"This is the peer reviewed version of the following article: **[**Security and Privacy, 2021] ***which has been published in final form at*** **[**https://onlinelibrary.wiley.com/doi/10.1002/spy2.160] ***purposes in accordance with Wiley Terms and Conditions for Self-Archiving."***

Developing an access control management metamodel for secure digital enterprise architecture modelling

Running title: Access control management metamodel

Kamrun Nahar[1], Asif Qumer Gill[1], Terry Roach[2]

[1]School of Computer Science, University of Technology Sydney, Ultimo NSW 2007, Australia
[2]Capsicum Business Architects Pty Ltd, 61 York St, Sydney NSW 2000, Australia

Acknowledgement: This work is supported by the Australian Government Research Training Program (RTP), and a joint grant from NSW Cyber Security Network and Capsicum Business Architects Pty Ltd, Australia. Grant No. PRO19-7879. This research was conducted at the University of Technology Sydney, Australia. We wish to thank the industry professionals and reviewers for providing valuable feedback in improving the design of the proposed metamodel. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Abstract

There is an increasing interest in embedding the security in the design of digital enterprise architecture (EA) modelling platform to secure the digital assets. Access control management (ACM) is one of the key aspects of a secure digital enterprise architecture modelling platform design. Typical enterprise architecture modelling approaches mainly focus on the modelling of business, information, and technology elements. This draws our attention to this important question: how to model ACM for a secure digital EA modelling platform to ensure secure access to digital assets? This paper aims to address this important research question in collaboration with our industry partner and developed an ontology-based ACM metamodel that can be used by enterprises to model their ACM for a particular situation. This research has been conducted using the well-known action-design research (ADR) method to develop and evaluate the ACM metamodel for the secure digital EA modelling platform.

Keywords: Access control management, Metamodel, Enterprise Architecture, Ontology, Model, Action Design Research.

1. Introduction

Security, impelled by the necessity of protecting digital assets (e.g. model, data, documents, images), is an essential element of a contemporary digital enterprise. As security threats, both external and internal[1], are evolving continually, ensuring digital assets' security is not an easy task to accomplish, particularly in the recent digital transformation and EA context. EA concepts, originated from the systems engineering community, intend to address the design concerns of highly distributed large information systems and organisations[2]. EA is a holistic representation of information about various enterprise components or assets such as business objectives, goals, strategies, processes, people, technology infrastructure, organisational structures, informational entities, and application systems, enabling the efficient planning of the organisational changes[3,4]. Nowadays, due to the vital role of digital technology (e.g. cloud, IoT, mobile) in the enterprise's success, it is important to consider digital asset security as part of digital EA[5].

ACM is one of the key components of enterprise security. To ensure protected and compliant access to digital assets, implementation of ACM is required. In this regard, having an appropriate modelling language that practitioners can use to model ACM as an integral part of EA will be empowering. Typical EA modelling approaches and their metamodels (e.g. ArchiMate) mainly focus on modelling business, information, and technology elements[6]. Seamless integration of ACM with business architecture can

provide a valuable extension for the remaining layers of information and technology architectures within the overall context of secure digital EA modelling (as shown in figure_1).

Mandatory Access Control (MAC) model[7], Discretionary Access Control (DAC) model[7], Role-Based Access Control (RBAC) model[7], and Attribute-Based Access Control (ABAC) model[7] are the standard available ACM models. As each model is different from another, with regard to their attributes and functionalities, an organization needs to consider the overall context of their enterprise while choosing the suitable ACM model. An ACM model that can serve any organization's security requirements is challenging. Hence, there is a need for a flexible specification of ACM systems using semantic relations among different entities and resources. Ontology can be used in this aspect to capture the semantic-based information of various concepts associated with a domain. An ontology-based adaptive metamodel can be instantiated for different situations and semantically expressed, communicated and managed[8]. In our earlier publication[9] we reviewed all the standard ACM models and the concepts of ontology, model and metamodel in order to develop the artefact.

This research applied well-known ADR methodology[10] to design, develop and evaluate the ACM metamodel by engaging with an Australian industry partner CP ('CP' is a coded name) to address their need for developing the ACM metamodel for their digital EA modelling platform, which is called JP here (for privacy purpose, we used coded name rather than using their actual modelling platform name). JP is a cloud-based collaborative digital EA modelling platform which offers a single consistent semantic expression of the enterprise and its digital assets, to guide the implementation of a digital technology-driven system, which, aligns information, people, processes, and business logic[11]. JP was initially developed using the CAPSICUM metamodel, which is a research artefact[12].

CP intends to create an ACM metamodel that will offer the necessary entities and relationships to model the ACM system to secure the platform's digital assets. This draws our attention to the following practice-oriented research question: how to model ACM for a secure digital EA modelling platform to ensure secure access to digital assets?. The purpose of this research project (2019 - 2020) was to develop an ontology-based ACM metamodel, which CP or any other organisations can adopt, irrespective of domain. Typically, when an ACM model is developed, modellers rely on ACM related scenarios, and models are built around those scenarios. Conceptual entities of the existing traditional ACM models are usually fixed and tied to an organisation, business domain or technology stack. Adapting such fixed models for ACM scenarios, where technology stack or business domain is different, can be cumbersome and challenging. An ontology-based adaptable ACM metamodel can help to achieve this objective. Furthermore, as the proposed metamodel will be founded on an appropriate ontology, each element will have an unambiguous and standardised meaning. Enterprises can use this metamodel to model their ACM uniformly. Furthermore, this technology-agnostic and business layer focused ACM metamodel could provide a generic and adaptable foundation for building technology-specific ACM architectures and solutions. To represent the metamodel, a graph modelling approach[13] is used in this research. This enables adaptability in the design of the metamodel by allowing the inclusion of new concepts or entities in the ontology and metamodel to accommodate the continuously evolving requirements of the ACM system.

To develop the artefact, existing available and published access control models have been reviewed to understand the research landscape. Afterwards, an ACM metamodel has been incrementally developed and evaluated. This paper is organised as follows. Section 2 describes the theoretical background and related work. Section 3 presents the research context. Section 4 presents the metamodel increments before concluding in section 5.

2. Theoretical Background and Related Work

2.1. Access Control Management

ACM is needed to mitigate the risks of unauthorised access to digital enterprise assets[14]. There are several existing ACM models. Based on organisational structure, requirements, available technology stack and technical capabilities organisation may choose and tailor their own ACM model. For effective and successful implementation of security, organisations need to support business objectives, and security needs[15]. In most organisations, security policy defines who has access to which resources and how this access has to be regulated and managed. In the RBAC model, organisations' security policy explains how permissions can be associated with the roles[16]. Access decisions depend on roles that a user has to perform in an organisation, and roles could represent tasks, responsibilities, and qualifications associated with an enterprise[17-19].In[19], the authors identified four RBAC levels, and each level contains the conditions of the previous one. In the first level, users are associated with roles, and roles are associated with permissions. One role can be given to multiple users, and one user can take multiple roles. The second level adds role hierarchies, where hierarchy defines a senior role that can access a junior role's permissions. The third level adds a constraint, which is a separation of duties (SOD) where SOD defines that a subject cannot assume multiple roles at the same time while accessing an object. Finally, level four adds a new requirement to perform the permission-role review similarly to the user-role review. This will allow finding the roles to which particular permission is assigned and vice-versa. This four-level of RBAC is recognised as the family of RBAC and considered as a standard RBAC model[20]. Figure_2 represents the main concepts of RBAC.

2.2. Enterprise architecture

EA frameworks provide guidance to practitioners regarding the dynamics of business operations and the underlying technology that supports a business plan through the development of conceptual models of architectural taxonomies and methods[21]. Therefore, EA provides a blueprint of an enterprise's structure and behaviours that link different aspects or domains of architecture[22]. To optimise organisation as a whole in a harmonious and coherent way, rather than considering small business unit level sub-optimisation, is one of the aims of an EA. The benefits of an enterprise approach are: improved overall organisation performance; increased competitiveness in the marketplace and operational excellence in service and product delivery[23]. EA defines how the systems can be used to meet the enterprise's needs in a more collaborative way[24]. There are a number of EA frameworks such as Zachman framework[21], The Open Group Architecture Framework TOGAF[25] etc. These frameworks are different from one another. For instance, the Zachman framework provides EA ontology [21], and TOGAF provides a concrete EA method[25]. There are also a number of high (e.g. ArchiMate, ADL) and low detailed level modelling standards (e.g. BPMN, UML, BMM)[26]. ArchiMate[6] provides high-level architecture modelling notation for EA. BPMN [27] is a business process modelling standard that specifies a standard business process model notation for formally describing and analysing the business processes. UML[28] is popular as software architecture and design modelling language, which has been developed by Object Management Group(OMG).BMM[29] is a business strategy or plan modelling language that offers a general-purpose modelling language. Model-Driven Architecture (MDA) is another popular approach which is also developed under the auspices of OMG[30].MDA has made a particularly significant contribution towards model-based software engineering approaches to design and deploy complex system architectures. Hence, it is clear that there are a number of EA frameworks and modelling approaches. However, these seem to provide the metamodels for modelling the business, information and technology layers of the EA.

Information security is a crucial aspect for today's enterprise as the volume of digital assets[31] is growing exponentially. The aim of security is to protect a system from malicious use of its resources[32]. Integrating information security and privacy in enterprise-wide business process management and technical infrastructure is an effective approach for enterprise-wide risk management[33]. In[33], the authors proposed a roadmap for establishing enterprise-wide information security using a systematic approach. This study[33] focused on how security and privacy can be addressed throughout the solution life cycle from proposal to retirement in EA. EA has several security aspects such as security information and event management, enterprise vulnerability and threat management, baseline policies, procedures and standards, security awareness for employee's, identity and access management, enterprise business continuity program, enterprise security incident management, and phishing[34,32]. Hence, an access management system is one of the critical components of the enterprise security for ensuring protected and compliant access to digital assets.

2.3. Related work

ACM is required to mitigate the risks of unauthorised access to digital assets[14]. Due to the rapid digitisation of information and highly connected business environment, it is essential to have the ability to model ACM as an integral part of digital EA. Organisation may choose and tailor their own ACM model based on organisational structure, requirements, available technology stack and technical capabilities. Numerous studies have been conducted in developing standardised access control model and new technology for access management.

In[35], Jung et al. focused on relationship-based access control where user relationships and user identification are considered as a contextual information. It is beneficial for the organisations and security architects to design a fine-grained and safe access control for the enterprise work environment. Authors used Near Field Communication techniques to design the relationship-based access control architecture. In[36], authors proposed a cryptographic mechanism to provide a fine-grained access control. This scheme is developed based on the privacy preserving Blockchain structure. Privacy and access control for the Blockchain data have also been incorporated to the scheme. Again, in[37], the authors proposed a decentralized elliptic curve-based access control protocol for the information-centric networking paradigm. This protocol seems to prevent man-in-the-middle attack, reply attacks, forward security, integrity, and privacy violations scenarios. Most of the above-mentioned studies focused on the technology aspect of the access management and seem to overlook the technology-agnostic people, process and information aspects of the access controls.

A plethora of research has been done on developing the RBAC model[38-44]. In order to add more granularity and flexibility to RBAC model, many researchers have developed RBAC model by adding attribute (user attributes, context attributes and resource attributes) and policy rules(object's access policy)[38-40]. As RBAC is one of the most popular models due to its robust access control facilities and ease of management few researchers attempted to develop RBAC metamodel that can be integrated with existing EA modelling languages such as ArchiMate, DEMO, BPMN. The proposed metamodel in[45] is an extension of ArchiMate which can represent a single access control mechanism or a combination of different access control mechanisms within a single IT system, or across an entire enterprise. This unified metamodel is primarily built on the conceptual model of ABAC. However, this unified metamodel lacks the concept of EA aligned responsibility which dictates how access rights will be granted to a user [46,47]. On the other hand, in[14] authors identified conceptual links among RBAC, Design and Engineering Methodology for Organization (DEMO) and ArchiMate metamodels to develop a consistent lightweight access control model for EA. Here, authors analysed standard RBAC model to map its constructs with ArchiMate and DEMO. Similarly, in[16], the authors incorporated

RBAC concepts to ArchiMate via a task-based resource allocation metamodel, which, can capture the resource access mechanism defined by RBAC specification. However, in RBAC, roles are commonly structured in static hierarchies, and users are authorised to play such fixed roles in order to exercise various organisational functions. Therefore, role configuring and modelling of an access control system for a dynamic organisation is not a straightforward task [43,48]. Above mentioned studies considered a role as a business role. Scope and responsibilities of such a role are defined in the organisation chart. Due to business roles and their strong coupling with an organisation chart, utilising it for defining access rights often acts as an impediment in the way of granting granular access to resources based on an actual day to day user operations or different transactional contexts. A detailed description of this gap is described in section 4.2 (Increment three) in this paper.

Furthermore, these studies focused on traditional RBAC models, which are difficult to adapt with regards to various user attributes and entitlements. ACM needs to consider additional attribute information to enforce the access control policies, for example, time, location, the load of the system, purpose etc. Therefore, ACM should provide support to enforce attribute oriented (location, time, purpose etc.) policies[40]. This research aims to contribute in this area through the development of an adaptable ACM metamodel for EA. The contribution of this research can be differentiated from similar studies in multiple aspects. Firstly, although proposed ACM metamodel is pivoted on core RBAC concepts, we incorporated concepts such as "access policy" to describe the context of executing a certain access right and "access role", as opposed to a business role, for grouping access rights. Inclusion of these concepts will allow building more adaptive and context-sensitive ACM model. Secondly, the graph modelling approach[49] is used to model the ACM due to its ability to capture the complex and dynamic relationships among entities without losing the semantic meaning, which is not possible with the available traditional models based on the static entity-relationship approaches.

3. Research Context

3.1. Goal

Digitisation of information in today's organisations is a remarkable development that demands an EA with the inherent capability of securing the organisation's digital assets. Incorporating ACM with digital EA can contribute to achieving this goal. Therefore, investigating existing research on various ACM models and developing an ontology-based ACM metamodel for EA are the main objectives of this research.

3.2. Kernel Theory

Kernel theories are used to guide and influence design research[50]. To design context-specific ADR artefacts, kernel theories like metamodels, graph theory and reference architectures can be used to inform the design of the proposed ACM [51]. Kernel theories play an important role in design research as they are formally documented and accessible, creates a knowledge base by going through a scientific validation process [50,52].On the other hand, there might be no kernel theories available for completely novel artefacts, where there is no grounding in the present knowledge base. However, kernel theories might be used for evaluation purpose as well[50]. The kernel theories used in this research are enterprise information security architectures (EISA)[53] Access Control constraints[54,55], RBAC policies[53,54], existing RBAC models[38-41], Graph theory based modelling approach[49]. These kernel theories are used to guide the design of the proposed ACM metamodel for our industry partner. Brief description of the above-mentioned kernel theories is presented in table 1.

3.3. Existing Industry Practice

Industry partner's EA metamodel, which, is called CAPSICUM, is also used along with the kernel theories. This is because, based on CAPSICUM metamodel, CP developed EA modelling platform (named JP)[11]. JP provides semantic modelling of the digital EA assets. It facilitates alignment and traceability from business strategy to execution through EA. It provides a management dashboard for managing change and establishes the foundation for an executable digital EA[12]. Therefore, this research uses the JP modelling platform as a baseline to further develop the proposed ACM metamodel.

CAPSICUM metamodel provides a business-focused taxonomical classification of architectural constructs[12]. Traditional EA framework like Zachman, TOGAF, FEA is a technology-focused with some alignment provided to associated business concepts. CAPSICUM is business focused and sets out to offer viewpoints and views for describing the complexities and dynamics of enterprise structure and behaviour in a systematic manner. The closest comparison is with ArchiMate, whereas ArchiMate's focus is on only notation and CAPSICUM's focus is on supporting a complete semantic modelling platform and underlying metamodel of EA[12]. CAPSICUM's business view metamodel(figure_3) constructs and their relationships are depicted by boxes connected with arrows like Resource Description Framework (RDF)[56] triples in semantic modelling where the originating box is the subject, the label on the arrow is the predicate, and the destination box is the object in a triple relationship. Goal, strategy, policy, objective, tactic and rule are the six high-level constructs of CAPSICUM metamodel. For instance, CAPSICUM business view metamodel consists of nine key constructs: role, outcome, undertaking, resource, intent, evaluation, activity, context, entitlement, compliance, condition, and assertion[12].

3.4. Methodology

ADR, an interventionist approach for practice-based research, is appropriate for designing, developing, and evaluating IT artefacts through an iterative cycle in an organisational setting. Unlike other design research methods that focus on the technological view while building the artefact [10], ADR values organisational relevance and ensures the artefact creation process does not overlook organisational context even though the initial design is directed by the researchers' intent and relevant kernel theories. ADR describes and interprets a practical phenomenon in its real-life context. In this method, practitioners from the industry and researchers from academia collaborate with a common view of addressing a practical research problem[57-59]. Therefore, building trust and commitment among the participants is crucial for ensuring the success of such research. ADR method aims to solve problems encountered in a specific organisational setting through an iterative process. Furthermore, Kernel theory offers the necessary knowledge base to build and evaluate the artefacts. In each iteration, developed artefacts are evaluated and communicated to stakeholders for early feedback and adjustments. Active collaboration between researchers and practitioners is the key to solve the given problem[51]. ADR adheres to four stages of activities where a number of tasks are performed in each stage following a set of principles[60]. These stages are - 1) Problem formulation, 2) Building, intervention, and evaluation (BIE) 3) Reflection and learning, and 4) Formalisation of learning[60] (figure_4). This research involves researchers from UT (coded name) and practitioners from CP to form a collaborative ADR team with an intent to solve the practical industry problem regarding access control of the digital resources in a digital EA context. ADR team used CAPSICUM framework as a reference metamodel and starting point in this research along with kernel theories (as indicated earlier).

4. Applying ADR in the project

4.1. Problem formulation

Industry partner CP offers EA modelling capabilities via their cloud-based modelling platform JP to its end users. However, JP needs an appropriate ACM in order to regulate access to the platform's various digital EA assets. Therefore, CP approached UT researchers to co-develop an ACM metamodel for secure digital EA. UT researchers collaborated with CP's team of business analysts and semantic architects to articulate the research problem to initiate the research. This stage relied on the theory-ingrained artefact and practice-inspired research principles of ADR.

ACM is required for ensuring secure access of different users (e.g. architects, analysts, business stakeholders) to different digital EA assets or resources (e.g. EA models, diagram, descriptions and sensitive data). Users of CP need to access organisations' resources to execute their day-to-day responsibilities. At times, multiple users of CP may have the same responsibilities, which would require access to the same set of resources. One way of achieving this objective is to assign the same set of access rights to all of these users. According to this approach, access rights are directly coupled with the user, leading to a situation where the administrator will need to assign the same set of access rights multiple times to multiple users. Although assigning access rights directly at the user level offers flexibility and granularity, as the number of users grows, the system's maintainability reduces and the likelihood of error or security breach increases. CP intends to eliminate these limitations from their ACM system. Furthermore, CP wants to associate certain constraints with each access right in the form of access policy to further control when a user can exercise that access right. In other words, an access policy will explain the context of when a particular access right can be exercised. Hence, CP desires to adopt an ACM that will enable them to achieve above-mentioned objectives.

RBAC, where individual access right is assigned to roles instead of users, is better suited to cater to such a scenario. Therefore, one role can be associated with multiple users, and one user can play multiple roles as well. User permissions to access a given set of resources is controlled by a role. When a user is no longer attached to the responsibilities of a certain project or a user is no longer working at that organisation, then the concerned authority simply needs to revoke the role from that user. Therefore, revoking access rights is as simple as assigning it. Hence, based on CP's practical need, researchers decided to develop an adaptable ACM metamodel, which would be centred around RBAC. Other functionalities of ACM would be added to the proposed metamodel to meet the requirements of CP. This research aims to develop an ACM metamodel which will cater to CP's business need and a similar class of problem. ADR teams drew on Kernel theory 1 and 5 knowledge base to inform the proposed metamodel design, including the industry partner's current metamodel.

4.2. Building, Intervention and Evaluation (BIE)

ACM metamodel for JP is incrementally developed through BIE activities of the ADR method. To achieve the research objectives, we organised the development into three increments. In the first increment, we reviewed existing research on various models of ACM to identify and synthesise the entities, relationships among entities (Kernel theory #3 & #4) and developed ontology using graph-based approach (Kernel theory #5). In the second increment, we reviewed existing related research to learn how ontology is used in this area to create a metamodel and developed our initial ACM metamodel. In order to study existing research, a keyword-based search was performed in various research databases coupled with the snowballing technique of literature review[61].Finally, in our last increment, we updated the initial metamodel to eliminate the limitations identified in the evaluation stage of increment two and developed the final ACM metamodel.

A. Increment 1

In order to develop the ACM metamodel, at first, we reviewed several models, modelling languages, ontology and their relationships, which we reported in our earlier paper[9]. RBAC policies and RBAC models (kernel theories) (table 1) were identified and reviewed to extract the entities for developing the initial ontology. Extracted entities are listed in table 4, and established relationships among the entities are shown in figure_5.

We used graph theory[62] (Kernel theory #5) for the proposed metamodel. Graph-based modelling approach seems useful for developing adaptable metamodel as required in this research[13]. This allows capturing dynamic entities, their properties and relationships without the need for using a fixed schema or relational structure[63]. Graph nodes represent the metamodel entities and edges represent the relationship between those entities[49,62,63]. Extracted entities and relationships among those entities are shown in figure_5 using the graph-based modelling approach. Advantages of using graph-based modelling approach are mentioned below [49,64,65]:

1. User can model complex real-world entities precisely as they exist or occur in real life using graphs, and this opportunity enhances the operations on data.
2. Graphs are very efficient for the representation and description of the complex relationships among elements and data.
3. Graph can store object information in a single node and display the related information through relationships.
4. Advanced queries can be developed based on the graph structure, such as the shortest path of two nodes can be considered as a subgraph of the original graph.
5. Graphs can be stored efficiently within databases by using special graph storage structure.
6. Graph database can process highly connected data compared to the relational database.
7. Graph database provides lower management and operational cost compared to the traditional relational database.

The key artefacts of increment 1 were the identification of kernel theories (table 1), extraction of entities (table 2) and identification of relationships among entities based on the graph modelling approach (figure_5).

B. Increment 2

As proposed ACM metamodel was developed incrementally, valuable and forthright feedback from the CP practitioners was obtained in design review workshop settings where researchers and practitioners reviewed and discussed their point of view about the ACM design. Several kernel theories (3 & 4) were reviewed to identify the set of entities and relationships in increment 1. According to CP's practical need, an initial ACM metamodel (figure_6) was developed in this increment. To implement the metamodel, a general purpose graph database Neo4j is used [66]. Among several graph database (e.g. Neo4j, Cosmos, Neptune and Titan), Neo4j is chosen in this research as it is highly scalable, open-source, robust native graph database[66]. Data is stored in Neo4j as nodes and edges. Each edge in the Neo4j graph database represents a bidirectional relationship. Hence there is no need to create a separate relationship for each direction[67]. For future emerging needs, new entities and their relationship can be easily added to the graph-based ACM as nodes and edges compared to fixed schema-based relational models, which are difficult to adapt and change in response to changing business needs.

According to the proposed graph-based metamodel, an assignor assigns a role to an assignee. Here, an assignor refers to an organisational admin or a system, and assignee is a user (e.g. employee, party). Each role is associated with a set of responsibilities which an assignee of that role carries out.

Furthermore, access rights are allocated to a role. When an assignee of a specific role intends to perform a certain operation to carry out a certain responsibility, assignee needs to access a specific set of resources. Access to these resources is controlled by the access rights granted to the assignee's role. Access rights can be controlled by access policy, which means at the time of accessing resources policies are checked to verify whether assignee meets the criteria required for accessing the resources. Access rights have two variations a) permission to access resources and b) prohibition from accessing resources (figure_6).

Researchers considered several experimental scenarios drawn from CP's practical need to assess the developed metamodel at the end of increment 2. While evaluating the metamodel researchers identified that 'role' is an ambiguous entity. Every employee holds a role in the organisation which comes from the role hierarchy of that organisation. Here, 'role' represents a business role like CEO, CFO, developer, customer coach, business architect etc., which represents the business role performed by an employee in the organisation. Hence, it was difficult to provide granular access to resources in digital EA modelling platform based on the business role. For example, there can be multiple employees in the business analyst role of an organisation. Although their business role is same, because of their job nature (e.g. business requirement analyst, modeller), the requirement for accessing resources can be different, which means the set of access rights will be different as well. In such a scenario, the business analyst role cannot be repurposed as an ACM role. To resolve this limitation of our initial ACM metamodel, we commenced increment 3 of BIE stage.

C. Increment 3

In increment two, we developed the initial version of the ACM metamodel by organising entities and relationships extracted during increment 1. However, evaluation of this initial metamodel identified the ambiguity of the proposed 'role' entity which manifests as the inability to grant access rights depending on what an assignee requires to perform for her day-to-day interactions without modifying the organisation's role hierarchy. In [46,54], authors discussed this particular limitation of using the business role as the role of RBAC (Kernel theory #3). This limitation stems from the fact that these roles are defined as a part of the organisation chart rather than for ACM. To overcome this limitation and provide unambiguous role ontology, we divided the role entity into two categories. One is 'business role', and the other one is 'access role' where business role represents the role form organisation's role hierarchy, and new access role represents a collection of access rights. Benefits of decoupling access role and business role are:

- We can provide granular access to users based on their actual day-to-day job responsibilities rather than the broad set of responsibilities associated with the business role.
- As different organisations will use JP, we do not need to know every organisation's business role hierarchy.
- We can create as many access roles as we need without changing business roles or organisation chart.

After decoupling access role and business role, we represent the ACM metamodel in figure_7 and table 3 represents the relationship matrix between entities (two different views of the ACM metamodel graph). According to this new graph-based metamodel, every assignee can be granted one or more access roles, which will then define assignees access to required resources.

ACM graph and matrix, from increment 3, are the final version of the proposed ACM metamodel for secure digital EA layer, which is developed by eliminating the limitations of the first version. ADR

team initiated a detailed evaluation of this metamodel by applying it to a case study. Findings of this case study are presented in the following section.

4.2.1. Business case evaluation and findings

CP provides strategic planning, business architecture modelling, business analysis and project management services via its cloud-based modelling platform JP. Senior management team, strategic planners, business architects, enterprise architects, data modellers, and business analysts are the platform's main users. CP wants to implement an ACM where the user will have access to digital EA resources based on their role. However, they want a flexible and granular way of assigning access rights so that user's day-to-day interaction with the platform is not hampered due to granting of a too narrow set of access rights and at the same time user does not get access to resources that they do not need due to granting of a too broad set of access rights. At present, JP needs to have this capability to control access to digital EA resource. Hence, CP is keen to incorporate ACM metamodel into their existing EA metamodel in order to provide a secure access mechanism to their digital assets.

To evaluate how proposed metamodel will serve CP's above-mentioned requirements, a practical business scenario is considered. CP has three business analysts (BA). Two of them primarily gather business requirements, and the third BA's primary responsibility is to create a model. Assignor (administrator) wants to allocate the same set of access right to two BA and a different set of access right to the third BA. Therefore, the assignor creates one 'Modeller' access role and one 'Business Requirement Analyst' access role. Then assignor allocates an appropriate set of access rights (permission/prohibition) to each role. Each of these access rights has associated access policy. An access policy defines the context in which an access right can be executed. The assignor can assign the 'Modeller' access role to first and second assignees (BA) and 'Business requirement analyst' role to the third assignee (BA). Here, all assignees are in the BA business role defined in the organisation chat. However, 'Modeller' and 'Business Requirement Analyst' are access roles which are defined based on access rights requirements and not linked to roles in the organisation chart. Access role will allow the assignee to access the required resources to perform job responsibilities. To explain this further, a scenario can be considered where 'Modeller' role has permission to add a new model "as a digital asset" to an EA project (permission) repository but cannot delete a model (prohibition), and both access rights have associated access policy with them, which states that associated access rights can be exercised only from office network by an active employee identity (Id) and within office time (8am-6pm) (note that policy defines a context that is set by the organisation and must exist at the time of accessing the resources). When an assignee, who is granted a 'Modeller' role, tries to add a new model to a project, context (e.g. active employee id, office network, office time) defined in the access policy must be satisfied. Figure_8 shows how the example scenario can be modelled using the proposed metamodel. In this stage, we used JP modelling platform to model the above scenario by instantiating proposed ACM metamodel. This platform uses a Resource Description Framework (RDF)[56] based graph database for storage. Data are represented as a subject, predicate, object triplet in RDF. This database supports full-text search with graph analytics and capable of logical reasoning in order to produce deeper insight from the stored data[66].

4.3. Discussion: Reflection, Learning and Formalisation

In previous sections, we briefly explained every increment of the proposed metamodel that was developed during the BIE stages of the ADR. Throughout this process of designing and developing the artefact, we resolved a number of design challenges to arrive at the final metamodel. Therefore, we aim

to briefly discuss the challenges we faced during the project development at this stage. We also formalised our reflections and learnings in the form of design principles (table 4), which can be adopted to design and develop such metamodels in a similar kind of context and class of problem.

Firstly, the appropriateness of a model should be determined by assessing the extent to which the functional and non-functional characteristics of that model satisfies the organisation's requirements. CP's modelling platform, which is developed based on Capsicum metamodel needed the ACM layer to secure their digital EA assets. As we adopted ADR methodology, researchers (UT) and practitioners (CP) were actively engaged and participated in the metamodel design workshops. Through these workshops, researchers studied kernel theories and industry partner practice framework. Practitioners were introduced to the theoretical aspects of developing an ACM metamodel. In the problem formulation stage of ADR, researchers identified that there is a need to develop an enhanced metamodel, which can capture all the practical requirements of CP. Therefore, we identified a unified set of metamodel entities and relationships for building the ACM metamodel.

Secondly, there are few challenges of using fixed schema-based relational models for ACM. One of the major challenges is the lack of ability to store semantics of the relationships and adapt to changing business needs. Hence, details of the semantics need to be captured outside of the relational system68. Furthermore, the relational model provides poor support to represent data compared to graph structures as it is less flexible and not expressive enough to visualise, manage and analyse a vast amount of information and complex real-life relationships[64,68]. Thus, while developing the metamodel, we choose graph modelling approach to overcome the limitations of the relational metamodel or model. To represent and describe the complex relationships among developed elements, graph models are extremely useful64. Graph technique provides a method to describe several real-life scenarios in a more comprehensive way and has the ability to include new entities and their relationships without the need for completely re-designing the existing metamodel or model. Further, a graph modelling approach can also be used for flexible and on-demand inter-agency ACM for secure information sharing during business as usual and emergency situations [69].

Thirdly, implementing an ACM that satisfies an organisation's information security need is a complicated endeavour. One of the key steps in this process is the choice of an appropriate ACM model. CP offers its modelling platform as a cloud-based SaaS product. The user base of the platform is diverse. It can range from organisations with a large number of users to organisations with few users. Large organisations may wish to implement a fine-grained ACM. On the other hand, organisations with a relatively small number of users may want to implement a coarse-grained mechanism to reduce the maintenance overhead. Therefore, selection of an optimal access control model is crucial. Hence during the ADR workshops, researchers reviewed all popular ACM models[9] (which we discussed our another paper[9]) and options to access the models and their functionalities. Therefore, in the ADR workshops, we tried to capture the important needs of CP. Based on the requirements, we developed the metamodel rather than trying to fit any existing model to CP modelling platform. Considering their business needs, we opted for RBAC based approach to ACM. It bundles a group of access rights and then associates those to a group of responsibilities via creating a role. Our metamodel is centred around the RBAC. Using the developed ACM metamodel, CP's platform will define their role and associate those with appropriate access rights.

Fourthly, while developing ACM metamodel for CP, we identified that 'roles' are not identical in every organisation. Despite the same business role, multiple users might need access to different resources based on their day to day activities. The business role is designed to conform to the organisation chart. Repurposing it for access control may not work in scenarios where multiple users in the same business role need to access a different set of resources. ADR team recognised this ambiguity of 'role' ontology

in the evaluation stage. Thus, we commenced a new iteration in order to appropriately resolve the identified ambiguity. Rigorous evaluation and forthright discussion after each increment are immensely important. It aids the team to assess the necessity of initiating new iterations to further refine the developed artefact. Therefore, provisioning sufficient time to resolve such issues, which are found in the evaluation stage is essential.

Fifthly, in ADR methodology researchers and practitioners both, work closely to develop the ACM metamodel artefact. However, along the way, we realised the difference of perspectives between researchers and practitioners as well. Researchers emphasised the process of developing the artefact to ensure that produced artefact is authentic and can be validated thoroughly. On the other hand, practitioners stressed on whether the model is implementable from a technical perspective and how much time it will take to implement. So, at the initial stage of the project, there was a conflict of understanding between both parties, which was resolved through mutual understanding and inclusion of both parties' perspectives.

In summary, ADR is an effective way to link practitioners and researchers in co-creating innovative artefacts that target the industry's challenges. ADR workshops play an essential role in this aspect. Active collaboration of practitioners with researchers help both parties to eliminate their difference in perspective and arrive at a common ground.

5. Conclusion

This paper presents an ontology-based ACM metamodel for secure digital EA assets using a graph modelling approach developed using ADR methodology. Kernel theories, existing industry practice and frameworks provided the necessary knowledge base for the ACM design. The benefit of using such an approach is that it offers a comprehensive way of developing an artefact, which is theory-ingrained and aligned to the practical business needs. This paper also presents an instantiation of the proposed ACM metamodel based on a case study relevant to our industry partner. The proposed ACM metamodel provides a mechanic to ensure secure access to digital EA assets. Furthermore, the graph modelling approach offers better adaptability as new entities and relationships can be easily added to the proposed ACM metamodel as required compared to the traditional fixed schema-based relational model. This metamodel will assist practitioners and researchers who are studying, designing, and developing access control related artefacts for extending traditional EA layers. Future study may focus on developing an identity management metamodel and integrating it with the developed ACM metamodel. This integrated identity and access management metamodel may provide appropriate building blocks to model enterprise identity and access management seamlessly from a business perspective. We also outlined this idea of ontology-based integrated identity and access management metamodel in our earlier paper[9]. Furthermore, according to the developed metamodel, the role assigned to a user is not dynamic. An administrator is expected to assign a role to a user. Developed metamodel can be extended by providing necessary elements to support dynamic role association based on users' attribute or biometric characteristics for a given transaction.

Data availability Statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Reference

1. Jouini M, Rabai LBA, Aissa AB. Classification of security threats in information systems. *Procedia Computer Science.* 2014;32:489-496.
2. Kale V. *Digital Transformation of Enterprise Architecture.* CRC Press; 2019.
3. Pereira CM, Sousa P. Enterprise architecture: business and IT alignment. Paper presented at: Proceedings of the 2005 ACM symposium on Applied computing2005.
4. Alzoubi YI, Gill AQ, Al-Ani A. Distributed Agile Development Communication: An Agile Architecture Driven Framework. *JSW.* 2015;10(6):681-694.
5. Zimmermann A, Schmidt R, Sandkuhl K, Wißotzki M, Jugel D, Möhring M. Digital enterprise architecture-transformation for the internet of things. Paper presented at: 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop2015.
6. The Open Group. The Archimate 3.1 Specification. https://pubs.opengroup.org/architecture/archimate3-doc/. Published 2019. Accessed 20 Nov, 2019.
7. Jayant D B, Swapnaja A U, Sulabha S A, Dattatray G MJIJoCA. Analysis of dac mac rbac access control based models for security. 2014;104(5):6-13.
8. Imran-Daud M, Sánchez D, Viejo A. Ontology-based access control management: Two use cases. Paper presented at: Proc. 8th Int. Conf. Agents Artif. Intell.2016.
9. Kamrun Nahar AQG. A Review Towards the Development of Ontology Based Identity and Access Management Metamodel. WAINA; 2020.
10. Sein MK, Henfridsson O, Purao S, Rossi M, Lindgren R. Action design research. *MIS quarterly.* 2011:37-56.
11. Capsifi. Strategic Planning Software for Business Transformation | Capsifi. @Capsifi. https://www.capsifi.com/. Published 2020. Accessed.
12. Roach T. *CAPSICUM–A Semantic Framework for Strategically Aligned Business Architecture*, Ph. D Thesis, UNSW, Sydney, Australia; 2011.
13. Ehrig H, Ehrig K, Prange U, Taentzer G. Formal integration of inheritance with typed attributed graph transformation for efficient VL definition and model manipulation. Paper presented at: 2005 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC'05)2005.
14. Gaaloul K, Guerreiro S, Proper HA. Modeling access control transactions in enterprise architecture. Paper presented at: 2014 IEEE 16th Conference on Business Informatics2014.
15. Park S, Ahmad A, Ruighaver AB. Factors influencing the implementation of information systems security strategies in organizations. Paper presented at: 2010 International Conference on Information Science and Applications2010.
16. Gaaloul K, Proper HA. An access control model for organisational management in enterprise architecture. Paper presented at: 2013 Ninth International Conference on Semantics, Knowledge and Grids2013.
17. Raje S, Davuluri C, Freitas M, Ramnath R, Ramanathan J. Using ontology-based methods for implementing role-based access control in cooperative systems. Paper presented at: Proceedings of the 27th Annual ACM Symposium on Applied Computing2012.
18. Tsai W-T, Shao Q. Role-based access-control using reference ontology in clouds. Paper presented at: 2011 Tenth International Symposium on Autonomous Decentralized Systems2011.
19. Sandhu R, Ferraiolo D, Kuhn R. The NIST model for role-based access control: towards a unified standard. Paper presented at: ACM workshop on Role-based access control2000.
20. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC).* 2001;4(3):224-274.

21. Zachman JA. A framework for information systems architecture. *IBM systems journal.* 1987;26(3):276-292.
22. Grov G, Mancini F, Mestl EMS. Challenges for Risk and Security Modelling in Enterprise Architecture. Paper presented at: IFIP Working Conference on The Practice of Enterprise Modeling2019.
23. Sherwood J, Clark A, Lynas D. Enterprise security architecture. *SABSA, White paper.* 1995;2009.
24. Alshammari B. Enterprise Architecture Security Assessment Framework (EASAF). *JCS.* 2017;13(10):558-571.
25. Harrison R. *TOGAF® 9 Certified Study Guide.* Van Haren; 2011.
26. Gill AQ. Agile enterprise architecture modelling: Evaluating the applicability and integration of six modelling standards. *Information and Software Technology.* 2015;67:196-206.
27. OMG. Documents Associated with Business Process Model and Notation (BPMN), . <http://www.omg.org/spec/BPMN/index.htm>. Published 2013. Accessed.
28. OMG. Documents associated with UML,. <http://www.omg.org/spec/UML/>. Published 2011. Accessed.
29. OMG. Business Motivation Model (BMM). <http://www.omg.org/spec/BMM/>. Published 2014. Accessed.
30. OMG. Model Driven Architecture (MDA),. <https://www.omg.org/mda/specs.htm>. Published 2014. Accessed.
31. Burkett JS. Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal: A Global Perspective.* 2012;21(1):47-54.
32. Tahajod M, Iranmehr A, Iranmehr A, Darajeh MR, Branch D, Branch S. A roadmap to develop enterprise security architecture. Paper presented at: 2009 International Conference for Internet Technology and Secured Transactions,(ICITST)2009.
33. Rachamadugu V, Anderson JA. Managing security and privacy integration across enterprise business process and infrastructure. Paper presented at: 2008 IEEE International Conference on Services Computing2008.
34. Sankhwar S, Pandey D, Khan RA, Mohanty SN. An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method. *Security and Privacy.* 2021;4(1):e132.
35. Jung K, Park SJIJoCT, Engineering. Context-aware role based access control using user relationship. 2013;5(3):533.
36. Adams C. A privacy-preserving Blockchain with fine-grained access control. *Security and Privacy.* 2020;3(2):e97.
37. AbdAllah EG, Zulkernine M, Hassanein HS. Preventing unauthorized access in information centric networking. *Security and Privacy.* 2018;1(4):e33.
38. Varadharajan V, Amid A, Rai S. Policy based role centric attribute based access control model policy rc-abac. Paper presented at: 2015 International Conference on Computing and Network Communications (CoCoNet)2015.
39. Aftab MU, Habib MA, Mehmood N, Aslam M, Irfan M. Attributed role based access control model. Paper presented at: 2015 Conference on Information Assurance and Cyber Security (CIACS)2015.
40. Tahir MN. C-RBAC: Contextual role-based access control model. *Ubiquitous Computing and Communication Journal.* 2007;2(3):67-74.
41. Ni Q, Bertino E, Lobo J, et al. Privacy-aware role-based access control. *ACM Transactions on Information and System Security (TISSEC).* 2010;13(3):1-31.
42. Madhusudhana K. An Ontological Approach for User Profile Based Access Control System. 2017.

43. Kayes A, Rahayu W, Dillon T. An ontology-based approach to dynamic contextual role for pervasive access control. Paper presented at: 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)2018.
44. Choi C, Choi J, Kim PJTJoS. Ontology-based access control model for security policy reasoning in cloud computing. 2014;67(3):711-722.
45. Korman M, Lagerström R, Ekstedt M. Modeling enterprise authorization: a unified metamodel and initial validation. *Complex Systems Informatics and Modeling Quarterly.* 2016(7):1-24.
46. Feltus C, Petit M, Sloman M. Enhancement of business it alignment by including responsibility components in RBAC. Paper presented at: Proceedings of the CAiSE 2010 Workshop Business/IT Alignment and Interoperability2010.
47. Petit M, Feltus C, Vernadat F. Enterprise Architecture Enhanced with Responsibility to Manage Access Rights-Case Study in an EU Institution. Paper presented at: IFIP Working Conference on The Practice of Enterprise Modeling2012.
48. Kuhn DR, Coyne EJ, Weil TR. Adding attributes to role-based access control. *Computer.* 2010(6):79-81.
49. Roy-Hubara N, Rokach L, Shapira B, Shoval P. Modeling graph database schema. *IT Professional.* 2017;19(6):34-43.
50. Mandviwalla M. Generating and justifying design theory. *Journal of the Association for Information Systems.* 2015;16(5):3.
51. Gill AQ, Chew E. Configuration information system architecture: Insights from applied action design research. *Information & Management.* 2019;56(4):507-525.
52. Hevner AR, March ST, Park J, Ram S. Design science in information systems research. *MIS quarterly.* 2004:75-105.
53. Kreizman G, Robertson B. Incorporating Security into the Enterprise Architecture Process. *Gartner Research.* 2006.
54. Samarati P, de Vimercati SC. Access control: Policies, models, and mechanisms. Paper presented at: International School on Foundations of Security Analysis and Design2000.
55. Bieber P, Cuppens F. Computer security policies and deontic logic. Paper presented at: Proc. of the First International Workshop on Deontic Logic in Computer Science1991.
56. Rodriguez MA. The RDF virtual machine. *Knowledge-Based Systems.* 2011;24(6):890-903.
57. Petersson AM, Lundberg J. Applying action design research (ADR) to develop concept generation and selection methods. *Procedia CIRP.* 2016;50:222-227.
58. Haj-Bolouri A, Bernhardsson L, Rossi M. Introducing PADRE: Participatory Action Design Research. Paper presented at: Pre-ICIS Workshop2015.
59. Gill AQ, Chew EK, Kricker D, Bird G. Adaptive enterprise resilience management: Adaptive action design research in financial services case study. Paper presented at: 2016 IEEE 18th Conference on Business Informatics (CBI)2016.
60. Baskerville R, Myers MD. Special issue on action research in information systems: Making IS research relevant to practice: Foreword. *MIS quarterly.* 2004:329-335.
61. Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. Paper presented at: Proceedings of the 18th international conference on evaluation and assessment in software engineering2014.
62. Voigt D-IK. Structural graph-based metamodel matching. 2011.
63. Mens T, Lanza M. A graph-based metamodel for object-oriented software metrics. *Electronic Notes in Theoretical Computer Science.* 2002;72(2):57-68.
64. Ismail A, Nahar A, Scherer R. Application of graph databases and graph theory concepts for advanced analysing of BIM models based on IFC standard. *Proceedings of EGICE.* 2017.
65. Angles R, Gutierrez C. Survey of graph database models. *ACM Computing Surveys (CSUR).* 2008;40(1):1-39.

66. Pokorný J. Graph databases: their power and limitations. Paper presented at: IFIP International Conference on Computer Information Systems and Industrial Management2015.
67. Neo4j Graph Database. Neo4j Graph Platform. https://neo4j.com/. Published 2019. Accessed 25 Nov, 2019.
68. Eessaar E. Using Relational Databases in the Engineering Repository Systems. Paper presented at: ICEIS (1)2006.
69. Gill AQ, Bunker D. Crowd sourcing challenges assessment index for disaster management. Paper presented at: 18th Americas Conference on Information Systems 2012, AMCIS 20122012.
70. Horne CA, Ahmad A, Maynard SB. Information security strategy in organisations: Review, discussion and future research directions. *arXiv preprint arXiv:160603528.* 2016.
71. Zhang R, Liu L, Xue R. Role-based and time-bound access and management of EHR data. *Security and communication Networks.* 2014;7(6):994-1015.
72. Ahn G-J, Ko M, Shehab M. Privacy-enhanced user-centric identity management. Paper presented at: 2009 IEEE International Conference on Communications2009.
73. Pokorný J. Conceptual and database modelling of graph databases. Paper presented at: Proceedings of the 20th International Database Engineering & Applications Symposium2016.
74. Angles R. The Property Graph Database Model. Paper presented at: AMW2018.
75. Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. *Computer.* 1996;29(2):38-47.
76. Lupu EC. *A Role Based Framework for Distributed Systems Management*, University of London; 1998.
77. Cruz IF, Gjomemo R, Lin B, Orsini M. A constraint and attribute based security framework for dynamic role assignment in collaborative environments. Paper presented at: International Conference on Collaborative Computing: Networking, Applications and Worksharing2008.

Tables

Table 1: Kernel Theories

#	Item	Description
1	Enterprise information security architectures (EISA)	Successful EA process should include principles, models for security, and privacy requirements. EISA prescribes how it can be achieved[53]. It guided us to understand the context and scope of security in EA during the problem formulation stage of ADR.
2	Access Control constraints	Confidentiality, integrity and availability are considered as the constraints of access control mechanism which ensure to protect resources from unauthorised disclosure(Confidentiality), unauthorised modifications(integrity) and confirm availability to legitimate users [54,55,70]
3	RBAC policies	RBAC policies control the access to organisational resources based on the activities and responsibilities of users in an organisation. In RBAC policy, it is essential to identity the 'role' whether it is a user's 'job title' or more specifically bunch of task that user needs to do[46,54]. In our increment three, we mainly focused on this policy. Furthermore, instead of granting accesses of objects on the user, authorisations are granted on roles. This is the core policy which is reflected in our metamodel[54].
4	RBAC models	National Institute of Standards and Technology (NIST) introduced a RBAC model which is considered as the standard for role-based access control mechanism. They developed a family of RBAC models named as $RBAC_0$, $RBAC_1$, $RBAC_2$, $RBAC_3$[19,20]. Then many researchers and industry practitioners modified standard RBAC concepts by adding new concepts like context, policies, time, dynamic role assignment based on organisation requirements[38-41,71]. Our proposed metamodel is based on $RBAC_0$ with the ability of modelling context dependent policies.
5	Graph Theory	Graph structures are originated from the field of mathematics[62]. There are a collection of nodes (vertices) and edges where a node represents an entity in the real world, and an edge represents a relationship between two nodes and establish a pair-wise relation[49,62,72]. On the other hand, the Graph database is a storage procedure where data are stored and represented using graph structures[73]. Graph database offers an efficient way to work with interconnected data and their relationships. Neo4j, Cosmos, Neptune and Titan are few popular graph databases[74].

Table 2: RBAC Constructs

Concept	Definition	References
Subject	An active entity, generally in the form of a person, process or device that causes information to flow among objects or changes the system state.	[75]
Assignee (User)	Any person who interacts directly with a system.	[75 20]
Role	A job function within the organisation that describes the authority and responsibility conferred on a user assigned to the role	[20,75]
Operation	A specific type of interaction between a subject and an object in the flow of information from one to the other.	[20]
Access Policy	A policy defines the rule which controls the access to resources.	[38-40]
Assignor (System administrator)	The individual who establishes the system security policies performs the administrative role and reviews the system audit trail.	[75]
Object	Anything used or consumed while performing a function.	[20]
Access rights (Permitted/ Prohibited)	A description of the type of actions subjects are permitted or prohibited to perform on a resource.	[20,75,76]
Responsibility	Is a charge assigned to an employee to signify his duties concerning a task.	[46]

Table 3: Final entity relationship matrix

	Subject	**Assignee**	**Assignor**	**Role**	**Business Role**	**Access Role**	**Responsibility**	**Access Rights**	**Access Policy**	**Operation**	**Object**
Subject		Base Class Of	Base Class Of	-	-	-	-	-	-	-	-
Assignee	Sub Class Of	-	-	-	-	Is Assigned	-	-	-	-	-
Assignor	Sub Class Of	-	-	-	-	Assigns	-	-	-	-	-
Role	-	-	-	-	Base Class Of	Base Class Of	Executes	-	-	-	-
Business Role	-	-	-	Sub Class Of	-	-	-	-	-	-	-
Access Role	-	Assign To	Assigned By	Sub Class Of	-	-	-	Allocated By	-	-	-
Responsibility	-	-	-	Executed By	-	-	-	-	-	Vests	-
Access Rights	-	-	-	-	-	Allocated To	-	-	Controlled By	Permit	-
Access Policy	-	-	-	-	-	-	-	Controls	-	-	-
Operation	-	-	-	-	-	-	Vested By	Permitted By	-	-	Access
Object	-	-	-	-	-	-	-	-	-	Accessed By	-

Table 4: Learning principle from ADR project

Challenges	Design Principle	Description
Identifying the correct model.	Requirements will drive the selection of an appropriate model.	Organisation's information security requirements should guide the selection of an ACM model, not the other way around. Selection of a model first and then tailoring requirements to adjust with it can lead to an impaired and ineffective implementation of the access control mechanism.
Assessment of existing research to decide whether it can be adopted as a practical solution.	Active involvement of practitioners and researchers to identify gaps in existing work in relation to the requirements.	ADR design review workshops play an important role in the development and evaluation of the artefact. Through these workshop's researchers can identify whether existing research or artefact can satisfy the practical needs, or there is a need for a new or improved artefact.
Identifying the straining point and foundation to assist in the development of the artefact.	Existing industry framework and artefacts aid in the development of the new artefact.	Existing frameworks and artefacts can be leveraged as kernel theories in ADR. These already validated artefacts offer the requisite foundation on which a new artefact can be built.
Appropriate ontology development.	Avoid ambiguity through iteratively defining and refining the set of entities and relationships as appropriate to the context.	Having a set of entities and relationships that convey unambiguous meaning is immensely important. It ensures the produced model is less erroneous, encapsulates requirements accurately and evolves more gracefully without the introduction of redundant entities.
Ensuring tailor ability of the proposed artefact.	Graph modelling approach can induce better tailor ability to the developed artefact.	Developing an adaptable artefact can be easy to tailor and accommodate in future. Graph modelling approach can depict complex semantic relationships among entities more efficiently and elegantly compared to the relational model. Therefore, a metamodel that uses graph modelling approach can be easily tailored as it evolves over time with the changing requirements.
Ensuring adaptability and integration.	Adaptive metamodel can serve evolving information security requirements.	As requirements for information security evolves over time, it is imperative to have a metamodel that can be used to build a model which is easy to extend and modify.

Figures

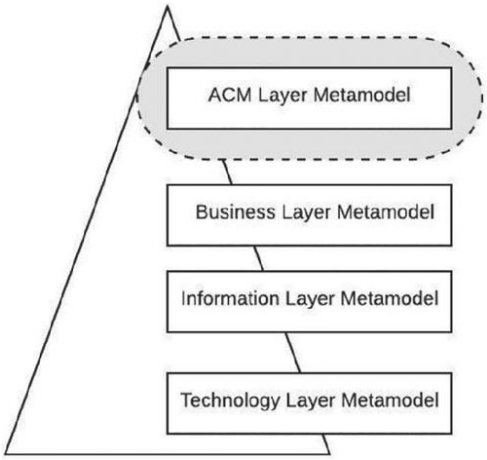

Figure _1: Secure Digital Enterprise Architecture with additional ACM Layer Metamodel

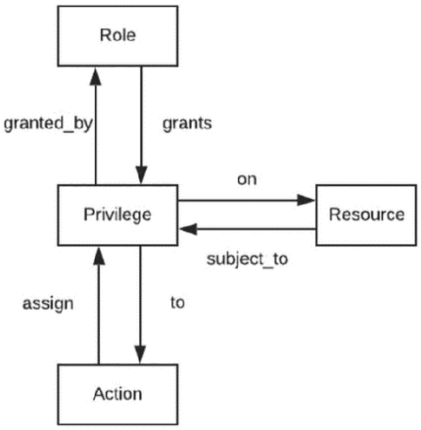

Figure _2: RBAC ontology[77]

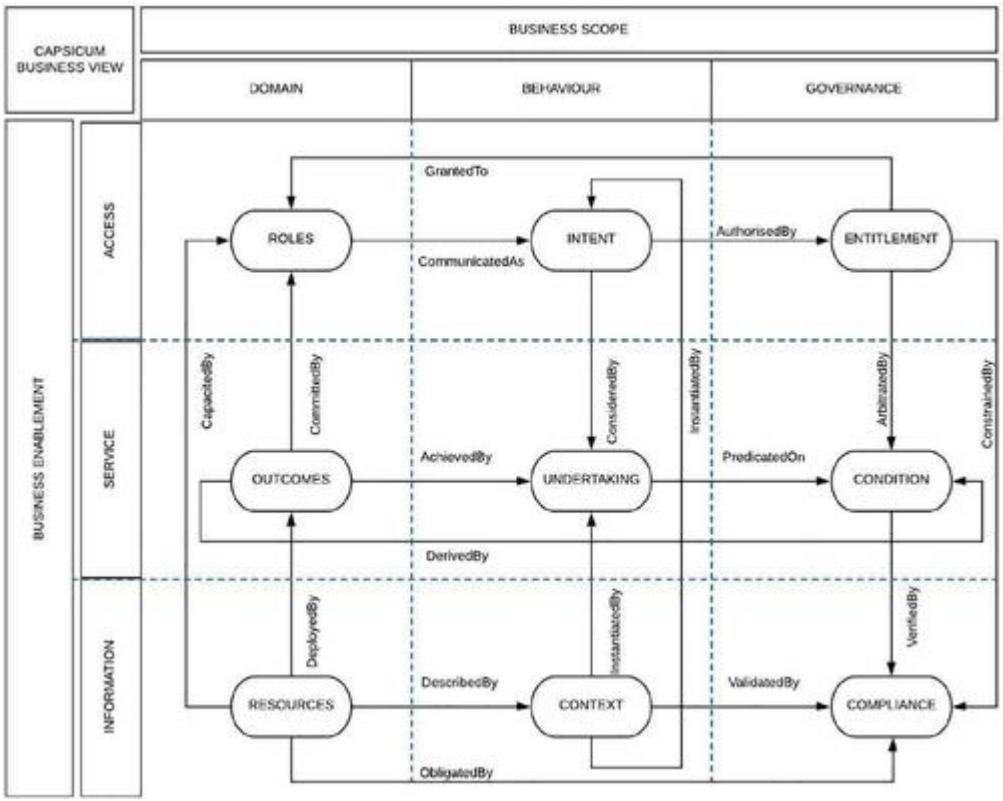

Figure _3: CAPSICUM Business View metamodel[12]

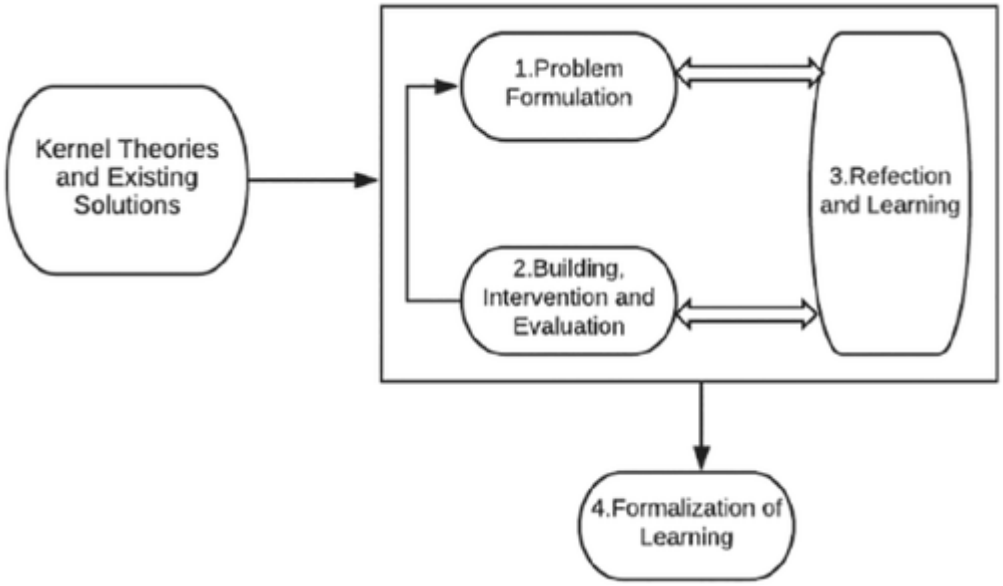

Figure _4: Research Methodology[10]

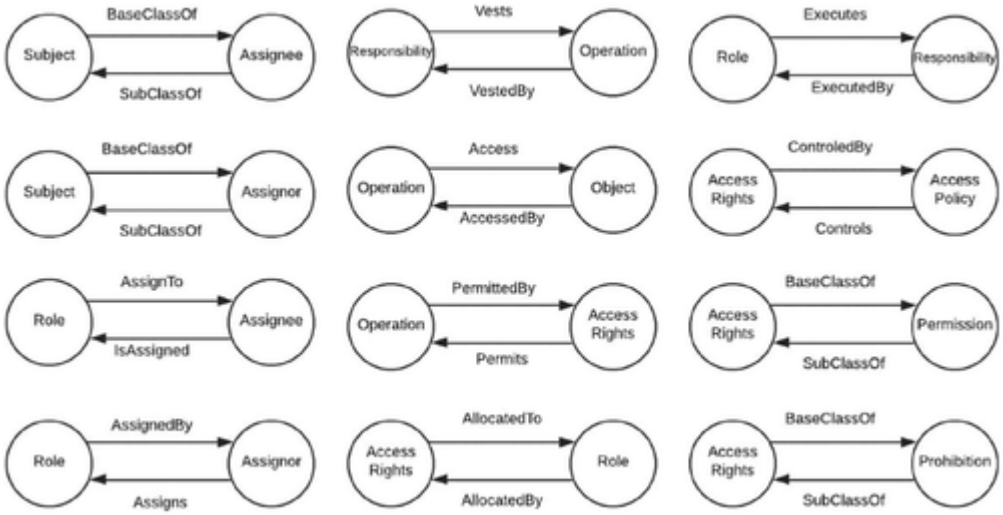

Figure _5: Entities and their relationships (based on graph modelling)

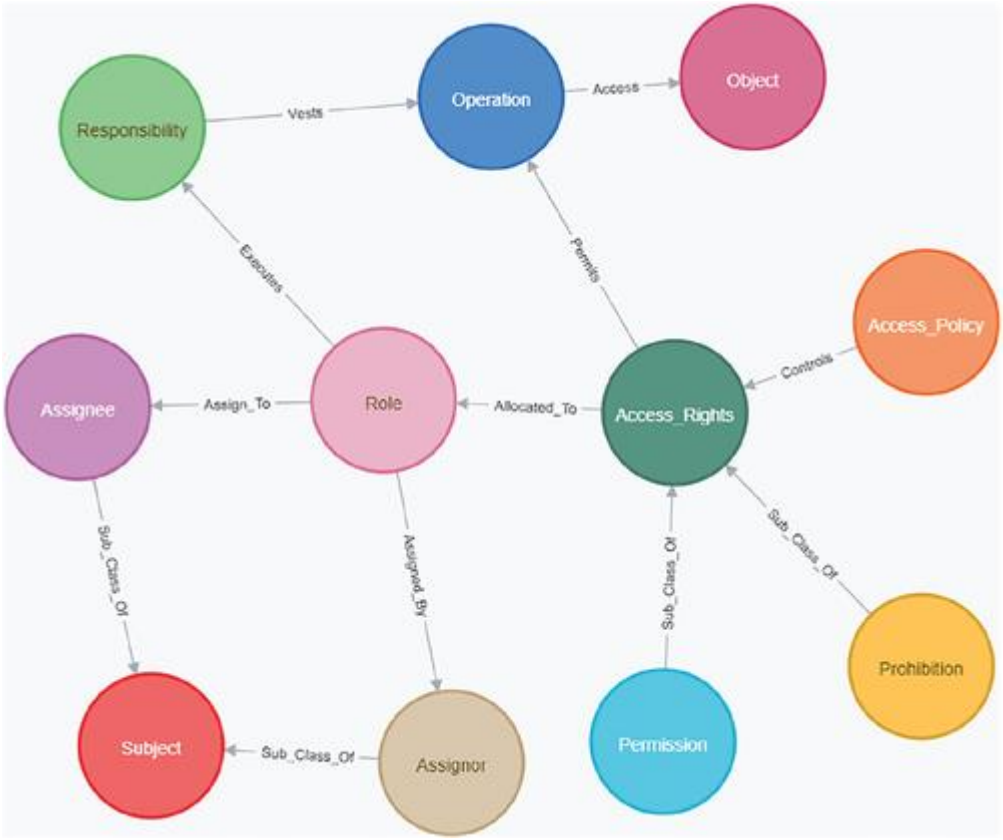

Figure _6: Access control metamodel graph after Increment 2

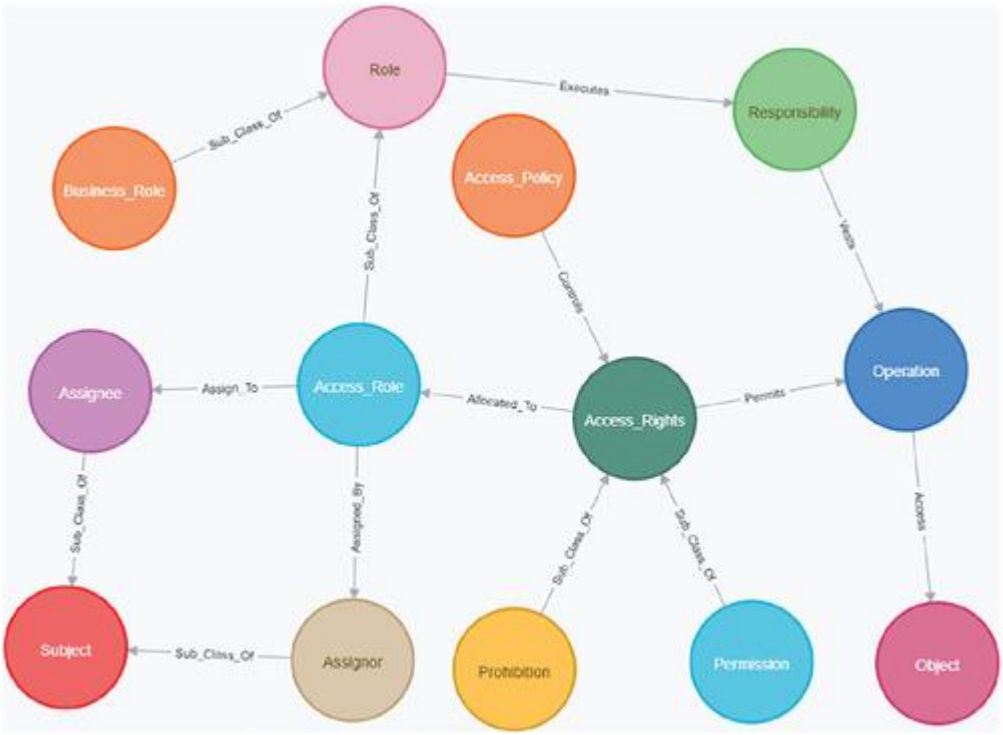

Figure _7: Access control metamodel graph after Increment 3

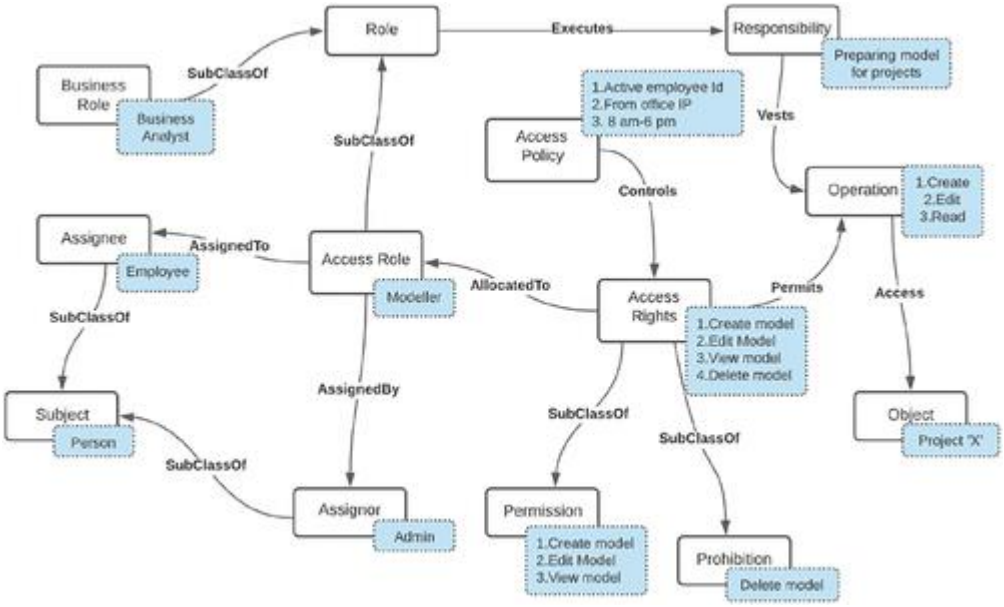

Figure _8: ACM metamodel evaluation for case study scenario