**GROUP 12 CONCEPT PAPER**

**TITLE:RBAC FOR SECURELY SHARING CLASSIFIED DOCUMEN** **TS**

Digital evidence is crucial in criminal investigations, but managing and securing it poses significant challenges. Unauthorized access, data breaches, and lack of accountability can compromise investigations. This paper proposes a secure Role-Based Access Control (RBAC) system to protect digital evidence. The system would limit access based on user roles, ensuring security, compliance, and traceability. By integrating this RBAC system, law enforcement agencies can effectively manage digital evidence while maintaining integrity a

**Problems It Solves**

* **Unauthorized Access**: Prevents unauthorized personnel from accessing, altering, or deleting critical digital evidence.
* **Data Breaches**: Mitigates the risk of data breaches by ensuring that only authorized individuals can interact with evidence.
* **Lack of Accountability**: Provides a transparent audit trail of user activities, ensuring that all actions related to evidence handling are traceable.
* **Inefficient Evidence Management**: Addresses challenges related to managing large volumes of digital evidence, ensuring organized and structured access control.
* **Compliance Issues**: Ensures compliance with legal standards and regulations governing the handling and storage of digital evidence, such as the Federal Rules of Evidence (FRE) or GDPR.

**Existing Solutions**

* **Traditional Access Control Systems**: Basic password-protected systems are often insufficient to control access to sensitive digital evidence, especially in large, multi-user environments.
* **Generic Role-Based Access Control (RBAC) Systems**: While general RBAC systems exist, they may not be tailored specifically for the intricacies of digital evidence management, including the need for detailed access control and audit capabilities.
* **Manual Processes**: Many law enforcement agencies still rely on manual, error-prone processes for tracking who accessed or modified digital evidence, leading to increased risks of mishandling.

**Proposed Solution**

* **Customizable RBAC Framework**: Develop a tailored RBAC system specifically designed for digital evidence management, allowing for customizable user roles, permissions, and access controls that align with organizational needs.
* **Advanced Security Features**: Implement encryption, multi-factor authentication (MFA), and secure communication protocols to safeguard evidence from unauthorized access.
* **Centralized Audit Logging**: Introduce a centralized logging system that automatically records and stores all user interactions with digital evidence, ensuring that actions are traceable and auditable for accountability.
* **Role-Specific Dashboards**: Provide role-specific dashboards that display only the relevant evidence and functionalities based on user permissions, ensuring ease of use while maintaining security.
* **Compliance and Legal Alignment**: Design the system to comply with regulatory standards and industry best practices, ensuring that all evidence handling procedures align with legal requirements.

**Key Features of the Role-Based Access System**

* **Role Definition**: Allows the creation of distinct user roles based on job responsibilities (e.g., investigators, evidence managers, auditors, IT personnel).
* **Granular Permissions**: Provides fine-grained access control, ensuring users only access digital evidence relevant to their role.
* **Audit Trail**: Logs all interactions with digital evidence (e.g., access, modifications, deletions) for accountability and compliance.
* **Scalability**: Can be scaled to accommodate large volumes of digital evidence and a growing number of users across different departments or jurisdictions.
* **Integration**: Designed to integrate seamlessly with existing digital evidence management systems.
* **Multi-Factor Authentication (MFA)**: Enhances security by requiring multiple forms of verification for sensitive access.