Achieving Security Scalability and Flexibility using Fog-Based Context-Aware Access Control

A. S. M. Kayes[a,*], Wenny Rahayu[a], Paul Watters[a], Mamoun Alazab[b], Tharam Dillon[a], and Elizabeth Chang[c]

[a] *La Trobe University, Melbourne, Australia*

[a] *Charles Darwin University, Australia*

[c] *University of New South Wales, Canberra, Australia*

Abstract

In the cyberspace environment, access control is one of the foremost fundamental safeguards used to prevent unauthorized access and to minimize the impact from security breaches. Fog computing preserves many benefits for the integration of both internet of things (IoT) and cloud computing platforms. Security in Fog computing environment remains a significant concern among practitioners from academia and industry. The current existing access control models, like the traditional Context-Aware Access Control (CAAC), are limited to access data from centralized sources, and not robust due to lack of semantics and cloud-based service. This major concern has not been addressed in the literature, also literature still lacks a practical solution to control fog data view from multiple sources.

This paper critically reviews and investigates the limitations of current fog-based access control. It considers the trade-off between latency and processing overheads which has not been thoroughly studied before. In this paper, a new generation of Fog-Based Context-Aware Access Control (FB-CAAC) framework is proposed to enable flexible access control data from multiple sources. To fill the gap in the literature this paper introduces i) a general data model and its associated mapping model to collate data from multiple sources. ii) a data view model to provide an integrated result to the users, dealing with the privacy requirements of the associated stakeholders, iii) a unified set of CAAC policies

with an access controller to reduce both administrative and processing overheads, and iv) a data ontology to represent the common classes in the relevant data sets. The applicability of FB-CAAC proposal is demonstrated via a walk-through of the entire mechanism along with several case studies and a prototype testing. The results show the efficiency, flexibility, effectiveness, and practicality of FB-CAAC for data access control in fog computing environment.
Keywords:

Access Control, Fog Computing, Cloud Computing, Security, Privacy, Cybercrime, Internet of Things

---

1. Introduction

Accessing data from multiple sources has increasingly become challenging due to the heterogeneous nature of data sources. It is particularly important from the viewpoint of selecting required data and information obtained from multiple sources and providing an integrated data view through information fusion (e.g., by considering who can access what data under what conditions). This is the case, for instance, in healthcare and defence applications where experts only want to share parts of the clients' records they have (such as, the patients' health records), which are usually associated with different data sources in today's interconnected environments. In the context of information fusion, the main question involves *how to acquire required data and information resources by incorporating multiple data sources.*

As a result, efficiently controlling the users' access to such data from multiple sources is one of the main challenges. How to provide integrated results to the users by maintaining privacy of client's records is another key challenge. In addition, controlling performance overheads and subsequent administrative costs is another associated challenge. Such new challenges require a new form of policy-based access control solution with the potential to include on-the-fly data integration in order to deliver an integrated data view to the users. The access

control decisions should be restricted to different granularity levels according to the relevant contextual conditions. For example, a data analyst's request to access and analyze the data about driving license holders (like the date-of-birth and address of the drivers) may be allowed from the inside of the office during his duty time, whereas a data scientist may access and use such records for research purposes in different contexts. However, they should not access/reveal the identity information of such clients. The main question revolves *how to protect all directly identifiable information of clients while data is coming from different sources*

A preliminary version of this paper appears as "Accessing data from multiple sources through context-aware access control". It has been published in the Proceedings of the 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2018) [1].

1.1. Background

Among the different access control models available in the literature, Role-Based Access Control (RBAC) [2] is a representative and reliable security model for many practical applications to protect data and information resources [3]. In accordance with the embodiments of the user-role and role-permission mappings, the traditional RBAC model [2] and spatial and temporal RBAC models (e.g., [4]) have been widely accepted by different scientific communities due to their flexibility and simplicity in administration when faced with a large number of users and large amount of data. Considering a wide range of relevant context information [5] explicitly for access control is another key research direction, mainly exploiting the context-aware policy models to prevent unauthorized access of such data and information resources. Thus, Context-Aware role-based Access Control (CAAC) models (e.g., [6], [7]) have been introduced over the last few years, incorporating the dynamically changing contextual conditions into the RBAC policies. These context-dependent models are mostly domain-specific and consider specific types of context information [1] [8].

Looking at the existing context-sensitive access control models, these solu-

tions extensively have been used to access data and information resources from centralized sources [9]. These models do not provide adequate functionality to access different data sets from multiple environments, by utilizing a single set of access control policies. Different data integration techniques have been developed over the last few decades to collate data from multiple sources, such as schema matching [10]. These integration techniques mostly have been used to map between original sources of data (i.e., different schemas) and result in a global schema. However, these techniques are still limited in order to provide the "granted" or "denied" access control decision to the users, supporting a single set of access control policies to overcome overhead issues. In this article, we utilize a global schema (i.e., a data model along with general and equivalent concepts) and apply a single set of policies to access data from multiple sources, instead of different sets of access control policies. Based on our experimental study, what we observe that the performance overhead dramatically increases due to the large number of policies and the reasoning task behind the data access query.

Due to the technological advancements in the online environment, currently, different stakeholders need to access data from many distributed sources. For example, the current cloud-based Internet of things (IoTs) paradigm [11] seeks a new form of context-sensitive access control model for building mechanisms of controlling data and information resources from multiple Big Data sources. The integration of such data directly from distributed sources raises semantic namespace and latency problems [12] due to lack of semantics and cloud-based services. The richer semantic of data model is needed to resolve the semantic namespace problem, dealing with the heterogeneous nature of such big data sets [13]. However, the latter is forcing the organizations to overcome the latency issue by adding intermediary computational nodes at the edges of the networks [14]. In recent years, fog computing models have been introduced to reduce the latency and processing overheads involved in managing and accessing cloud-based data and services (e.g., [15]). These fog nodes usually provide intermediary computation and networking services between the end-users and

the data servers. Over the last few years, several fog-based access control models have been proposed (e.g., [16], [17]) in the literature.These fog-based access control models are developed to access data and information resources from centralized environments. However, they are not truly context-aware and robust enough to develop CAAC mechanisms for accessing data from different sources and consequently providing integrated results to the users.

1.2. Research Issues

From our analysis of the literature and based on the identified characteristics of data sources, there is still a gap relating to the data access from multiple environments. Such a gap raises the following research problems (RP1 to RP4).

(RP1) *How to effectively model access control policies to access data from multiple sources by means of reducing performance overheads and administrative costs?* Thus, there is a need to specify a single and unified set of policies instead of multiple sets of policies.

(RP2) *How to define a unified data model to support accessing different data sets from multiple sources?* Usually, different organizations have their own local schemas with different data structures. There is a need to define a generic/global schema for all data sources, considering the identical attributes of the similar data objects.

(RP3) *How to map these access control policies to multiple data sources?* There is a need to codify the mapping rules in terms of correlating different data sources.

(RP4) *How to create an integrated view of data from multiple sources by maintaining privacy requirements (i.e., privacy preservation) of the stakeholders?* There is a need to model privacy control policies and preserve private and sensitive information of the clients.

1.3. The Contributions and Extensions

Our aim in this research is to introduce a new generation of *Fog-Based Context-Aware Access Control (FB-CAAC)* framework, combining the benefits of edge computing, context-sensitive access control and traditional data integration solutions, in terms of defining a unified global data model and its associated data view model to facilitate access control to necessary data from multiple data sources. Based on the identified research issues (RP1 to RP3), in our earlier research [1] we have proposed a CAAC model, which will be the base model of our FB-CAAC framework. It can provide an ideal platform to support a new direction of context-sensitive access control solution. However, one of the important research issues (RP4) was not covered in the earlier proposal. We believe that a full-fledged FB-CAAC framework based on RBAC may have a great potential because it could be easily deployed in the cloud or at the edges of the networks, and may allow users to access data from multiple sources with preserving personally identifiable information. This article consolidates and extends our core FB-CAAC. Major contributions of this article are as follows.

1. We have now extended the application scenario, mainly including the associated requirements for providing an integrated data view to the authorized users, whereas our earlier paper [1] lacks the detailed analysis and the relevant data view requirements for developing context-sensitive access control to necessary data from multiple sources (see Section 2).

2. For the theoretical formulation of the unified data model, we have now extended our initial model, including an integrated data view model and its associated privacy model. In particular, we have now incorporated a new set of privacy policies into our initial policy model (see Section 3).

3. We have made a significant extension to our ontology-based approach, including a new privacy control policy ontology in order to facilitate privacy by preserving confidential/sensitive information, using ontology languages OWL, DL and SWRL. In particular, we have included separate

ontologies for data model, access control policy model and the associated mapping and privacy control policy models (see Section 4). Whereas, the context-sensitive access control model proposed earlier [1] lacks a complete representation of the ontologies (upper and domain-specific).

4. We have now introduced the detailed implementation of the components of the software prototype, including the practical assessment of our proposed framework through an empirical evaluation in a real laboratory setup with respect to our initial framework [1]. In particular, we have now included a set of privacy control policies and evaluated our proposed framework accordingly. Whereas, in our previous framework, the evaluation only has been conducted considering a unified set of policies to access data from different sources. We have also demonstrated our framework through several case studies, including a new application scenario where the relevant users (e.g., data analyst and scientist) should have controlled access (particularly, an integrated view by ensuring privacy preservation) to necessary data from multiple sources (see Section 5).

5. We have now provided relevant research directions for future scholars according to our findings in this work (see Section 7). In addition, we have now presented a comparative analysis of the existing context-aware access control approaches. We have also included the privacy-preserving access control approaches. The comparative assessment has shown that our FB-CAAC approach offers a range of new benefits for context-sensitive access control in the cloud and edge computing environments, collecting data from multiple sources and ensuring privacy.

1.4. Organization of Paper

We present a *data access scenario* to motivate our research in Section 2. We propose a *formal approach to a general data model* with the aim of accessing different data sets from multiple sources in Section 3. Particularly, we introduce a unified data model and its associated mapping model to collate data from

different sources. We also introduce a set of fog-based access and privacy control policies to access required data coming from such multiple sources. In Section 4, we introduce a *unified data ontology* to represent the common classes in the relevant data sets and a *mapping ontology* to correlate these common classes with other equivalent classes. In this perspective, the proposed ontology-based approach performs schema mapping and correlates the multiple data sources accordingly. In Section 4, we also propose a *policy ontology* to provide access control decisions to the users, specifying a unified set of context-sensitive access control policies for all the different data sources and providing an integrated data view to the users. We evaluate our proposed approach by demonstrating a *walkthrough of our entire mechanism* via several case studies and a *prototype testing* through healthcare scenarios (see Section 5). Section 5 also demonstrates the practicality of our approach through an empirical evaluation with respect to our initial context-sensitive access control approaches. Section 6 briefly discusses the related work and presents a comparative analysis of our approach with respect to existing CAAC approaches. Finally, the conclusion and a roadmap for future research are presented in Section 7.

2. Research Motivation and Requirements

A large number of data has been produced as a result of the abundance of Big Data sources about business and government services, their environments, and their end-users. Such data collection might be coming from centralized and/or distributed environments. This data abundance creates new opportunities and also raises new challenges to develop new form of access control mechanisms along with data integration capabilities. In the following, we consider an application scenario for our road traffic project, which illustrates an access control to multiple data sources for different types of users within the distributed system. One of the specific aims of this project is to explore how Australian business and government can better enable and use the infrastructure of transport logistics data in order to more effectively and efficiently access them from multiple

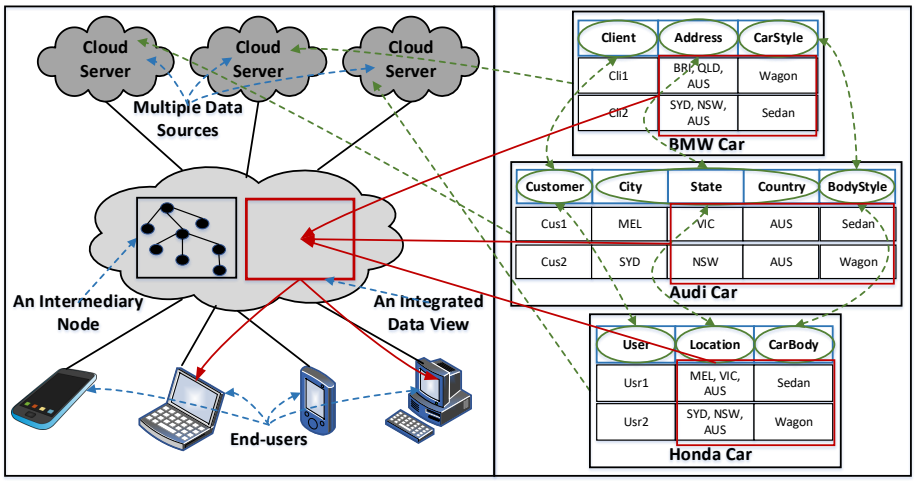

Figure 1: The Relationship Chain from End-users to Multiple Data Sources (left) and Three Car Databases (right)

environments.

2.1. Motivating Scenario

We consider the following application scenario: *John, who is a data analyst, is currently working with the Australian department of transport. His role is to deliver high quality services to record and visualize data usage statistics based on the data from different sources. On the other hand, Richard, who is a data scientist, is working with the same department. His role is to further analyze these statistics to assist law enforcement and government policies through high-quality data analysis, using creative design and advanced statistical analytics on the resulting data sets. Currently, they both are assigned to the transport logistics project in a team to analyze the data on sedan cars (including the car owners' insurance data) from all around Australia.*

In this application scenario, John and Richard both need to access different types of car records (e.g., data about cars, car registrations, driving license owners and their insurance policies). However, they should maintain the security and privacy requirements of different stakeholders. For example, a data analyst only can access data about driving license owners' from his office location and

during his working hours. Also, he only can see and visualize the statistical results, but not the detailed records. On the other hand, a data scientist can see such records from anywhere at anytime, even when he is on the move. In addition, he can access the detailed car data from recorded car details (such as the date-of-birth and address of the drivers) for research purposes. Based on the analysis of the scenario, one thing is common here, the requesters (John and Richard) need to access data from multiple sources in different contexts. That is, such data might be associated with centralized or distributed environments. Also, the requesters need to deal with multiple data sets within different organizations (e.g., BMW, Audi and Honda companies). We can make two possible observations to facilitate context-sensitive access control to such data sets from distributed sources.

1. ***Build a generic data model and specify a single set of policies subsequently to access data from multiple sources by utilizing mapping of generic schema to local schemas:*** In order to access data from multiple sources, we can build a unified data model to specify generic concepts and map all the local data schemas to the generic unified schema. Using this data model, we can introduce a policy model by taking into account a single set of data access policies for accessing data from distributed sources. In this fashion, we can reduce the number of access control policies, which in turn reduces the processing overheads (i.e., the time taken to process users' data access request), as well as administrative overheads (i.e., the time taken to specify access control policies). In addition, we need to build a data view model to provide an integrated result to the end-users. Accordingly, we can specify privacy control policies towards data confidentiality. Our proposed data model and ontology can be found in Sections 3 and 4.

2. ***Specify different sets of policies or use existing policies to access data from multiple sources:*** As an alternative to building a generic data model and specifying a single set of policies accordingly, we can use

different sets of policies individually to access data from multiple sources. In today's dynamic environments, this is really a big challenge to statically model different sets of access control policies according to the local data sources. On the one hand, it may impose extra burdens to policy administrators' to specify and manage such polices by means of multiple data sources. On the other hand, the number of policies involved in multiple data sources might potentially be quite large. However, in order to reduce the processing overheads for an access control system, we should avoid an excessive amount of access control policies [5]. The specification of a unified set of access control policies for this work can be found in Sections 3 and 4.3.

2.2. General Requirements

In the light of Observation 1, we illustrate the relationship chain among requesters (end-users), multiple data sources and an intermediary computational node, which is shown in the left part of Figure 1. Concerning the application scenario, different car companies such as BMW, Audi and Honda have their own data schemas. For instance, An ontological approach has been used to extract BMW, Ford, Audi and Honda car data from source records into a target data schema [18]. Three snapshots of raw data from the car databases are shown in the right part of Figure 1. The relationship chain in Figure 1 mainly outlines the mapping between different end-users and multiple data sources. In order to support such mapping to different car databases and access data subsequently, there is a need for a context-sensitive access control application such as the Transport Logistics Information system (TLIS) [19]. In particular, an intermediary computational node is required to facilitate access control to the multiple car databases in such a TLIS application. In this paper, we only consider the homogeneous data from multiple sources. The term homogeneous is used to describe different databases which have similar kind of field names and types across data sources, but not the same. We propose that future research should continue experimenting with the proposed data and access control policy

models, ideally with larger sample of policies and heterogeneous selections of data from different data stores including IoT devices, exploring the full potential and additional applications of the findings presented here.

We model a single set of policies to access necessary data from multiple sources based on the relevant contextual conditions. The intermediary computational node in Figure 1 can enable a data view for the users according to the data sets that are coming from multiple sources. In particular, the node can serve as a centralized index by which the authorized users can access all distributed data from its connected data sets as a single view [20].

Concerning the scenario in Figure 1, there is a need to integrate data from multiple data sources. For example, in our application scenario, John (who is a data analyst) can access clients' addresses and locations from the BMW data source. Let us consider he has also right to access the relevant insurance information of the clients from other data sources. However, he should not have an integrated and single view of address, date-of-birth, location and insurance information so that the clients can not be identified. In such a case, he might share their financial data to any unauthorized parties. This is really a privacy issue. As such, in the integrated data view, we have to take into account the relevant privacy requirements of the associated stakeholders.

Many organizations have been seeking a proper solution to access data from multiple sources and consequently maintain the associated privacy and security requirements. For example, in our application scenario, different users need to access car records that may come from many internal and external databases. There is a need for semantic interoperability among different data sources in order to integrate such car records. These data have to evolve due to the changing nature of the requirements and thus richer semantics of data are needed through schema mapping and integration. In particular, the constitution of the coherent data sets obtained from multiple data sources dealing with such an interoperability issue is a grand challenge that traditional access control solutions and measures cannot meet the requirements identified above. Our aim in this research is to build a new fog-based context-sensitive access control

solution for data and information resources coming from multiple data sources.

Overall the key requirements for the fog-based CAAC framework can be listed as follows: (i) a General Data Model to codify the characteristics of data from multiple sources as a global schema, (ii) a Mapping Model to highlight the relationship between the local schemas of multiple data sources, (iii) a Data View Model in collating data from multiple sources, and (iv) a Unified Policy Model towards considering the efficiency, flexibility and effectiveness of the new fog-based CAAC framework. Recently, the view-based data integration is widely used in data warehouse and enterprise-based application integration research. Other fog-based requirements such as (v) multi-tenancy fog devices to execute applications in isolation and (vi) policies for fog-based service orchestration and management may be considered, in order to further explore the performance and optimization problems.

3. Formal Approach to Data View

In this section, we provide some preliminary definitions with the purpose to illustrate our proposed solution approach. In addition, we show the related examples from the application scenario.

Definition 1. ***Unified Data Model.*** *A unified data model (UDM) is represented as a 2-tuple relation, including base and equivalent concepts. UDM also includes the associations involving these concepts, what we call relationships.*

$$UDM \ = \ \langle BC, \ RE, \ EC \rangle \tag{1}$$

In our ontology, the base and equivalent concepts are represented by *classes* and *subclasses*, and the *object properties* are used to represent the associations or relationships between the base and equivalent concepts.

$$\begin{aligned} BC \ &= \ \{(bc_1, bc_2, ..., bc_i) | bc \in BC\} \\ EC \ &= \ \{(ec_1, ec_2, ..., ec_j) | ec \in EC\} \\ RE \ &= \ \{(re_1, re_2, ..., re_k) | re \in RE\} \end{aligned} \tag{2}$$

Thus, two sets of concepts (BC and EC) and a set of relationships (RE) form our UDM data model.

In the above relations 1 and 2, we use

- $bc \in BC$ to represent a base concept,
- $ec \in EC$ to represent an equivalent concept, and
- $re \in RE$ to represent a relationship between bc and ec.

Example 1. *Looking at our application scenario, Customer (see the Audi car records in Figure 1) is a base concept that is equivalent to the concept of Client (see the BMW car records in Figure 1) and an association, named equivalentTo, is used to represent the relationship between them. In the next section, Figure 2 shows such relationships.*

Definition 2. ***Policy Model.*** *A policy model (Policy) is represented as a 4-tuple relation, including the following components: requesters, roles, contexts and permissions.*

$$Policy \ = \ \langle Req, \ R, \ CC, \ P \rangle \tag{3}$$

In the above relation 3,

- Req represents a set of requesters ($req \in Req$),
- R represents a set of roles ($r \in R$),
- CC represents a set of contexts or contextual conditions ($cc \in CC$), and
- P represents a set of permissions ($p \in P$).

Similar to the basic RBAC model [2], in our policy model, a user can be assigned to a role under relevant policy constraints (e.g., the static conditions such as user's credentials), however the user needs to satisfy the necessary contextual conditions (e.g., the dynamic temporal and spatial conditions) [5]. Consequently, the user can access the necessary data from different sources (e.g., multiple databases, data clouds).

In our policy model, a permission is a set of 2-tuple relation on the base concepts with different operations.

$$Permission \subseteq BaseConcept \times Operation \tag{4}$$

Our policy model is based on the notions of different components and the associations that are included in the base concepts. In the following, we specify the mapping rules that are used to correlate these base concepts with other equivalent concepts with the aim of accessing data from multiple sources through a unified set of context-sensitive access control policies.

Definition 3. ***Mapping Rule.*** *A mapping rule is represented as a one-to-one or one-to-many relationship between the base and equivalent concepts.*

$$BC \equiv EC \tag{5}$$

An equivalent concept is either a single concept or can be formed based on the multiple concepts. Let us consider another set of concepts C ($c \in C$), each equivalent concept $ec \in EC$ is represented by the following relations.

$$\begin{aligned} C &= \{(c_1, c_2, ..., c_x) | c \in C\} \\ EC &= \{(..., (c_1), (c_2), (c_1 \wedge c_2), (c_1 \wedge c_2 \wedge c_3), ...) | \\ &\qquad ec \in EC \ \& \ c \in C\} \end{aligned} \tag{6}$$

In the above relations 5 and 6, we use

- $c \in C$ to represent a concept, and
- $ec \in EC$ to represent an equivalent concept.

Example 2. *Looking at the application scenario, the combination of three concepts* ***City****,* ***State*** *and* ***Country*** *in the Audi car data snapshot is equivalent to the concept of* ***Address*** *in the BMW car data snapshot. Also, the concept* ***User*** *is equivalent to the concept of* ***Customer****. These examples are represented in the following relations.*

$$\begin{aligned} Address &\equiv City \wedge State \wedge Country \\ Customer &\equiv User \end{aligned} \tag{7}$$

For simplicity, we have used Address = {City, State, Country}, instead of Address $\equiv$ City $\wedge$ State $\wedge$ Country in our UDM ontology (see Section 4).

Definition 4. ***Integrated View Model.*** *An integrated view model is represented as a number of data records coming from different sources.*

$$V = \bigcup_{s=1}^{n} R_s \tag{8}$$

In the above relation 8, we use

- V to represent an integrated data view,
- R to represent a number of data records from multiple sources, and
- s to represent the number of data sources.

A subsequent privacy model that is associated with an integrated view of data can be defined as follows.

Definition 5. ***Privacy Model.*** *A privacy model (Privacy) is represented as to preserve clients' confidential and sensitive records from different data sources when dealing with an integrated data view model from such sources.*

$$Privacy = \bigcup_{i=1}^{n} PA_i \tag{9}$$

In the above relation 9, we use

- PA to represent the data attributes that cannot be revealed individually or together with other attributes (privacy attributes), and
- n to represent the number of different combinations of data attributes.

Actually, these privacy attributes 'PA' are the identifiers of the clients that should not be revealed as a single and integrated data view to the users. A set of privacy control policies are being specified based on the requirements

(e.g., considering the relevant data attributes that should not be revealed with a single and integrated data view) from relevant domain experts [21] (see our ontology-based approach in Section 4).

These policies are specified for expressing privacy in the context of data rules, based on the privacy attributes from the domain experts (i.e., following the standards for privacy of individually identifiable health information [21] [22]. For example, the date-of-birth (DOB) and zip code of any individual client are both individually safe for release, but these are together are not safe for release. However, if there is only one client in the database with this combination or any other combinations that are not safe to release, we can incorporate k-anonymity mechanism [23] in our proposed access control framework.

Example 3. *Concerning our application scenario, a requester/user can access car and insurance records of a single client from multiple data sources, however the user should not be allowed to access the sensitive information so that a client can be identified. In this application scenario, a user should not have a single and integrated view of the address and/or date-of-birth (DOB) of the clients. This is potentially a privacy issue when these records from different sources are pooled into an integrated and single view. A client can be potentially identified using the records of address and/or DOB.*

$$PA \cup \{Address, DOB\} \tag{10}$$

4. FB-CAAC Ontologies

In this section, we introduce our ontology-based approach, including a *unified data ontology*, a *mapping ontology* and the associated *access and privacy control policy ontologies*. We first introduce a unified data ontology (UDM ontology) where we model the concepts and associations with respect to the multiple data sources. It has mainly two layers.

- The upper layer contains the general ontology that includes the core concepts or classes and the relationships among classes.

- The bottom layer contains the specialization ontology that includes the domain-specific classes and relationships.

The object properties are used to represent the associations (i.e., logical relationships) between these concepts. We also introduce a mapping ontology, including the reasoning rules to correlate different data sources. The associated access and privacy control policy ontologies are also introduced to facilitate necessary data access and subsequently provides an integrated view to the users.

Different modeling languages have been used in the literature to represent the concepts and the logical associations between concepts within different domains. The expressiveness and conceptual structure of the Web Ontology Language (OWL) [24] are very suitable for modeling information in accordance with different direct and RDF-based semantics [25]. The formal semantics of Description Logics (DL) [26] are embraced by the modeling constructs of OWL because of the knowledge representation schema that underlies the DL syntax. As such, we use the OWL language to model the UDM concepts and associations, and we use the DL grammar to specify the mapping rules and incorporate them into the UDM data ontology. We use the Protégé-OWL graphical API [27] to implement the data, mapping and different policy ontologies. The DL semantics are not always sufficient to specify the reasoning rules for inferring high-level implicit semantics [5]. In such cases, we use the SWRL language [28] and its built-in functions [29] to specify the reasoning rules (e.g., access and privacy control policy rules, mapping rules) for making context-sensitive access control decisions through such policies.

4.1. UDM Data Ontology

Concerning our TLIS application, let us consider three car databases that have already been shown in Figure 1. Based on the TLIS application, a two-layered ontology, named *Unified Data Model (UDM)*, is represented in Figure 2. The UDM data ontology illustrates the main constructs, where we model the general core classes, domain-specific classes, and the logical relationships among

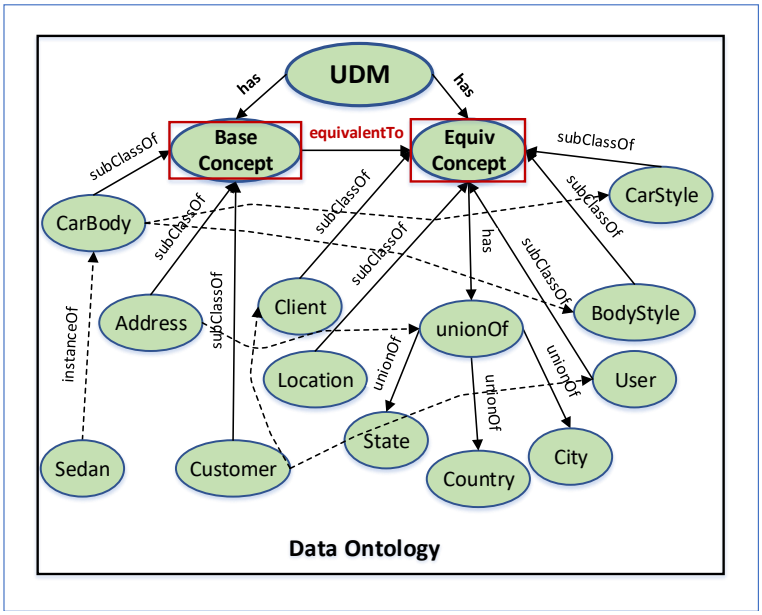

Figure 2: UDM Data Ontology for Mapping Base to Equivalent Concepts

them. The ontology has two core classes *BaseConcept* and *EquivConcept* which are organized into a hierarchy, named *UDM*. In this ontology, the logical associations between different classes are usually represented by is-a (*subClassOf*), union (*unionOf*) and equivalence (*equivalentTo*) relationships.

For example, the classes *BaseConcept* and *EquivConcept* are linked by an arrow with a label *equivalentTo*. The UDM model shown in Figure 2 defines that the class *Location* is equivalent to the class *Address* and the *CarStyle* class is equivalent to the *CarBody* class. In the UDM ontology, the classes *Customer*, *Location* and *CarBody* are the three domain-specific concepts and they are the sub classes of the core class *BaseConcept*, which are represented by *subClassOf* relationships. In Figure 2, an individual named *Sedan* car is represented as an instance of the class *CarBody*, which is represented by a dashed arrow labelled *instanceOf*. Accordingly, we show all the logical associations (object properties) between concepts for our TLIS application.

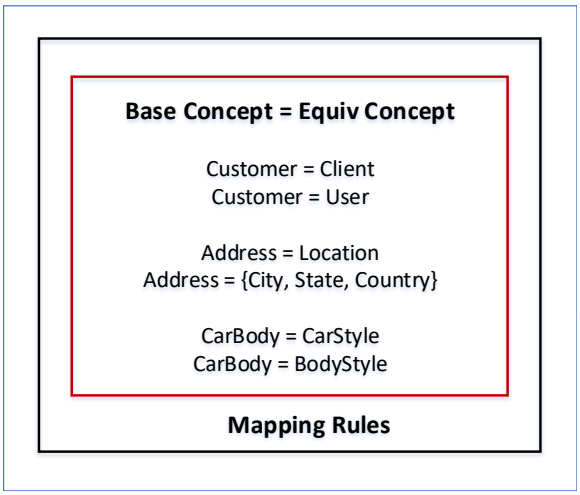

Figure 3: An Excerpt of the Mapping Rules for Collating Data from Multiple Sources

4.2. Mapping Ontology

We incorporate the mapping rules into our ontology-based approach. The mapping rules are specified to correlate data sources, and to model and apply a unified set of access control policies for accessing data from multiple sources reducing the administrative costs and processing overheads.

For our TLIS application, we illustrate the domain-specific mapping rules in Figure 3. For example, the concepts *BodyStyle* and *CarBody* are two equivalent concepts of the base concept *CarBody*, which are specified using two mapping rules. As we consider multiple data sources, there are some equivalent concepts which are formed based on the other different concepts. For example, another mapping rule specifies the combination of *City*, *State* and *Country* concepts is equivalent to the *Address* concept.

4.3. Access Control Policy Ontology

A policy-driven data access model, simply policy ontology, has been introduced to access data from multiple sources. In particular, we specify a unified set of context-sensitive access control policies. In this research, we mainly focus on policy-driven data access from multiple homogeneous sources. Different pol-

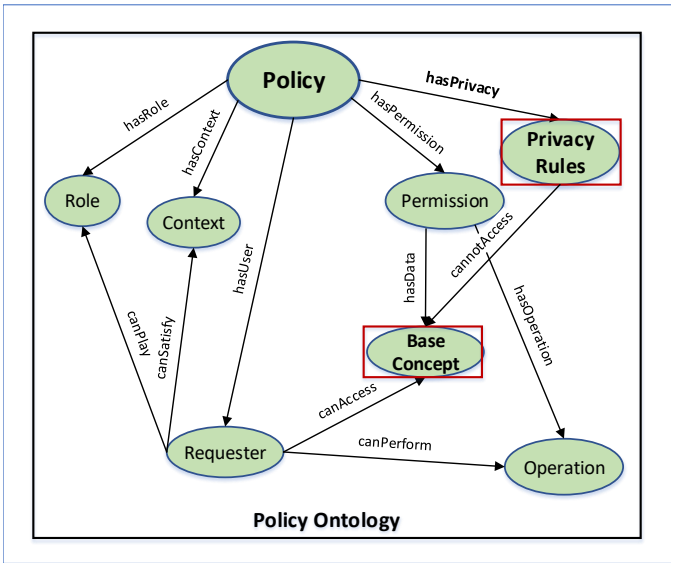

Figure 4: The Main Concepts of the Policy Ontology to Facilitate a Single Data View to the User

icy languages have been proposed in the literature. In this paper, we provide a guideline in which a unified set of access control policies can be applied to multiple data sources. As such, the basic elements of our policy model have been represented in Figure 4.

The following core concepts are organized in a *Policy* hierarchy into the ontology: *Requester*, *Role*, *Context*, *Permission*, *Operation*, *PrivacyRules* and *BaseConcept*. An access control policy can be read as follows: "*a user, who is the requester, by playing an appropriate role and under satisfying the necessary contextual conditions, can access data from multiple sources*". A privacy control policy can be read as follows: "*a user, who is the requester, by playing an appropriate role, cannot access data which includes personal identifiable information*". More details about privacy control policies can be found in the next section (see Section 4.4). Our access and privacy control policies are specified and applied to the base concepts. The mapping rules in Figure 4 are used to associate these base concepts with equivalent concepts.

4.4. Privacy Control Policy Ontology

Similar to access control policies for collating data from multiple sources, we incorporate the privacy control policies into our ontology-based approach. The privacy ontology safeguards clients' sensitive records that are obtained from different data sources when building an integrated view for the users.

The relevant classes for specifying privacy-control policies are already specified in our policy ontology in Figure 4. The following code fragment in OWL shows the definition of such classes: *Policy*, *PrivacyRules* and *BaseConcept* (see Definition 6). The object properties '*hasPrivacy*' and '*cannotAccess*' are used to express the relationships between these classes.

Definition 6. *(Definitions of Main Classes for Specifying Privacy Rules).*

<owl:Class rdf:ID="Policy">
<owl:Class rdf:ID="PrivacyRules">
<owl:Class rdf:ID="BaseConcept">

Definition 7 shows the class *Policy* has an object property '*hasPrivacy*', which is used to link the classes *Policy* and *PrivacyRules*.

Definition 7. *('hasPrivacy' Object Property Definition).*

<owl:ObjectProperty rdf:ID="hasPrivacy">
<rdfs:domain rdf:resource="#Policy"/>
<rdfs:range rdf:resource="#PrivacyRules"/>
</owl:ObjectProperty>

Similar to Definition 7, we define another object property '*cannotAccess*' to link the classes *PrivacyRules* and *BaseConcept* (see Definition 8).

Definition 8. *('cannotAccess' Object Property Definition).*

<owl:ObjectProperty rdf:ID="cannotAccess">
<rdfs:domain rdf:resource="#PrivacyRules"/>

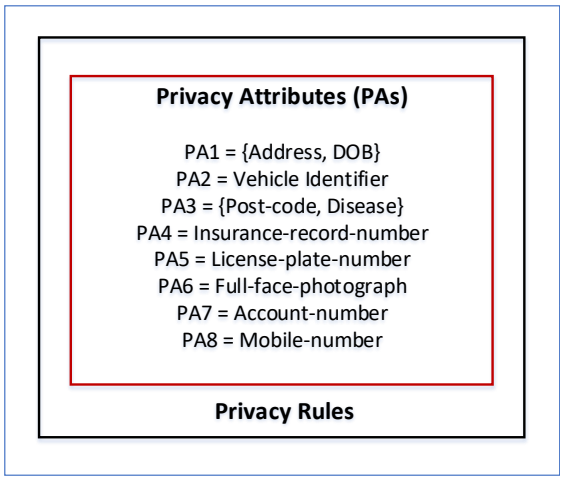

Figure 5: An Excerpt of the Privacy Rules to Facilitate Privacy Preservation of the Client

Table 1: The Privacy Control Policy for a Data Analyst

1	<**Policy** rdf:ID="$policy_1$">
2	<hasUser rdf:resource="#Requester_req"/>
3	<hasRole rdf:resource="#Role_$dataAnalyst$"/>
4	<hasPermission rdf:resource="#Permission_p_1"/>
5	<hasData rdf:resource="#BaseConcept_p_1_$Address$"/>
6	<hasData rdf:resource="#BaseConcept_p_1_DOB"/>
7	<hasOperation rdf:resource="#Operation_p_1_$read$"/>
8	<hasPrivacy rdf:resource="#PrivacyRules_$privacyAttributes_1$"/>
9	<cannotAccess rdf:resource="#$req\_dataAnalyst\_p_1$"/>
10	</**Policy**>

<rdfs:range rdf:resource="#BaseConcept"/>
</owl:ObjectProperty>

For our TLIS application, we illustrate the domain-specific privacy control rules in Figure 5. These privacy rules contain the information pertaining to the sensitive records to protect individually identifiable information. These rules are

specified according to the privacy attributes from the domain experts, based on the standards for privacy of individually identifiable health information [21]. For example, a data analyst would not have access to a single view of the address and/or date-of-birth (DOB) of any individual client, which is specified as first privacy rule in Figure 5. This is potentially a violation of privacy as the client can be individually identified based on such records. Table 1 specifies a privacy control policy for such a data analyst. Similar to mapping rules, an excerpt of the privacy attributes for the TLIS application has been specified in Figure 5.

Overall, this article presents a new context-sensitive access control framework which comprises of two main contributions. One of the main contributions of our proposal is its ability to model and apply a unified set of context-sensitive access control policies for accessing data from multiple sources targeting low processing and administrative overheads. Another subsequent contribution is to provide a data view to the users that includes necessary data from different sources, without including the possible combinations of sensitive records that may lead to a violation of privacy. Towards assessing the practicality of our proposed framework, we conduct several sets of experiments and demonstrate a software prototype through several case studies in the next section.

5. Evaluation of Our FB-CAAC Approach

In this section, we demonstrate the applicability of our CAAC approach. We first provide a walkthrough of our entire CAAC mechanism via several case studies. We then demonstrate a prototype implementation and its associated application scenarios from the healthcare domain. In addition, we conduct several sets of experiments to evaluate our current proposal with respect to the context-sensitive access control model proposed earlier, which only covers data access from multiple sources [1].

5.1. Walkthrough of Our Proposal

We analyse the access requests from different users and the subsequent results with necessary data in the laboratory setups. The purpose of these case

studies is to demonstrate the practical applicability of our proposed Fog-Based Context-Aware Access Control (FB-CAAC) approach.

When a data access request arrives from a user (requester), it includes the user-role and role-permission (data access permission) assignments based on our UDM ontology and its associated policy ontologies. In particular, the applicable policies include the access control rules in that different users can facilitate access to relevant data. In addition, the policy ontologies also include the privacy control rules containing the sensitive information (i.e., privacy attributes) that the users cannot access. In the following case studies, we consider the dynamically changing context information, such as request times (e.g., John's data access request is within his duty time or not), locations (e.g., John is located in his office or not), inter-personal relationships between different persons (e.g., Jane is a treating doctor of the patient Bob or not), health conditions (e.g., Bob's current health status is highly critical, critical or normal), and co-located relationships (e.g., Jane and Bob are located in the emergency department of the hospital or not), as contextual conditions.

5.1.1. Revisiting Our Application Case Study

Consider our application scenario where Richard wants to access different car owners' records from multiple sources. Table 2 shows the specification of such data scientists' policy in OWL and Table 3 shows the relevant reasoning rule in SWRL for making context-sensitive access control decision through the applicable policies.

In this policy (see Table 2), the access control decision is based on the following constraints: *who the requester is* (which is specified in *Line# 2*), *what role the requester can play* (*Line# 3*), *under what contextual conditions* (*Line# 4 and 5*) and *what resource is being requested* (*Line# 6 to 8*). For simplicity, we do not include the data type properties in Table 2. Looking at the scenario, we can observe that Richard, who is a data scientist, can access different types of car records from multiple sources. Table 3 specifies a reasoning rule to access the records of different car addresses. Richard can access such records from

Table 2: The Data Scientists' Policy

1	<**Policy** rdf:ID="$policy_2$">
2	<hasUser rdf:resource="#Requester_req"/>
3	<hasRole rdf:resource="#Role_$dataScientist$"/>
4	<hasContext rdf:resource="#Context_$anyLocation$"/>
5	<hasContext rdf:resource="#Context_$anyTime$"/>
6	<hasPermission rdf:resource="#Permission_p_2"/>
7	<hasData rdf:resource="#BaseConcept_p_2_$Address$"/>
8	<hasOperation rdf:resource="#Operation_p_2_$write$"/>
9	</**Policy**>

Table 3: The Reasoning Rule for Accessing Data from Multiple Sources

1	Policy(?policy$_2$) $\wedge$
2	Requester(?req) $\wedge$ hasUser(?policy$_2$, ?req) $\wedge$
3	Role(?dataScientist) $\wedge$ hasRole(?policy$_2$, ?dataScientist) $\wedge$
4	Context(?anyLocation) $\wedge$ hasContext(?policy$_2$, ?anyLocation) $\wedge$
5	Context(?anyTime) $\wedge$ hasContext(?policy$_2$, ?anyTime) $\wedge$
6	Permission(?p$_2$) $\wedge$ hasPermission(?policy$_2$, ?p$_2$) $\wedge$
7	BaseConcept(?Address) $\wedge$ hasData(?p$_2$, ?Address) $\wedge$
8	Operation(?write) $\wedge$ hasOperation(?p$_2$, ?write) $\wedge$
9	$\rightarrow$ canAccess(?req, ?carAddress) $\wedge$ canPerform(?req, ?write)

any location at any time, however, a data analyst John only can access relevant records from his office location and during his duty time.

The specification of the different contextual conditions is out of the scope of this paper. In this respect, we adapt our context models [5][8] towards modeling the dynamic contextual conditions (fuzzy and normal contexts) and incorporating such conditions into our context-sensitive access control policies.

Table 4: The Reasoning Rule for Preserving Privacy

1	Policy(?policy$_1$) $\wedge$
2	Requester(?req) $\wedge$ hasUser(?policy$_1$, ?req) $\wedge$
3	Role(?dataAnalyst) $\wedge$ hasRole(?policy$_1$, ?dataAnalyst) $\wedge$
4	Context(?anyLocation) $\wedge$ hasContext(?policy$_1$, ?anyLocation) $\wedge$
5	Context(?anyTime) $\wedge$ hasContext(?policy$_1$, ?anyTime) $\wedge$
6	Permission(?p$_1$) $\wedge$ hasPermission(?policy$_1$, ?p$_1$) $\wedge$
7	Operation(?read) $\wedge$ hasOperation(?p$_1$, ?read) $\wedge$
8	PrivacyRules(?privacy$_1$) $\wedge$ hasPrivacy(?policy$_1$, ?privacy$_1$) $\wedge$
9	BaseConcept(?privacyAttributes$_1$) $\wedge$
10	cannotAccess(?privacy$_1$, ?privacyAttributes$_1$)

5.1.2. Data View Case Study

In this section, we include another application scenario where the data analyst would not have right to access specific records of clients (i.e., an integrated result) from multiple sources. Actually, using our proposed FB-CAAC approach, we provide a controlled data view to the users without violating privacy of clients' records (e.g., protect the individually identifiable information).

In Figure 5, we have already specified a set of privacy attributes and in Table 1, we have specified an specific privacy control policy for this case study. In this case, a data analyst would not have access to the address and date-of-birth of any individual car owner, which is the personally identifiable information. Table 4 specifies a relevant reasoning rule to protect relevant data (i.e., individually identifiable information), in which the privacy rules are specified in *Line# 8 to 10*. The rule shows that a data analyst cannot access the address and date-of-birth together in a single, integrated view with whatever the context is, i.e., from any location or at anytime. However, an access control policy in Table 3 shows that a data analyst can access the address of the clients. Actually, a client cannot be individually identified only from such records.

5.1.3. Other Real-World Case Studies

As contextual conditions are involved in the access control process, in our approach, the access control decisions depend on the wide range of contextual conditions, such as the request time, location, health status and so on. The context ontology proposed in our earlier research [5] that discusses the rich contextual conditions and extends in this research. We can apply our proposed CAAC approach in other real-world applications. For example, concerning the emergency hospital scenario from our previous research [5], Jane can play the emergency-doctor role when she is present in the emergency ward of the hospital, where a patient is admitted due to a severe heart attack. Consequently, she can access the emergency medical records (including other relevant records like previous medical history) of that patient to save his life from such a critical health condition.

Let us consider another application scenario from our previous work [8], a paramedic John is allowed to play the emergency-paramedic role if he is co-located with the patient Tom at the scene of an accident. Using our proposed approach, he can acquire all the permissions (data access permissions) assigned to both paramedic and emergency-paramedic roles to provide emergency treatments. Overall, this paper aims to address a significant research issue in the area of data access from multiple sources. We introduce an intermediary computational node to control data and information resources from multiple sources, which mainly includes a unified data model and its associated access and privacy control policy models. We introduce a single set of context-sensitive access control policies to access data from multiple sources by utilizing this unified data model. As such, we include the mapping rules about semantic mapping from individual local data schemas to unified data schema.

5.2. Prototype Development and Its Associated Application Scenarios

We evaluate our proposed FB-CAAC approach through prototype testing. In this section, we present several CAAC applications that have been developed in our laboratory setup, in order to illustrate the use of our proposed FB-CAAC

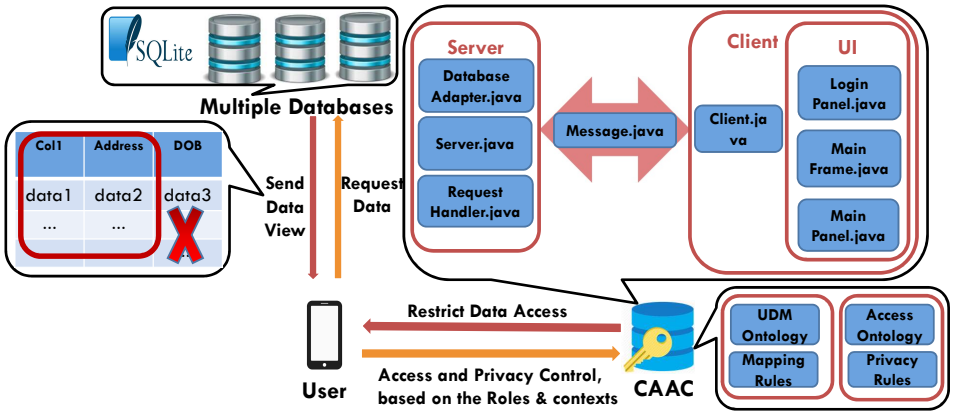

Figure 6: The Development Environment of Our Prototype

approach.

Figure 6 illustrates a complete prototype architecture of our development environment. We have used the Java language and SQLite database to build our application. When an access request comes from the user (Client part in Figure 6) using UI (user interface part), the server part in our prototype generates the relevant query (data access query) according to the applicable policies (Ontology part in Figure 6). The user can access the required data from multiple databases accordingly. In this application, we have used three databases (one for access control logic and other two for different data records) and we actually limit the users to access data from these databases based on their roles and the relevant contextual conditions.

According to our CAAC solution to access data from healthcare databases [5], Figure 7 presents a screenshot that shows the access control decision for doctor's access request. In this scenario, Amanda, who is a doctor, can access patients' information by satisfying the relevant contextual conditions. Figure 8 presents another screenshot that shows the access control decision for nurse's access request. In this scenario, Amanda, by playing a nurse role, can only have very limited access to patients' information, such as phone numbers and times for last visit. In this application, we have not considered the privacy rules.

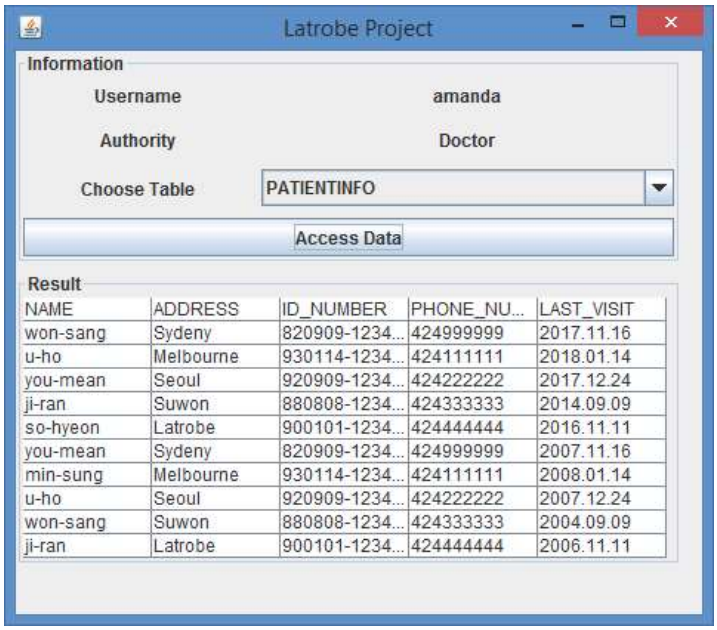

Figure 7: A Screenshot of Our CAAC Application (Doctor's Request)

We have developed another CAAC application for the scenario mentioned in Section 2. In this case, John, who is a data analyst, can access clients' address from one car source. He also can access the clients' insurance records from another source. However, he is not allowed to have a single, integrated view of the addresses and date-of-births together. It is potentially a privacy issue as a client can be potentially identified based on such records (address and DOB). Our proposed FB-CAAC approach can facilitate to handle such a privacy issue and consequently denies the users to access such an integrated view of personally identifiable information through our specified privacy rules.

Overall, the above-conducted case studies through different test scenarios demonstrate the applicability of our proposed FB-CAAC approach to build context-sensitive access control applications in today's dynamic computing environments and facilitates access to data from multiple databases accordingly.

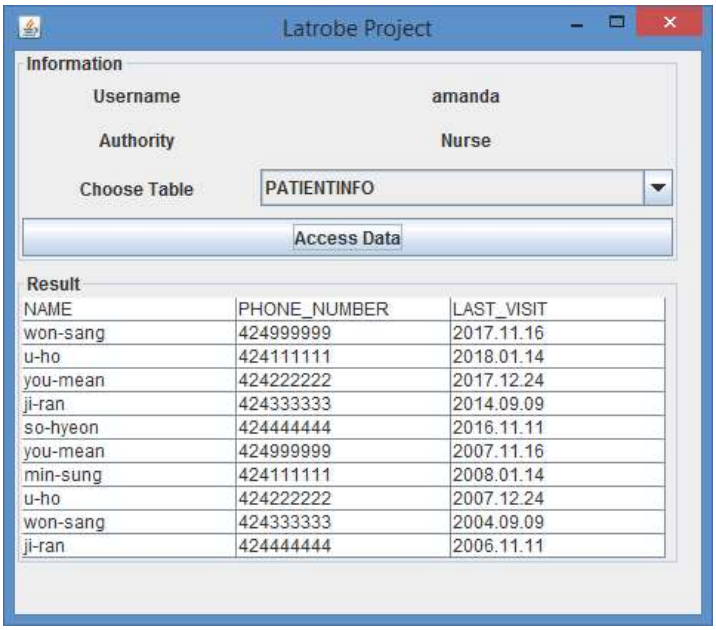

Figure 8: A Screenshot of Our CAAC Application (Nurse's Request)

5.3. Empirical Evaluation

In this section, we aim to demonstrate an empirical study on the performance of our current approach with respect to the context-sensitive access control model proposed earlier [1], which only covers data access from multiple sources. We conduct several sets of experiments and measure the query response time (i.e., processing overheads) with respect to different number of context-sensitive access control policies in conjunction with relevant contextual conditions. In order to model the users' roles (e.g., doctors, nurses, paramedics, researchers, data scientists and data analysts, and so on) and data resources from multiple sources (e.g., daily medical records, historical medical records, insurance records, and so on), we adapt and extend the role and resource ontologies from our previous research [5][8] [1]. The experiments are conducted in our laboratory setups using an Intel machine with Core i7@3.6GHz Processor and 16GB of memory. We deduce the average response time by executing the experiments 10 times and compute an arithmetic mean of them.

Table 5: Different Sizes of the Ontology Knowledge-Base w.r.t. Different Numbers of Policies

Number of Policy	Ontology Knowledge-Base Size
100	394
200	519
300	748
400	1026
500	1250
1000	2570

5.3.1. Experiment #1: The Context-Sensitive Access Control Approach [5]

In our first set of experiments, we specify all the different sets of context-sensitive access control policies for multiple databases and measure the CAAC performance.

Based on the Australian Standard Classification of Occupations (ASCO) of the health professionals [30], for our application we have codified the access control policies. The policies are written using OWL and SWRL ontologies. In particular, we model the users' roles (e.g., doctors, data scientists) and specify the context-sensitive access control policies for the health and other relevant professionals. Table 5 shows the corresponding sizes of the ontology knowledge-base according to different sizes of access control policy. The number of policies has been increased from 50 to 1000 to evaluate the performance of our proposed FG-CAAC framework. As such, we have captured the response time, i.e., the time taken from the arrival of user's data access request to the end of its execution.

We vary the number of policies up to 1000 with respect to 138 different roles. We also consider the different types of contextual conditions in these variations. We specify the separate access control policies for multiple databases/sources, an initial size of 100 policies and we increase this size up to 500 for an increment of 100 (see Figure 9). As such, we specify a large number of access control policies,

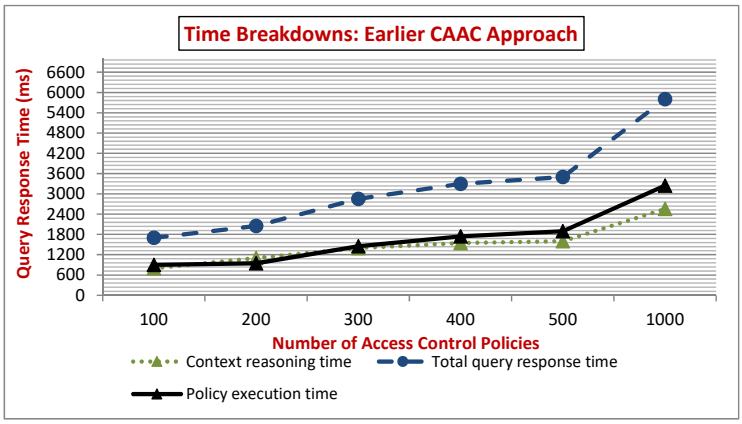

Figure 9: Time Breakdowns of the Query Response Time

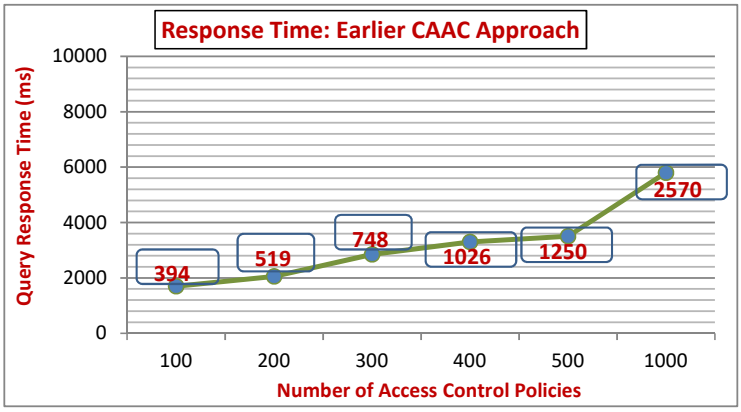

Figure 10: Response Time w.r.t. Number of Access Control Policies

which is 1000. In Figures 9 and 10, we can see that the performance overhead varies from 1.7 seconds (sec) to 5.8 sec with respect to the increasing size of the ontology knowledge-base. The red numbers in Figure 10 are the sizes of ontology knowledge-base according to the increasing number of access control policies. For instance, the sizes of the ontology knowledge-base are 394 Kb and 519 Kb when there are 100 and 200 policies, respectively. Table 5 shows the corresponding sizes of the ontology knowledge-base according to different sizes of access control policy.

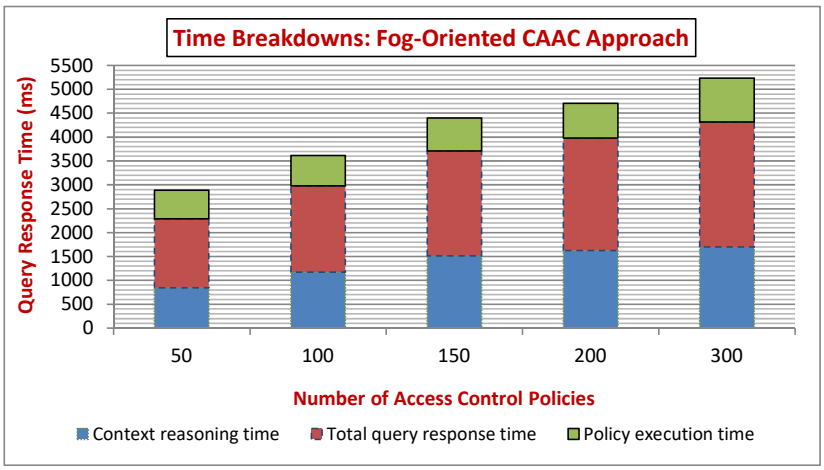

Figure 11: Time Breakdowns using Bar Chart

In this setup, using our earlier CAAC approach [5], we can see that the query response time is linearly increasing according to the number of policies up to 500, with respect to small size of the ontology knowledge-base. The performance overhead increases dramatically when the ontology size is big with respect to 1000 policies. This is due to the large number of policies and the reasoning task behind the data access query.

5.3.2. Experiment #2: The Fog-Oriented Context-Aware Access Control Approach [1]

In our second set of experiments, we specify a unified set of context-sensitive access control policies in order to access data from multiple databases. Based on the fog-oriented CAAC approach from our earlier work [1], a unified set of access control policies is the main contributor in this experiment setup. Thus, the number of policies is smaller than the previous CAAC approach [5].

The experiment results are illustrated in Figures 11 and 12. Particularly, a bar chart is shown in Figure 11 based on the fog-oriented CAAC approach. In this setup, a unified set of context-sensitive access control policies is used for accessing data from multiple sources. The time taken to perform the reasoning

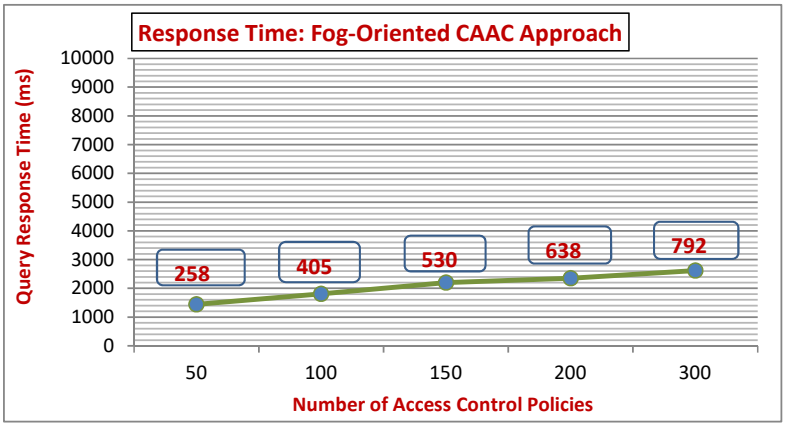

Figure 12: Response Time w.r.t. Number of Access Control Policies

task in this fog-oriented CAAC approach is a little bit expensive than the earlier CAAC approach, as we have a data ontology and its associated mapping ontology in our proposed FB-CAAC approach.

However, we can see that an extra reasoning task concerning a unified set of policies does not have great impact in total query response time. In this setup, the query response time measures 2.6 sec with respect to 300 policies, which actually covers all the 1000 policies in our previous setup. Overall, we can see that we need an small number of policies using our FB-CAAC approach and subsequently the performance overhead decreases using our unified set of context-sensitive access control policies to access data from multiple databases. In this setup, we have not incorporated the privacy control policies.

5.3.3. Experiment #3: Our Current FB-CAAC Approach

In this set of experiments, we assess an extra overhead of our current FB-CAAC approach with respect to our fog-oriented CAAC approach from the previous work [1]. As such, we now incorporate a new set of policies for providing a controlled data view to the users. Particularly, we specify the relevant privacy rules to access necessary data from different sources. We provide a data view to

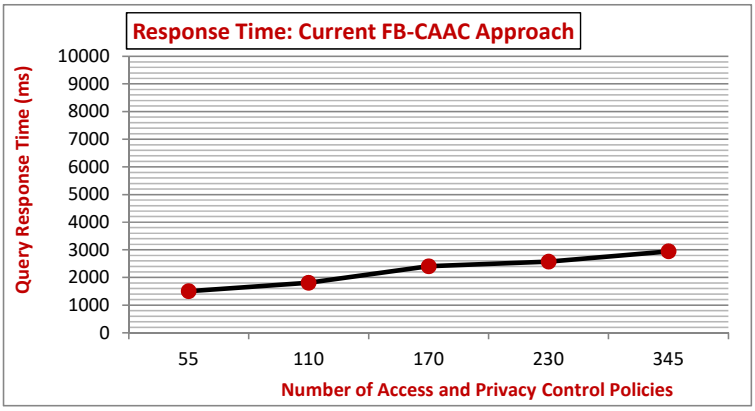

Figure 13: Response Time w.r.t. Number of Access and Privacy Control Policies

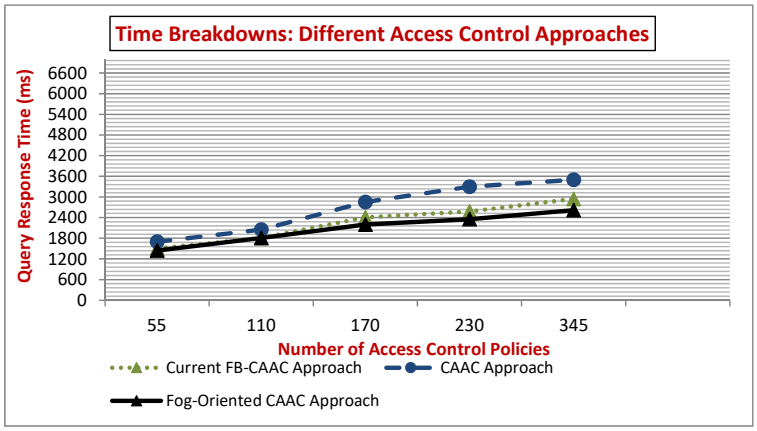

Figure 14: Response Time w.r.t. Different Access Control Approaches

the users by protecting the personally identifiable information that may lead to a violation of privacy. For example, a client can be potentially identified from the records of address and date-of-birth.

The experiment results are illustrated in Figure 13. A new set of privacy control policies is the main contributor in this current setup, which was not included in the fog-oriented CAAC approach [1]. Consequently, an extra reasoning task to check potential privacy violation is involved in this setup. In this case, the query response time measures 2.94 sec with respect to 345 access

control policies, including a new set of privacy control policies comparing to earlier approach [1]. For better understanding, the various query access times of the three proposed CAAC approaches are shown in Figure 14 on a single plot. Overall, we can see that an extra reasoning task according to the new set of privacy policies does not have a much impact in total query response time.

5.3.4. Lessons Learnt from the Experiment

This section summarizes our experience to build a new fog-based CAAC model that can be applied at the edge of the network. The following are few technical challenges that we have experienced during the experiment.

- We have evaluated our proposed fog-based CAAC framework in response to different data access requests from users in our in-lab setup and through our implemented prototype. In particular, we have simulated the fog node and other user/server nodes in our laboratory setup on a single desktop machine. Towards this end, we need to consider the network latency according to the distance between fog and user nodes. In addition, we may need to consider an extra latency that would arise from both the cloud and fog intermediary nodes.

- The aim of this research is to develop a context-aware access control model and its associated data and mapping model to link multiple data sources and consequently access data from these data sources. This research paper investigates the key factors determining the adoption of fog-based access control solution. However, integrating streaming data and information resources from multiple sources has increasingly become challenging due to critical aspect of economic growth in the IoT-enabled infrastructures. It is particularly important from the viewpoint of integrating necessary data from multiple sources with the aim of trading-off utility and privacy. This research paper explains how developed models would help stakeholders to understand the importance of privacy and access control factors for fog-based access control adoption. This is the case, for instance, in medical, manufacturing and agricultural ap-

plications, where stakeholders only want to share parts of the clients' data they have. As a result, how to provide an integrated data view to the users by ensuring privacy of clients' records is a key research challenge that is required to be investigated in the broader direction of streaming data integration from multiple sources. More specifically, how we can implement our proposed fog-based access control approach using such streaming data is a key research challenge. In our earlier research [31], we have introduced a window-based data integration approach to collate IoT streaming data from multiple data sources. In particular, we have extended basic windowing algorithm for real-time data integration and to deal with the associated issues of timing conflicts, timing alignments and data duplication. We have conducted several sets of experiment on a real streaming data platform [31]. In our current research, we can adopt this earlier framework to integrate streaming data from multiple sources and apply our fog-based access control proposal to provide a unified data view to the users.

- A data breach (e.g., an unauthorized data access) while data is coming from IoT-enabled infrastructures remains another challenging task that requires further research beyond the scope of this paper. A matter of data breaches, once combined with the properties of machine learning, may have major implications as a countermeasure to data and information access. Indeed, defining and managing tangible and intangible cost estimations against any data breaches is a considerable task that will require future research to establish.

5.3.5. Overall Discussion

In these sets of experiments, we separate the access request processing time from the ontology loading time, as the ontology loading occurs once when our system runs for the first time. In this empirical study, we have only assessed the access request processing time, which is the main contributor in our experiments. Considering the above-conducted experiment results, we can conclude that our current FB-CAAC approach offers better response time in controlling users' access to data from multiple sources with the benefits of a unified data model

and its associated access and privacy control policies. However, there is still a possibility of dealing with further performance overheads by using more powerful machines.

6. Related Work and Comparative Analysis

In this section, we provide a short overview of some relevant access control approaches as the related area of our research. The overview includes:

- the existing context-sensitive role-based access control,
- the fog-based access control, and
- the privacy-preserving access control approaches.

In addition, this section includes a brief comparative analysis by positioning the new contributions of our proposed FB-CAAC approach in relation to the current state-of-the-art context-sensitive access control approaches.

6.1. Context-Sensitive Access Control

The Role-Based Access Control (RBAC) approach [2] is well recognized by security and privacy practitioners for its many advantages in large-scale authorization management [3]. It includes two fundamental parts: the first part provides the basic concept of user-role associations in which the users can play necessary roles that are usually organized in the organizational role hierarchies; and the second part provides another basic concept of role-permission associations in which the users can exercise necessary organizational functions that are associated with their roles. However, the computing technologies have been changing over time and in today's open and dynamic environments, many organizations have been targeted to build appropriate context-sensitive access control solutions for utilizing data and information resources from multiple environments.

Over the last few years, different Context-Aware Access Control (CAAC) approaches have been introduced using role-based policies in conjunction with different contextual conditions. Bertino et al. [32], Joshi et al. [33] and Damini et al. [4] have extended the traditional RBAC approach by incorporating the temporal and spatial conditions into the access control policies. Recently, Schefer-Wenzl and Strembeck [34], Trnka and Cerný [6] and Hosseinzadeh et al. [7] have proposed several CAAC approaches in which access control is managed by means of different contextual conditions (e.g., locations, request times and resource-centric conditions).

Similar to above-mentioned RBAC approaches, Colombo and Ferrari [9] have introduced a fine-grained access control approach utilizing NoSQL-based datastores. Using these context-sensitive RBAC approaches, users can access the necessary resources from centralized sources by playing their appropriate roles and based on the contextual conditions. These approaches are mostly domain-specific and are not adequate enough to utilize a wide variety of dynamically changing conditions of the environments (e.g., the interpersonal relationships, the critical situations). Towards this end, in this paper, we adapt our initial context model [5] to capture and infer the access control-specific contextual conditions. Different from these existing context-sensitive approaches, we in this article propose a unified data model and its associated access and privacy control policy models in order to access data from multiple sources and to deal with the processing and latency overheads.

We have a successful history of using a wide range of contextual conditions for context-oriented decision making [5] [35] [36]. These existing context-sensitive access control approaches do not provide adequate functionalities to access data from multiple sources utilizing a unified set of access control policies. Different from our previous research, we have incorporated a new set of privacy control policies in our current FB-CAAC approach. Our approach can be applied to protect individually identifiable information and control users to have an integrated view of such records.

The access control policies in the above-discussed traditional and context-

sensitive RBAC approaches are based on involving the normal contextual conditions, which can be usually derived from the crisp sets (e.g., an event such as "surgery in progress" or "not", a patient is located "in the emergency department of the hospital" or "not"). In [8], we have introduced a Fuzzy logic-based CAAC (FCAAC) approach in order to facilitate context-sensitive access control to resources according to the fuzzy conditions. Using our FCAAC approach, a fuzzy contextual condition such as a patient's current health status is "60% normal with criticality level 0.40" can be derived from other relevant information (e.g., pulse rate and body temperature of the patient).

Recently, we have introduced an extensive policy model and framework for context-sensitive access control to data and information resources [25]. Our initial CAAC approaches are developed to access data and resources from centralized environments. However, like the existing context-sensitive RBAC approaches, the previous CAAC approaches are not adequate to access data coming from multiple sources by dealing with overheads and administrative issues.

6.2. Fog-Based Access Control

Recently, several fog-based access control approaches have been proposed to overcome the latency and processing overheads by moving the execution of application logic from the cloud levels to the edges of the network [14].

Due to the rapid development and technological advancements in the cloud-based environments, users need to access data and information resources from multiple sources. The integration of such data and information resources usually raises semantic namespace and latency problems [12], due to the lack of semantics and data coming from multiple environments. In order to deal with such issues, there is a need for the richer semantic of data model, dealing with the nature of such data sets from multiple sources. However, currently, these issues have been forcing the organizations to overcome the associated overheads by adding intermediary computational nodes at the edges of the networks.

Zaghdoudi et al. [16] have proposed a fog-based access control approach to

overcome the overhead issue. They consider the information about the subjects, objects and operations as contextual conditions. Salonikias et al. [37] have presented a recent study on intelligent transport systems by utilizing the fog computing nodes and corresponding fog-based access control models. Both of the research works have been concerned with several important requirements of the fog-based access control schemes, such as context-awareness and processing overheads. The authors also have discussed the decentralization of authority from a single administrative location to other locations in order to overcome the associated overheads.

Recently, Yu et al. [17] and Zhang et al. [38] have also proposed the fog-based access control approaches in order to share and access data along with the benefits of encryption and decryption mechanisms. Overall, these existing fog-based approaches have been developed to access data and information resources from centralized environments. However, these access control approaches are not truly context-aware and robust enough to build fog-based CAAC applications when accessing data from multiple sources according to the relevant contextual conditions.

In this respect, different from these existing fog-based access control approaches, our proposed FB-CAAC approach in this paper is robust enough and truly context-aware. It considers a wide range of contextual conditions and introduces a unified data model and its associated access and privacy control policies to deal with data obtained from multiple sources.

6.3. Privacy-Preserving Access Control

In the literature, the privacy-preserving access control approaches have been proposed towards the development of possible solutions with the goal of preserving users' privacy and protecting sensitive information.

Ardagna et al. have proposed [39] a privacy-aware access control approach in terms of protecting personal information that is being collected by a number of commercial and public services. They include the privacy-aware data handling policies into the access control approach. These data handling poli-

cies usually allow users to communicate to other parties and to deal with their data accordingly. This privacy-aware approach is introduced, integrating access and privacy control requirements towards developing relevant solutions for supporting users' privacy preferences. However, this approach is not adequate to protect privacy or personally identifiable information while integrating data from different sources.

Ni et al. [40] have introduced the core Privacy-aware Role-Based Access Control (P-RBAC) approach to support privacy control policies, extending the traditional RBAC models [2] [3]. Later, Ni et al. have been proposed an obligation model for the core P-RBAC approach towards bridging access control policies and privacy policies [41]. Very recently, privacy-preserving context-aware policies (e.g., location-aware) for web service recommendations [42], for secure exchange of digital identity assets [43] and for user profile matching in social networks [44].

These privacy policies have been designed to protect privacy when using, collecting and disclosing personal identifiable information. However, in these privacy-aware access control approaches, the authors have not considered the privacy perspectives while integrating data and information resources from multiple sources. Thus, there is an ultimate need to include users' privacy preferences into the policies so that the different parties can access required data from multiple sources through an integrated view.

Overall, the existing privacy-preserving access control approaches are not context-aware and robust enough to apply for accessing data from multiple sources. Specifically, these approaches are not adequate to protect privacy (e.g., individually identifiable information) when different data accesses are associated with multiple sources and integrated results from such data sources. Different from these approaches, our FB-CAAC approach can be applied to access data from multiple sources and consequently provides an integrated data view to the users by protecting individually identifiable information.

Table 6: Comparative Analysis of the Existing CAAC Approaches

CAAC Approaches	**Data, Mapping & Privacy Models**			**Policies**
	Context-awareness	**Privacy-preservation**	**Integrated view**	**Policies for Multiple Sources**
Spatio-Temporal RBAC [4] [32] [33]	*P/A*	*NO*	*NO*	*NO*
CAAC [6] [7] [34]	*P/A*	*NO*	*NO*	*NO*
Our CAAC [5] [36] [8] [25]	*YES*	*NO*	*NO*	*NO*
Earlier FB-CAAC Approach [1]	*YES*	*NO*	*NO*	*P/A*
Current FB-CAAC Approach	*YES*	*YES*	*YES*	*YES*

6.4. Comparative Assessment

Tables 6 and 7 show the results of comparative studies in which we use "**NO**" when a feature is not available, "**P/A**" when a feature is partially available, and "**YES**" when a feature is available.

In our comparative assessment, we consider the following aspects of our proposed access control approach. The existing context-sensitive access control approaches have been applied to access data and information resources mostly from centralized environments. However, these approaches are not adequate to access data from **multiple sources** in decentralized control due to the problems of administrative and latency overheads. On the other hand, the existing fog-based and privacy-preserving access control approaches are not truly dynamic and robust enough for today's interconnected environments, as the **context-**

Table 7: Comparative Analysis of Other Access Control Approaches

AC Approaches	**Data, Mapping & Privacy Models**			**Policies**
	Context-awareness	**Privacy-preservation**	**Integrated view**	**Policies for Multiple Sources**
Privacy-aware AC [39]	NO	P/A	NO	P/A
Privacy Preserving Policies [40] [41] [42] [43] [44]	NO	P/A	NO	P/A
Fog-based AC [16] [17] [37] [38]	P/A	NO	NO	P/A
Current FB-CAAC Approach	YES	YES	YES	YES

awareness capability has not been extensively incorporated. With the increasing demand of accessing data and information resources from multiple sources, different stakeholders' requirements for security and privacy are becoming more challenging. Therefore, there is a grand challenge that traditional access control solutions and measures cannot meet such requirements in today's dynamic computing environments. As a result, in this paper, we introduce a new FB-CAAC approach in order to support access control to data and information resources from multiple sources and **protect personally identifiable information**. Our aim is to protect sensitive records that cannot be publicly disclosed. For example, from the records of address and date-of-birth, users could reveal individually identifiable information about specific clients. We include both the formal and ontology-based implementation models to specify a unified context-

sensitive access control policies with the benefits of mapping functionality. In particular, in includes a unified data model and a mapping model in order to correlate data and information resources from multiple sources.

The fog-oriented CAAC approach that we proposed in our earlier research [1] can be applied to access data from different databases utilizing a unified set of access control policies with the goal of reducing the associated overheads. However, this earlier FB-CAAC approach is not adequate to protect personally identifiable information obtained from multiple data sources. In this aspect, we specify a set of privacy control policies to protect individually identifiable information while required data are coming from different sources. Our current access control approach can be applied to protect such sensitive information and control users to have an **integrated view** of required records obtained from multiple data sources. We present a walkthrough of our entire context-sensitive access control mechanism by using several case studies and a prototype testing. Finally, we present an empirical evaluation to validate the feasibility of our proposed approach, comparing the existing context-sensitive access control approaches.

7. Conclusion and Future Research Directions

In the recent years, considerable interest in accessing data from multiple environments through appropriate access control mechanisms has been received by the practitioners from academia and industry. A key factor in the success of such an approach is the need to access necessary data obtained from different sources beyond that which normally associated with users' roles. To date, several role-based, fog-based and context-aware access control approaches have been introduced to access data and information resources from centralized sources. However, these existing approaches are not robust enough in today's interconnected environments for accessing data from multiple sources due to the problems of latency and processing overheads and the lack of context-awareness as well. Many cloud-based organizations have been targeted to avoid such over-

heads and latency issues by adding an intermediary computational node at the edges of the networks. Another subsequent issue is to protect sensitive records which cannot be publicly disclosed.

In this paper, we introduced a new direction of Fog-Based CAAC (FB-CAAC) solution that facilitates context-sensitive access control to data and information resources from multiple sources. Our proposed FB-CAAC approach provides a flexible policy specification solution to the problem of reducing processing overheads, by specifying unified CAAC policies and consequently controlling users' access to data at multiple granularity levels. Our solution significantly differs from the existing access control solutions in that it utilizes the benefits of a unified set of policies and its associated mapping functions in order to access data from multiple sources. In addition, our proposed approach can facilitate programmers or security experts in avoiding potential privacy pitfalls and to build relevant CAAC solutions for addressing privacy preservation in the development process.

We introduced a conceptual definition of the unified data model and its associated data view model to collate integrated data from different sources. We proposed the relevant access control policies and a set of mapping rules to facilitate context-sensitive access control to data from multiple data sources. We introduced an ontology-based approach in realizing these preliminary definitions, including the data, access control policy, mapping and privacy control ontologies. We demonstrated the feasibility of our proposal through a walk-through of our whole approach, using the OWL, DL and SWRL languages to model the core and domain-specific ontology concepts. We also demonstrated the applicability of our approach through a prototype testing. Finally, we carried out several sets of experiments and presented an empirical comparison of the performance of our proposed FB-CAAC approach compared to our first fog-oriented CAAC approach [1]. Our proposed FB-CAAC approach can be effectively used to access data from multiple sources in practice and to provide a controlled data view to the users without violating the privacy. In particular, it can be used to protect personally identifiable information about individual

clients while integrating data from multiple sources.

Our proposed Fog-Based CAAC approach can be applied to deal with the issue of data heterogeneity and subsequent semantic heterogeneity while integrating data from distributed cloud sources. It is particularly important when the necessary data and information resources have been obtained from distributed and heterogeneous sources towards an integrated data view for the end-users. There is a need to investigate a generic data model to achieve semantic interoperability between data schemas from distributed sources.

In the context of integrating data from multiple sources, in this research, we modeled the knowledge in our proposed UDM data ontology and mapped all the data sources through incorporating semantic mapping rules (e.g., SWRL rules) into the ontology. Nevertheless, there is other way to investigate the performance issue by modeling a global schema according to the local data schemas. Future research directions according to our research findings through UDM data ontology compared to utilizing global data schema will be required to investigate further utilizing the concept of information fusion and the heterogeneous data sources.

In this paper, we proposed a novel fog-based access control framework for large-scale decentralized environments. Comparing to the classical access control like Context-Aware Access Control (CAAC) framework, the proposed fog-based CAAC framework can map a unified set of policies into multiple data sources. IoT devices continuously collect personal data with and/or without authorization of the users. The privacy model is one of the main building blocks of our framework while collating data from multiple sources towards developing a unified data view. Our proposed fog-based CAAC framework can be applied in today's IoT-based infrastructures. It can contribute in satisfying the privacy and security requirements of the associated stakeholders.

In this paper, the experiments were conducted to evaluate the performance of the proposed CAAC framework in the decentralized fog computing environment. From the experimental results, we observed a significant improvement in the performance while there was a small population size (i.e., the number of

policies). Our framework can be used for not only the fog computing networks but also other dynamic networks considering IoT data. One interesting problem is to extend fog-based CAAC framework to further explore the performance and optimization issues. In order to explore the framework deeply and explain the associated concepts in different viewpoints considering the IoT-enabled environments, future scholars can use IoT datasets from multiple sources and conduct different sets of experiments. However, enlarging the number of access control policies may increase computational overhead.

Acknowledgments

The authors would like to thank their internship students, Yuho Lee and Minsung Han from Gachon University, South Korea, for the development of healthcare application that has been used in this article. The students are partially supported by the Korea Ministry of ICT and Future Planning grant to Gachon University National Program of Excellence in Software. The statements made herein are solely the responsibility of the authors.

References

[1] Kayes, A., Rahayu, W., Dillon, T., Chang, E.: Accessing data from multiple sources through context-aware access control. In: TrustCom 2018, IEEE Computer Society (2018)

[2] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. IEEE Computer **29** (1996) 38–47

[3] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. TISSEC **4**(3) (2001) 224–274

[4] Damiani, M.L., Bertino, E., Catania, B., Perlasca, P.: GEO-RBAC: a spatially aware RBAC. TISSEC **10**(1) (2007) 1–42

[5] Kayes, A.S.M., Han, J., Colman, A.: OntCAAC: An ontology-based approach to context-aware access control for software services. Comput. J. **58**(11) (2015) 3000–3034

[6] Trnka, M., Cerný, T.: On security level usage in context-aware role-based access control. In: SAC. (2016) 1192–1195

[7] Hosseinzadeh, S., Virtanen, S., Rodríguez, N.D., Lilius, J.: A semantic security framework and context-aware role-based access control ontology for smart spaces. In: SBD@SIGMOD. (2016) 1–6

[8] Kayes, A., Rahayu, W., Dillon, T., Chang, E., Han, J.: Context-aware access control with imprecise context characterization through a combined fuzzy logic and ontology-based approach. In: CoopIS. (2017) 132–153

[9] Colombo, P., Ferrari, E.: Fine-grained access control within NoSQL document-oriented datastores. Data Science and Engineering **1**(3) (2016) 127–138

[10] Bellahsène, Z., Bonifati, A., Rahm, E.: Schema matching and mapping. Springer (2011)

[11] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems **29**(7) (2013) 1645–1660

[12] Ylitalo, J., Nikander, P.: A new name space for end-points: Implementing secure mobility and multi-homing across the two versions of ip. In: 5th European Wireless Conference. (2004) 435–441

[13] Nicklas, D., Schwarz, T., Mitschang, B.: A schema-based approach to enable data integration on the fly. International Journal of Cooperative Information Systems **26**(01) (2017)

[14] Saurez, E., Gupta, H., Mayer, R., Ramachandran, U.: Demo abstract: Fog computing for improving user application interaction and context aware-

ness. In: Internet-of-Things Design and Implementation (IoTDI), 2017 IEEE/ACM Second International Conference on, IEEE (2017) 281–282

[15] Stojmenovic, I., Wen, S., Huang, X., Luan, H.: An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience **28**(10) (2016) 2991–3005

[16] Zaghdoudi, B., Ayed, H.K.B., Harizi, W.: Generic access control system for ad hoc mcc and fog computing. In: International Conference on Cryptology and Network Security, Springer (2016) 400–415

[17] Yu, Z., Au, M.H., Xu, Q., Yang, R., Han, J.: Towards leakage-resilient fine-grained access control in fog computing. Future Generation Computer Systems **78**(2) (2018) 763–777

[18] Embley, D.W., Tao, C., Liddle, S.W.: Automatically extracting ontologically specified data from html tables of unknown structure. In: International Conference on Conceptual Modeling, Springer (2002) 322–337

[19] Australian Industry Standards (Skills Service Organisation): Key findings discussion paper, https://www.australianindustrystandards.org.au/wp-content/uploads/2018/02/rail-key-findings-paper2018web3.pdf (2018)

[20] Babuji, Y.N., Chard, K., Duede, E., Foster, I.: Safe collections and stewardship on cloud kotta. In: 2017 IEEE 13th International Conference on e-Science (e-Science), IEEE (2017) 498–503

[21] HIPAA Privacy Rules: Standards for privacy of individually identifiable health information, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt (2002)

[22] Personally Identifiable Information: Standards for privacy of individually identifiable health information, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf (2019)

[23] Clifton, C., Tassa, T.: On syntactic anonymity and differential privacy. In: 2013 IEEE 29th International Conference on Data Engineering Workshops (ICDEW), IEEE (2013) 88–93

[24] OWL2: OWL 2 Web Ontology Language (W3C recommendation: 11 december 2012), https://www.w3.org/tr/owl2-overview/ (2018)

[25] Kayes, A., Han, J., Rahayu, W., Dillon, T., Islam, M., Colman, A.: A policy model and framework for context-aware access control to information resources. Comput. J. (2018) 1–36

[26] De Bruijn, J., Lara, R., Polleres, A., Fensel, D.: OWL DL vs. OWL Flight: Conceptual modeling and reasoning for the semantic web. In: Proceedings of the 14th international conference on World Wide Web, ACM (2005) 623–632

[27] Protégé: OWL Graphical API, http://protege.stanford.edu/ (2018)

[28] SWRL: Semantic Web Rule Language, http://www.w3.org/submission/swrl/ (2018)

[29] SWRLB: SWRL Built-Ins for comparisons and Math Built-Ins, http://www.daml.org/2004/04/swrl/builtins.htm (2018)

[30] ASCO: Australian Standard Classification of Occupations of Health Professionals, http://www.abs.gov.au/ (2018)

[31] Tu, D.Q., Kayes, A., Rahayu, W., Nguyen, K.: Isdi: A new window-based framework for integrating iot streaming data from multiple sources. In: International Conference on Advanced Information Networking and Applications, Springer (2019) 498–511

[32] Bertino, E., Bonatti, P.A., Ferrari, E.: TRBAC: A temporal role-based access control model. TISSEC **4**(3) (2001) 191–233

[33] Joshi, J.B., Bertino, E., Latif, U., Ghafoor, A.: A generalized temporal role-based access control model. TKDE **17**(1) (2005) 4–23

[34] Schefer-Wenzl, S., Strembeck, M.: Modelling context-aware rbac models for mobile business processes. IJWMC **6**(5) (2013) 448–462

[35] Kayes, A.S.M., Han, J., Colman, A., Islam, M.S.: Relboss: A relationship-aware access control framework for software services. In: CoopIS. (2014) 258–276

[36] Kayes, A.S.M., Han, J., Colman, A.W.: An ontological framework for situation-aware access control of software services. Inf. Syst. **53** (2015) 253–277

[37] Salonikias, S., Mavridis, I., Gritzalis, D.: Access control issues in utilizing fog computing for transport infrastructure. In: International Conference on Critical Information Infrastructures Security, Springer (2015) 15–26

[38] Zhang, P., Chen, Z., Liu, J.K., Liang, K., Liu, H.: An efficient access control scheme with outsourcing capability and attribute update for fog computing. Future Generation Computer Systems **78**(2) (2018) 753–762

[39] Ardagna, C.A., Cremonini, M., De Capitani di Vimercati, S., Samarati, P.: A privacy-aware access control system. Journal of Computer Security **16**(4) (2008) 369–397

[40] Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.M., Karat, J., Trombeta, A.: Privacy-aware role-based access control. ACM Transactions on Information and System Security (TISSEC) **13**(3) (2010) 24

[41] Ni, Q., Bertino, E., Lobo, J.: An obligation model bridging access control policies and privacy policies. In: Proceedings of the 13th ACM symposium on Access control models and technologies, ACM (2008) 133–142

[42] Badsha, S., Yi, X., Khalil, I., Liu, D., Nepal, S., Bertino, E., Lam, K.Y.: Privacy preserving location-aware personalized web service recommendations. IEEE Transactions on Services Computing (2018)

[43] Gunasinghe, H., Kundu, A., Bertino, E., Krawczyk, H., Chari, S., Singh, K., Su, D.: Prividex: Privacy preserving and secure exchange of digital identity assets. In: The World Wide Web Conference, ACM (2019) 594–604

[44] Yi, X., Bertino, E., Rao, F.Y., Lam, K.Y., Nepal, S., Bouguettaya, A.: Privacy-preserving user profile matching in social networks. IEEE Transactions on Knowledge and Data Engineering (2019)

A. S. M. Kayes is a Lecturer in Cyber Security in the Department of Computer Science and Information Technology, La Trobe University, Australia. He received his PhD from Swinburne University of Technology, Australia in 2014. His research interests include information modeling, cyber security, context-aware access control, big data integration, IoTs, cloud and fog computing, advanced data analytics, fuzzy computation, security and privacy protection.

Wenny Rahayu is a Professor and the Head of School of Engineering and Mathematical Sciences at La Trobe University, Australia. Prior to this appointment, she was the Head of Department of Computer Science and Information Technology from 2012 to 2014. The main focus of her research is the integration and consolidation of heterogeneous data and systems to support a collaborative environment within a highly data-rich environment. In the last 10 years, she has published two authored books, three edited books and more than 150 research papers in international journals and conference proceedings.

Paul Watters is a Professor and leading expert in Cyber Security in the Department of Computer Science and Information Technology, La Trobe University, Australia. He began his first R&D role in security in 2002, joining the CSIRO's Networking Applications and Technologies (NAT) Group, and leading a programme in secure, distributed storage. In 2013, he took up a Professorship in IT at Massey University in New Zealand. In 2015, Prof Watters also became an Adjunct Professor at Unitec Institute of Technology, the home of New Zealand's first Cyber Security research centre. In recognition of his track

record combating child abuse material online, he received an ARC Discovery grant in 2015.

Mamoun Alazab is an Associate Professor in the College of Engineering, IT and Environment, Charles Darwin University, Australia. He is a cyber security researcher and practitioner with industry and academic experience. His research is multidisciplinary that focuses on cyber security and digital forensics of computer systems including current and emerging issues in the cyber environment like cyber-physical systems and internet of things, by taking into consideration the unique challenges present in these environments, with a focus on cybercrime detection and prevention. A/Prof Alazab received his PhD degree in Computer Science and has more than 100 research papers. He presented at many invited keynotes talks and panels, at conferences and venues nationally and internationally (22 events in 2018 alone). He is a Senior Member of the IEEE. He is an editor on multiple editorial boards including Associate Editor of IEEE Access and Editor of the Security and Communication Networks Journal.

Tharam Dillon is an adjunct Professor in the School of Engineering and Mathematical Sciences at La Trobe University, Australia. He has published eight authored books and more than 500 research papers in international journals and conference proceedings. His research works have been widely cited and therefore have considerable impact. Over the last few years, he has been cited several times in over 1000 scientific articles (source: Google Scholar). He has an H-index of 55 (Google Scholar) and over 14,000 citations, which put him in the top percentile of researchers. He is a Fellow of the Institution of Electrical and Electronic Engineers (USA), Fellow of the Institution of Engineers (Australia), Fellow of the Safety and Reliability Society (UK), and Fellow of the Australian Computer Society.

Elizabeth Chang is a Professor of Logistics in IT at University of New South Wales, Canberra, Australia. She currently leads the Defence Logistics research group at UNSW Canberra, targeting the key issues in Logistics ICT, Big Data

Management, Defence Logistics and Sustainment, Predictive Analytics, Situation Awareness, IoT and Cyber-Physical Systems, Trust, Security, Risk and Privacy. In a 2012 article, published in MIS Quarterly vol. 36 issue 4, she was listed fifth in the world for researchers in Business Intelligence. She has published 7 authored books and over 500 international journals and conference papers with an H-Index of 45 (source: Google Scholar) and she has over 11,000 citations.