making dynamic and secure access decisions.

The web-based architecture with mobile platforms was used in implementing the system, which proved the feasibility of the proposed model being implemented in real-life settings. The framework was shown to be highly accurate in policy enforcement, responds effectively and is easy to use in experiments. The combined security features of the system allowed it to prevent unauthorized access and, at the same time, achieve efficiency in its operations. The given solution proves that access control policies together with contextual

and cryptographic mechanisms can contribute greatly to the improvement of the system security. In contrast to the classical models with a fixed set of roles, the suggested model allows the access control to be dynamic and adaptive, depending on the real-time circumstances.

Future development will be directed towards improving the smartness and scalability of the system. These involve the addition of machine learning methods of behavior analysis and anomaly detection, better real-time monitoring, and automated response mechanisms, and extending the framework to multi-cloud and large-scale distributed environments. Further improvements can be made to better profile devices and apply risk-based access controls to enhance decision accuracy.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research and the publication of this article does not have any fund No external funding bodies, grants, or institutional financial support were involved in the conduct of this study or the preparation of the manuscript.

References

- [1] Jiang Bian et al., "Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8364-8386, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Lo'ai Tawalbeh et al., "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences*, vol. 10, no. 12, pp. 1-17, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [3] Sunday Adeleke Salimon et al., "Technological Advancements and Legacy Systems in Electrical Building Services: Emerging Trends, Challenges and Strategic Solutions for Seamless Integration," *2025 Conference on Information Communications Technology and Society (ICTAS)*, Durban, South Africa, pp. 1-6, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Muhammad Akmal Husaini Bin Haris, Mohammad Izmin Haiqhal Bin Yahya, and Muhamad Nidzam Bin Ibrahim, "Security and Privacy Issues in Internet of Things (IoT)," *TechRxiv*, vol. 1-14, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] Fatemeh Yadegari, and Abbas Asosheh, "A Unified IoT Architectural Model for Smart Hospitals: Enhancing Interoperability, Security, and Efficiency through Clinical Information Systems (CIS)," *Journal of Big Data*, vol. 12, no. 1, pp. 1-26, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Junaid Latief Shah, Heena Farooq Bhat, and Asif Iqbal Khan, *Integration of Cloud and IoT for Smart E-Healthcare*, Healthcare Paradigms in the Internet of Things, Academic Press, pp. 101-136, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Jianming Du et al., "Blockchain-based and Multi-Authority Hierarchical Access Control Data Sharing Scheme," *Computers and Electrical Engineering*, vol. 119, pp. 1-17, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Hai Lu et al., "Policy-Driven Data Sharing over Attribute-based Encryption Supporting Dual Membership," *Journal of Systems and Software*, vol. 188, pp. 1-14, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Randhir Kumar, and Rakesh Tripathi, "Scalable and Secure Access Control Policy for Healthcare System using Blockchain and Enhanced Bell-Lapadula Model," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2321-2338, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] D. Shivaramakrishna, and M. Nagarathna, "A Novel Hybrid Cryptographic Framework for Secure Data Storage in Cloud Computing: Integrating AES-OTP and RSA with Adaptive Key Management and Time-Limited Access Control," *Alexandria Engineering Journal*, vol. 84, pp. 275-284, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [11] Maximiliano Cristiá, and Gianfranco Rossi, "Automated Proof of Bell-Lapadula Security Properties," *Journal of Automated Reasoning*, vol. 65, no. 4, pp. 463-478, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [12] Nastaran Farhadighalati et al., "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges," *IEEE Access*, vol. 13, pp. 17777-17806, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Jaibir Singh, Suman Rani, and Vipin Kumar, "Role-based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks," *International Journal of Communication Networks and Information Security*, vol. 16, no. 2, pp. 91-103, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] M. Kokila, and K. Srinivasa Reddy, "Authentication, Access Control and Scalability Models in Internet of Things Security: A Review," *Cyber Security and Applications*, vol. 3, pp. 1-18, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Sarkar Hasan Ahmed, and Subhi R.M. Zeebaree, "A Survey on Security and Privacy Challenges in Smarthome based IoT," *International Journal of Contemporary Architecture*, vol. 8, no. 2, pp. 489-510, 2021. [[Google Scholar](#)] [[Publisher Link](#)]
- [16] Banavathu Rajarao, and Meruva Sreenivasulu, "Hierarchal Attribute based Cryptographic Model to Handle Security Services in Cloud Environment: A New Model," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 1, pp. 1102-1111, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Jianfei Sun et al., "Sanitizable Cross-Domain Access Control with Policy-Driven Dynamic Authorization," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 4, pp. 4126-4142, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [18] Scott W. Rose et al., "Zero Trust Architecture," *National Institute of Standards and Technology Special Publication*, pp. 1-52, 2020. [[CrossRef](#)] [[Google Scholar](#)]
- [19] Yuanyu Zhang et al., "Smart Contract-based Access Control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594-1605, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [20] D. Prabakaran, and Shyamala Ramachandran, "Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment," *Computers, Materials and Continua*, vol. 70, no. 10, pp. 1781-1798, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [21] Naga Kumari Odugu, and A. Rajesh, "A Fine-Grained Access Control Survey for the Secure Big Data Access," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 4180-4186, 2021. [[Google Scholar](#)] [[Publisher Link](#)]
- [22] N. Sivaselvan et al., "SUACC-IoT: Secure Unified Authentication and Access Control System based on Capability for IoT," *Cluster Computing*, vol. 26, no. 4, pp. 2409-2428, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]