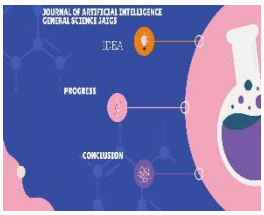
Vol.4, Issue 01, April 2024
Journal of Artificial Intelligence General Science JAIGS

https://ojs.boulibrary.com/index.php/JAIGS



DNA Cryptography for Enhanced Data Storage Security in Cloud Environments

Mithun Sarker

Independent Researcher Beaumont, Texas, United States

ARTICLEINFO
Article History:
Received: 01.05.2024
Accepted: 15.05.2024
Online: 22.05.2024
Keyword: Secure Data Management: Context-Aware Access Control, Entity Governance, and Advanced Reasoning Mechanisms

ABSTRACT

Despite the persistent security challenges inherent in cloud systems, a distributed cloud environment necessitates an access control model that is contextually aware to effectively manage these challenges. This model should incorporate a role activation process based on the user's contextual information. Within this role activation process, the rationale behind data collection and usage is disclosed, enabling administrators to establish context-based policies. Consequently, role permissions are dynamically activated based on the association of roles with context. To mitigate complications in the role-based access control model, users are categorized into classes or groups, each with its own access control standards. Access to specific resources is determined by the user's identity upon request.

Traditional access control models often fall short in cloud environments due to their inability to address all aspects of the diverse entities, resources, and users present. In the proposed access control system with perception reasoning, entities are expanded using Extensible Access Control Markup Language (XACML), while a trust module monitors user behavior dynamically, detecting and restricting malicious users attempting illegal data access. This includes assigning an identity tag to malicious users, which involves task and data classification along with database tagging.

Introduction:

Cloud computing offers scalable processing and storage capabilities, facilitating broad network access and reliable services. It enhances organizational productivity, development, and resource utilization by providing shared infrastructure, dynamic software provisioning, and online accessibility [1]. Once the cloud setup is established, services are deployed based on business requirements, reducing costs and complexity in managing computer and network processes [2].

Cloud deployment models categorize clouds into four types: Public, Private, Hybrid, and Community. Public clouds offer services over the internet to users via web applications, while Private clouds limit resource access to enterprise customers. Hybrid clouds combine aspects of Public and Private clouds, and Community clouds distribute resources among users managed by a third party [3].

Despite the advantages of cloud computing, security concerns such as threats, attacks, and vulnerabilities exist. These issues are classified into taxonomy, stemming from cloud providers or customers. Access security issues, prevalent in SaaS systems, require appropriate access conditions to prevent data leakage. Malicious insiders pose a threat by compromising physical security and accessing systems, leading to significant data breaches. Authorization plays a crucial role in maintaining integrity and avoiding security issues, with coarse authorization control models managed by system administrators. Identity management involves identifying entities based on pure identity, service paradigms, and log-on information [4].

The distributed nature of cloud environments presents challenges in handling various entities across different cloud regions. Establishing strong relationships between resources and users is crucial for access control. The Secure Data Access Control with Perception Reasoning (SDACPR) model addresses limitations of traditional models by considering configuration points and defining relationships between multiple entities. This enhanced access control model, managed by Administrators, ensures secure entity management and privileged authorization without compromising user rights in cloud environments. It also identifies and prevents unauthorized access by malicious users [6].

The rest of the paper is organized as follows: Section 2 outlines different approaches to access control models. Section 3 details the proposed role-based access control. Section 4 presents simulation setup and results to evaluate the SDACPR model's performance. Finally, Section 5 offers analysis, and Section 6 concludes the paper.

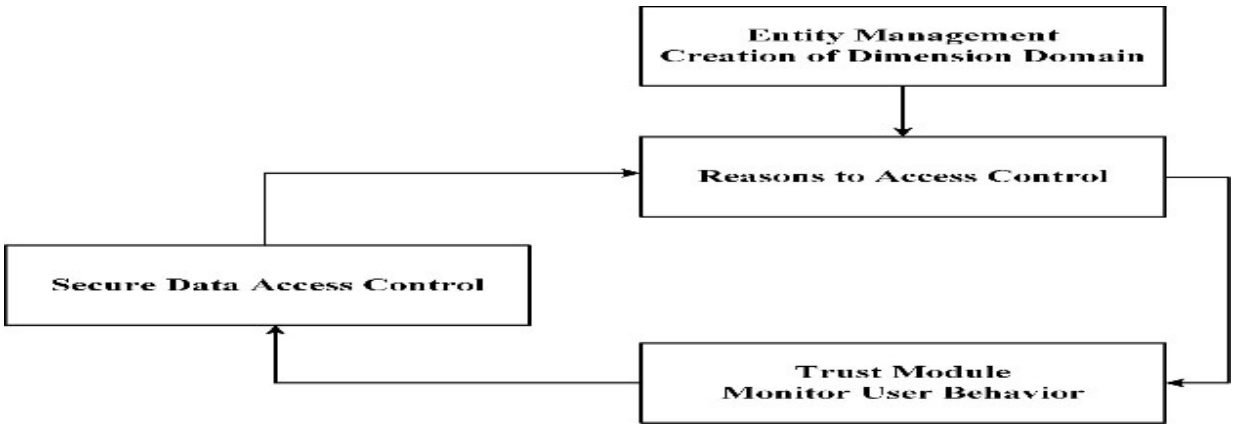
Related Work

RBAC lacks dynamic access control in cloud computing environments due to the absence of context-aware elements. Adaptive access control algorithms based on AAC, time constraints, and context technology have been proposed to enhance security by building trust levels for users. However, these mechanisms often lack location constraints and face challenges in measuring trust levels [7]. Distributed RBAC and cloud-optimized RBAC models aim to increase scalability and flexibility by allowing a single data manager to control access but struggle with heterogeneity and security domain issues [8][9]. Semantic access control schemes combined with RBAC have been explored in healthcare units to manage access based on various attributes, but complexity remains a challenge [10].

Healthcare units also utilize access control models combining TRBAC and workflow authorization, which can lead to security issues depending on active/passive workflows [11]. Additionally, the association of RBAC with ontology frameworks has been proposed, where ontology domains control hierarchical roles [12]. The integration of ABAC and RBAC forms the ARBAC model, enhancing system privacy by associating role activation processes with context information [13].

Delegation principles, reasoning mechanisms, and security environments maintain a hierarchical order in permission assignment, ensuring secure role-based access control. Usage-based access control (UBAC), service-based access control (SBAC), and trust-based access control (TBAC) differ from RBAC in their approach. UBAC verifies user access periodically but lacks support for private cloud environments [14]. SBAC is challenging to implement and prone to information leakage [15]. Trust management models associate trust with identity and behavior, but they may fail in multi-domain cloud environments [16].

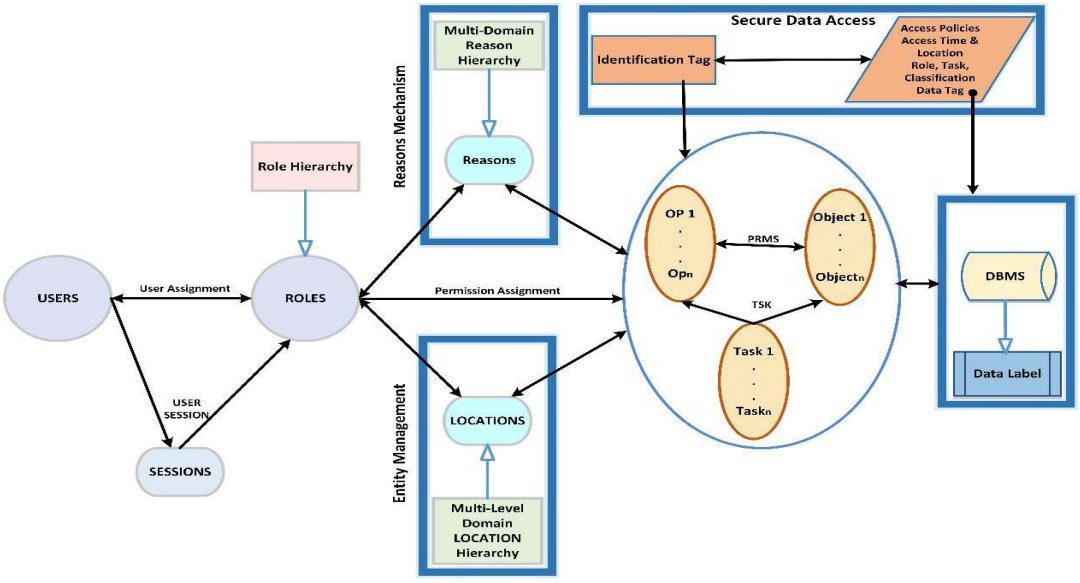
Contract RBAC lacks context reasoning and cannot prevent information leakage [17]. Context RBAC addresses integrity breaches but lacks definition for trust relationships [18]. ARBAC may suffer from uncontrollable user behavior and lacks data protection and access control within the cloud environment [19]. ABAC is not suitable for multi-tenancy cloud environments and lacks mechanisms for device registration and entity management [20]. Ontology-based access control detects and prevents insider intrusion but may fail to protect against external intruders [21]. Table 1.1 provides a comparison of access control models based on context-awareness parameters such as time, location, platform trust, and support for malicious insiders, malicious outsiders, and cloud environments.



The proposed model comprises applications grouped as objects, symbolizing the various departments within an organization, thus fostering a flexible cloud environment. These applications span multiple domains interconnected by reasons and domains, where roles serve as participants dictating job functions for employees to access resources and manage entities. The proposed access control model is well-suited for highly distributed cloud computing environments, featuring user and device registration. Roles within the RBAC mechanism are structured hierarchically based on their respective applications, assigned dynamically or statically to prevent information loss. Leveraging reasoning for data collection and utilization, the RBAC model enables administrators to establish context-based policies, ensuring user credentials' protection without third-party involvement. Streamlined policy management and enhanced control are enforced on both access and administrative policies. Reasoning mechanisms are implemented using extended XACML entities. Upon identification of a malicious user by the trust module, an identity tag is issued to prevent unauthorized data access. The following diagram illustrates the operation of the proposed access control scheme.

Enhanced Data Access Control with Reasoning Mechanisms

Expanding upon traditional RBAC, the integration of reasoning capabilities empowers administrators to establish context-based policies. Illustrated in Figure 2, the extended RBAC model with reasoning-to-access role assignment enhances organizational understanding of user permissions, operations, and associated objects. Diverse resources and users are effectively managed, forming a dimensional domain where all entities are meticulously logged and bound within the extended RBAC framework. A trust module diligently monitors user behavior, swiftly detecting any potential malicious activity. Upon identification, a unique identity tag is promptly issued to the malicious user. Task classification and data tagging, based on sensitivity parameters, further fortify the system, thereby restricting unauthorized access to secure data.



Entity Management within Role-Based Access Control

Domain

A domain refers to a logically bounded space containing at least one object or a list of objects. These objects could be applications within a fully or partially ordered domain. Domains serve to represent the departmental structure of an organization, offering flexible methods for partitioning objects. Relationships among domains are established through purposes and domains. Roles, on the other hand, represent participants within a domain and serve as a grouping mechanism for various job functions. This grouping is organized based on the job functions performed by employees, reflecting the organizational structure. Therefore, it is imperative for the system to possess complete knowledge and identification of domains, objects, and roles [27].

Physical Organization of the Domain

Objects within the domain are managed by the domain administrator, who also oversees the organization of network objects and establishes a logical hierarchy. Each organization has specific administrative requirements, often addressed through the delegation of authority and operational responsibilities to control various operations. Thus, the domain serves as a logical structure utilized to manage the administrative needs of the organization. Some key features of the proposed physical layout of the domain include:

i. Context Collection

ii. Reason Management

iii. Policy Unit

iv. Reason Hierarchy Management

v. Dimensional Reasons Role (DRS) and Dimensional Domain (DD) Relation Management

The physical layout encompasses characteristics such as context collection, reason management, policy management unit, reason hierarchy management, dimensional reason role, and dimensional domain relation management. The physical domain consists of the reason module and policy unit. Within the reason module, the context collector gathers contextual information from the context analyzer, generated through the context generator. The reason module also includes the reason manager, responsible for activating reasons through the reasons activator and maintaining the Reason Hierarchy. Furthermore, it contains the Dimensional Reasons Manager (DRS), which maintains dimensional reasons at both the Generalized Local Hierarchy (GLH) and Specific Local Hierarchy (SLH) levels through DRS-GLH

allocator and DRS-SLH allocator, employing the DRS transmitter. This technique is based on context values to capture the reasons effectively. The physical layout of the domain is depicted in the diagram below, illustrating the trust relationship in the model.

Simulation and Results

XACML

The Extensible Access Control Markup Language (XACML) [29] facilitates the implementation of complex permissions within systems. It defines role hierarchies, permissions, and permission-role assignments, thus offering support for implementing role-based access control models tailored for the cloud computing environment.

Table2:Extended Entities of CPR-TRBACModel.

Extended Entities of SDA CPR Model using XACML

CPR-TRBACEntities	XACMLImplementation
PHYSICALLOCATION	<PL>
LOGICALLOCATION	<LL>
GERNERALLOCATIONHIERARCHY	<GLH>
SPECIFICLOCATIONHIERARCHY	<SLH>
DIMENSIONALDOMAINOVERGLH	<GSDD>
DIMENSIONALDOMAINOVERSLH	<SSDD>
REASONTOACCESS	<RS>
DIMENSIONALREASONTOACCESS	<DRS>
DIMENSIONALREASONS ROLE	<DRSR>

Analysis

Within a cloud computing system, users are allocated roles which, in turn, are assigned tasks based on their requirements. These tasks encompass permissions that authorize users to access various resources, each with specific classifications and data tags. Users assigned tasks are regulated by a reasoning mechanism that issues identity tags in response to their dynamic behavior. The proposed security model for the cloud relies on time/location constraints and delegation principles to meet security needs.

Roles play a pivotal role in the functionality of cloud computing systems, as they govern access properties. Within an organization, roles might correspond to job titles such as accounting, secretary, or manager roles. Tasks assigned to these roles determine the permissions granted to users, enabling resource access. Each role is assigned tasks that undergo an authorization process to ensure system management integrity.

Constraints like time/location and principles like least privilege and Separation of Duties (SOD) are crucial for secure management. The security model also includes classifications and tags such as identity and data tags, which facilitate resource access and data usage, respectively. These classifications are hierarchical, ranging from top-secret to unclassified, ensuring proper resource access.

The reasoning mechanism is another vital component, issuing identity tags to users based on their dynamic behavior. These tags enable secure resource access. The model encompasses both active and passive workflows, addressing a large user base with dynamic behavior using heterogeneous techniques and enforced policies.

The security environment is categorized into secure and unsecured environments. In a secure environment, identity tags are not required, and permissions are granted based on assigned tasks and roles using the reasoning mechanism. In contrast, an unsecured environment relies on identity tags at each step to maintain security.

Conclusion

This study delves into the essential security measures necessary for the cloud computing environment. By augmenting the task-role-based RBAC model with the knowledge of reasoning, we introduced a more robust system capable of detecting reasons for accessing specific resources. Our exploration included concepts such as dimensional reasoning, dimensional reason roles, and their interrelations, enhancing our understanding of resource-user relationships.

The proposed model, termed Reasoning RBAC, not only retains the features of traditional task-role-based RBAC models but also introduces context awareness, flexibility, and heightened security. Moreover, it incorporates access control policy enforcement through a novel policy syntax, ensuring comprehensive time/location-based, context-based, reason-oriented, and temporal-based access control within the cloud computing realm.

Implemented in the Extensible Access Control Markup Language (XACML) and Windows 2012 Policy Server, our approach establishes strong relationships between users and resources using domains. This comprehensive framework promises a cloud computing environment devoid of security and privacy

vulnerabilities, offering robust defense mechanisms against malicious insider and external threats through secure data access control.

References List:

[1]. Prakash, S., Malaiyappan, J. N. A., Thirunavukkarasu, K., & Devan, M. (2024). Achieving Regulatory Compliance in Cloud Computing through ML. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2).

[2]. Malaiyappan, J. N. A., Prakash, S., Bayani, S. V., & Devan, M. (2024). Enhancing Cloud Compliance: A Machine Learning Approach. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2).

[3]. Devan, M., Prakash, S., & Jangoan, S. (2023). Predictive Maintenance in Banking: Leveraging AI for Real-Time Data Analytics. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(2), 483-490.

[4]. Eswaran, P. K., Prakash, S., Ferguson, D. D., & Naasz, K. (2003). Leveraging Ip For Business Success. International Journal of Information Technology & Decision Making, 2(04), 641-650.

[5]. Prakash, S., Malaiyappan, J. N. A., Thirunavukkarasu, K., & Devan, M. (2024). Achieving Regulatory Compliance in Cloud Computing through ML. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2).

[6]. Malaiyappan, J. N. A., Prakash, S., Bayani, S. V., & Devan, M. (2024). Enhancing Cloud Compliance: A Machine Learning Approach. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2).

[7]. Biswas, A. (2019). Media Insights Engine for Advanced Media Analysis: A Case Study of a Computer Vision Innovation for Pet Health Diagnosis. International Journal of Applied Health Care Analytics, 4(8), 1-10.

[8] Chopra, B., & Raja, V. (2024). Toward Enhanced Privacy in Digital Marketing: An Integrated Approach to User Modeling Utilizing Deep Learning on a Data Monetization Platform. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 1(1), 91-105.

[9]. Raja, V. (2024). Fostering Privacy in Collaborative Data Sharing via Auto-encoder Latent Space Embedding. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), 152-162.

[10]. Raja, V. ., & chopra, B. . (2024). Exploring Challenges and Solutions in Cloud Computing: A Review of Data Security and Privacy Concerns. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 4(1), 121–144. https://doi.org/10.60087/jaigs.v4i1.86

[11]. SARIOGUZ, O., & MISER, E. (2024). Data-Driven Decision-Making: Revolutionizing Management in the Information Era. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), 179-194.

[12]. Raja, V. (2024). Exploring Challenges and Solutions in Cloud Computing: A Review of Data Security and Privacy Concerns. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), 121-144.

[13]. Biswas, A. (2019). Media Insights Engine for Advanced Media Analysis: A Case Study of a Computer Vision Innovation for Pet Health Diagnosis. International Journal of Applied Health Care Analytics, 4(8), 1-10.

[14]. Chennupati, A. (2024). The evolution of AI: What does the future hold in the next two years.

[15]. Chennupati, A. (2024). Addressing the climate crisis: The synergy of AI and electric vehicles in combatting global warming. World Journal of Advanced Engineering Technology and Sciences, 12(1), 041-046.

[16]. Chennupati, A. (2024). The threat of artificial intelligence to elections worldwide: A review of the 2024 landscape. World Journal of Advanced Engineering Technology and Sciences, 12(1), 029-034.

[17]. Talati, D. (2023). Telemedicine and AI in Remote Patient Monitoring. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3), 254-255.

[18]. Talati, D. (2023). Artificial Intelligence (Ai) In Mental Health Diagnosis and Treatment. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3), 251-253.

[19]. Talati, D. (2023). AI in healthcare domain. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3), 256-262.

[20]. Talati, D. (2024). AI (Artificial Intelligence) in Daily Life. Authorea Preprints.

[21]. Fan, K. (2024). Implications of Large Language Models in Medical Education. https://doi.org/10.62594/brmo4385

[22]. Warnes, M. (2024). The Efficacy of NVivo in Conducting Literature Reviews: A Case Study on Defining “Teaching Excellence.” https://doi.org/10.62594/vraa3705

[23]. Ferdinand, J. (2024). Recognising Clinical Signs and Symptoms on Black, Asian and Minority Ethnic (BAME) Skin Types. https://doi.org/10.62594/ovfn5405

[24]. Chaudhary, G., Yadav, S., Bastola, P., & Limbu, S. (2024). Challenges and Opportunities in Applying Transformative Learning Theory (A Critical Reflection): A Collaborative Autoethnography. https://doi.org/10.62594/qwfc9551