IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

A Secure Task Management System for Employee Workflow Optimization

G. Priyadharshini M.E.[1], Priyadharshene R[2], Vimandhani G[3]

Assistant Professor, CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[1]

CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[2]

CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[3]

Abstract: A task management system for employees to work better is a website that helps people do their jobs. It is made to help people in the company work together in a way. This system can put all the tasks in one place so everyone can see what is going on. The tasks include finding security risks fixing problems checking what people are doing making sure only the right people can do things and dealing with incidents that happen during work. The task management system is, like a place where everything is organized and easy to find which helps the company security team do their job better. It is also hard to figure out who is responsible, for what task. The task management system provides role-based access. This means tasks are assigned to users based on their responsibility. Tasks are secure because authorized users can see and manage the tasks that are related to the tasks. The back end of the system uses PHP and MySQL. The system gives us a place to manage tasks create user accounts and store data for audits. It uses HTML5, CSS3 and JavaScript to make dashboards and interfaces that're easy to use. These interfaces help the user track progress check when things are due and get updates. The system lets the team manage tasks based on how important they're work. This means the team can work on the important tasks and fix problems first. The audit log is, like a record that shows what actions the user has taken. The user can check this record to see what they have done. This project is about making task management. It brings together ideas from task management, security operations and compliance tracking. The Secure task management project can help the team do tasks in a secure way. It also helps the team follow standards like the ISO/IEC 27001.The system is good at handling cybersecurity operations. The Secure task management project is useful for making the workflow platform better. It can help the team achieve 90% of the Secure task management projects goals. The Secure task management project is really good, for getting work done in a way. It may support the real-time task execution and monitoring of the audit tracking.

Keywords*:* Secure Task Management, Role-Based Access Control (RBAC), Cybersecurity Workflow, Audit Logging and Compliance, Web-Based Management System.

I. INTRODUCTION

In the digital landscape, there is an unprecedented rise in dependence on information technology systems, cloud, web applications, and networks in the current digital world. Even though the digital revolution has led to an efficient and scalable process, it has also significantly increased the attack surface against cyber threats. The attacks against organizations in relation to data breaches, ransomware, abuse of privilege, and web applications are increasing in intensity, leading to risks for organizations in matters pertaining to assets, reputation, and compliance [21]. Cybersecurity has, thus, emerged as an important operations function rather than a technical one.

Cyber security operations encompass a number of tasks, which include vulnerability scanning, risk analysis, remediation planning, compliance audits, managing access control, and incident response. The challenge with carrying out these operations in a timely and secure manner, whenever they are conducted, is that current task management practices in most organizations encompass the use of traditional methods that include the use of emailing, spreadsheets, ticket systems that lack security awareness, and manually written documentation. The net effect of this approach can negatively compromise the ability of the organization to address security incidents and adhere to the current standards of security operations [1], [21].

Cybersecurity governance involves a proper task allocation and monitoring process. Studies by Mosli et al. show the significance of mapping cybersecurity-related tasks to regulatory controls and employee roles to ensure synergy in both compliance and efficiency [1]. As a matter of fact, the lack of a systematic process to map these tasks against employee roles and security controls makes it difficult to ensure compliance and continuity in the process of ensuring security. Additionally, comparative analyses on cybersecurity standards, including the adoption of the ISO/IEC 27001 standard, shed more light on the need for access control, auditability, and traceability as essential criteria in information security

DOI: 10.17148/IJARCCE.2026.15555

management systems [2], [19]. In fact, these standards require organizations to not only secure their systems but also keep a record of actions carried out by authorized personnel.

Role-Based Access Control (RBAC) is one of the most significant security mechanisms used to implement security policies in organizational systems. RBAC allows user permissions to be controlled by their role or security responsibilities in order to minimize the chances of improper access to security privileges. Various studies have shown that by using secure access methods along with RBAC, system security can be improved [17]. In order to properly implement RBAC in a security environment, it should be security-aware. This means that task assignments as well as access permissions have to be defined based on risk sensitivity rather than using general job descriptions to perform significant security tasks.

Besides access control, modern cybersecurity operations also require constant monitoring and effective task prioritization. Many vulnerability detection and assessment processes utilize structured workflows in order to manage the findings through static and dynamic analysis techniques. As discussed by Nunes et al., this combining of static and dynamic vulnerability analysis improves the detection accuracy while reducing false positives, but such methods require effective task coordination in order for findings to translate into remediation actions [4]. Similarly, in vulnerability scoring and risk assessment frameworks—such as those that integrate CVSS with Bayesian models—emphasis is placed on prioritizing tasks based on real-world impact and risk severity [5]. Without a centralized task management system, these may well fail to lead to timely and effective remediation.

Another crucial area underlying effective cybersecurity processes is audit logging and traceability. Audit logging is a mechanism that maintains a comprehensive and detailed trail with regard to user interactions and activities such as task updates and system changes. Through such logs, various activities within an organization are traceable and allow businesses to play critical roles in facilitating forensic analysis and business compliance. Systemic analysis carried out during cybersecurity processes identifies logging and monitoring as crucial for maintaining situational awareness and business compliance [16].

To overcome such issues, a Secure Task Management System for cybersecurity tasks is proposed. This task management system has a centralized web-based interface for handling security tasks such as vulnerability management, remediation tasks, preparing for audits, and responding to security incidents. The integration of a security-focused role-based access control mechanism ensures that security tasks are only visible to authorized personnel with certain roles. This is according to global security norms, especially ISO/IEC 27001, which focuses on restrictive access and accountability, as well as continuous security surveillance [2], [19].

The system would be designed using universally accepted technology such as PHP & MySQL for developing logic & data security storage and HTML5, CSS3, & JavaScript for developing user-friendly applications. This would enable functionality like interactive dashboards to monitor tasks & various user activity in real time for making efficient security decisions & allowing security teams to concentrate on risky & time-critical events. The system would enable scheduling of tasks considering priority & risk levels for efficient resource allocation & quick response to critical security events [3],[5].

An important aspect of this system is its audit logging feature, which offers end-to-end logging of activities where each important activity carried out by a user, such as task creation, updates, allocation, and status changes, has been recorded. It offers traceability and audit trails, which help ensure governance requirements as well as compliance from a third-party perspective. It offers organizations a way to comply with certain standards by recording all activities carried out in a task [16], [19].

Nevertheless, the above-mentioned project fills the gap between the analysis and the operation conducted for cybersecurity by combining task management, access control, monitoring, and governance into the proposed platform. The Secure Task Management System increases collaboration and efficiency in the workflow, strengthens the management of cybersecurity from the perspective of governance, and facilitates compliance with the regulations of the international community. By addressing the issue of scalability and cybersecurity, the proposed project aims to make cybersecurity management more efficient and responsible in modern organizations [1], [2], [17], [21].

II. LITERATURE REVIEW

Mosli et al., (2024) In this respect, an optimization technique has been proposed by Mosli et al. to align Essential Cybersecurity Controls (NCA-ECC) by the National Cybersecurity Authority with the Saudi Cybersecurity Workforce Framework. The paper identifies and connects regulatory controls to tasks in the cybersecurity workforce to achieve

DOI: 10.17148/IJARCCE.2026.15555

optimal compliance. An optimization technique has been presented to optimize the jobs needed to be performed to accomplish every control throughout NCA-ECC. The significance of strategic cybersecurity jobs has been identified by this technique. Song et al., (2025) recommend a hybrid security system that combines Attribute-Based Encryption (ABE) and Role-Based Access Control (RBAC) in cloud music classrooms. The proposed system includes Trust-Based Access Refinement (TBAR) and an intrusion detection system that detects anomalies. The encryption method allows only approved users to read the data. The simulation results show that the system can detect threats correctly and emits very few false alerts, making it reliable and easy to use. Djebbar & Nordström., (2023) also perform a comparative study on the ISO/IEC 27001:2022, ISA/IEC 62443-3-3, and ETSI EN 303 645 security standards for cybersecurity. In their study, control mapping and overlap analysis are employed by the authors to identify duplicate and shared security requirements. The study shows an overlap in the security requirements among the security standards despite their different application domains.

Nunes et al., (2025) describe a hybrid vulnerability detection method that merges static analysis and dynamic analysis techniques in detecting vulnerabilities of web applications. Static analysis initializes vulnerability detection, and the results of runtime execution guide dynamic analysis. The proposed method effectively overcomes the problem of false positives and the need for manual validation. Experimentation on WordPress plugins results in the robust verification of SQL injection vulnerabilities. Wang et al., (2023) propose a new improved cybersecurity vulnerability assessment framework for connected and self-driving cars based on the integration of the use of the CVSS system along with the Bayesian Networks. The proposed use of the Bayesian system rectifies the issues of the incompleteness of the data and the datasets being small, considering the real-world impact values.

Li et al., (2025) introduce Event Mon, an event-based network data recovery system with real-time capability. The proposed approach combines offline learning with an online streaming encoder for ultra-low latency recovery. The researchers also introduce the Stream2Batch learning algorithm that facilitates incremental learning with streaming data. The experiment reveals better accuracy and latency compared with matrix completion techniques. Yang and Shinjo., (2025) propose a Compounded Real-Time Operating System (cRTOS) that combines GPOS and tRTOS through hypervisor-based partitioning. It provides a way to support a wide range of real-time applications through remote system calls without modifying the Linux kernel. This is implemented through Jailhouse, Linux, and FreeRTOS/NuttX, which have a lower overhead compared to PREEMPT_RT and Xenomai. Guo., (2025) also suggests an engineering construction quality risk prediction system based on a deep learning model of existing IoT sensor data. This involves real-time monitoring and intelligent anomaly alerts. Deep learning helps to identify risk with high accuracy even in intricate construction environments. Findings indicate that there is high accuracy compared with other statistical models.

Wei et al., (2024) A security risk assessment system for power monitoring systems based on Zero Trust Architecture (ZTA) is also proposed by Wei et al. This model relies on real-time data acquisition, modular analysis, and changing scores to assess levels of trust. The system also changes security policies through continually updated risk scores. The test result shows effectiveness in decreasing false alarms and enhancing detection capabilities. Dong et al., (2025) offer a collaborative compliance control strategy for biped robots based on multi-priority inverse kinematics (MPIK) and multi-priority dynamic control (MPDC). The technique focuses on high-level task satisfaction, along with stable gaits and accurate positioning. Nonlinear centroid dynamics help the robots walk in unstructured terrains. The technique exhibits excellent disturbance suppression and stable gaits.

Ko et al., (2025) propose a sensorless control method for robots through the implementation of a nonlinear Disturbance Observer (DOB) with compensation modulation via the Gaussian Process. The strategy makes a distinction between forces of distraction and forces of interaction with a purpose to ensure correct tracking and compliance. The stability of the method is demonstrated through passivity analysis. Alshammari et al., (2025) perform a systematic review of the literature on cybersecurity challenges in cyber logistic chains based on 61 studies. The researchers underline some big challenges related to confidentiality, integrity, and availability, the increase in ransomware attacks being the most serious problem among them. The paper critically discusses various mechanisms of prevention and access control. The authors develop the Cyber Chain Guard framework based on the review. This framework leverages blockchain and integrated access mechanisms supported by the Clark-Wilson model.

Zhang et al., (2025) propose a distributed task scheduling algorithm for MEC emergency networks based on Multi-Agent Deep Deterministic Policy Gradient. By employing one agent on each computation node, local network information is used to make decisions. An asymmetric multi-agent architecture is developed to resolve the challenge of heterogeneous capabilities among nodes. It introduces a mechanism called dual-buffer learning that accelerates convergence. Low task latency and strong adaptability in dynamic network environments can be exhibited using this approach. Alamri et al., (2024) offer a cybersecurity risk assessment framework for blockchain-based identity management in health IoT using the Delphi

DOI: 10.17148/IJARCCE.2026.15555

technique and SMART multi-criteria analysis. The study uses experts to rank risks according to their relative importance, which include security risks, risks related to privacy, and technology risks. The study finds that security and privacy risks are preeminent risks. Vaarandi et al., (2025) have conducted a systematic literature review related to maritime cybersecurity monitoring with a focus on IT/OT. They have followed the PRISMA protocol in their research. They have used bibliometric as well as taxonomy-driven analysis. They have commented upon the limitations of the data set as well as the gaps in the evaluation process.

Existing studies of these ideas may focus on the cybersecurity analysis, threat detection, and risk and compliance management frameworks, but they lack a practical system for securely managing, tracking, and auditing the day-to-day cybersecurity tasks. There is no unified platform that integrates all such as role-based access, priority-driven workflows, and audit-ready traceability for cybersecurity operations.

1) Contribution Of The The Paper

- There will also be a task management system that will be safe and very convenient for use. It will also be a unique system that will only be applied in the field of cybersecurity.
- It will include features like checking for vulnerabilities, fixing them, performing audit operations, and preparing for security incidents. It ensures that all key operations in the area of cybersecurity are effectively managed and monitored.
- The current method of using spreadsheets, emails, and basic task management systems to organize work in the security teams is not effective for collaboration and also results in errors.
- The focus of the project is on RBAC that is security-aware, where the duty assignments of the users depend on the things they need to do to ensure security rather than on their job names.
- The system enables teams to determine which tasks should take priority by evaluating the risks associated with each task as well as their respective importance. The system is able to perform risk-based task scheduling as well as priority-based task scheduling.
- An RMS-secured role-based system will allow authorized employees only to work on certain tasks, thus minimizing the possibility of mistakes happening while at the same time maximizing the following of security policies.
- The system has the ability to record the activities that the users perform. Activities are basically used for audits. In reality, the system is a source for evidence of meeting the requirements of standards such as ISO/IEC 27001.
- The application makes it possible to incorporate real-time dashboarding features for giving a complete understanding of the ongoing processes to teams. The person can take responsibility for their actions and decisions regarding the workflow.

III. METHODOLOGY

A. a) system preliminary

*I. User Authentication and Authorizatio***n**

User authentication ensures that only registered users can access the Proposed system by validating their login credentials. Authorization further restricts system operations based on user roles such as Admin and User. This mechanism protects the system from unauthorized access and enforces controlled task management.

The authentication condition is defined as:

$$Auth(U) = Verify(email, password) \qquad (1)$$

If the authentication result is **True**, the user is allowed to access the system; otherwise, access is denied.

Where,

- U = User attempting to log in
- email = Registered email address
- password = User password
- Verify(.) = Credential verification function
- Auth(U) = Authentication result (True / False)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

1) II. Task Data Modeling and Management

Task data modeling defines the structure used to represent tasks within the system. Each task is treated as a structured data object containing essential attributes such as title, description, priority, deadline, and status. This structured representation enables efficient task creation, assignment, updating, and tracking.

The task model is expressed as:

$$T = \{ID, Title, Desc, Priority, DueDate, Status, AssignedUser\} \quad (2)$$

This formulation ensures consistency, integrity, and efficient retrieval of task information from the database.

Where,

- T = Task object
- ID = Unique task identifier
- Title = Task name
- Desc = Task description
- Priority = Task priority level
- DueDate = Task deadline
- Status = Task state (Pending / In Progress / Completed)
- AssignedUser = User responsible for the task

2) III. Role-Based Access Control and Task Operations

Role-Based Access Control (RBAC) ensures that system operations are executed only by authorized users. Admin users are granted higher privileges such as user management and task deletion, while regular users are restricted to managing their assigned tasks. This control mechanism prevents misuse and maintains system security.

The access validation is defined as:

$$\text{Access} = \text{CheckRole}(U, \text{Action}) \quad (3)$$

RBAC guarantees secure task operations and maintains operational integrity across the system.

Where,

- U = User
- Action = Requested system operation
- CheckRole(.) = Role validation function
- Access = Permission status (Granted / Denied)

B. system architecture

The Secure Cyber-Security Task Management System design has a layered and role-based architecture. The architecture aims at ensuring safe authentication and access, as well as efficient management and monitoring for security compliance. It includes a variety of logical levels such as User Interface Layer, Authentication and Authorization Layer, Role-Based Access Control Layer, Secure Task Management Layer, Risk Assessment and Prioritization Layer, Data Storage Layer, and Monitoring and Compliance Layer. This enables easier maintainability and scalability with reduced chances of any kind of unauthorized access.

This process starts at the User Interface Layer, implemented using HTML, CSS3, and JavaScript languages. This is basically the main interaction portal where users register and log in to gain access to the system. When users enter their credentials to register and log in via the web portal, such credentials are sent to the Authentication Module. Here, identity validation takes place. Unauthenticated users are denied access immediately, and authenticated users are allowed to continue the further into the system.

If authentication was successful, Role-Based Access Control takes over and performs Role Identification. Every authenticated user is assigned to a pre-defined role such as Admin, Security Analyst, Manager, or Auditor. Roles define what access is to be given and operational permissions to the user. The Authorization and Role Verification Layer checks whether the role of the user fits within the requested operations or not. The Access Control Enforcement mechanism will stop any attempt to go beyond the assigned privileges. After successful authorization, the user enters the Secure Cyber-Security Task Management Layer, where security-related tasks such as VAPT, incident response, and audit activities are created, assigned, and managed. All the ask operations are subjected to role-based permission checks, which prevent unauthorized execution. Subsequently, approved tasks are safely stored in the MySQL Database Layer, allowing confidentiality, integrity, and availability of the data regarding tasks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

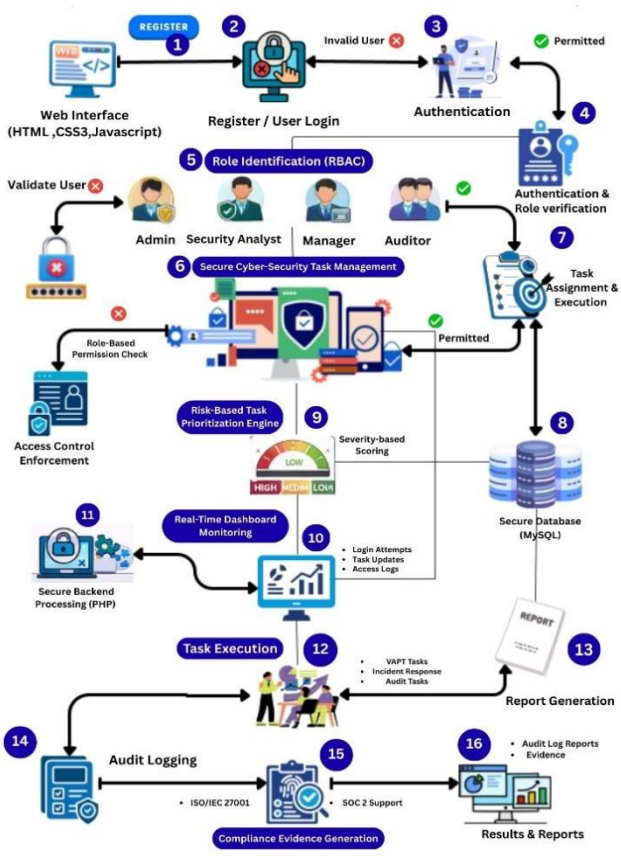
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

For better decision-making and efficiency, the system also includes a Risk-Based Task Prioritization Engine. This engine assesses the risk-based score for the tasks and rates them as High, Medium, or Low risk. High-risk tasks are given priority for early mitigation of critical security risks.

The architecture is accompanied by a Real-Time Dashboard Monitoring Layer, in which activities such as login requests, task updates, and access requests are continually monitored. The backend processing is done using PHP for secure handling of data. All actions taken by users as well as activities in systems are recorded in an Audit Logging Layer.

Lastly, the platform incorporates Report Generation & Compliance Evidence Creation. The platform generates audit trails, security audit reports, and other forms of compliance documents in alignment with ISO/IEC 27001 norm requirements and SOC 2. The outcome of the reports is tangible evidence that is used during the audit process. The Results & Reports Layer offers the results of the analyses together with the level of compliance.



C. implementation of the proposed work

Step 1: User Registration and Role Assignment

A system begins with user registration and where individuals create an account by providing essential details such as username, email address, password, and role type. Let U denote the user registration data. Each user is assigned a role for admin and user. which determines access privileges within the proposed system. This step ensures controlled access and also establishes responsibility-based task management.

The user registration function is defined as:

$$U_{reg} = Register(U) \qquad (1)$$

Where,

- U = User details (name, email, password, role)
- Register(.) = User registration function
- U(reg) = Registered user profile

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

Step 2: User Authentication and Login Validation

After registration the users must authenticate themselves to access the system and the Authentication is performed by validating login credentials against stored records. Only authenticated users are permitted to interact with the task management functionalities, preventing unauthorized access.

The authentication condition is expressed as:

$$Auth_U = Verify(email, password) \qquad (2)$$

If $Auth_U = True$, the user is successfully logged in.

Where,

- **email** = Registered email ID
- password = User password
- Verify(.) = Credential verification function
- Auth_U = Authentication status

Step 3: Task Creation by Authorized User

Once authenticated perfectly an authorized user can create a task by specifying task title, description, priority, due date, and status. This step enables systematic task planning and ensures that tasks are well-defined before assignment.

The task creation process is defined as:

$$T = CreateTask(title, desc, priority, due) \qquad (3)$$

Where,

- T = Task object
- title = Task name
- desc = Task description
- priority = Task priority level
- due = Task deadline
- CreateTask(.) = Task creation function

Step 4: Task Assignment to Users

After the task creation, the tasks are assigned to the specific users based on the roles or workloads. This step ensures accountability and clear responsibility for task execution.

The task assignment operation is expressed as:

$$\text{Assign}(T, U) \qquad (4)$$

Where,

- **T** = Created task
- **U** = Assigned user
- **Assign(.)** = Task assignment function

Step 5: Task Storage in Database

All task created and assigned tasks are securely and that stored in the system database. This ensures persistence, reliability, and easy retrieval of the task information. Each task record in an uniquely identified and linked to the corresponding user.

The database storage function is defined as:

$$Store(T) \qquad (5)$$

Where,

- **T** = Task details
- **Store(.)** = Database storage function

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

Step 6: Task Status Update and Progress Tracking
Users can update task status as Pending, In Progress, or Completed. This allows that the real-time tracking of task progress and that improves productivity and transparency.

The status update is represented as:

$$Status_T = UpdateStatus(T, s) \qquad (6)$$

Where,
- Status_T = Updated task status
- s = New status value
- UpdateStatus(.) = Status update function

Step 7: Notification Generation
Whenever the task is assigned or its status to the user that is updated, the system generates notifications for relevant users. This ensures timely awareness and improves communication among the team members.

The notification function is defined as:

$$N = Notify(U, T) \qquad (7)$$

Where,
- N = Notification message
- U = Target user
- T = Task information
- Notify(.) = Notification generation function

Step 8: Task Retrieval and Dashboard Display
Users can view the assigned tasks through a personalized dashboard of them. Tasks are fetched from the database and that display based on role, status, and priority of the task and that enabling efficient task monitoring.

The retrieval operation is defined as:

$$T_{list} = FetchTasks(U) \qquad (8)$$

Where,
- **T_{list}** = List of tasks
- **U** = Logged-in user
- **FetchTasks(.)** = Task retrieval function

Step 9: Task Modification and Deletion
Authorized users can also modify the task details or delete tasks if its required. That ensures the flexibility in handling dynamic task requirements while maintaining system integrity.

The modification operation is defined as:

$$T' = Modify(T) \qquad (9)$$

Where,
- T′ = Updated task
- Modify(.) = Task modification function

Step 10: Role-Based Access Control
The system enforces the role-based access control to ensure that only authorized users through that users can perform sensitive operations such as deleting tasks or managing users. That enhances system security and prevents misuse access control.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

The access control check is expressed as:

$$Access = CheckRole(U, Action) \qquad (10)$$

Where,

- Access = Permission status
- U = User
- Action = Requested operation
- CheckRole(.) = Role validation function

Step 11: Logout and Session Termination

After completing the operations, the users can securely log out. The system terminates the session to prevent unauthorized reuse of user credentials.

The logout operation is defined as:

$$Logout(U) \qquad (11)$$

Where,

- **U** = Logged-in user
- **Logout(.)** = Session termination function

IV. EXPERIMENTAL SETUP

The system initialization all phase that prepares all essential components required for conducting the experimental evaluation of the Proposed Task Management System. This application server is initialized to handle user requests and system logic. The authentication module is configured to manage secure login and role-based access. The task management module is prepared to support the task creation, assignment, and status tracking. The database is initialized to store user and task data, while the notification service is enabled to deliver real-time alerts during the task operations. This setup ensures that the system is fully functional and ready for the experimental execution.

Algorithm 1A: User Registration and Authentication
Input:
User data

$$\boldsymbol{U = \{username, email, password, role\}}$$

1. $U_{reg} \leftarrow Register(U)$
2.if $U_{reg} = False$ then
3. Reject registration
4. else
5. Store user credentials in database
6. end if
7.$Auth_U \leftarrow Verify(email, password)$
8. if $Auth_U = False$then
9. Deny system access
10. else
11. Grant access and create user session
12. end if

This algorithm ensures that the secure user onboarding and access control. During registration, user details are validated and that stored securely in the database. Authentication is performed by verifying the login credentials before granting system access. This process ensures that the only authorized users participate in the experimental evaluation and prevents unauthorized access to task data.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

Algorithm 1B: Task Creation and Assignment

Input: Task details T_d, Assigned User U
1: $T \leftarrow CreateTask(T_d)$
2: Assign task $T$to user U
3: Store Tin database
4: Set initial status of Tas *Pending*
5: Generate notification for assigned user

This algorithm evaluates the that task creation and assignment functionality of the system. Tasks are created with defined attributes such as title, description, priority, and due date. Each task is used to assigned to a specific user and stored in the database. In initial status is set to track task progress, and notifications are generated to inform the assigned user. This process validates task workflow efficiency during experimentation.

Algorithm 1C: Task Status Update and Progress Tracking

Input: Task ID T_{id}, New Status s
1: Retrieve task Tusing T_{id}
2: Update task status to s
3: Save updated status in database
4: Generate notification for status update
5: Display updated task on user dashboard

This algorithm evaluates the task progress tracking within the system. Users update task status and the work progresses, enabling real-time monitoring. Database synchronization that ensures consistency, while notifications keep relevant users informed and updated. This experiment validates the effectiveness of task tracking and workflow transparency.

Algorithm 1D: Task Retrieval and Dashboard Display

Input: Logged-in user U
1: Fetch tasks assigned to user U
2: Sort tasks by priority and due date
3: Display tasks on user dashboard
4: Highlight completed and overdue tasks
This experiment evaluates the user dashboard functionality. that tasks are retrieved dynamically from the database and displayed in the organized manner. The dashboard enables users to monitor the workload efficiently and validating system usability and responsiveness.

Algorithm 1E: Role-Based Task Control

Input: User U, Task ID T_{id}
1: Check role of user U
2: if role = Admin then
3: Allow task modification or deletion
4: else
5: Restrict operation
6: end if
This experiment validates role-based access control. An administrative users are granted higher privileges compare to the normal user. while regular users are restricted to assigned tasks. This confirms the enforcement of access policies and system security.

V. RESULT AND DISCUSSION

A. performance metrics

1) A. Response Time Analysis

The response time performance of the proposed solution of the task management system is summarized in Table 1 and Figure 2. The results show that core operations are executed with low latency, demonstrating efficient system performance. And the user login achieves the fastest response time at 220 ms and that indicating a quick authentication and the session handling. Task creation and task status updates record response times at 310 ms and 290 ms and reflecting efficient

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

database operations and audit logging. Task assignment shows a slightly higher response time of 340 ms due to the role validation and access control checks. The highest response time is observed during dashboard loading 420 ms and as it involves real-time aggregation of multiple task and audit datasets. Overall, the analysis confirms that the proposed system maintains responsive performance while enforcing the security and the role-based access that making it suitable for real-time task execution and monitoring in an secure organizational environments.

Table 1: Response Time Analysis of proposed system Operations

Operation	Average Response Time (ms)
User Login	220
Task Creation	310
Task Assignment	340
Task Status Update	290
Dashboard Loading	420

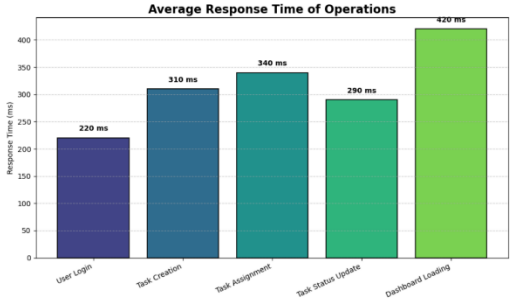


Fig. 1. Response Time Analysis of proposed system Operations

B. Task Search Performance

Figure 3 and Table 2 present the task search performance comparison of the proposed system. Each case is represented by the distinct coloured line, with the false case demonstrating consistently low response times due to the early task absence detection and minimal query execution. In contrast, the true case shows higher processing time, particularly during database querying and result rendering, as the system retrieves task details and that enforces role-based access validation. Despite the additional processing steps, the proposed system maintains the optimized search performance with the controlled latency. These results highlight Proposed solution efficiency in quickly rejecting invalid searches while reliably retrieving valid tasks, demonstrating its robustness and suitability for secure real-time task management.

Table 2: Task Search Performance

Component	Description	False Case (Task Does Not Exist, ms)	True Case (Task Exists, ms)	Component
T_index	Indexed lookup time	20	20	T_index
T_query	Database query execution	5	50	T_query
T_render	Result rendering time	10	30	T_render
T_search (Total)	Tsearch= T_index + T_query + T_render	35	100	T_search (Total)
Analysis	Summary of performance scenario	Quickly determines task absence with minimal processing	optimized queries minimize latency	Analysis

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

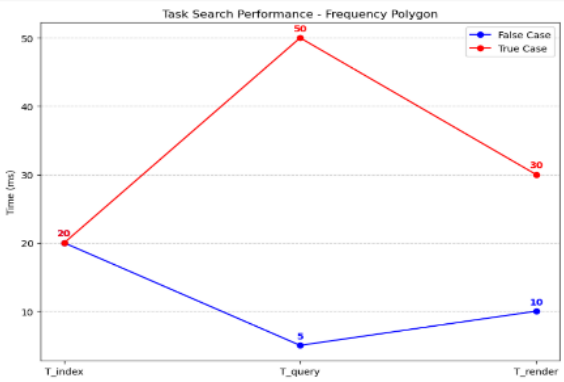


Fig. 2. Task Search Performance

C. Comparison with Existing Task Management Systems

Figure 4 and Table 3 present a comparative feature analysis between existing task management systems and the proposed system secure task management systems. Each axis represents a critical system features that including architecture design, role-based access control, task search optimization, concurrent user support, and real-time updates. The existing systems show limited performance across most features, particularly in task search optimization and real-time updates, due to monolithic architectures and partial access control mechanisms. The proposed system demonstrates consistently higher performance across all dimensions, enabled by its modular architecture, full role-based access control, optimized task search, and robust support for concurrent users. The graph clearly highlights the overall superiority of the proposed system, confirming its effectiveness in delivering secure, scalable, and real-time task management capabilities.

Table 3: Comparison with Existing Task Management Systems

Feature	Existing Systems	Proposed System
Architecture	Monolithic	Modular
Role-Based Access Control	Partial	Full
Task Search Optimization	No	Yes
Concurrent User Support	Limited	High
Real-Time Updates	Limited	Yes

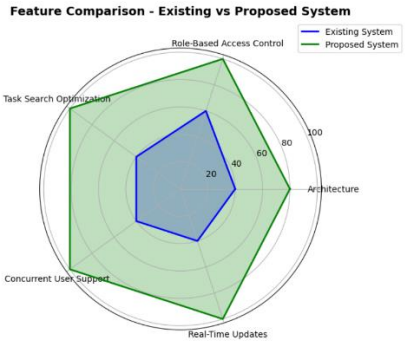


Fig. 3. Comparison with Existing Task Management Systems

D. Scalability Analysis

Figure 5 and Table 4 present the scalability analysis of the proposed system in comparison with existing systems by measuring response time under increasing numbers of concurrent users. The results show that as user load increases from 10 to 500 users, the response time of the existing system grows sharply from 120 ms to 1200 ms, indicating poor scalability and performance degradation under heavy load. In contrast, the proposed system exhibits a more gradual increase in response time, rising from 100 ms to 450 ms, due to its modular architecture, optimized database access, and efficient task handling mechanisms. The bar graph clearly illustrates that Proposed solution consistently outperforms the existing system across all load levels. This analysis confirms that the proposed system is highly scalable and capable of supporting a large number of the concurrent users while maintaining the acceptable response times.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

Table4: Scalability Analysis

Concurrent Users	Response Time (ms) - Existing System	Response Time (ms) – Proposed System
10	120	100
50	200	150
100	350	220
200	600	300
500	1200	450

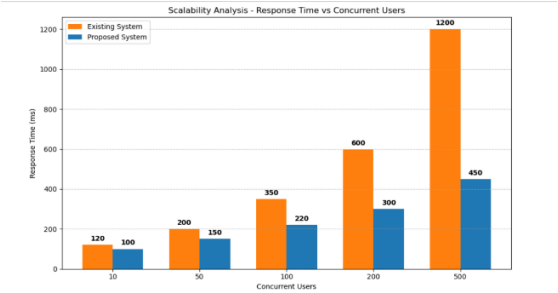


Fig. 4. Scalability Analysis

B. E. Security analysis of the Proposed system

Figure 6 and Table 5 present the security analysis of the proposed system, highlighting its effectiveness across key security dimensions chart visualization. An unauthorized access the protection that achieves the highest score due to the implementation of secure the authentication mechanisms and strict role-based access control. Data integrity and data privacy also demonstrate the strong performance, with the high security scores reflecting robust validation of task updates and controlled access to sensitive user and task information. Session security shows that a slightly lower yet strong score, and it involves continuous session monitoring and protection against hijacking attacks. The graphical distribution clearly indicates that the balanced and comprehensive security coverage across all the evaluated parameters. Overall analysis confirms that Proposed solution provides a secure and reliable environment for task management system while maintaining compliance with organizational security requirements.

Table5: Security analysis of the Proposed system

Security Feature	Description	Security Level (Score 0–100)
Unauthorized Access	Secure authentication & role-based access control	100
Data Integrity	Task updates validated before database modification	95
Session Security	Secure session handling to prevent hijacking	90
Data Privacy	Access to user and task data restricted to authorized roles	95

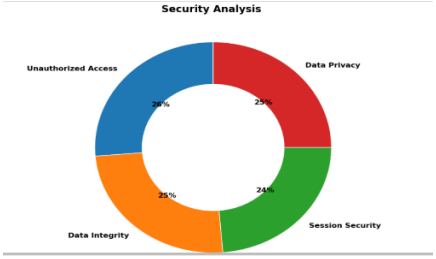


Fig. 3. Securtity analysis of proposed system

C. Static Security Analysis

Figure 7 and Table 6 show that the static security analysis results of the proposed solution, showing the distribution of vulnerability severity across key system modules. The histogram indicates that the most modules fall under the Secure

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

category, reflecting the absence of critical security flaws in core components such as authentication, access control, and input handling. Only the task processing module exhibited minor low-severity issues, which were identified and resolved during development, indicating proactive security refinement. The overall security posture is classified as High, demonstrating strong resistance against common web-based attacks and secure implementation practices. This analysis confirms that the proposed system is robust, well-hardened, and suitable for deployment in security-sensitive task management environments.

Table6: Static Security Analysis

Analysis Aspect	Observation	Severity Level
Authentication Module	No authorization flaws or insecure logic detected	Secure
Task Processing Module	Minor low-severity issues identified and resolved	Low
Access Control Module	Proper role and permission checks enforced	Secure
Input Handling	No insecure input handling vulnerabilities found	Secure
Overall Security Posture	Strong resistance to common web-based attacks	High

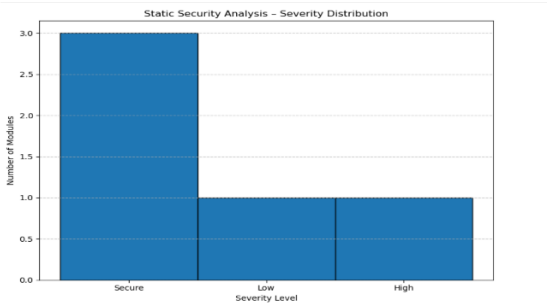


Fig. 5. Static Security Analysis

a) comparative analysis

A comparative performance analysis the existing task management and security-oriented systems against the Proposed system. The bar chart approaches achieve task or search efficiency values ranging from approximately 55% to 70%, reflecting their focus on isolated aspects such as role compliance, security analysis, or access control, often without real-time task handling or optimized search. Systems based on Zero Trust and RBAC improve security but still lack efficient task search and scalability. That the proposed system achieves the highest efficiency of 92%, owing to its integrated web-based architecture, full role-based access control, optimized task search, and scalable design. Although the limited automation remains a constraint, Proposed solution clearly outperforms existing works by providing a balanced solution that simultaneously addresses security, scalability, cost efficiency, and high task/search performance, making it well-suited for secure organizational task management.

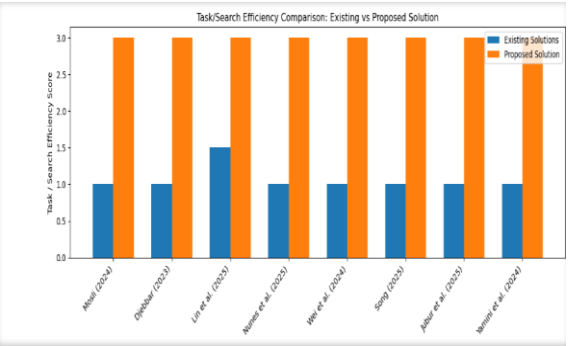


Fig. 6. Comparative analysis with proposed

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

D. Table7: Comparative analysis with proposed

Authors & Year	Core Technology	Key Strength	Major Limitation	Privacy	Scalability	Cost	Role / Access Authentication	Task / Search Efficiency
Mosli (2024) [1]	Workforce role allocation framework	Optimal role compliance	No real-time task tracking	Medium	Medium	Medium	Yes	No
Djebbar & Nordström (2023) [2]	Cybersecurity standards analysis	Strong compliance coverage	No system implementation	High	Low	Low	No	No
Lin et al. (2025) [3]	Priority queue scheduling	Efficient burst handling	Network-focused only	Low	High	Medium	No	Partial
Nunes et al. (2025) [4]	Static & dynamic security analysis	Strong vulnerability detection	High processing overhead	High	Medium	High	No	No
Wei et al. (2024) [9]	Zero Trust Architecture	Strong access control	Complex configuration	High	Medium	Medium	Yes	No
Song (2025) [17]	ABE + RBAC	Fine-grained access control	Cryptographic complexity	High	Medium	High	Yes	No
Jubur et al. (2025) [20]	Secure authentication system	Strong password protection	Limited task features	High	Medium	Medium	Yes	No
Yamini et al. (2024) [21]	Cybersecurity strategies	Sector-wide security insight	No operational system	Medium	Low	Low	No	No
Proposed Work	Web-based Task Management + RBAC	Fast, scalable, secure task handling	Limited automation features	High	High	Low	Yes	High

VI. DISCUSSION

The Secure Task Management System provides for the need for well-structured, secure, and accountable task management of cybersecurity processes. With every passing day, cybersecurity threats are becoming increasingly complex in nature; traditional methods of task management

do not suffice to handle such security processes. This project confirms that the inclusion of cybersecurity concepts in task management is a vital step that increases efficiency, accountability, and governability.

It uses RBAC so that a user can perform only those functions and access data that their role prescribes. This greatly helps in reducing unauthorized access to functions and data, as well as in enforcing the principle of least privilege. By centralizing security-related tasks, such as creating, assigning, and marking the completion of tasks, this system enhances collaboration within teams of security personnel, hence preventing delays in the execution of tasks.

One of the main advantages in the proposed system can be identified in the audit logging process; in fact, the proposed system ensures the logging of the critical actions carried out by the user. This feature holds great importance as it provides traceability and accountability along with the support of information security standards compliance, including the ISO/IEC 27001 standard.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15555

The technologies that are employed in the development of the website solutions, such as PHP, MySQL, HTML, CSS, and JavaScript, make the solution highly scalable and user-friendly. The secure handling of the database and the controlled flow of data in the business logic layer of the system enable the security of data in the system. The system uses the dashboard and reporting tool, which makes it easy for the user to track the progress of the tasks carried out.

On the whole, the Secure Task Management System acts as a superb link between analysis and implementation in the area of cybersecurity. This particular project proves that access control, traceability, as well as security-sounding workflows incorporated with task management technology definitely do and will very soon play a vital role in the safety of any business organization. This particular project may possess some additional features in the future that could serve as an essential component for the task management services associated with cybersecurity for any business organization once the features of risk score calculation as well as the alert feature are incorporated.

REFERENCES

[1]. R. Mosli, "Optimal Job Role Allocation for Compliance With NCA-ECC Controls Using the Saudi Cybersecurity Workforce Framework," in IEEE Access, vol. 12, pp. 128235-128245, 2024, Doi: 10.1109/ACCESS.2024.3457025.
[2]. F. Djebbar and K. Nordström, "A Comparative Analysis of Industrial Cybersecurity Standards," IEEE Access, vol. 11, pp. 85315–85332, 2023, Doi: 10.1109/ACCESS.2023.3303205.
[3]. R. Lin et al., "Real-Time Priority Queue Scheduling for Bursty Traffic," IEEE Internet of Things Journal, vol. 12, no. 24, pp. 55883–55892, Dec. 2025, Doi: 10.1109/JIOT.2025.3627212.
[4]. P. Nunes, J. Fonseca, and M. Vieira, "Blending Static and Dynamic Analysis for Web Application Vulnerability Detection: Methodology and Case Study," IEEE Access, vol. 13, pp. 3139–3153, 2025, Doi: 10.1109/ACCESS.2024.3522094.
[5]. Y. Wang et al., "Automotive Cybersecurity Vulnerability Assessment Using the Common Vulnerability Scoring System and Bayesian Network Model," IEEE Systems Journal, vol. 17, no. 2, pp. 2880–2891, June 2023, Doi: 10.1109/JSYST.2022.3230097.
[6]. Y. Li et al., "Event Mon: Real-Time Event-Based Streaming Network Monitoring Data Recovery," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 3, pp. 2413–2429, May–June 2025, Doi: 10.1109/TDSC.2024.3519197.
[7]. C.-F. Yang and Y. Shinjo, "Compounded Real-Time Operating Systems for Rich Real-Time Applications," IEEE Access, vol. 13, pp. 26079–26104, 2025, Doi: 10.1109/ACCESS.2025.3538561.
[8]. H. Guo, "Research on Engineering Quality Risk Prediction and Real-Time Monitoring Technology Based on Deep Learning," Proc. 2nd Int. Conf. Telecommunications and Power Electronics (TELEPE), Frankfurt, Germany, 2025, pp. 534–538, Doi: 10.1109/TELEPE66277.2025.00101.
[9]. F. Wei et al., "Security Risk Assessment System for Power Monitoring Systems Based on Zero Trust Architecture," Proc. 4th Int. Conf. Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI), Guangzhou, China, 2024, pp. 215–218, Doi: 10.1109/CEI63587.2024.10871505.
[10]. I. Sadooghi et al., "Albatross: An Efficient Cloud-Enabled Task Scheduling and Execution Framework Using Distributed Message Queues," Proc. IEEE 12th Int. Conf. e-Science, Baltimore, MD, USA, 2016, pp. 11–20, Doi: 10.1109/eScience.2016.7870881.
[11]. S. Dong et al., "Joint Compliance Control of Biped Robot Considering Position Tracking and Task Priority," IEEE Canadian Journal of Electrical and Computer Engineering, vol. 48, no. 2, pp. 66–77, Spring 2025, Doi: 10.1109/ICJECE.2025.3542792.
[12]. D. Ko et al., "Compensation Modulation for Tracking Accuracy in Free Motion and Compliance During Interaction," IEEE/ASME Transactions on Mechatronics, vol. 30, no. 1, pp. 180–190, Feb. 2025, Doi: 10.1109/TMECH.2024.3392308.
[13]. B. Alamri et al., "Cybersecurity Risk Management and Evaluation Framework of Blockchain Identity Management Systems in HIoT: Experts Evaluation," IEEE Access, vol. 12, pp. 144652–144683, 2024, Doi: 10.1109/ACCESS.2024.3468379.
[14]. R. Vaarandi et al., "A Systematic Literature Review of Cyber Security Monitoring in Maritime," IEEE Access, vol. 13, pp. 85307–85329, 2025, Doi: 10.1109/ACCESS.2025.3567385.
[15]. L. Song, "A Hybrid Data Protection Mechanisms Using Attribute Based Encryption and Role Based Access Control Mechanism for Digital Music Classrooms," Journal of Cyber Security and Mobility, vol. 14, no. 5, pp. 1033–1066, Sept. 2025, Doi: 10.13052/jcsm2245-1439.1451.
[16]. S. Murlidharan, V. Ravulakole, J. Karnati and H. Malik, "Battery Management System: Threat Modeling, Vulnerability Analysis, and Cybersecurity Strategy," in IEEE Access, vol. 13, pp. 37198-37220, 2025, Doi: 10.1109/ACCESS.2025.3543249.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15555

[17]. H. Boyes and M. D. Higgins, "An Overview of Information and Cyber Security Standards," in Journal of ICT Standardization, vol. 12, no. 1, pp. 95-134, March 2024, Doi: 10.13052/jicts2245-800X.1215.

[18]. M. Jubur, C. R. Price, M. Shirvanian, N. Saxena, S. Jarecki and H. Krawczyk, "Building and Testing a Hidden-Password Online Password Manager," in IEEE Transactions on Information Forensics and Security, vol. 20, pp. 7454-7468, 2025, Doi: 10.1109/TIFS.2025.3583459.

[19]. B. Yamini, P. M. Appa M.A.Y., R. Shobana, A. T P, M. Nalini and S. S. R, "Cybersecurity: Strategies, Sector-Specific Challenges, and Future Prospects," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1338-1345, Doi: 10.1109/ICUIS64676.2024.10866441.

