Hindawi
Security and Communication Networks
Volume 2022, Article ID 7026779, 20 pages
https://doi.org/10.1155/2022/7026779

Review Article

SoK: Context and Risk Aware Access Control for Zero Trust Systems

Shiyu Xiao,[1] **Yuhang Ye**,[1] **Nadia Kanwal**,[2] **Thomas Newe**,[3] **and Brian Lee**[1]

[1] *Software Research Institute, Technological University of the Shannon, Athlone, Ireland*
[2] *School of Computing and Mathematics, Keele University, ST5 5GB, UK*
[3] *CONFIRM Smart Manufacturing Centre, Dept of Electronic & Computer Engineering, University of Limerick, Limerick, Ireland*

Correspondence should be addressed to Brian Lee; brian.lee@tus.ie

Received 14 February 2022; Revised 15 April 2022; Accepted 30 April 2022; Published 30 June 2022

Academic Editor: AnMin Fu

Evolving computing technologies such as cloud, edge computing, and the Internet of Things (IoT) are creating a more complex, dispersed, and dynamic enterprise operational environment. New security enterprise architectures such as those based on the concept of Zero Trust (ZT) are emerging to meet the challenges posed by these changes. ZT systems treat internal and external networks as untrusted and subject both to the same security checking and control to prevent data breaches and limit internal lateral movement. Context awareness is a notion from the field of ubiquitous computing that is used to capture and react to the situation of an entity, based on the dynamics of a particular application or system context. The idea has been incorporated into several access control models. However, the overlap between context-aware access control and zero-trust security has not been fully explored. In this SoK, we conduct a systematic examination of ZT, context awareness, and risk-based access control to explore the critical elements of each and to identify areas of overlap and synergy to enhance the operation and deployment of ZT systems.

1. Introduction

In recent years, there has been a trend to move away from traditional "perimeter security defence" systems. These are based on the so-called Demilitarised Zones (DMZ), i.e., a subnetwork(s) containing an enterprise's external facing services, typically bookended by internal and external facing firewalls. The fundamental premise behind this defence system is that anything outside the perimeter is untrusted, whilst everything inside is trusted. A major weakness of this however is that once an adversary gains access to the internal network it becomes easy for them to move laterally throughout the network and so compromise other hosts and servers.

There have been several drivers for this weakening of the perimeter security model. The nature of enterprise networking has become more complex through the evolution of computing technology. Initial developments in this regard included cloud computing and Bring Your Own Device (BYOD), whilst more recent approaches such as the Internet of Things (IoT) and edge computing have increased the complexity level further. The increase of remote working brought about by COVID-19 has added even more to the mix. The net effect of these trends has been to create a highly dispersed and fragmented enterprise architecture, often with many of the enterprise applications running on third-party hardware. Moreover, the operating environment may often be highly dynamic due to end-users being situated in different locations or changes in operating conditions for devices in environments where the resources are constrained, or their availability may vary from moment to moment.

A new enterprise security model has consequently emerged to meet the challenges posed by these changes. This is designated as Zero-Trust Networking (ZT/ZTN) which essentially regards the internal enterprise network as untrusted. It thus treats internal and external networks with the same degree of suspicion and subject to the same security checking and control, and in this way seeks to prevent data breaches and limit internal lateral movement [1]. Key principles of ZT include the requirement to validate every access on a per-session basis as well as the use of dynamic policy enforcement taking into account device and user attributes as well as, perhaps, other behavioural and environmental attributes. The zero-trust concept was introduced by Forrester Research Group [2] as a new, radical approach to enterprise security. The ZT approach truly took wings when Google implemented a ZT-based enterprise security architecture called "BeyondCorp" [3,4]. ZT has since therefore, unsurprisingly, been embraced with gusto by the commercial world and many vendors today have ZTN product offerings leading to somewhat different definitions of the concepts.

Alongside commercial offerings, a number of researchers have proposed solutions for different domains. Mujib and Sari [5] investigated the application of micro-segmentation for ZTN in Software Defined Networks (SDN). Meheraj examined how to define a ZT strategy for cloud computing [6], while Zaheer et al. [7] applied ZT to microservice-based applications. Likewise [8–10] examined the application of ZT to the Internet of Things (IoT) domain. The ZT approach to dynamic policies and its associated use of trust or risk-based evaluation of device and user attributes implies a similarity to the large existing body of work on *context aware access control (*CAAC). Some authors have explored this theme for ZT. Luskaseder et al. [11] explore the use of ZT on a German university based on their notion of *context* as "checks such as device certificates, 2-factor authentication, or patch status of the accessing device." Lee et al. [12] explored incorporating situational awareness as a factor in ZT policy evaluation process, while Vanickis outlined at a high level an approach for enterprise ZT policy enforcement [13] including the outline of a risk-based policy language, PAROLE, for ZT.

However, the overlap between zero-trust security and the earlier body of work on Context-Aware Access Control (CAAC) and risk-based access control has not been systematically examined. This SoK therefore sets out to consider this earlier corpus and to compare and contrast the proposals and concepts therein to frame solutions for zero-trust needs and requirements. In this way, we seek in this study to fulfil the Usenix goal for a SoK as "a survey paper that provides a useful perspective on a major research area" [14] with Zero Trust as the "major research area" and our "useful perspective" being our contributions enumerated below:

(1) We systematically review and contextualise previous research in context-aware access control to identify general patterns of context and situation awareness across all access control types as well as different application domains (cloud, enterprise, health, etc.) and show how these can be applied to provide dynamic policy-based solutions for ZT applications.

(2) We systematically review and evaluate previous research on risk- and trust-based approaches that have been proposed for access control and identify commonalities and mechanisms that can be applied to fulfil the needs for trust and uncertainty management in ZT applications.

(3) We identify key open areas where further research is needed and we identify the main challenges in these areas and suggest some possible approaches to solve these challenges.

Table 1: Abbreviations/definitions.

ABAC	Attribute-based access control
ABE	Attribute-based encryption
AC	Access control
ACL	Access control list
BYOD	Bring your own device
CA-ABAC	Context-aware ABAC
CAAC	Context-aware access control
CASM	Context-aware security model
CP-ABE	Ciphertext policy based ABE
DAC	Discretionary access control
DMZ	Demilitarised zone
KP-ABE	Key policy-based ABE
MAC	Mandatory access control
NIST	National Institute of Standards and Technology
OT	Operational technology
PA	Policy administrator
PDP	Policy decision point
PE	Policy engine
PEP	Policy enforcement point
PKI	Public key encryption
QRACC	Quantified risk adaptive access control
RAdAC	Risk adaptive access control
RBAC	Role-based access control
SA-ABAC	Situation aware ABAC
SAM	Situation aware matrix
SASE	Secure access services edge
SDN	Software-defined networks
SD-WAN	Software-defined wireless area network
T-RBAC	Temporal RBAC, Trust-RBAC
UCON	Usage control
WBAN	Wireless body area network
ZT	Zero trust
ZTE	Zero trust edge
ZTN	Zero trust network

CAAC has been a very heavily researched area over many years with many published papers; the works reviewed in this study are therefore a representative sample of the field.

The remainder of the study is structured as follows. Section 2 describes the background approaches and concepts including Zero Trust, Context Awareness, and Access Control. Section 3 describes the previous research in CAAC, while Section 4 elaborates the use of risk and trust in CAAC. Section 5 summarises the findings from the previous two sections. Section 6 contains conclusions. Table 1 lists the abbreviations that are used in this study.

2. Background

2.1. Zero-Trust. Zero-trust [1, 2] is an approach that assumes an attacker may be lurking in the intranet and that the enterprise environment is therefore no more trustworthy

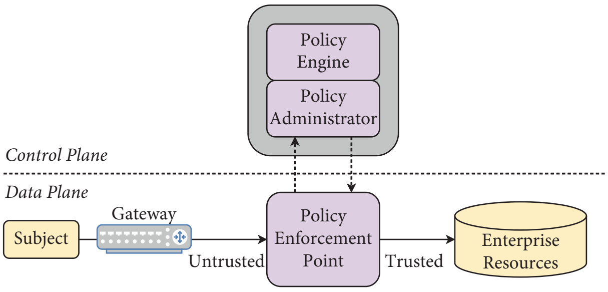


Figure 1: ZT logical components [1].

than an external environment. Security teams must continually evaluate the risk to assets and services and implement suitable controls to mitigate these risks. This entails the rigorous application of least privilege principles by minimising access to assets and services through fine-grained access controls and continuously verifying the security posture of each access request. Zero-trust is a set of concepts and best practises designed to enforce least-privilege access rather than a particular security infrastructural approach. In that perspective, a zero-trust architecture is defined by [1] as an enterprise's cybersecurity plan that utilises zero-trust concepts and includes system components, workflow planning, and access policies. In the next two sections, we expand on these key features to elaborate the ZT concept.

2.2. Zero-Trust Principles. We are interested in particular in how the notions of context and trust are significant in zero-trust. Requirements in this case are well articulated by [1, 3]. Key tenets of the ZT include the following.

(i) All data and services are considered as resources.

(ii) Access to resources is granted on a per-session basis and may be reviewed during the session.

(iii) Access to resources is determined by dynamic policy based on the observable state of the client identity, application/service, the requesting asset and may include environmental behavioural attributes such as requestor network location and reported active attacks.

(iv) Access is evaluated using a trust algorithm that takes into account the above attributes. The algorithm may be binary or assign a confidence level. Moreover, the algorithm may consider the subject or networks recent history into account when evaluating access requests. [1] terms this "Singular versus Contextual" where contextual refers to maintaining a historical record—note that is a somewhat different definition of context to the more widely used notion of context elsewhere in the literature and which we use in the remainder of this study.

(v) The enterprise monitors and collects information about the current state of the assets and environments and measures integrity and security posture on a continuing basis.

2.3. Zero-Trust Architecture. The logical view of ZT architecture for an enterprise system is shown in Figure 1.

The Policy Engine (PE) makes the decision on whether to grant access or not. It uses enterprise policy rules with input from the actors in the access chain (subject, gateway, target resource) as well as information from external and environmental sources (such as threat intelligence, activity logs, asset inventory management systems, and so on) as input to a *Trust Algorithm* to grant, deny, or revoke access to the resource. The Policy Administrator (PA) is responsible for establishing or shutting down the communication path between a subject and a resource (via management of the Policy Enforcement Points (PEP)). It issues any required authentication tokens. The PEP enables and terminates the connection between the resource and subject. It is a single logical component but may be broken down into components on the client side and the resource side (e.g., gateway) depending on the implementation. Additionally, a number of other data sources may be used in making an access decision such as a SIEM [15] and inventory management system.

Zero-Trust Edge (ZTE) [16] or Secure Access Services Edge (SASE) [17] is a recent evolutionary step of the ZT architecture that moves ZT functions to the cloud/network edge to connect Internet traffic to remote sites using ZT access principles, primarily by utilizing cloud-based security, and networking services—see Figure 2. As envisaged by Forrester and Gartner [16, 17], a ZTE network is a virtual network that spans the Internet and is directly accessible from every major city in the world and which uses ZT principles to authenticate and authorize users as they connect to it and through it. In this view, ZTE builds on and is closely coupled with SDWAN services (Software Defined—Wide Area Network) to provide the global networking reach and the flexibility need to provision and operate large-scale ZT access. As shown in Figure 2, a ZTE node can contain a range of networking and security services and these services can be deployed flexibly on premise, in the edge or central cloud. The primary goal of ZTE/SASE is to securely connect remote sites and users to both on-premises and in-cloud corporate services, replacing VPN in doing so.

The migration of ZT functions to the edge can be seen as a natural progression following, for example, the migration of artificial intelligence to the edge for certain cases. ZTE/SASE represents one particular take on that progression, and it is to be expected that other examples will emerge as edge and IoT deployments become more prevalent.

2.4. Context Awareness. The concept of context awareness computing originated in the field of pervasive or ubiquitous computing and the notion of what it means is often expressed in terms of ideas from that field. Perhaps the most widely cited definition is that of Dey [18], i.e., "Context is any information that can be used to characterize the situation of a person, place, or object that is considered relevant to the interaction between a user and an application." A non-complete list of context categories includes:

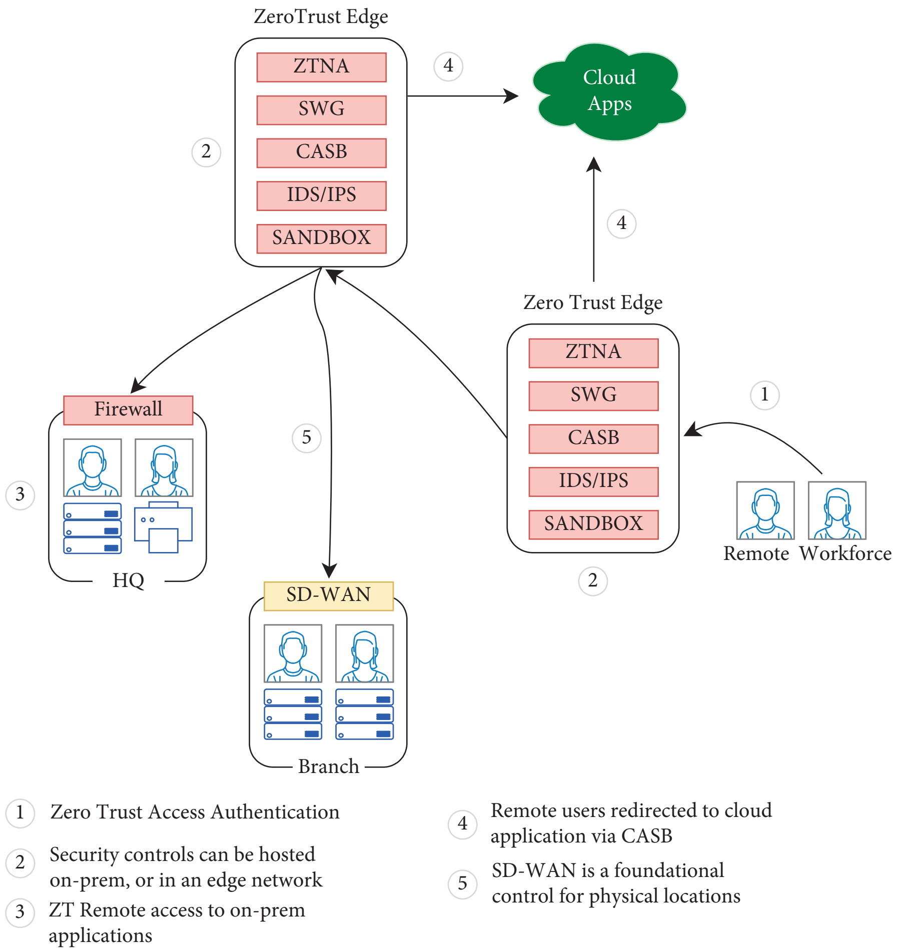

ZeroTrust Edge
ZTNA
SWG
CASB
IDS/IPS
SANDBOX
4
Cloud Apps
2
4
Zero Trust Edge
ZTNA
SWG
CASB
IDS/IPS
SANDBOX
1
Firewall
3
HQ
5
Remote Workforce
2
SD-WAN
Branch
1 Zero Trust Access Authentication
2 Security controls can be hosted on-prem, or in an edge network
3 ZT Remote access to on-prem applications
4 Remote users redirected to cloud application via CASB
5 SD-WAN is a foundational control for physical locations

Figure 2: Zero-Trust edge [16].

(i) Spatial information (e.g., location, orientation, speed, and acceleration).

(ii) Temporal information (e.g., time of the day, date, and season of the year).

(iii) Environmental information (e.g., temperature and air quality).

(iv) Social situation (e.g., who you are with and people that are nearby).

(v) Resources that are nearby (e.g., accessible devices and hosts).

(vi) Activity (e.g., talking, reading, walking, and running).

(vii) Communication and networking information (network states, battery levels, signal-to-noise ratios, network services, etc.) [19, 20].

Abowd et al. [21] distinguish context as either primary (location, identity, time, and activity) or secondary, i.e., context that can be derived from primary. For example, given identity, one can find e-mail address and phone number. Perera [22] cautions that in some cases the same information may be acquired by different means and consequently may be either primary or secondary depending on the circumstances. He gives the example of blood pressure information which can be considered primary if taken from a sensor, or secondary if taken from the patients' health record. Considering specifically the IoT, he expands the definitions above as follows.

(i) *Primary*: Any information retrieved without using existing context and without performing any kind of sensor data fusion operations.

(ii) *Secondary*: Any information that can be computed using primary context. The secondary context can be computed by using sensor data fusion operations or data retrieval operations such as web service calls or database retrievals.

Perera defines a four-step context lifecycle that, although specified for IoT, will be useful for CAAC purposes also. It comprises the following components.

(i) *Context Acquisition*: data needs to be acquired from various sources, i.e., (i) directly from the physical sensors, i.e., hardware, (ii) from virtual sensors through a middleware infrastructure, or (iii) from context servers such as databases and web services.

(ii) *Context Modelling*: represents the collected data in a meaningful way that can be processed by an application. He identifies a number of representation schemes including key-value, mark-up scheme (e.g., XML), based on relationship (UML), object based, logic based, or ontology based.

(iii) *Context Reasoning*: can be defined as a method of deducing new knowledge, and understanding better, based on the available context or inferring higher-level context information from a lower level context(s) (primary or secondary) through either a single or multiple interactions. Reasoning should deal with uncertainty and probabilistic scenarios. Techniques include (un)supervised learning, rules, fuzzy logic, ontology based, and probabilistic logic (e.g., Dempster-Shafer). Perera advocates a combination of techniques in order to get the best results. For example, statistical techniques could be used at the lowest level to fuse sensor data, whilst fuzzy logic can convert fixed data to more natural terms as well as handle uncertainty and ontological approaches could be to infer additional context at a higher level using domain knowledge.

(iv) *Context Dissemination*: this is the distribution of context to end-users. Techniques include query based and publish-subscribe.

2.5. Traditional Access Control Models. Context-aware access control extends and builds upon existing access control approaches and for that reason we review these briefly.

2.5.1. Discretionary Access Control (DAC). The basic notion behind DAC is that access to a resource is controlled by (at the discretion of) the owner of that resource [23]. DAC access controls base access rights on the identity of the subject and object involved. Access is enabled by means of Access Control Lists (ACL) which associates a set of pairs with each object where each pair contains a subject and a set of permissions (e.g., subject Mike has read and write permission on file MyFile.). DAC underpins access control systems on most computer operating systems.

2.5.2. Mandatory Access Control (MAC). In mandatory access control, access to the resources is controlled by the computer system and not by the resource owner. MAC is sometimes associated with Multi-Level Security, which is based on a combination of the sensitivity (classification) of a resource/object and the privilege (clearance) level of a subject [24]. MAC is not as widely used as DAC but does appear in computer operating systems in the form of Mandatory Integrity Control on Windows and in Linux as SELinux or AppArmour.

2.5.3. Role-Based Access Control (RBAC). RBAC is one of the most widely used forms of access control in modern computer environment [25]. It differs from MAC/DAC as it is defined to provide security administration at a business level rather than at a user level. Permissions to access resources are granted based on the job function, i.e., role within the organisation. Because roles are organisation specific and are a form of aggregation, RBAC provides a very flexible way to define scalable access control in large organisations. In contrast to DAC/MAC where subject and object have a direct relationship in RBAC, the 'role' serves as an intermediate construct, i.e., roles have permissions assigned, subjects (i.e., users) are assigned roles and roles are associated to objects/resources.

2.5.4. Attribute-Based Access Control (ABAC). ABAC grants access to resources based on a combination of the attributes of the subject and object [26]. Like RBAC, ABAC is also based on providing security administration at the business rather than user level. However, the permissions are associated with the attributes rather than roles. ABAC is sometimes called *policy-based* access control as policy rules are used to define the attribute combination that grants access [27]. ABAC has gained in popularity because it provides more fine-grained control than RBAC and is applicable to a broader set of circumstances such as arise with CAAC.

2.6. Attribute-Based Encryption (ABE). ABE applies public-key cryptography to control data decryption according to attributes, first proposed by Sahai and Waters [28], and which is often proposed for use in AC schemes. ABE is further categorized into ciphertext-policy ABE (CP-ABE) [29] and key-policy ABE (KP-ABE) [30]. In KP-ABE, attributes are used to describe the encrypted data and policies are built into user's keys; while in CP-ABE, the attributes are used to describe a user's credential, and the encryptor determines a policy on who can decrypt the data. CP-ABE has gained more popularity especially to manage outsourced data such as cloud data [31] because the data owner has the authority to control the accessibility of the data remotely through the policy designed by himself/herself. We consider the use of ABE in CAAC schemes in the next section.

3. Context-Aware Access Control

Context becomes important for access control because of the dynamic nature of modern-day computing environments. This trend began, naturally enough, with the advent of pervasive computing some decades ago and has grown significantly in the last few years with the use of mobile and cloud computing and the more recent emergence of IoT and edge computing.

3.1. Nature of Context Information for Access Control. The notion of context in the access control domain embodies many of the same ideas as its use in pervasive computing (i.e., identity, time location, etc.) though there are some variations. Kayes et al. [32] attempt to answer this question by extending Dey's [18] definition for pervasive computing as shown in Table 2 which shows the respective scopes and context-aware entities.

Table 2: Context information.

Context definition	Entity	Scope
..Any information that can be used to characterize the situation of an entity [18]	Person, place or object	Pervasive computing
..Any information that can be used to characterize the state of relevant access control-specific entities and the state of relevant relationships between different entities [32]	User, resource and environment	Access control

This provides a useful starting point for exploring CAAC in more detail. Broadly speaking we have:

(i) User-centric contexts—information representing the user.

(ii) Resource-centric contexts—information representing data or information resources.

(iii) Environment-centric contexts—information representing the environment and the resource such as the location where the access request originated.

In subsequent sections, we consider how various researchers have elaborated these definitions in the scope of their work and in particular how context can be defined for any or all of the entities.

We can also consider context information as either primary or derived. Primary context includes, for example, location and time, whilst derived context includes entity profile information (attributes) and relationships. Moreover, as with the previously described context lifecycle higher level, access control contexts can be inferred from lower level contexts through single or multiple interactions.

Such inferencing is particularly relevant for dealing with uncertainty or probabilistic scenarios and this capability becomes critically important for estimating risk when making an access control decision by considering all relevant factors—stated another way it minimises risk by giving access only to trustworthy subjects. How to define trustworthiness or risk and enforce related access control has been, and is, an active area of research and uses many of the *context reasoning* techniques previously outlined by Perera et al. [22]. Context-aware access control enforcement can be viewed as a form of the context lifecycle model described by Perera.

A related notion that arises is that of *mission*, i.e., how to incorporate the purpose or goals of an organisation into the access control decision. This is related to activity (as a type of context) but is not the same thing. Mission arises from the situational awareness domain [33] and has been addressed in the access control context under the heading of Risk Adaptive Access Control (RAdAC) [34]. Nonetheless mission can be considered a form of context and RAdAC as a form of CAAC and is discussed as such later in the document.

Context then provides a critical input to the access control decision and much research has been carried out to find ways to define and capture context as well as efficiently implement enforcement mechanisms. Context-aware access control has been extensively investigated over a number of years from different viewpoints, in particular as extensions to the existing access control models discussed above, and to the domains of application, e.g., health/medical, cloud computing and IoT [35–38]. In the rest of this section, we provide a review of the most widely discussed viewpoints.

3.2. RBAC-Based Context Schemes. The majority of CAAC models that have been developed over the last two decades have been based on the RBAC model. This is especially true for the earlier part of this time period. Kayes et al. [32] identify the key components of RBAC-based CAAC systems, namely

(i) User: Humans interacting with an information system.

(ii) Role: reflects job functions within an organisation.

(iii) Permission: right to perform certain operations on data/resources.

(iv) Context: information used to specify the situation of entities.

(v) Context-aware user role assignment policy: rules assigning user to certain roles predicated on the entity context values.

(vi) Context-aware role permission assignment: rules assigning permissions to certain roles predicated on the entity context values.

Approaches to RBAC-based CAAC vary based on the specific type of context that is modelled and we now review some of the more common approaches in the rest of this section.

3.2.1. General Context. Generalized Role-Based Access Control (GRBAC) [39, 40] extends traditional role-based access control by incorporating subject roles, object roles, and environment roles into access control decisions. Subject roles are like traditional RBAC roles: they abstract the security-relevant characteristics of subjects into categories that can be used when defining a security policy. Similarly, object roles abstract the various properties of objects, such as object type (e.g., text, JPEG, executable) or sensitivity level (e.g., classified, top secret) into categories. Environment roles capture environmental information, such as time of day or system load so it can be used to mediate access control.

Kayes considered how context-aware access control can be defined by extending the RBAC model with context information [41–43]. In [41], he develops a context-aware access control framework based on RBAC in which he seeks to address the following requirements.

(i) (Req.1) Representation of contextual conditions: What access control-specific basic and derived (simple and complex) context information should be considered to express the relevant contextual conditions as part of building context-aware access control?

(ii) (Req.2) Specification of user-role assignment policies: How to specify the user-role assignment policies based on the relevant contextual conditions?

(iii) (Req.3) Specification of role-permission assignment policies: How to specify the role-permission assignment policies based on the relevant contextual conditions?

He defines context as any relevant information about the state of an entity or the state of a relationship between persons (as entities) relevant to access control (cf. Table 2). He classifies context as

(i) Simple context—a context fact, i.e., an attribute of an entity that specifies the state of the entity based on a single information source, e.g., user identity.

(ii) Complex context—a combination of the values of attributes that characterize the state of one or more entities, based on one or more context information sources, e.g., an interpersonal relationship between two users.

In order to express contexts, he introduces a Context Specification Language which enables the definition of simple and complex contextual expressions (or conditions). A simple contextual expression is a relational expression over a simple context attribute of the form:

entity.simple-context rel_op value.

where rel_op is a relational operator and the value is some value from the type domain of the context attribute, e.g.,

iphone_2.version = 8.

A complex contextual expression is a logical composition (AND, OR, etc.) of a number of simple or complex expressions, e.g., (iphone_2.version >7) AND (iphone_2.patch_level = = uptodate).

So in answer to Req.1—Representation of contextual conditions 1—Kayes proposes that:

(i) Context is based on the values of one or more attributes of one or more entities, and

(ii) Context is expressed in access control policies by contextual conditions which are defined as relational operation over entity attributes (simple conditions) and logical combination of either simple conditions (complex conditions) or other complex conditions.

Using this mechanism to express context, Kayes goes on to answer Req.2 and Req.3 i.e. how to assign roles to users depending on the context and the complementary problem of how to assign permission to roles depending on the context. Moreover, in this same study [41], he goes on to define an ontology-based policy model for policy specification and a related policy enforcement framework.

The UbiCOSM context model [44] also draws inspiration from RBAC to suggest context as a means to provide a level of indirection between users and permissions, i.e., permissions are defined for each context and a subject acquires the permissions when he/she operates in a specific context. A context may be either physical (which identify physical spaces delimited by specific geographical coordinates) or logical (which identify the logical states of "entities composing a ubiquitous service deployment, i.e., users and resources"). Logical states depend on logical properties of relevant attributes such as temporal and environmental information as well as user activities and device characteristics.

Logical and physical contexts comprise

(i) a context_name that uniquely identifies the context, e.g., Tourist defines a role;

(ii) a context_type identify the context type, i.e., Physical or Logical;

(iii) one or more context_activation_conditions that represent the physical/logical conditions that determine the activation of the context.

A UbiCOSM logical context then is essentially a named grouping of certain entity attributes the captures non-location-based context information such as temporal, environmental, device, and task. A physical context is a named geographically bounded location that contains an associated logical context defining activation conditions as well as the set of resources that are contained within the context. In this regard, UbiCOSM physical contexts seem somewhat similar to the notion of *resource groups* as used in the Azure cloud computing system [45]—although the latter does not embody physical location. The authors note that the description of physical and logical entities is static but that the entities associated with them are dynamic. They show how a logical context can define the assignment of dynamic permissions for a role (as in RBAC)—however, it is not entirely clear to this reader how they would be useful for the arbitrary specification of contexts, i.e., whether a large number of logical contexts would be needed to define different activation contexts for the same entity/attribute pairing? Nor is it clear if multiple entities can be defined in the same logical context.

Zhu et al. [46] consider how to combine RBAC with ABE to provide finer-grained access control on cloud data of the users, where RBAC controls the accessibility of the subjects and ABE promises the confidentiality and integrity of the medical data. Tian et al. [47] proposed an RBAC scheme extending CP-ABE. The scheme divides the patient's medical data into separate parts based on the contents that will be required by different kinds of roles. Each part of the medical data then is encrypted with its targeting role, and different each role can only use the secret key specially generated for itself to decrypt the corresponding part of the data.

Jafarian and Amini [35] examine context-aware access for mandatory access control (CAMAC). They define context in terms of *context types* and *context predicates*. A context type represents a contextual attribute of the system,

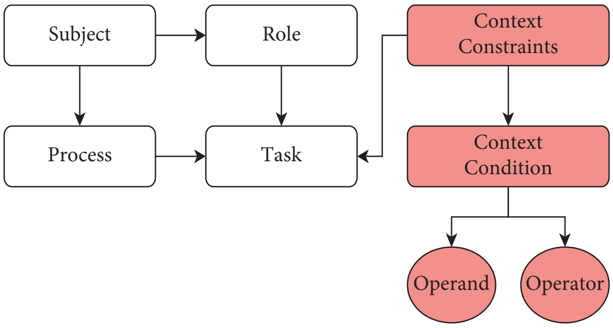


Figure 3: Metamodel for context-aware process AC [48].

e.g., the time or location of entities. Formally, a context type defines a context value set, operators on the value set, and entity types which may use the context and well as update rules to change the confidentiality of the concerned entity types. A context predicate specifies a value for a contextual attribute, e.g., <*John, Location, Is, Classroom*> specifies Johns' current location is in the classroom. CAMAC also includes the use of derived context, noting that a context-type value set may be a function of other primary context types, e.g., *Load* may be a function of *CPU Load* and *Bandwidth*.

3.2.2. Workflow-Related Context. Another use of RBAC to capture access control context is presented in [48], where the authors consider how to capture *business process context*. In this regard, they introduce a business process-related RBAC model that they had previously developed. The essential idea is that subjects (human users or software agents) engage in workflows/processes during their daily work. Subjects must be authorised to execute relevant processes. A process in turn is composed of one or more tasks and a role groups a number of tasks as shown in Figure 3.

Tasks defined in business processes are always performed within a certain context, e.g., time, location, or the executing subject. Different authorization rules might apply for executing a particular task in different contexts as defined by context constraints, i.e., certain contextual attributes must meet certain predefined conditions to permit the execution of a specific task. These in turn consist of context conditions, i.e., Boolean expressions that restricts the permitted values of a context attribute (e.g., date >01/01/2012).

A similar context-aware workflow RBAC model is suggested by Park et al. [49]. He defines a workflow schema to consist of a number of activities which in turn are connected to user roles—as with [48]. He does not, however, associate the context with the task but rather with the access control session by means of a context role. A context role contains a number of context instances which are logical predicates asserted over one or more context types of which there are four—User, Activity, Environment, and Object. A context role groups a set of context instances and is used to present abstract, human-understandable terms such as "LoanServiceTime," "ReviewSalesReportCt"—seemingly along the lines of the Logical Context presented by UbiCOSM.

3.2.3. Temporal and Spatial Context Approaches. Spatial and temporal information were first considered as a way to add more adaptivity for user–role assignment in RBAC. GEO-RBAC [50] is an extension of RBAC which introduces the idea of a *spatial role*, i.e., a role to that can be enabled/disabled based on the geographical position of a user-different permission may be granted for different locations. Similar to UbiCOSM, GEO-RBAC enables modelling of both physical (e.g., latitude/longitude) and logical positions (region, town, point of interest). Bertino et al. [51] introduced Temporal RBAC to support limited or periodic temporal duration of a role and temporal dependencies among actions expressed by means of role triggers (active rules that are automatically executed when the specified actions occur).

Other researchers have attempted to simultaneously include spatial and temporal context into RBAC. Chandran [52] proposed the Location- and Time-based RBAC which uses a fine-grained spatial model including a detailed location hierarchy with the notion of relative locations, and is integrated with a fine-grained logic and event-based temporal constraint specification framework. Location context for users indicates the location of the mobile device the user is using to access information or resource. Role location is also defined by the location of the mobile device in which the role is enabled or activated. Ray and Toahchoodee [53] proposed a spatio-temporal RBAC adding spatial and/or temporal constraints on user-role assignment, role-permission assignment, and discussing the impacts of these constraints on static and dynamic separation of duty (SoD), where static SoD ensures that a user does not get assigned conflicting roles or a role is not assigned conflicting permissions while dynamic SoD duty addresses the problem that a user is not able to activate conflicting roles during the same session. Aich et al. [54] describe STARBAC, a model that allows role enabling and disabling based on reasoning with spatio-temporal conditions expressed by space time (the physical location and a time instance) point. Aich et al. [55] further extend this for mobile application with confined availability of role and permissions to predefined spatio-temporal extents.

There are some common traits across the above research efforts include the following:

(i) The models adopt a general approach to vary role permissions or assignments to match varying temporal and/or spatial conditions.

(ii) Logic is used to express and trigger context conditions and updates through the use of predicates and rules, respectively.

(iii) The use of logical location and physical location, with logical locations being the preferred or dominant form—all spatial models assume the existence of some mapping function to map from the physical coordinates to the logical location. The location can capture either a point location or bounded area—represented as a set of points.

(iv) A number of the models include spatial specific relational operators such as *touches, contains, in*, *disjoint* to capture the relationship between different locations.

(v) Temporal models capture both point and period time semantics to trigger access changes.

3.3. ABAC-Based Context Schemes. Context-Aware-Attribute-Based Access Control (CA-ABA C) has also been widely applied to different domains for the purpose of providing more comprehensive and finer-grained access control.

Picard et al. [56] examine how secondary context can be derived from sensors for IoT-based ABAC-based CAAC. He proposes the "Proactive Engine," a rule-based engine for access context acquisition, modeling, and reasoning and embeds the engine in an ABAC framework to implement access control expression and enforcement. Chukkapalli et al. [57] create a smart farming ontology to represent various physical entities like sensors, workers on the farm, and their interactions with each other, as well as context. They develop an ontology-based context-aware ABAC system. Dutta [58] also proposes a cloud-based semantic web-based ABAC system captures physical context collected from sensed data (attributes), and performs dynamic reasoning over these attributes and context driven policies to execute access control decisions for IoT-based cyber-physical systems.

Psarra et al. [59] proposed a health-care Context-Aware Security Model (CASM) based on a combination of ABAC and Attribute-Based Encryption (ABE). The model acts as a configurable, common vocabulary for application-related access policies, with attributes which can be further tailored to each application's needs and can serve as background knowledge for creating and enforcing access control policies for electronic health records. The same combination of approaches (ABAC/ABE) is used in [60] to provide a concrete CA-ABAC that incorporates contextual information with ciphertext-policy attribute-based encryption (CP-ABE) to define access structure and encrypt data according to dynamic context changes in the IoT paradigm. Gupta et al. [61] proposed a two-level access control model for next-generation smart cars: external environment and in-vehicle. Access control for the external environment prevents vehicles from unauthorized access and in-vehicle access control protects essential components from adversaries. The model categorized vehicles into different groups for the purpose of notifying location-specific messages to relevant groups and to reduce administrative overhead.

Hsu and Ray [62] proposed a location-aware ABAC model to provide additional security for online social networks. The user location attribute authenticates user credentials (user name, password) in conjunction with location dependent geographic metadata (latitude, longitude, postal code). Burmester et al. [63] proposed T-ABAC which extends ABAC with real-time contextual attributes of ABAC components (user, environment, objects, etc.) and take into account the priority of access requests to support real-time availability within the strict time constraints of physical processes.

3.4. Situation Awareness in CAAC. The concept of situational awareness is often found alongside context awareness and indeed the two concepts are often conflated. The term was first introduced by Endesely with respect to the military domain as: "Situational awareness comprises the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."

The term has become widely used in the IT domain in the last ten years and has been incorporated into access control schemes also. As noted above, sometimes situation and context are conflated as in the Situational Aware-RBAC (SA-RBAC) model [64]. Here situation is defined as "context information such as location, time, and system resources such as network bandwidth and memory usage." Access is controlled by making a role active or inactive depending on the context value—more accurately they define a situation-aware matrix (SAM) for each context type (e.g., time or location) and the set of roles supported where each cell in the matrix is either active or inactive.

For any real-world scenario, a number of situation matrices may be used, corresponding to the number of context attributes used for the access control decision, e.g., [64] gives an example with separate matrices for *time*, *location*, and *resource*. The matrices are arranged in a 3D stack and the value of a role is the logical AND for that role across all the matrices. It can be noted here that SA-RBAC has a strong resembles to the spatio-temporal RBAC models discussed above.

Yau and Liu [65] present Situation-Aware Access Control which includes situation-aware constraints in RBAC models. Situations are *Atomic* or *Composite*. An atomic situation binds an entity (e.g., user) with a *SituationAssertion*, e.g., User A (entity) is bound with "Location is in Building B" yields "User A is in Building B." A composite situation is a logical or temporal combination of atomic situations.

Kayes has also examined and extended the use of situation in access control and extended it through the introduction of the *purpose* of the request as a factor in granting access. In [66] he defines a 'situation' as *"a specific subset of the complete state of the universe of access control entities that are relevant to a certain goal or purpose of a resource."* This is represented as a purpose-oriented situation model which is defined as a tuple:$S = \{p, c_1, c_2, \ldots, C_n\}$, where p is the *purpose* and $c_i\,(i = 1, 2, \ldots, n)$ are the values for each relevant entity. He gives an example situation record—Figure 4 for a medical scenario.

Kayes further examines situation in the Purpose-Oriented Situation-Aware Access Control (PO-SAAC) model [67]. Situation and purpose are defined as before and are seen as domain dependent. An atomic situation is defined as

$$S_a = \mathrm{PANDS}_t, \tag{1}$$

```
emergencyMedicalRecordAccess = {
        Purpose = 'Treatment';
        User_Role = 'ResidentDoctor';
        Owner_Category = 'Patient';
        Resource_PrivacyAttribute = 'EmergencyMedicalRecord';
        User_LocationAddress = 'EmergencyRoom';
        Owner_LocationAddress = 'EmergencyRoom';
        User_Owner_Relationship = 'NonTreatingPhysician';
        Patient_HealthState = 'Critical';
        Owner_Identity = Patient_Identity;
}
```

Figure 4: Example of purpose in situational awareness [66].

where P is the purpose or users' intention in requesting access and S_t denotes the state of a relevant entity, e.g., user location. Complex situations can be inferred as the logical combination of already existing atomic situations—specifically Kayes uses an OWL-based ontology to represent atomic situations and an inference engine to infer complex situations. Note both [66, 67] are based on the use of RBAC as the underlying access control model.

Kayes' interpretation of situation as aligned with *purpose* is very much in line with the notion of *mission* in situation awareness literature. "Human activities, organised as space and time processes" and are referred to as *missions* in a military context and as *business processes* in civilian applications [68]. We will see this interpretation recur in the discussion below on risk-based access control.

4. Risk and Trust in CAAC

Trust and Risk are two complementary factors that heavily influence the access control decision making in CAAC, either standalone or in combination.

4.1. Trust-Based CAAC. A well-known definition of trust is given by McKnight [69] as

"Trust is the extent to which one party is willing to depend on somebody, or something, in a given situation with a feeling of relative security, even though negative consequences are possible."

The use of "situation" in the definition captures the application of trust in context-aware dynamic environments. According to Bishop [70], trust is a measure of trustworthiness, i.e., "an entity is trustworthy if there is sufficient credible evidence leading one to believe that the system will meet a set of given requirements." Bishop remarks further that claims for trust or trustworthiness should not be accepted without "concrete evidence" that the system meets its requirements. However, as will be seen from the subsequent discussion, there is no single accepted definition of what "concrete evidence" is. Trust can be calculated in several ways depending on the application context [71]. Examples include *reputation models* in which trust ratings from third parties are combined to give a trust rating; *behavioural trust* where trust is estimated based on a record of historical transaction. Trust can also be calculated from assessing a set of *trust indicators* including security metrics (method of authentication) and from trust assertions (PKI certificates)—this interpretation of trust seems in line with Bishop's notion of "sufficient credible evidence."

From an access control perspective, trust expresses the level of confidence the resource controller has in the user not misusing the resource(s) that she wants to access [71] and several trust-based CAAC methods have been proposed.

Bernabe et al. propose a multi-dimensional trust CAAC approach for IoT [72]. Their model takes into account reputation, quality of services, security, and social relationships (between IoT devices, e.g., between all the devices belonging to one person). They use fuzzy logic to compute trust and define four trust levels as *Distrust*: the device will act against the best interests of another; *Untrust*: corresponds to the space between distrust and trust, in which a device is positively trusted, but perhaps not sufficiently to cooperate with it; *Trust:* represents the range where the device ensures a minimum of reliability and acts as expected; *HighTrust:* corresponds to the space where the evaluated entity can be confidently trusted.

Ouechatati and Azzouna [73] use reputation as a base for Trust-ABAC which includes trust in an ABAC-based CAAC system by means of a *trust value*, obtained from a reputation manager for each subject requesting access. It uses a Trust Management Broker framework to collect and disseminate transaction feedback from each CAAC system. The access control enforcement (specifically a PEP) provides a trust rating for each subject after each access control request and this transaction rating is forwarded to the local broker which includes it in the trust estimation. The basis for the transaction rating is not provided. In a similar manner, Wang et al. [74] propose a combined Trust and ABAC approach—T-ABAC (not to be confused with Time-based ABAC of [63]—to also include a *trust attribute* along with entity attributes into the access control calculation. He describes an abstract trust model that combines trust evidence from a number of sources into a fuzzy evaluation matrix. The evaluation algorithm is based on fuzzy sets is adopted to consider the fuzziness of the trust. Entropy is used to determine the weights which will be corrected by expert experience. The study offers no concrete trust model however.

More recently, the use of blockchain to manage trust for decentralised access control has become something of a hot topic for IoT applications [75–79]. These systems use blockchain for the most part as a secure, trusted, and decentralised storage system and encode trust models based on the approaches outlined above such as reputation, trust attributes, and behaviour as well as combining trust with ABAC. Tang et al. [75] describe a trust-based access control system for interaction between different IoT systems by means of an *IoT Passport*. A passport is issued to each device by its operating platform under common rules enforced by smart contracts. Additional rules between platforms, including details about how collaboration should happen, which attributes should be used for authorization and how rewards should be given to incentivize participants, etc., are agreed upon and programmed in smart contracts so that the execution can be dynamically and precisely enforced during every collaborative transaction. Putra et al. [77] developed a blockchain-based Trust and Reputation System (TRS) for IoT access control, which evaluates and calculates the trust and reputation score of each participating node to achieve a self-adaptive access control system. Trust and reputation are incorporated in the ABAC control policy, so that different nodes can be assigned different access rights, resulting in dynamic access control policies. Likewise, [78] describes a distributed ABAC control mechanism, relying on the blockchain technology to dynamically manage multi-endorsed attributes and trust anchors.

4.2. Risk-Based Access Control. Risk is defined as "A measure of the extent to which an entity is threatened by a potential .. event and is a function of ..the impact that would arise ..and the likelihood of occurrence" [80]. Risk is material when the value of a transaction is high, or when the transaction has a critical role in the security or the safety of a system [81].

Risk-aware access control was introduced to address challenges of allowing access to resources and information in dynamic environments. The access control system estimates the costs and benefits of giving access for each particular transaction and grants access if the risk is below a certain level. Risk-based access control is more permissive than traditional policy-based systems which do not consider contextual risk in making a decision. Risk-based access control system may include a risk mitigation mechanism [71, 82, 83] to reduce the risk associated with a transaction to an acceptable level—generally an obligatory action to be taken before or after access is granted [84]. Many factors can be included in the risk calculation including contextual, situational/mission, and environmental factors as well as trustworthiness of the subject making the request.

Cheng et al. [83] developed QRACC—see Figure 5, a fuzzy logic-based *quantified risk adaptive access control* model for a multilevel security system. QRACC defines multiple bands of risk between the normal binary "allow" and "deny." The quantified risk estimates for any access falls into one of these risk bands. Each band is associated with a decision and a risk mitigation action, e.g., such as increased auditing, application sandboxing, charging the risk to the user; the decision, the action, and band boundaries are all determined according to risk tolerance and can be changed when risk tolerance changes. Risk is estimated on the sensitivity of the information and the trustworthiness of the subject. Ni et al. [82] investigated the applicability of fuzzy inference for risk-based access control for multilevel security with a banded risk gradation similar to Cheng. However, their focus is more on the design choices of the fuzzy inference systems than defining a model for risk.

Armando considered the balance between risk and trustworthiness (of the requestor) in access control [71]. He defines a trust and risk access control architecture as shown in Figure 6. It contains the following modules:

(i) *Trust Estimation module*—adopts a trust indicators/trust assertion trust model to estimate trustworthiness of the user (subject) and the contextual conditions.

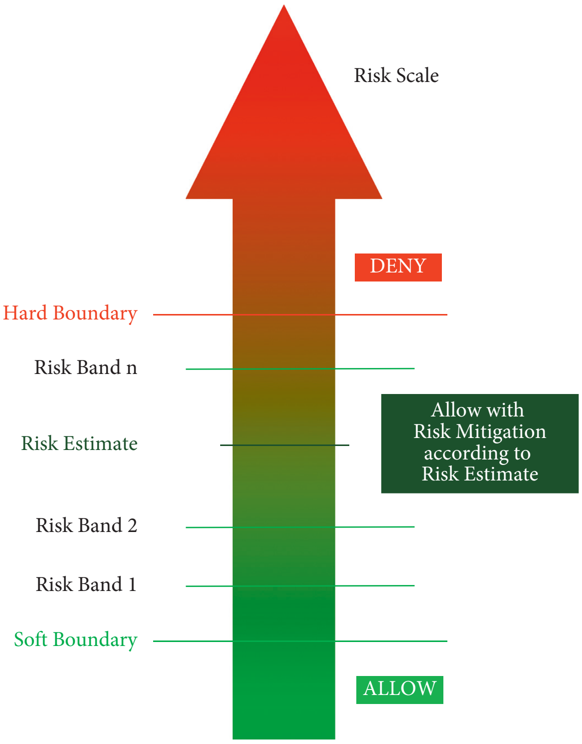


Figure 5: QRAAC [83].

(ii) *Risk Estimation module*—used to determine the level of risk, based on the data requested, context and on the criteria defined in the risk estimator.

(iii) *Trust and Risk Adjustment module*—this module is used to either mitigate risk or increase trust based on the particular use case and context. The system considers the use of *obligations* as a means to mitigate risk. Obligations are actions that must be carried out as a result of an authorization decision and are enforced by the Policy Enforcement Point. In the *Usage Control* (UCON) [84] model, obligations may also be enforced at any time during the user session.

(iv) *Risk-Aware Access Control module*—This is an ABAC-based CAAC through which users submit requests access requests.

Manchala [85] considers that the overall risk of a transaction is a function of *trust variables*. He introduces a trust model based on trust-related variables such as the cost of the transaction and its history and defines risk-trust decision matrices as illustrated in Figure 7. The risk-trust matrices are then used together with fuzzy logic inference rules to determine whether or not to transact with a particular party. The figure describes a trust matrix with a single matrix action, V, which signifies that a particular transaction should be verified—note that V might represent a range of mitigation action depending on the risk. Actions that need not be verified are grouped into a trust zone; the boundary of which zone is a trust contour. Note that the model may be extended with a third (or more) trust variable to form a 3D

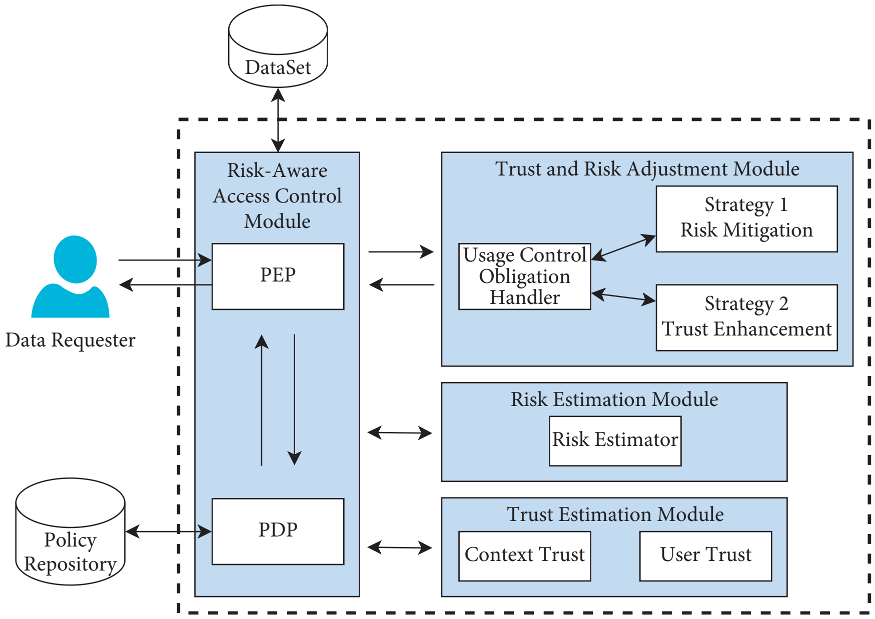
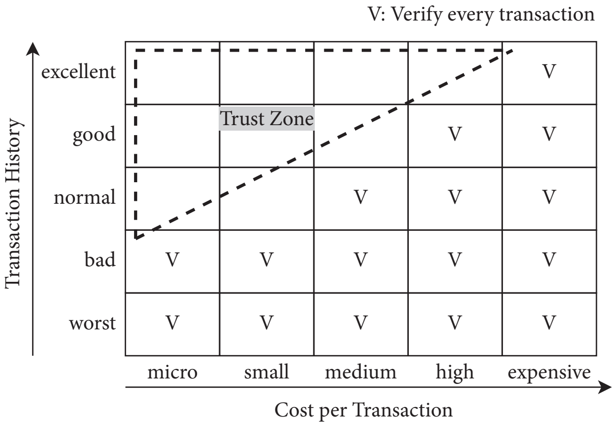

DataSet
Risk-Aware Access Control Module
PEP
PDP
Data Requester
Policy Repository
Trust and Risk Adjustment Module
Usage Control Obligation Handler
Strategy 1 Risk Mitigation
Strategy 2 Trust Enhancement
Risk Estimation Module
Risk Estimator
Trust Estimation Module
Context Trust
User Trust

Figure 6: Risk and Trust enforcement framework [71].



	micro	small	medium	high	expensive
excellent					V
good				V	V
normal			V	V	V
bad	V	V	V	V	V
worst	V	V	V	V	V

Figure 7: Trust matrix [84].

Table 3: Situation-aware matrix [64].

Role	Context1	Context2	. . ..	Contextn
Role1	Val	Val	Val	Val
Role1	Val	Val	Val	Val
. . .	Val	Val	Val	Val
Rolen	Inactive	Active	Active	Inactive

The table's parameters are: Contexti-: possible cases of specific situation information. Role: Access control roles. val: value of role activation, i.e., active | inactive.

matric stack in a manner similar to Table 3. Josang and Presti [81] elaborate this model to explore the balance between risk and trust in decision making to derive a computational model integrating the two notions.

The linking of access control with purpose/mission is considered in RAdAC [34] which bases access decisions on *operational needs* and *situational factors*. The proposed model allows operational need to enable access, and under specified conditions, to override security risk in determining access. The definition of operational need is very general, i.e., “The requestor's membership in some community of interest or organisation, their location, their rank, or some other discretionary factor might be used to determine operational need.” In the same way, situational factors are attributes which describe the operating environment, i.e., in effect context awareness. “Situation” in the RAdAC context is thus linked to risk assessment.

Kandala et al. [84] propose an ABAC framework for risk-adaptive access control based on the UCON access control approach—shown in Figure 8. UCON is an extended access control approach that seeks to unify both traditional access control, i.e., access at the start of the transaction with the need for ongoing control of access to the object during the transaction—what UCON terms *decision continuity*. This latter property is a significant addition to RAdAC as it allows adaptation to changing environment conditions. In Figure 8, the subject concept has been decomposed into a number of components, i.e., users, devices, connections, and purposes. The usage/access control decision process is shown to include Risk Evaluation component as well predicate/rule-based components for *Authorisation* (based on the attributes), *Obligations*, and *Conditions*. Obligations are functional predicates that verify mandatory requirements that a subject has to perform before or during a usage session—in RAdAC obligations can be used for risk mitigation as proposed in other risk-aware research works reviewed earlier. Conditions are environmental or system-oriented decision factors. Kandala incorporates situation related to a particular user or a group of users such as location, as *Local Situational Factors* which are defined as functional predicates that can be evaluated to be true or false. Usage access decision-making is based on all three rule/predicate components, i.e., authorization, obligation, and conditions and all can be evaluated pre, during, or post the session.

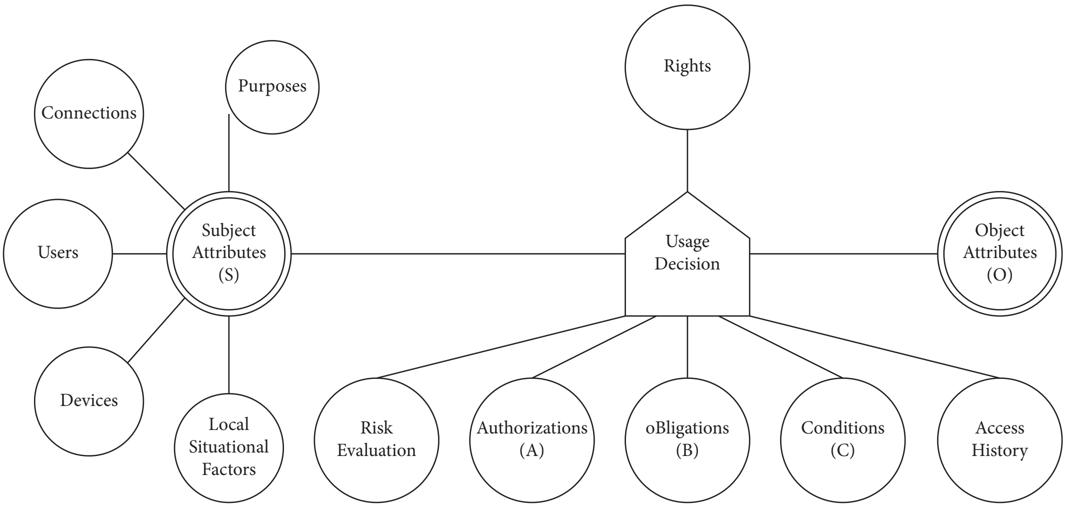


Figure 8: UCON-based RAdAC [85].

4.3. Application CAAC Usage. In the health domain, Khan and Sakamura [86] combine RBAC, which is used to manage hospital staff, with DAC, to offer patients the rights to delegate the access-rights to his/her trustable persons if an emergency occurs. The proposed CAAC model includes environmental contexts dealing with common situations to handle emergencies, rights delegation, and legislative guideline and technical standards. To respond to the trade-off among policy acuteness, privacy, and safety in different critical levels of contextual situations of pervasive medical sensor network, Garcia-Morchon and Wehrle [87] present a two-layer (engine and data) Criticality-Aware-RBAC system to provide granular access control decisions. Most situations are subject to safety and acuteness and least privacy; therefore, Criticality-Aware AC policies are enforced before role enrolment of RBAC—this is a form of purpose-oriented CAAC. Other situations' policies are enforced after a role has been verified to promise a degree of safety and privacy.

Applications installed on *mobile platforms* can abuse system permissions to surreptitiously record user privacy. Shebaro et al. [88] describe a context-based mechanism that allows Android system users to set configuration policies to control how applications are to use device resources and services under different contexts—mainly location and time. CBAC needs accurate positions of the user to provide related restrictions on applications; therefore, the proposed mechanism uses Wi-Fi APs and their signal strength to provide acute positions of each subarea inside a relatively big location. Miettinen et al. [37] provide a CA platform that uses a machine learning approach to automatically classify context rather than user-/pre-defined static AC policies to avoid laborious policy setup and maintenance as well as reflect true preference of users. The CA platform uses two kinds of context: location and social. These are used to model familiarity of the specific location and the surrounding people, respectively.

The *edge and cloud computing* domain implies remote access to distributed resources. Satoh [89] presented a CAAC model to deal with malicious insider attacks in cloud computing. The context used in this model is defined as a 3-tuple including spatial state, temporal state, and trust level of platform. A resource management role activation is associated with context and separation of duty. Kayes et al. [42] introduced a CAAC model which uses fuzzy logic and logical comparison to deal with imprecise context and crisp context for cloud-based resources. To respond to distributed and multisource characteristics of cloud-based data, the mechanism has data integration and mapping capabilities.

Arfaoui et al. [90] proposed a novel CAAC for Wireless Body Area Networks (WBAN). This approach aims to secure personal body information records in communications among the stakeholders and provide adaptive context-aware privacy. A network manager provides encrypted connection between the WBAN user and other data consumers based on the contextual information. The data consumers are further divided into public domain, mainly hospital-side staff, and personal domain those who have close relationship with the user. Zheng et al. [91] described a CAAC model for a building information model on mobile cloud architecture. The proposed CAAC mechanism is based on RBAC. To respond to increasing number of subjects, a user grouping method is used to improve scalability and efficiency—the model group users based on user's privileges and advanced model correspond to contextual information.

Salonikias et al. [92] examine how ABAC may be provided for Intelligent Transportation Systems paradigm based on fog computing. He proposes a distributed CAAC architecture, where the PIP, PDP, and PEP are deployed in the fog.

Rosenberger and Gerhard [93] explored context awareness specific to *industrial applications*. They proposed a framework with a number of industry-specific context types, some of which are: *(i) Personal information*: who is the user and what role do they serve in the company. *(ii) Personal condition:* fatigue sensing sensors to aid worker safety. *(iii) Location:* to facilitate option selection available to the operator in that domain. *(iv) Date and Time:* facilitate specific event options like maintenance. *(v) Environment conditions:* awareness of temperature, humidity, etc., to facilitate environment control. *(vi) Resource condition:* being able to sense and understand equipment and supply conditions. *(vii) Task:* user allowed tasks. These contexts are an inherent part of most manufacturing activities and are important for machine, plant, and operator safety. CAAC systems can significantly benefit the industrial domain through identifying situations and acting accordingly to ensure security and safety for equipment and personnel.

5. CAAC, Trust, Risk, and ZT

In this section, we identify some of the main patterns from the previous CAAC and Risk/Trust analysis and consider how these may apply to ZT.

5.1. Context Patterns. We can derive the following points from the analysis of context.

(1) Although the definition and usage of context vary from work to work, the representation of context exhibits a high degree of commonality across the various works.

(2) Context is generally defined as an attribute or combination of attributes that characterize the state of one or more entities. Context may also include the state of the relationship between entities. More formally, Kayes et al. [32] define access control related context as "..*any information that can be used to characterise the state of relevant access control-specific entities and the state of relevant relationships between different entities (an access control-specific entity is a user, a resource and an environment*."

(3) Context-aware access control models contain several different entities which vary depending on the model. User, object, subject, role, and environment are typical entities.

(4) Context is expressed in access control policies by contextual conditions/expressions/predicates which are defined as relational operations (=, ! = , > etc.) over entity attributes (simple conditions) and/or a logical combination of either simple conditions (complex conditions) or other complex conditions. This mode of expressing context occurs repeatedly throughout the surveyed works.

(5) Situation can be considered as equivalent to or a form of context and as such may be expressed by context expressions also.

(6) Situation is often associated with mission or purpose. In such cases situation may be represented by a data tuple or data aggregate.

(7) Context and situation may be primary, i.e., emanating directly from the entities or secondary, i.e., inferred or retrieved using the primary context information.

(8) RBAC-based context models adapt to dynamically changing context by varying role assignment and/or permissions to match the context. In some examples, roles may be activated/deactivates based on context.

(9) ABAC-based context models adapt to dynamically changing context by invoking appropriate rules/policies based on the values of entity attributes.

(10) Context and situation have some well-known examples, e.g., spatial, temporal. More generally, contexts/situations are domain specific and require definition of domain attributes. The most common example found in the literature is the medical/health domain.

5.2. Risk and Trust. We can derive the following points from the analysis of risk and trust.

(1) Trust is linked to context by its definition as the degree of willingness of one party to depend on someone or something in a given situation.

(2) Trust can be calculated in several ways including reputational trust and behavioural trust as well as from assessing trust indicators such as security metrics and from trust assertions such as PKI certificates.

(3) In context-aware access control trust expresses the level of confidence the resource controller has in the user not to misuse the resources being accessed.

(4) Trust many is often combined with ABAC through the use of a specific Trust attribute.

(5) Blockchain based trust systems are being extensively researched to manage trust for decentralised access control for IoT systems. Typically, these also use ABAC.

(6) Risk-aware access control balances the trade-off between benefits and potential costs (downsides) of giving a user access to a resource.

(7) The benefit (or need) from giving access is often related to the purpose or mission of an entity/situations.

(8) Cost is related to misuse of the resource, e.g., breach of confidentiality, integrity or availability. Cost may therefore be related to the sensitivity or priority of the resource to the organisation.

(9) Risk may be calculated based on many factors (entity attributes) including context. The trustworthiness of the user is often a particularly important factor.

(10) Risk-aware access decisions may be binary (allow/deny) but more often are scaled in some way i.e., may give different degrees of access or enforce some form of risk mitigation/trust enhancement actions before giving access. Such approaches attempt to deal with the intrinsic uncertainty and probabilistic nature of dynamic contexts.

(11) This "scaled" decision making model is a form of context-reasoning and many of those proposed

technologies (e.g., ontologies, fuzzy logic) have been proposed for risk-based access control.

(12) Risk mitigation or trust enhancement actions may be ongoing during the access session. These are often referred to as obligations and are included in most risk-aware access control schemes.

5.3. Application to ZT. The CAAC formalisms and models explored above provide a rich canvas to capture and express the dynamic policies anticipated by ZT. We note the following.

(1) Different entity contexts may be appropriate for the different ZT approaches described in Rose et al. [1]. For example, the Enhanced Identity Governance approach may benefit from an emphasis on User-centric context, while the microsegmentation-based approach may benefit from an environment-centric context focus.

(2) In principle, either ABAC- or RBAC-based schemes could be used to provide ZT access control. In practice, ABAC gives more fine-grained control and is the dominant access control approach explored in the literature and in commercial systems. However, it is very likely that RBAC systems will be used to provide primary or secondary context information sources for user-centric contexts.

(3) ZT places very strong focus on user credentials and device state when making access control decision. As a result, the main ZT trust mechanisms proposed in the literature are trust indicators and trust assertions [1,3,4]. Behavioural trust based on users historical access is also strongly suggested for use (as alluded to earlier Rose et al. [1] refer to behavioural trust as "contextual trust assessment). Although not explicitly described reputation-based trust systems could in principle also apply.

(4) The line between ZT trust assessment and risk-aware access control risk assessment is very imprecise. Calculation of access benefit through mission or purpose is not explicitly referenced in the ZT literature—rather the potential damage or cost arising from subject, object or environment entity sensitivities is the main factor considered in making the access decision. However, as the range of dynamic context increase as ZT is more widely deployed we are likely to see increasing convergence between the two.

(5) Real-world ZT systems access decisions may be binary or scaled. NIST [1] defines this as "criteria" vs "score" based where the former permits or denies access based on the values of a set of attributes while the latter assigns a confidence level based on the values of different attributes and grants access if the confidence value is higher than a given threshold. Access maybe either denied or restricted if the confidence level is too low. Google employs a tiered-trust scheme [3]. In order to access a given resource, a device's trust tier assignment must be equal to or greater than the resource's minimum trust tier requirement.

(6) The calculation of ZT trust confidence levels can be based on any of the context reasoning techniques outlined in [22] such as fuzzy logic, probabilistic logic, ontology-based, or machine learning. The numerous fuzzy logic risk-aware access control approaches could be adapted for ZT trust calculation, e.g., Manchala's [85] fuzzy trust matrix approach could provide a comprehensive access control approach that would map well to both NIST and Google's BeyondCorp ZT architectures. Moreover, Armando's the trust and risk-aware access control framework [71] points out an approach to implementing a trust/risk evaluation system.

(7) Continual monitoring of the access control decision is a key ZT tenet and thus the use of risk-aware access control obligation-type mechanisms will be required as part of ZT access control.

(8) Since ZT is essentially a set of concepts and ideas rather than a functional architecture, it can be applied to many different enterprise information systems configurations including IoT, cloud, and remote working. Moreover, diverse technologies such as blockchain could be used in the implementation. Our focus in this work is primarily on the traditional enterprise—which may include cloud and remote working component but does not explicitly consider IoT and edge computing. These latter two may require consideration of extra details such as those outlined by Kayes et al. [32].

5.4. Future Research Areas. ZT to date has been mainly applied to enterprise systems and most commercial offerings address this marketplace. As outlined earlier, researchers are exploring the use of ZT in more distributed scenarios including Operational Technologies (OT) domains such as smart manufacturing and smart grid as well as IoT and edge computing. These efforts are however in an early stage and many open challenges remain to be solved to successfully deploy ZT in these domains. Also, CAAC for such distributed environments is still an open problem. In the rest of this section, we address some areas requiring further research.

5.4.1. Distributed and Federated Environments. Edge computing and IoT fundamentally extend and reshape cloud computing. Many challenges still remain for CAAC in these areas. Kayes et al. [32] outline some such challenges including

(i) How to capture and derive the relevant contextual conditions from IoT, fog and cloud environments?

(ii) How to effectively specify the context-aware access control policies to manage and control data from distributed cloud sources by means of reducing computational overheads?

(iii) How to protect the privacy requirements of the multiple stakeholders?

(iv) How to build an appropriate data sharing mechanism for all the entities involved, i.e., IoT devices, edge servers and cloud data centres?

Kayes proposes an approach to answer these questions, however many alternative approaches could also be explored.

ZT for cross-organisational or federated interaction is also an area identified by NIST [1] as needing further study. A number of researchers have looked at use of ZT for different organisation federation scenarios including federated identity management [94], federated clouds, [95] and cross network orchestration [96] but research in this area can be considered at an early stage. Similarly, the use of ZT for supply chains is barely explored as of yet [97, 98].

5.4.2. Trust Models and Mechanisms. ZT trust models in-the-wild seem to be largely based on *trust indicators* such as security metrics and *trust assertions* such as PKI certificates. The NIST ZT architecture [1] also specifies that *behavioural trust*, i.e., users access transaction history as well as users computer usage behaviour history—using, for example, anomaly detection—as a means of taking access control decisions. So far, we have not seen evidence for this type of use in deployed systems and there are many opportunities to research new approaches, e.g., based on the use of machine learning. *Reputation trust* approaches such as those described in [72, 73] may also be a feasible approach for ZT based IoT-based scenario involving multiple parties. A number of researchers have examined blockchain based trust mechanisms for ZT in IoT—however the range of blockchain-based approaches is likely to expand as the ZT solutions are increasingly deployed towards the edge. Moreover, approaches based on a combination of trust mechanisms, e.g., blockchain and reputation may also be interesting to explore in IoT and edge scenarios.

5.4.3. CAAC Policy Enforcement for ZTA. Although ZT is widely deployed and researched there has been very little published to date on ZT policy specification languages. In our own group, Vanickis et al. [13] have outlined one such language, PAROLE. PAROLE is an ABAC approach that is influenced by ALFA [99] and UCON-based RAdAC [84]. It inherits much of the language structures described by ALFA but extends ALFA to include an event handling loop to enable real-time interaction with the ZT environment in order to implement the authorisation, obligations and conditions of the UCON model. Moreover, it also includes a fuzzy logic-based risk assessment component based on FCL to enable risk-based access control. This element reuses the jFuzzyLogic language [100] to implement risk-based CAAC. We are currently implementing this language. As outlined by Perera et al. [22], there are many approaches for *context reasoning* besides fuzzy logic including ontology based, machine learning, probabilistic logic as well as rules. Many authors have explored the use of a number of these techniques for CAAC and it is reasonable to expect that these efforts could be extended without great effort to ZT scenarios.

Another challenge will be the huge numbers of policies that have to be specified, implemented, deployed, and managed [101]. This will require innovative approaches perhaps using machine learning, e.g., to estimate risk-based criteria to be used for control-related decisions [101] or for learning attributes ABAC policies in collaborative IoT/edge applications [102].

5.4.4. ZT-Aware Analytics. The ZTE architecture introduces the possibility to deploy ZT functions at the network edge including analytic functions for malware analysis, intrusion detection, and security situational awareness assessment [103]. While ZTE is focused on SDWAN edge deployments, we believe that there will be a wide range of edge ZT deployments and the drivers of remote access, collaboration/federation of edge devices, and the continued deployment of AI to the edge combine to create both need and opportunity for deployment of security analytics at the edge in domains such as smart grids [103] and 5G networks [104]. This will create opportunities for innovative enclave-based AI-based solutions addressing, e.g., collaborative and distributed intrusion detection, multisource data fusion to combine heterogeneous data streams for intrusion detection, and new approaches to edge malware analysis and detection, to name but a few.

Another interesting possibility to explore will be the use of digital twin-based cybersecurity to assist with ZT threat detection and analysis functions to proactively detect possible attacks [105]. This type of analysis may be particularly effective for scenarios where it may not be possible to directly deploy agents such as OT installations.

6. Conclusion

Context awareness is a very well-studied phenomenon in pervasive computing and, more recently, in IoT. The use of context awareness in access control has also been widely researched as the inclusion of trust and risk assessment into the access control decision. The widespread emergence of Zero-Trust-based security models in recent years has created renewed interest in the application of these techniques. In this study, we have reviewed previous research in CAAC and risk and trust in access control with a goal to identify common concepts and themes in these fields and to examine their potential use in ZT security models. We find that there are indeed many underlying commonalities across the various research works that we have studied and that many of these ideas can be, and in some cases, and are being applied to ZT models and deployments and we have elaborated these findings in the previous section. We have, moreover, identified areas for future research. We intend to develop a context and risk-aware access control policy language for ZT systems based on the finding outlined above.

This involves the extension of a draft language, PAROLE, outlined in the authors' previous works [12, 13].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This publication has emanated from research conducted with the financial support of Athlone Institute of Technology under its President's Seed Fund (2021) and Science Foundation Ireland (SFI) under Grant Number SFI 16/RC/3918, co-funded by the European Regional Development Fund.

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, National Institute of Standards and Technology, 2019.

[2] J. Kindervag, *No More Chewy Centers*, Vol. 18, The Zero Trust Model Of Information Security, Cambridge, England, 2016.

[3] B. Osborn, J. McWilliams, B. Beyer, and M. Saltonstall, "BeyondCorp: Design to Deployment at Google," *LOGIN*, vol. 41, pp. 28–34, 2016.

[4] R. Ward and B. Beyer, "Beyondcorp: A New Approach to enterprise Security," *LOGIN*, vol. 39, no. 6, pp. 6–11, 2014.

[5] M. Mujib and R. F. Sari, "Design of implementation of a zero trust approach to network micro-segmentation," *Int. J. Adv. Sci. Technol.*vol. 29, no. 7, pp. 3501–3510, 2020.

[6] S. Mehraj and M. T. Banday, "Establishing a zero trust strategy in cloud computing environment," in *Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–6, IEEE, Coimbatore, India, January 2020.

[7] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van der Merwe, "Eztrust: network-independent zero-trust perimeterization for microservices," in *Proceedings of the 2019 ACM Symposium on SDN Research*, pp. 49–61, Association for Computing Machinery, New York, NY, USA, April 2019.

[8] S. Li, "Editorial: zero trust based internet of things," *EAI Endorsed Transactions on Internet of Things*, vol. 5, pp. 165168–20, 2020.

[9] M. Samaniego and R. Deters, "Zero-trust Hierarchical Management in IoT," in *Proceedings of the 2018 IEEE international congress on Internet of Things (ICIOT)*, pp. 88–95, IEEE, San Francisco, CA, USA, July 2018.

[10] S. Dhar and I. Bose, "Securing IoT devices using zero trust and blockchain," *Journal of Organizational Computing & Electronic Commerce*, vol. 31, no. 1, pp. 18–34, 2020.

[11] T. Lukaseder, M. Halter, and F. Kargl, "Context-based Access Control and Trust Scores in Zero Trust Campus Networks," in *Proceedings of the 2020 Sicherheitshalber*, 2020.

[12] B. Lee, R. Vanickis, F. Rogelio, and P. Jacob, *Situational Awareness Based Risk-Adapatable Access Control in Enterprise Networks*, 2017, https://arxiv.org/abs/1710.09696.

[13] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access control policy enforcement for zero-trust-networking," in *Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC)*, pp. 1–6, IEEE, Belfast, UK, June 2018.

[14] "Call for Papers, ," USENIX, 2015, https://www.usenix.org/conference/woot15/call-for-papers.

[15] *What Is Security Information and Event Management (SIEM)?*, IBM, https://www.ibm.com/topics/siem.

[16] H. David, "Take security to the zero trust edge," *Forrester*, vol. 16, 2021, https://www.forrester.com/blogs/take-security-to-the-zero-trust-edge/.

[17] L. Andrew, *Say Hello to SASE (Secure Access Service Edge)*, Andrew Lerner, 2019, https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/.

[18] A. K. Dey, "Understanding and using context," *Personal and Ubiquitous Computing*, vol. 5, no. 1, pp. 4–7, 2001.

[19] J. Wu, I. Bisio, C. Gniady, E. Hossain, M. Valla, and H. Li, "Context-aware networking and communications: Part 1 [guest editorial]," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 14-15, 2014.

[20] j. Wu, I. Bisio, C. Gniady, E. Hossain, M. Valla, and H. Li, "Context-aware networking and communications: part 2 (guest editorial)," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 64-65, 2014.

[21] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Proceedings of the International Symposium on Handheld and Ubiquitous Computing*, pp. 304–307, Atlanta, GA, USA, November 1999.

[22] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[23] C. S. Jordan, *A Guide to Understanding Discretionary Access Control in Trusted Systems,* NATIONAL COMPUTER SECURITY CENTER FORT GEORGE G MEADE MD, Maryland, MD, USA, 1987, https://apps.dtic.mil/sti/citations/ADA392813.

[24] Us Department of Defense, "Department of defense trusted computer system evaluation criteria," in *The 'Orange Book' Series*, pp. 1–129, US Department of Defense, London,UK: Palgrave Macmillan UK, 1985.

[25] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[26] I. T. L. Computer Security Division, *SP 800-162, Guide to ABAC Definition and Considerations | CSRC*CSRC NIST, Gaithersburg, Maryland, 2016.

[27] A. Singhal, T. Winograd, and K. A. Scarfone, *Guide to Secure Web Services*, National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

[28] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the Advances in Cryptology – EUROCRYPT 2005*, pp. 457–473, Berlin, Heidelberg, July 2005.

[29] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, CA, USA, May 2007.

[30] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Public Key Cryptography – PKC 2011*, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds., vol. 6571, pp. 90–108, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[31] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.

[32] A. S. M. Kayes, R. Kalaria, I. H. Sarker et al., "A survey of context-aware access control mechanisms for cloud and fog

networks: taxonomy and open research issues," *Sensors*, vol. 20, no. 9, p. 2464, 2020.

[33] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors Journal*, vol. 37, pp. 9–42, 2017.

[34] R. McGraw, "Risk-adaptable access control (radac)," in *Proceedings of the Privilege (Access) Management Workshop*, vol. 25, pp. 55–58, National Institute of Standards and Technology–Information Technology Laboratory, Gaithersburg, Maryland, 2009.

[35] J. H. Jafarian and M. Amini, "CAMAC: a context-aware mandatory access control model," *ISeCure*, vol. 1, no. 1, 2009.

[36] A. Almutairi, *Context-aware and Adaptive Usage Control Model*De Montfort University, Leicester, UK, , 2031, https://www.semanticscholar.org/paper/Context-aware-and-adaptive-usage-control-model-Almutairi/1af57017a3cccdf7b1fa3dd726c8cb022229794e.

[37] M. Miettinen, S. Heuser, W. Kronz, A.-R. Sadeghi, and N. Asokan, "Conxsense: automated context classification for context-aware access control," in *Proceedings of the 9th ACM Symposium on Information*, pp. 293–304, computer and communications security, New York, NY, USA, June 2014.

[38] J. H. Jafarian, M. Amini, and R. Jalili, "A context-aware mandatory access control model for multilevel security environments," in *Proceedings of the International Conference on Computer Safety*, pp. 401–414, Reliability, and Security, Berlin, Heidelberg, September 2008.

[39] M. J. Covington, M. J. Moyer, and M. Ahamad, *Generalized Role-Based Access Control for Securing Future Applications*https://smartech.gatech.edu/handle/1853/6580 Technical Report, Georgia Institute of Technology, Atlanta, GA, USA, 2000, https://smartech.gatech.edu/handle/1853/6580 Technical Report.

[40] M. J. Moyer and M. Abamad, "Generalized role-based access control," in *Proceedings of the 21st International Conference on Distributed Computing Systems*, pp. 391–398, IEEE, Mesa, AZ, USA, April. 2001.

[41] A. S. M. Kayes, J. Han, W. Rahayu, T. Dillon, M. S. Islam, and A. Colman, "A policy model and framework for context-aware access control to information resources," *The Computer Journal*, vol. 62, no. 5, pp. 670–705, 2019.

[42] A. S. M. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization for cloud-based data resources," *Future Generation Computer Systems*, vol. 93, pp. 237–255, 2019.

[43] A. S. M. Kayes, W. Rahayu, P. Watters, M. Alazab, T. Dillon, and E. Chang, "Achieving security scalability and flexibility using fog-based context-aware access control," *Future Generation Computer Systems*, vol. 107, pp. 307–323, 2020.

[44] A. Corrad, R. Montanari, and D. Tibaldi, "Context-based access control management in ubiquitous environments," in *Proceedings of the Third IEEE International Symposium on Network Computing and Applications*, pp. 253–260, IEEE, Cambridge, MA, USA, January 2004.

[45] Mumian, *Manage Resource Groups - Azure portal - Azure Resource Manager*, 2022, https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal.

[46] Y. Zhu, D. Ma, C.-J. Hu, and D. Huang, "How to use attribute-based encryption to implement role-based access control in the cloud," in *Proceedings of the 2013 International Workshop on Security in Cloud Computing - Cloud Computing '13*, p. 33, May 2013.

[47] Y. Tian, Y. Peng, G. Gao, and X. Peng, "Role-based access control for body area networks using attribute-based encryption in cloud storage," *International Journal on Network Security*, vol. 19, pp. 720–726, 2017.

[48] S. Schefer-Wenzl and M. Strembeck, "Modeling context-aware RBAC models for business processes in ubiquitous computing environments," in *Proceedings of the 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing*, pp. 126–131, IEEE, Vancouver, Canada, June 2012.

[49] S.-H. Park, J.-H. Eom, and T.-M. Chung, "A Study on Access Control Model for Context-Aware Workflow," in *Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC*, pp. 1526–1531, IEEE, Seoul, Republic of Korea, August 2009.

[50] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: a spatially aware RBAC," in *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, p. 29, February 2005.

[51] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: a temporal role-based access control model," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 191–233, Aug. 2001.

[52] S. M. Chandran and J. B. D. Joshi, "LoT-Rbac: A location and time-based RBAC model," in *Proceedings of the Web Information Systems Engineering – WISE 2005*, pp. 361–375, Berlin, Heidelberg, 2005.

[53] I. Ray and M. Toahchoodee, "A spatio-temporal role-based access control model," *Data and Applications Security XXI*, vol. 4602, pp. 211–226, 2007.

[54] S. Aich, S. Sural, and A. K. Majumdar, "STARBAC: spatiotemporal role based access control," in *Proceedings of the On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS*, pp. 1567–1582, Springer-Verlag, Berlin, Heidelberg, November 2007.

[55] S. Aich, S. Mondal, S. Sural, and A. K. Majumdar, "Role based access control with spatiotemporal context for mobile applications," in *Transactions on Computational Science IV: Special Issue on Security in Computing*, M. L. Gavrilova, C. J. K. Tan, and E. D. Moreno, Eds., Springer, Berlin, Heidelberg, pp. 177–199, 2009.

[56] N. Picard, J.-N. Colin, and D. Zampunieris, "Context-aware and attribute-based access control applying proactive computing to IoT system," in *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security*, pp. 333–339, Funchal, Madeira, Portugal, 2018.

[57] S. S. L. Chukkapalli, A. Piplai, S. Mittal, M. Gupta, and A. Joshi, "A smart-farming ontology for attribute based access control," in *Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 29–34, IEEE, Baltimore, MD, USA, May 2020.

[58] S. S. Dutta, S. S. L. Chukkapalli, M. Sulgekar, S. Krithivasan, P. K. Das, and A. Joshi, "Context sensitive access control in smart home environments," in *Proceedings of the 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity)*, IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, May 2020.

[59] E. Psarra, I. Patiniotakis, Y. Verginadis, D. Apostolou, and G. Mentzas, "Securing access to healthcare data with context-

aware policies," in *Proceedings of the 2020 11th International Conference on Information, Intelligence, Systems and Applications IISA*, pp. 1–6, IEEE, Piraeus, Greece, July. 2020.

[60] A. Arfaoui, S. Cherkaoui, A. Kribeche, and S. M. Senouci, "Context-aware adaptive remote access for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 786–799, 2020.

[61] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Cars," in *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy*, Texas, TX, USA, March 2019.

[62] A. C. Hsu and I. Ray, "Specification and enforcement of location-aware attribute-based access control for online social networks," in *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*, pp. 25–34, New York, NY, USA, March. 2016.

[63] M. Burmester, E. Magkos, V. Chrissikopoulos, and T. Abac, "An attribute-based access control model for real-time availability in highly dynamic systems," in *Proceedings of the 2013 IEEE Symposium on Computers and Communications (ISCC)*, Article ID 000143, Split, Croatia, July 2013.

[64] Y.-G. Kim and J. Lim, "Dynamic activation of role on RBAC for ubiquitous applications," in *Proceedings of the 2007 International Conference On Convergence Information Technology (ICCIT 2007)*, pp. 1148–1153, Gwangju, Republic of Korea, November. 2007.

[65] S. S. Yau and J. Liu, "A situation-aware access control based privacy-preserving service matchmaking approach for service-oriented architecture," in *Proceedings of the IEEE International Conference on Web Services (ICWS 2007)*, pp. 1056–1063, Salt Lake City, UT, USA, July 2007.

[66] A. S. M. Kayes, J. Han, and A. Colman, "ICAF: a context-aware framework for access control," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 442–449, Wollongong, Australia, July 2012.

[67] A. S. M. Kayes, J. Han, A. Colman, and S. A. A C. Po, "A purpose-oriented situation-aware access control framework for software services," in *Proceedings of the International Conference on Advanced Information Systems Engineering*, pp. 58–74, Thessaloniki, Greece, June 2014.

[68] G. Jakobson, "Mission resilience," in *Cyber Defense and Situational Awareness*, A. Kott, C. Wang, and R. F. Erbacher, Eds., vol. 62, pp. 297–322, Springer International Publishing, Berlin, Germany, Cham, 2014.

[69] D. Harrison McKnight and N. L. Chervany, "Trust and distrust definitions: one bite at a time," *Trust in cyber-societies*, vol. 2246, pp. 27–54, 2001.

[70] M. Bishop, *Introduction to Computer Security*, Addison-Wesley, Boston, 2005.

[71] A. Armando, M. Bezzi, F. Di Cerbo, and N. Metoui, "Balancing trust and risk in access control," in *Proceedings of the OTM Confederated International Conferences on the Move to Meaningful Internet Systems*, pp. 660–676, Berlin, Heidelberg, October 2015.

[72] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "TACIoT: multidimensional trust-aware access control system for the Internet of Things," *Soft Computing*, vol. 20, no. 5, pp. 1763–1779, 2016.

[73] H. Ouechtati and N. B. Azzouna, "Trust-abac towards an access control system for the internet of things," in *Proceedings of the International Conference on Green, Pervasive, and Cloud Computing*, pp. 75–89, Amalfi Coast, Italy, May 2017.

[74] J. Wang, H. Wang, H. Zhang, and N. Cao, "Trust and attribute-based dynamic access control model for internet of things," in *Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 342–345, Nanjing, China, October. 2017.

[75] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT passport: a blockchain-based trust framework for collaborative internet-of-things," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, pp. 83–92, Toronto ON Canada, New York, NY, USA, May 2019.

[76] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: a smart contract enabled decentralized capability-based access control mechanism for the iot," *Computers*, vol. 7, no. 3, p. 39, 2018.

[77] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trust management in decentralized iot access control system," in *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–9, Toronto, ON, Canada, May 2020.

[78] S. Dramé-Maigné, M. Laurent, and L. Castillo, "Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts," in *Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1582–1587, Tangier, Morocco, June 2019.

[79] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[80] S. R. Ronald, *Risk Management Framework for Information Systems and Organizations:: A System Life Cycle Approach for Security and Privacy*National Institute of Standards and Technology, Gaithersburg, MD, 2018.

[81] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *Trust Management*, C. Jensen, S. Poslad, and T. Dimitrakos, Eds., vol. 2995, pp. 135–145, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[82] Q. Ni, E. Bertino, and J. Lobo, "Risk-based access control systems built on fuzzy inferences," in *Proceedings of the 5th ACM Symposium on Information*, pp. 250–260, Computer and Communications Security, Beijing, China, April. 2010.

[83] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger, "Fuzzy multi-level security: an experiment on quantified risk-adaptive access control," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2007.

[84] S. Kandala, R. Sandhu, and V. Bhamidipati, "An attribute based framework for risk-adaptive access control models," in *Proceedings of the 2011 Sixth International Conference on Availability*, pp. 236–241, Reliability and Security, Vienna, Austria, August. 2011.

[85] D. W. Manchala, "E-commerce trust metrics and models," *IEEE Internet Comput*, vol. 4, no. 2, pp. 36–44, 2000.

[86] M. F. F. Khan and K. Sakamura, "Context-aware access control for clinical information systems," in *Proceedings of the 2012 International Conference on Innovations in Information Technology (IIT)*, pp. 123–128, Abu Dhabi,UAE, March 2012.

[87] O. Garcia-Morchon and K. Wehrle, "Efficient and context-aware access control for pervasive medical sensor networks," in *Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 322–327, Mannheim, Germany, March 2010.

[88] B. Shebaro, O. Oluwatimi, and E. Bertino, "Context-based access control systems for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 2, pp. 150–163, 2015.

[89] I. Satoh, "Context-aware access control model for services provided from cloud computing," in *Intelligent Distributed Computing XI*, M. Ivanović, C. Bădică, J. Dix, Z. Jovanović, M. Malgeri, and M. Savić, Eds., Springer International Publishing, Berlin, Germany, pp. 285–295, 2018.

[90] A. Arfaoui, O. R. M. Boudia, A. Kribeche, S.-M. Senouci, and M. Hamdi, "Context-aware access control and anonymous authentication in WBAN," *Computers & Security*, vol. 88, Article ID 101496, 2020.

[91] R. Zheng, J. Jiang, X. Hao, W. Ren, F. Xiong, and T. Zhu, "CaACBIM: a context-aware access control model for bim," *Information*, vol. 10, pp. 47–2, 2019.

[92] S. Salonikias, I. Mavridis, and D. Gritzalis, "Access control issues in utilizing fog computing for transport infrastructure," in *Critical Information Infrastructures Security*, E. Rome, M. Theocharidou, and S. Wolthusen, Eds., vol. 9578, pp. 15–26, Springer International Publishing, Berlin, Germany, 2016.

[93] P. Rosenberger and D. Gerhard, "Context-awareness in industrial applications: definition, classification and use case," *Procedia CIRP*, vol. 72, pp. 1172–1177, 2018.

[94] W. R. Simpson and K. E. Foltz, "Maintaining zero trust with federation," *International Journal of Emerging Technology and Advanced Engineering*, vol. 11, no. 5, pp. 17–32, 2021.

[95] K. Olson and E. Keller, "Federating trust: network orchestration for cross-boundary zero trust," in *Proceedings of the SIGCOMM'21 Poster and Demo Sessions*, pp. 48-49, New York, NY, USA, August 2021.

[96] M. Ahmed and K. Petrova, "A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-Based Computing Environments," in *Proceedings of the WISP 2020*, Austin TX, September 2020.

[97] T. M. S. do Amaral and J. J. C. Gondim, "Integrating Zero Trust in the Cyber Supply Chain Security," in *Proceedings of the 2021 Workshop on Communication Networks and Power Systems (WCNPS)*, pp. 1–6, Brasilia, Brazil, November 2021.

[98] Z. A. Collier and J. Sarkis, "The zero trust supply chain: managing supply chain risk in the absence of trust," *International Journal of Production Research*, vol. 59, no. 11, pp. 3430–3445, 2021.

[99] Tutorial, *A Beginner's Guide to XACML (Part 2) Getting Started with ALFA*, Axiomatics, 2021, https://www.axiomatics.com/resources/tutorial-a-beginers-guide-to-xacml-part-2-getting-started-with-alfa/.

[100] P. Cingolani and J. Alcalá-Fdez, "jFuzzyLogic: a java library to design fuzzy logic controllers according to the standard for fuzzy control programming," *International Journal of Computational Intelligence Systems*, vol. 6, no. 1, p. 61, 2013.

[101] E. Bertino, "Zero trust architecture: does it help?" *IEEE Security & Privacy*, vol. 19, no. 5, pp. 95-96, 2021.

[102] A. A. Jabal, E. Bertino, J. Lobo, D. Verma, S. Calo, and A. Russo, *FLAP - A Federated Learning Framework for Attribute-Based Access Control Policies*, 2020, https://arxiv.org/abs/2010.09767.

[103] W. Lei, H. Wen, J. Wu, and W. Hou, "MADDPG-based security situational awareness for smart grid with intelligent edge," *Applied Sciences*, vol. 11, no. 7, p. 3101, 2021.

[104] R. Atat, "Enabling Cyber-Physical Communication in 5G Cellular Networks: Challenges, Solutions and Applications," *Internet of Things, Cyber-Physical Systems*, vol. 2, 2017 https://kuscholarworks.ku.edu/handle/1808/25917.

[105] "Predict Cyber-attacks via digital twins," 2022, https://cybersecurity.att.com/blogs/security-essentials/predict-cyber-attacks-via-digital-twins.