IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received December 15, 2019, accepted December 30, 2019, date of publication January 9, 2020, date of current version January 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965333

Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments

RUBINA GHAZAL[1,2], AHMAD KAMRAN MALIK[1], NAUMAN QADEER[3], BASIT RAZA[1], AHMAD RAZA SHAHID[1], AND HANI ALQUHAYZ[4]

[1]Department of Computer Science, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan
[2]University Institute of Information Technology, Pir Maher Ali Shah (PMAS) Arid Agriculture University, Rawalpindi 46300, Pakistan
[3]Department of Computer Science, Federal Urdu University of Arts, Science, and Technology at Islamabad, Islamabad 44080, Pakistan
[4]Department of Computer Science and Information, College of Science Al-Zulfi, Majmaah University, Al Majma'ah 11952, Saudi Arabia

Corresponding author: Ahmad Kamran Malik (ahmad.kamran@comsats.edu.pk)

This work was supported by the Dean of scientific research with Majmaah University.

ABSTRACT Today's rapidly developing communication technologies and dynamic collaborative business models made the security of data and resources more crucial than ever especially in multi-domain environments like Cloud and Cyber-Physical Systems (CPS). It enforced the research community to develop enhanced access control techniques and models for resources across multi-domain distributed environments so that the security requirements of all participating organizations can be fulfilled through considering dynamicity of changing environments and versatility of access control policies. The popularity of Role-Based Access Control (RBAC) model is irrefutable because of low administrative overhead and large-scale implementation in business organizations. However, it does not incorporate the dynamically changing policies and lacks semantically meaningful business roles which could have a diverse impact upon access decisions in multi-domain business environments. This paper describes our proposed novel access control framework that uses semantic business roles and intelligent agents through implementation of our Intelligent RBAC (I-RBAC) model. It encompasses occupational entitlements as roles for multiple domains. We use the dataset of original occupational roles provided by Standard Occupational Classification (SOC), USA. The novelty of the paper lies in developing a core I-RBAC ontology using real-world semantic business roles and intelligent agent technologies together for achieving required level of access control in highly dynamic multi-domain environment. The intelligent agents use WordNet and bidirectional LSTM deep neural network for automated population of organizational ontology from unstructured text policies. This dynamically learned organizational ontology is further matched with our core I-RBAC ontology in order to extract unified semantic business roles. The proposed I-RBAC model is mathematically described and the overall I-RBAC framework and its implementation architecture is explained. At the end, the I-RBAC model is validated through the implementation results that show a linear runtime trend of the model in presence of a large number of permission assignments and multiple queries.

INDEX TERMS Access control, multi-domain distributed environment, secure collaboration, ontology, multi agent system, LSTM.

I. INTRODUCTION

Information is one of the most significant assets of an organization and requires an appropriate protection. Organizations use *authentication* and *authorization* to ensure the information security. A user always needs authentication before her authorization to perform an activity. An effective information security mechanism decides that who should have access to which information or resource. Another fundamental question in information security is that how to control the access to resources to protect them from unauthorized modification [1]. Information security can be assured through

The associate editor coordinating the review of this manuscript and approving it for publication was Xiwang Dong.

an access control model that provides a secure mechanism to control the communication and interaction among different users and system resources. An access control model serves as a framework that demonstrates how users access the resources using access control technologies and implying certain security rules [2]. However, today's distributed and dynamic environments need change in existing access control decision making processes. Particularly, there is need for such a security mechanism that can automatically or intelligently adapt changes in the system. These changes, due to cyber business paradigm, create new challenges. It is therefore required to address and incorporate dynamic environment parameters and attributes into the security policy.

For dynamic business collaborations in multi-domain environments, like multi-domain cloud and Cyber-Physical Systems (CPS), the user's roles and tasks are inevitable. Access needs to be dynamically granted based on user's role in currently assigned task in addition to other data elements and conditions like attributes and context. A lot of work has already been done in literature. However, this paper focuses on the issues that are uncovered yet. Those issues include: general classification of business roles for multiple domains (classification of real-world dataset of general roles), creation of semantically meaningful roles (roles with business meaning) and the appropriate definition of task-based dynamic roles to access the organizational assets. The next paragraphs provide what has been done so far by access control community in this regard and what we propose to do in this work.

In the literature, many access control approaches have been proposed during last couple of decades. Amongst these approaches, some are general purpose and some are application specific. The study shows the significance of the Role-Based Access Control (RBAC) model [3], [4] that allows resource permission assignment to different users with respect to their roles in their respective organization. This model gained great popularity as a general approach for access control. The RBAC model typically forms the access control policy with the combination of users and permissions [5]. The role is the basic element of RBAC model and the whole access control policy is formulated to address this element. A role undertakes different presentations and can be mapped to different scenarios. Although the RBAC approach simplifies the access control policy management, however, it lacks to adapt the dynamically changing information of the users and resources. In order to manage dynamic changes and to provide adaptability with changing temporal and/or spatial context, the context-aware access control model was proposed [6]. However, this model is highly domain specific. It can handle different contexts in the form of attributes for software services, however, it is unable to manage the issues of multi-domain collaborative scenarios.

In a task-based multi-domain collaboration scenario, the users from multi-domain distributed organizations gather to perform some specific task. These users request access to different resources in order to perform their assigned tasks. Furthermore, the user's roles are dynamically changing according to the task. These roles need to be mapped to the real scenarios and, at the same time, the security policies need to be aligned with the organizational structure and business needs [12], [13]. The business requirements must be considered while defining roles [7], [11], [12], [9], [14]–[17]. Therefore, a key problem that still exist in distributed collaborative environments is to propose roles with business meaning [9]. The research on role mining [7], [11]–[13], [14], [16], [18] merged the business concepts with roles, however, it has not been used for multiple domains collaborative environment [8]. In such environment, the techniques to discover roles with business semantics and proving the effectiveness of these techniques is still an unaddressed problem [13], [19]. Moreover, the general classification of such business roles for multiple domains is also uncovered yet [14]. Therefore, creation of semantically meaningful roles, their classification and effectiveness incorporating multiple domains need further investigation. In addition, there is also substantial need for security policy enforcement and management in multi-domain collaborative environment as the organizational policy must be updated to reflect changes in a dynamic business environment, however, it is complicated due to certain organizational constraints [15].

In the light of above-mentioned issues, the following research challenges arise in access control of multi-domain collaborative setup: *(1) How to specify general access control policy to compensate the dynamically changing user to role assignment? (2) How to create corresponding modifying roles? (3) How to activate the changed role at runtime? (4) How to handle diversity of roles in distributed heterogeneous environment automatically? (5) How to map roles according to the real scenarios as business roles? (6) How to formulate and dynamically update policies for data sharing?*

Our proposed Intelligent Role Based Access Control (I-RBAC) model addresses these research challenges. It consists of multi-agent architecture that is coupled with a knowledge base, in the form of ontology, for mining semantically meaningful roles. It enables automatic agent-based role mining and role assignment in multiple domains. The knowledge about multiple domain roles is stored in the form of ontological RDF schema and utilized by multiple software agents responsible for creating and mining task-based semantic roles intelligently. There are certain issues for RBAC in collaborative multi-domain environment. For example, ambiguous separation of duties among roles from multiple domains, difficulty to manage enormously growing organizational data, improper role mining, limitation to handle dynamicity of rapidly changing multi-domain environment, and requirement of adaptable policies for each collaborating organization. Ontology plays a vital role in solving these issues. Ontology can be reformed easily to accept and adjust the new concepts and relationships. In other words, ontology possesses reusability and scalability features. Ontology is also helpful to capture data in a meaningful way and to discover relationships among heterogeneous data [16].

Furthermore, the hierarchically related concepts within ontology lead to generate role classification rules. In fact, the agents and ontology jointly provide formal specification of concepts and their relationships for inter-operation among different domains [17].

The literature study indicates that an extensive research has been done individually on the RBAC model and its different components as well as multi-agent ontological systems. However, there is no significant work found that combines the advantages of RBAC model with intelligent agents and ontology for finding semantically meaningful roles to users in multi-domain collaborative environment. Our proposed I-RBAC model is the novel effort in this direction. Upon implementation in a multi-domain collaborative scenario, our proposed model proved itself as the solution of above-mentioned research challenges and it enhances the dynamicity and adaptability of the access control system by using ontological relationships and rules. This paper provides formal modeling as well as practical implementation (framework) of the proposed I-RBAC model. At the end, the I-RBAC model is validated for its efficiency using the real data of roles and large number of access control rules (permissions) and requests.

The rest of the paper is organized as follows: Section 2 describes related work regarding RBAC, ontology and intelligent agents. Section 3 explains our I-RBAC model and semantics i.e. its formal definitions and ontology details. Section 4 describes multi-agent system architecture and the overall I-RBAC framework. Section 5 illustrates implementation of the I-RBAC framework and results. Finally, section 6 concludes paper and describes limitations and future work.

II. RELATED WORK

The application of traditional RBAC model in business workflows can reduce the privilege management. However, for eliciting semantically meaningful roles, user-permission relationships alone are not adequate. There is always a need to construct roles that are configurable with structure of multiple domains. To resolve this issue, various approaches have been proposed. These approaches are usually classified as top-down and bottom-up [13]. A top-down approach, called role engineering, works in a systematic way. Role engineering is concerned with the identification of roles from raw procedure and facts which is a difficult and complex task [18]. There is a need for an in-depth analysis of business processes for the identification of certain permissions to perform certain tasks. Whereas the bottom-up approach, called role mining, finds roles from existing data about users and permissions. It implies data mining techniques to identify roles. The role mining approaches have attracted most of the researchers [7], [11]–[13] due to the availability of data about users and assigned permissions. Both role engineering and role mining approaches have their pros and cons. Role engineering is unable to explore business processes completely and may ignore existing permissions and exceptions, whereas role mining may not consider business processes of an organization. Therefore, a hybrid approach is proposed in [19].

There are different types of permissions in an organization. The significance of the existing permissions in an organization highly depend upon the nature of resources and associated operations and varies accordingly. To cope up with an organization needs, the main idea is to map tasks in a workflow to the RBAC scheme. Many researchers tried to fulfill this need, such as the idea proposed by [20] was an improved version of the traditional RBAC model with tasks for enterprise environment. As a task is the primary unit of business activities, they introduced the classification of tasks and task-level access control. Likewise, an organizational and task-based access control model for workflow system was proposed by [21] to maintain the consistency between users and organizational structure. Moreover, a personal health record system was proposed in [22] using task-role based access control. Combined context of team collaboration and workflow was proposed in [23]. Task-based access control system for dynamic multi-domain environment is proposed in social network domain in the form of multiple social communities [24]. Role mining and role engineering are the main concerned research areas in RBAC research. A role mining framework was proposed in [25] taking into account the organizational entity-relation information. The work done in [26], [27] showed the role mining and role engineering optimization with separation of duty and cardinality constraints.

Another aspect that needs attention towards this issue is the creation of roles that are semantically meaningful with respect to an organization. A role mining technique was proposed in [28] that assigns weights to permissions and mine the roles accordingly. The optimization of different quality metrics for policy have been proposed in [11] using role mining algorithms. Role mining algorithms grounded upon machine-learning models [29], [30] have been proposed in [10], [31]. The role mining techniques proposed in [6]–[8], [12], [9], [32] produce generative RBAC models. A number of researchers have discussed the importance of agent technology in security mechanism. The development of distributed multi-agent systems shows the importance of this technology in state of the art research areas like cloud computing, block chain and IoT [33]. In [34] a security scheme was proposed with mobile agent paradigm and cryptographic techniques. The research conducted in [35] proposed a method for role assignment to mobile agents for distributed environment. In [36], smart agents are used to access distributed healthcare services. Security of agent for information retrieval is discussed in [37] through RBAC with one time pad security encryption techniques. A multi-agent system was proposed by [38] to access distributed healthcare data using middle facilitator agent. In [39], authors proposed an access control model for mobile agent to provide a secure communication channel for health domains. A knowledge management approach in distributed designs was proposed by [40] based on agent technology. The work of [41] proposed an ontology for task representation to enhance agent coordination and collaboration through reasoning over tasks. An agent coordination context based approach was proposed in [42] for RBAC-MAS infrastructure. A semantic-based approach was proposed in [14] to add a new user in the existing access control system using classification methods. Adaptive mobile agent was proposed for dynamic role adaptation [43]. Genetic algorithm based approach was proposed in [44] for solving role mining problem in RBAC. Similarly, a unified approach based on genetic algorithm was proposed in [45] to design and reconfigure the RBAC schemes.

A rapid evolution has been observed in the area of distributed computing, specifically in the perspective of efficient storage technologies. These technological advancements make it feasible to share and diffuse the system resources. However, it necessitates the development of an improved security mechanism possessing certain features such as automatic acquisition, processing and management of information. It helps to protect information systems from serious damages. The agent technology is considered as a feasible solution in a distributed environment. It offers an autonomous behavior to the systems. However, it lacks the aspects of knowledge and intelligence. The literature reviewed so for, showed that there is need to explore this research area with respect to ontology-based knowledge management for agents to successfully deploy an access control system.

III. INTELLIGENT ROLE-BASED ACCESS CONTROL (I-RBAC) MODEL

The primary aim of this research is to develop an Intelligent Role Based Access Control (I-RBAC) framework that provides role engineering, role mining and role assignment for multiple domains. Our I-RBAC framework consists of two major deliverables; (i) an I-RBAC model and its ontological knowledge base (ii) implementation of the model using multi-agents.

In the first step, the I-RBAC model is proposed that consists of occupational/business roles and set of related tasks. Secondly, the ontology for the I-RBAC model is developed. The ontology-based knowledge is helpful in role mining. This ontology is based upon occupations and tasks data from Standard Occupational Classification (SOC) [46], [47]. The ontology serves as a part of designing a scalable knowledge base, capable of dealing with large number of roles and their related set of tasks. Rules are generated from the ontological relationships that help agents to learn task-based user role assignments.

A. FORMAL DEFINITIONS OF I-RBAC MODEL

The proposed I-RBAC model is an enhancement of the RBAC model with occupational roles and associated tasks. The core concept of the I-RBAC model is to use multiple agents with learning capabilities and to design roles based on user's formal functionality within an organization and assigned tasks. Moreover, this model presents a new concept of dynamic access control based on changing organizational policies. The intelligent agents are adaptable to changing environment. They can keep track of the changing environment, information sources available to the system and the required access methods. Agents can activate new roles and can also change granted roles according to new policy. The role hierarchy concept is bound to assigned tasks according to organizational hierarchy which is different from the standard RBAC model. The main components of the proposed I-RBAC model are user (agent), business role, task role, set of task and permission as shown in the Figure 1.

Formal definitions of the main components and their relationships in the I-RBAC model are given below.

Definition 1 (User (Agent)): An agent is an entity that has knowledge of the surroundings and can assimilate and interpret the environment changes independently. It acts according to the changes which further affect the environment. Therefore, agent is autonomous and possesses social abilities.

$$\begin{aligned}&Users(U_{Ag_i}) = \{U_{Ag_i} | i = 1, 2, 3 \ldots n\}\\&\text{Whereas } \forall U_{ag} \in U_{Ag}\\&U_{ag} = \{AID, Ontology, Communication, Action, Result\}\end{aligned}$$

Definition 2 (Role): A title belonging to an organization – describing the responsibilities of a user. Roles are classified according to tasks assigned to each user. We categorize the Roles as Business Roles (BR) that are exact entitlements of job position held in an organization. Task roles are a subset of the business roles set but are dynamic as per assigned tasks and named as Task Roles (TR). There is many-to-many relationship between roles and agents.

$$\begin{aligned}&Business\ Roles(BR\ or\ TR) = \{BR_i | i = 1, 2, 3 \ldots n\}\\&Whereas\ \forall br \in BR\\&br = \{U_{ag_1}, U_{ag_2}, \ldots U_{ag_n} | U_{ag_i} \in U_{Ag}\}\end{aligned}$$

Definition 3 (Permission): Authorization to access system resources. It is the combination of actions performed on certain objects. It is the power set of permissions associated with different tasks.

$$\begin{aligned}Objects(Obj) &= \{Obj_i | i = 1, 2, 3 \ldots n\}\\Operations(Opr) &= \{Opr_i | i = 1, 2, 3 \ldots n\}\\Permission(P) &= \{P_i = Obj_m \times Opr_n | i, m, n = 1, 2, 3 \ldots n\}\end{aligned}$$

Definition 4 (Task): A specific predefined set of tasks associated with a specific business role owned by different organizations.

$$Tasks(T) = \sum_{n=1}^{N} T_n = T_1 \cup T_2 \cup \ldots T_N = \{t | \exists\, n(t \in Tn)\}$$

Definition 5 (Attribute): A set of attributes related to users, roles and objects (resource).

$$\begin{aligned}Attributes(Attr_{user}) &= \{Attr_{user_i} | i = 1, 2, 3 \ldots n\}\\(Attr_{obj}) &= \{Attr_{obj_i} | i = 1, 2, 3 \ldots n\}\\(Attr_{role}) &= \{Attr_{role_i} | i = 1, 2, 3 \ldots n\}\end{aligned}$$

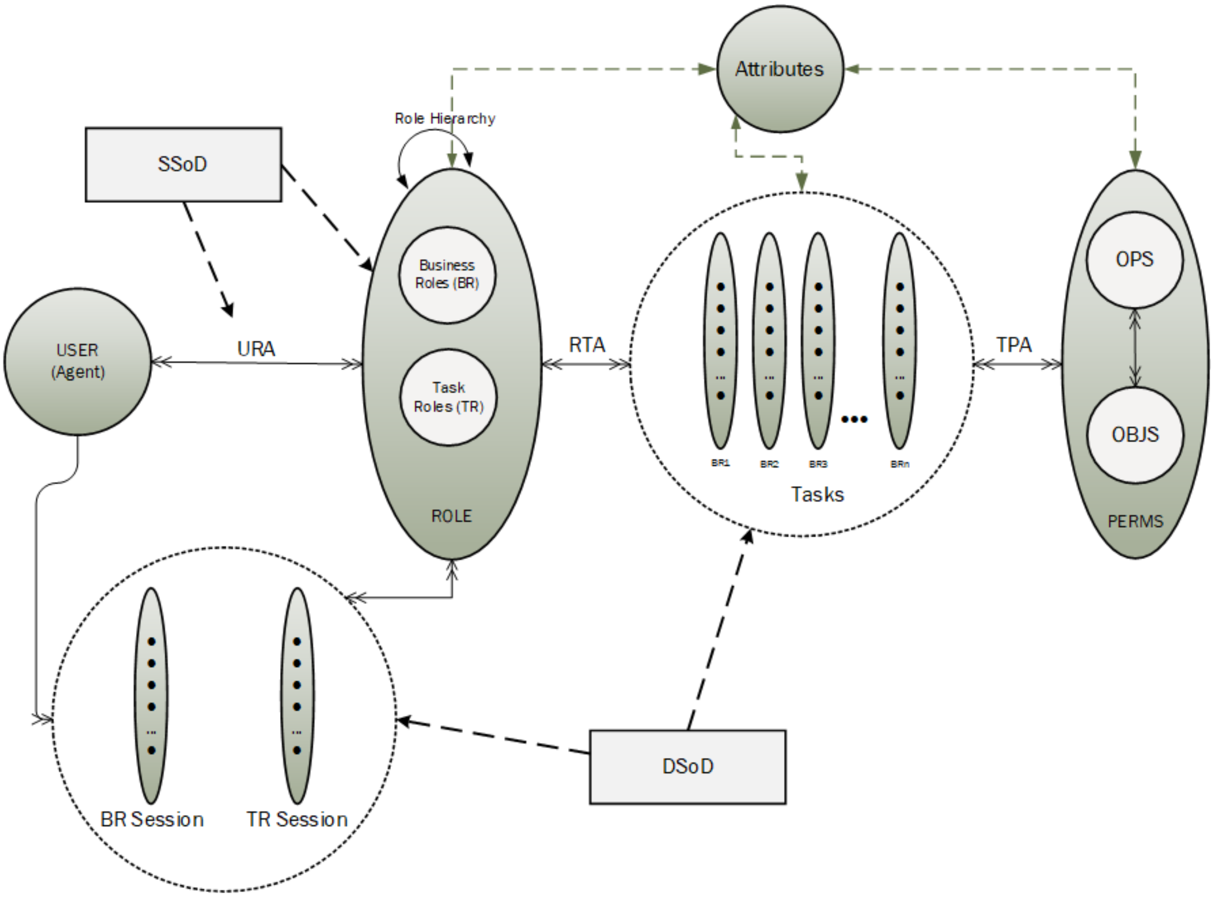

FIGURE 1. **I-RBAC model.**

Definition 6 (Task-Permission-Assignment (TPA)): The permission to task association is defined as:

$$\begin{aligned} TPA &= \{(P, T, Attri_{obj}, Attri_{opr}) | Permission\ P\ is \\ &\qquad\qquad assigned\ to\ Task\ T\} \\ &\subseteq P \times T \times Attr_{Obj} \times Attr_{Opr} \end{aligned}$$

Definition 7 (Role-Task-Assignment (RTA)): The task to role association is defined as:

$$\begin{aligned} RTA &= \{(BR, T) | Task\ T\ is\ assigned\ to\ TaskRole\ TR \in BR\} \\ &\subseteq T \times BR \end{aligned}$$

Definition 8 (User-Role-Assignment (URA)): The role to user assignment is defined as:

$$\begin{aligned} URA &= \{(BR, U_{Ag}) | Business\ Role\ BR\ assigned\ to\ User \\ &\qquad\qquad (agent)\ U_{Ag} \subseteq BR \times U_{Ag}\} \end{aligned}$$

Definition 9 (Session): A session is the time stamp allocated to a user while working under certain role.

$$\begin{aligned} Session(S) &= \{S_{role_i} | role_i \in Br\ or\ role_i \\ &\qquad \rightarrow T_j | i, j = 1, 2, 3 \ldots n\} \\ &\qquad \boldsymbol{Session - User_{Ag}} : \ \boldsymbol{S \rightarrow U_{Ag}} \end{aligned}$$

A function that maps each session $\boldsymbol{S_i}$ to the single user $\boldsymbol{User(S_i)}$ that remains constant throughout the session.

$$\boldsymbol{Session - BR} : \boldsymbol{S \rightarrow 2^{BR}}$$

A function that maps each session $\boldsymbol{S_i}$ to a set of Task Roles $\boldsymbol{TR\ (S_i) \subseteq \{BR | User\ (S_i)\ , BR) \in URA\}}$

B. ONTOLOGY LEARNING FOR I-RBAC MODEL

Knowledge extraction from various sources and its representation in a useful manner is essential while sharing information and facts in a distributed environment. Knowledge representation helps in storing complex information in a knowledge base and ensures its availability for different applications. There exist different strategies for the management of distributed knowledge such as using same language, introducing similar terms or constructing comprehensive knowledge bases. Effective knowledge management helps to minimize the efforts in solving complex problems and assists in effective decision mechanisms. Knowledge management (KM) solutions evolved from the concepts of ontology and semantic web.

Resource Description Framework (RDF) provides knowledge representation mechanism in the form of a triplet which contains a subject, an object and a predicate along

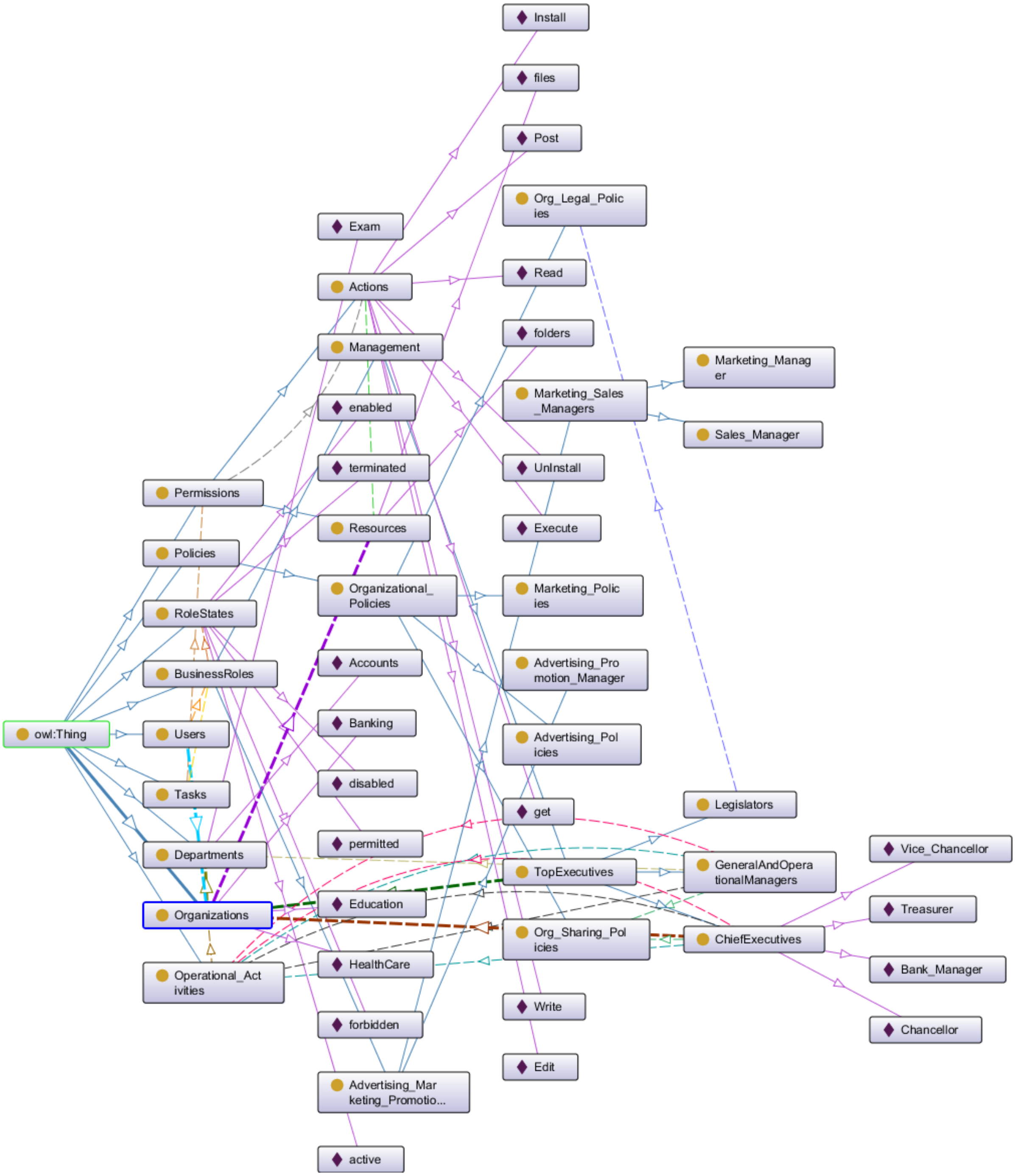

FIGURE 2. A snippet of I-RBAC core ontology.

with the description of relationship among them. These triplets can be represented in the form of a graph. Additionally, RDF schema (RDFS) can be defined to build up an ontology which is called ontology learning. Ontologies are built up to extract meaningful information from various data sources. The aim of ontology construction is to collect domain knowledge which can be used in different applications.

There is a need of KM solutions to be implemented into various multi-agent systems where agents can learn from the ontology. The distribution of data, information retrieval and integration of knowledge become simple and efficient for agents when the knowledge is formulated in the form of ontology. The proposed I-RBAC model is based upon the knowledge designed in the form of ontology. Figure 2 shows the ontological formation of the I-RBAC model. A knowledge system must contain two key components – a good knowledge base and an excellent inference mechanism. Ontology is one of the most influential formal representations for knowledge in modern knowledge systems. Ontology has ability to express relationships among different entities under certain constraints of a domain. Additionally, it facilitates precise interpretation of data using semantic processing mechanism of inferring relationships among entities to enhance the usability and effectiveness of any decision support system. The first phase of this research work is to construct an ontology for access control and role mining in the I-RBAC model. Information extraction tools and techniques are used to automatically populate the organizational ontology from the policy text documents with the help of core ontology and bidirectional LSTM deep neural network. The extracted information is analyzed for duplication and stored in a knowledge base. In the second phase, the multi-agent system is developed to search and retrieve relevant facts from the ontology server to select and assign a proper role to the user.

C. THE I-RBAC CORE ONTOLOGY

The term ontology is a formal and explicit specification of shared concepts [48]. Ontology is used to model a phenomenon that is a collection of certain relevant concepts. It is machine understandable, constraints-defined and can be shared among different individuals. Ontology development should be simple, practical and according to the standard methodologies of software development. The ontology for I-RBAC model is formalized with the help of Protégé ontology editor. The classes of this ontology and their hierarchy are shown in Figure 2.

BusinessRoles class is the main class of the I-RBAC model's ontology in which 1300 occupations (roles) are included from the standard occupation classification (SOC), USA. These roles are classified according to the tasks performed by different users in different scenarios. These tasks have their relationship with certain set of permissions. These permissions are subdivided into actions (like copy, paste, update, delete, etc.) and resources (like files, folders, etc.). These resources are also classified according to their contents e.g. documents, audio, video, etc. We also introduce role states e.g. active, enabled, disabled, granted, denied, etc. This novel combination of classification of roles, actions, resources and states of roles enhances the process of role mining. We used departmental task hierarchy for our roles instead of junior or senior roles. Additionally, keeping in view that there are different types of organizational policies that help in role assignment, organizational policies are categorized as general policies, security policies and sharing policies in our I-RBAC model's ontology. The use of ontologies provides us scalability by adding a new class within the existing ontology. Our novel idea of developing an ontology for occupational roles is an important contribution of this research that addresses scalability issue for roles in RBAC as well as helps in mining semantic business roles.

D. ORGANIZATIONAL KNOWLEDGE EXTRACTION

Organizational policies describing roles and their task descriptions are usually given as text documents. Many information extraction tools are available that use machine learning techniques or predefined templates to extract information from text documents. However, information extraction from these documents is challenging because of varying structural and compositional styles of written documents along with countless vocabulary lists. We used bidirectional LSTM (Long Short Term Memory) deep neural network for extracting knowledge from policy text file. This extracted knowledge is in the form of RDF structured triples represented in the form of 'subject-predicate-object'. This LSTM network is initially trained using I-RBAC model's ontology. The knowledge obtained as output of LSTM network is further utilized to populate organizational ontology as XML document. The overall organizational knowledge extraction procedure is explained in following subsections.

1) ORGANIZATIONAL ONTOLOGY POPULATION

The organizational ontology is automatically learned from the knowledge extracted through the role and task description available in organizational policy text documents. This overall knowledge extraction and learning procedure is elaborated in Figure 3. Each definition of role and task is further broken down into sentences. The syntactic and semantic analysis of each sentence is done to recognize a pertinent knowledge. The syntactic analysis includes lemmatization, stemming and POS-tagging whereas the main components of the sentence (subject, predicate and object) are identified through word sense disambiguation and word embedding approach as applied in [49]. It includes the alignment between I-RBAC core ontology, as our top-level-ontology, and Wordnet 3.0 [50] which is a publically available lexical database.

The relationships among subject, predicate and object are discovered through semantic analysis which is done through a pre-trained deep neural network (NN) called bidirectional LSTM Network. Our approach is inspired by the work of [51]. In fact, our bidirectional LSTM Neural Network is already trained through I-RBAC model's core ontology. It learned roles, tasks and structural relationships between them under different domains. The output of semantic analysis is in the form of triplets ⟨subject, predicate, object⟩ which are the facts regarding roles, tasks, resources and the structural relationships among them. Finally, an XML file is generated from extracted triples and hence organizational policy is populated in an automated fashion.

2) UNIFIED ROLE EXTRACTION

Automatic ontology population helps to manage dynamically changing access control policies of the organization. This automatically learned organizational ontology is then matched with core ontology of the I-RBAC model in order to extract unified roles ontology which is subsequently stored in

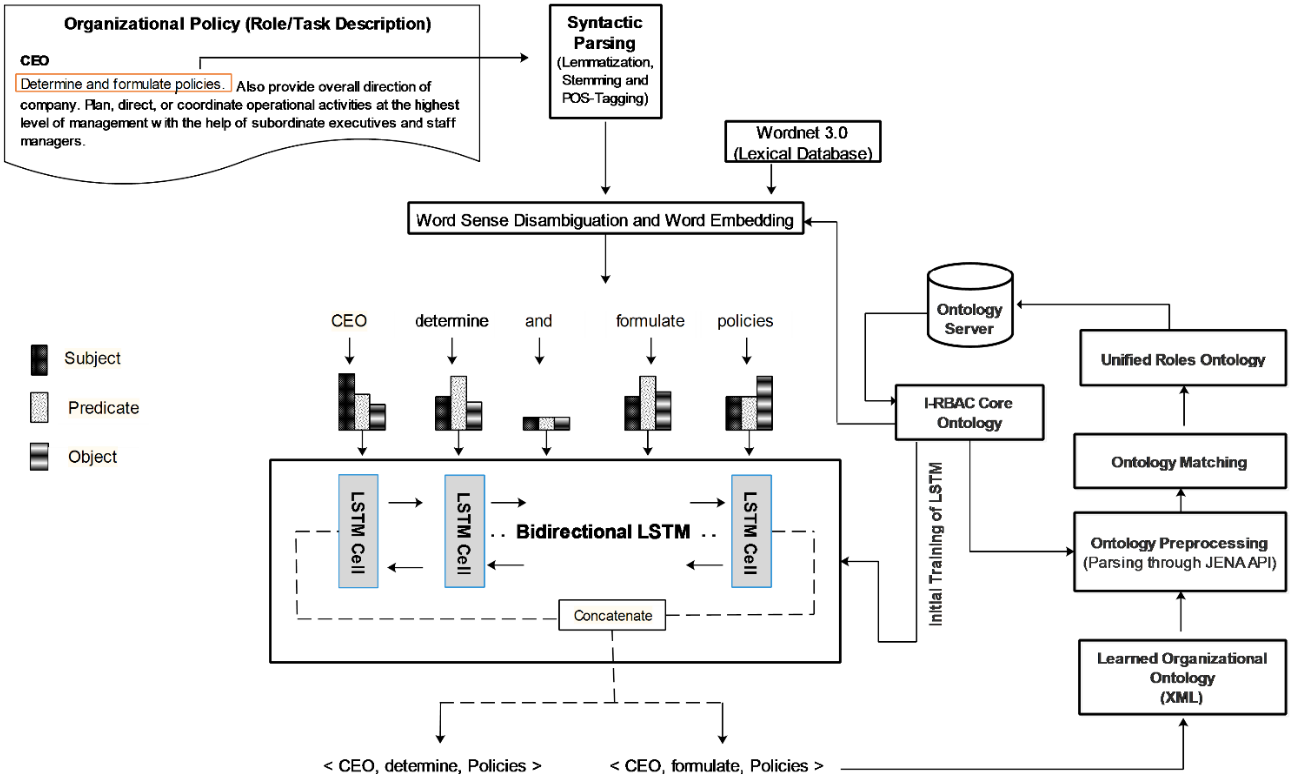
Organizational Policy (Role/Task Description)
CEO
Determine and formulate policies. Also provide overall direction of company. Plan, direct, or coordinate operational activities at the highest level of management w ith the help of subordinate executives and staff managers.
Syntactic Parsing (Lemmatization, Stemming and POS-Tagging)
Wordnet 3.0 (Lexical Database)
Word Sense Disambiguation and Word Embedding
CEO
determine
and
formulate
policies
Subject
Predicate
Object
LSTM Cell
LSTM Cell
.. Bidirectional LSTM ..
LSTM Cell
Concatenate
< CEO, determine, Policies >
< CEO, formulate, Policies >
Ontology Server
I-RBAC Core Ontology
Initial Training of LSTM
Unified Roles Ontology
Ontology Matching
Ontology Preprocessing (Parsing through JENA API)
Learned Organizational Ontology (XML)

FIGURE 3. Organizational knowledge extraction and ontology population.

the knowledge base on ontology server. In the next section, we are going to introduce multi-agent system for I-RBAC framework that make use of extracted roles ontology.

IV. I-RBAC MULTI-AGENTS SYSTEM ARCHITECTURE AND FRAMEWORK

The advancement in the field of ontology helps in knowledge management for different environments where agents can learn ontology and are capable for working in distributed environments. Ontology helps an agent to accomplish different tasks such as distribution and communication of collection of data in different environments as well as increased performance in information retrieval and knowledge extraction. This paper focuses on the problem of accessing and sharing knowledge in distributed heterogeneous environments and proposes a multi-agent system in which individual self-authorized agents work together and develop new facts. Due to several machines in a distributed system that are interacting with one another through the network, there is need for an autonomous entity that can manage and control the complex processing problems related to multiple environments. Thus, agent technology gains attention from the researcher community as it brings enhancements in different application areas.

Agent is an autonomous software entity [52] which has ability to observe and react according to its surrounding environment. In other words, agents have knowledge about their world. Agents follow certain available plans and their action are defined through some external stimulus and available information [53]. Ontology-based knowledge enhances the capabilities of agents to organize diverse data sets and give a uniform view. In multi-agent systems (MAS) numerous agents accomplish distinct tasks and operations in different capabilities. The advantages of MAS include customization based on individual organizational requirements, facilitating data integration, maintaining data security and integrity. The Foundation of Intelligent Physical Agents (FIPA) provides a standard open specification for developing agent-based applications [54]. FIPA open architecture provides MAS architecture, Agent Communication Language (ACL) and communication protocols.

The proposed core ontology for the I-RBAC model serves as knowledge base for agent. The agents are autonomous bodies equipped with knowledge about the domains and their policies. Agents extract knowledge from relationships among different classes of the ontology, object properties and data properties in the ontology to provide required access to resources and define appropriate roles. Ontology continues to evolve through learning the concepts and relationships. Agents are trained from the existing ontology and with the passage of time they improve their learning for decision making. In a multi-domain environment where different organizations are collaborating and sharing information/resources with each other, different agents are responsible for managing knowledge and performing organizational activities for its corresponding organization. Every agent has the following properties:

- Learning and classification mechanism for ontology.
- Acceptance and denial thoughts ($\mathrm{Th_k}$) with respect to that concept.
- Unique DomainConcepts denoted as $\mathrm{DC_i}$
- A set of features for representing concepts denoted as $\mathrm{FoC_i}$.
- Knowledge of core/base I-RBAC ontology denoted as BaseOnto.

So the overall I-RBAC model for particular organization is represented as:

$$I - RBAC(O_i) = \sum_{i=1}^{N} Agent_i\{\text{BaseOnto}, Th_i, DC_i, FoC_i\}$$

- Base Ontology (BaseOnto): JADE agents are capable of learning rules from ontology relationships. JENA framework helps in transforming relationships to rules. The agents learn these rules from BaseOnto and classify unseen concept of BusinessRoles and Tasks into predefined classes.
- Thoughts' Set ($\mathrm{Th_i}$): Ontology-based rules serve as thoughts for agents in decision making of granting or denying access to a particular user having certain roles.
- Features' Set ($\mathrm{FoC_i}$): Features are the factors that differentiate between concepts. Agents intelligently select corresponding features to identify a concept and to develop a comprehensive concept.
- Domain Concepts ($\mathrm{DC_i}$): It is the combination of Meta concepts and fine-grained concepts of ontology. Fine-grained concepts are achieved through the multi-level division of Meta concepts until an atomic concept is reached.

In collaborative scenario, all the organizations' agents require ontology-based semantic integration of data to resolve the differences that arise during the execution of agents in the system. These issues are resolved with the help of semantic mapping on ontology. Semantic mapping is concerned with finding solution while considering the relative concepts used in different domains. The adaptive nature of intelligent agent nurtures our system with autonomous bodies which enhances the adaptability of new and dynamic changes in access control policies. Through these capabilities, our proposed I-RBAC framework tries to resolve the issues of scalability, adaptability and dynamicity in RBAC for multiple domains.

The I-RBAC framework provides an intelligent agent-based authorization mechanism for multiple domains. System architecture for the I-RBAC model is proposed in the Figure 4 that combines different functionalities in a layered model. In the following, layers of the I-RBAC framework are described.

A. INTERFACE LAYER

The top layer provides an interface of the proposed I-RBAC framework using GUI components for users to interact with the system. It is connected to the second layer using multiple intelligent agents.

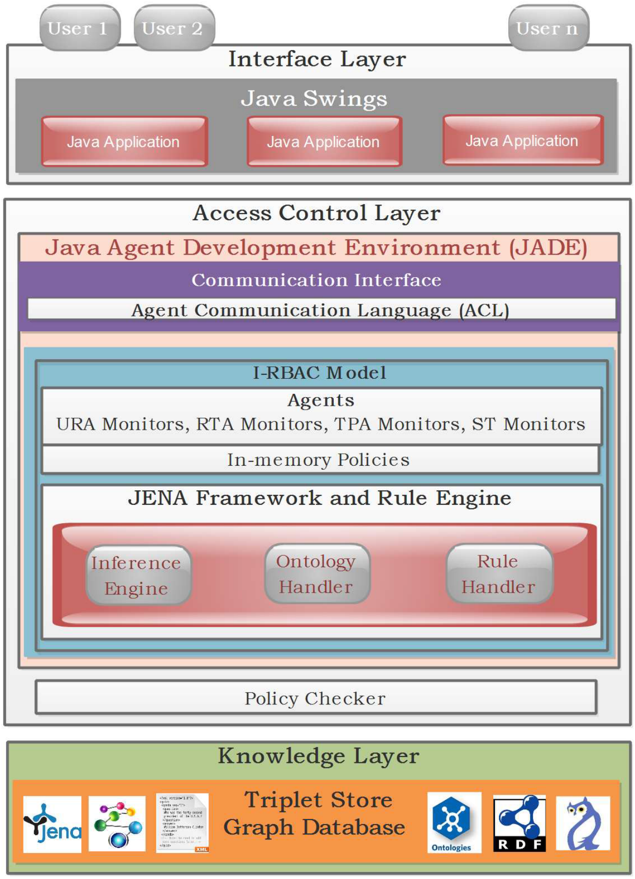

FIGURE 4. I-RBAC framework.

B. ACCESS CONTROL LAYER

Access control layer is responsible for overall security mechanism based on role assignment to different users in multiple organizations.

- Inference Engine: It generate rules from ontological relationships among different components of the I-RBAC model, i.e. users, roles, permissions, etc.
- Ontology and Rules Handlers: The Ontology handler and rule handler components are responsible for loading the knowledge base triplet store with data related to users/roles and data related to permissions/access control policy respectively in the form of RDF/XML files.
- I-RBAC Model: It is the main component of the I-RBAC system. It provides the base for whole I-RBAC policy that is permission to task assignment, task to role assignment and role to user assignment.
- Policy Checker: It performs user identification, processing and management of users, roles and permission information. Moreover, it also provides information about dynamically changing policy rules that helps in decision making of assigning new roles to users.
- RBAC states storage: It is an in-memory storage of intelligent agent in which the information of a user regarding her

assigned role and permissions related to her relevant tasks is maintained. This information is then permanently stored to a triplet store for further usage.

Agents provide all the services required to implement the I-RBAC model to generate RBAC states. The services of agent are described below.

- User-Role Assignment (URA) Monitors – a group of agents responsible of role assignment to users.
- Role-Task Assignment (RTA) Monitors – a group of agents responsible for task assignment to roles.
- Task-Permission Assignment (TPA) Monitors – a group of agents responsible for permission assignments to tasks.
- Session Tracking (ST) Monitors – a group of agents monitoring overall activities performed by users.

These monitors are multi-agent subsystems composed of intelligent agents. The agents are equipped with knowledge of organizational security policy and help to infer and assign a suitable role depending upon the tasks assigned to an employee. Policy Checker analyses the previous logs and current security policy to decide the access rights.

C. THE KNOWLEDGE LAYER

It provides knowledge base in the form of triplet store, graph databased. These ontologies help rule handler agents to extract rules / knowledge from knowledge base for further decision making about roles using inference engine.

The next section describes the complete process of authorization offered by the I-RBAC framework using intelligent agents.

V. IMPLEMENTATION AND RESULTS

This section describes implementation details of the proposed I-RBAC framework. In addition, it presents the results related to the performance of the I-RBAC model.

A. IMPLEMENTATION

In our system, the attributes related to roles are taken as textual information which formulate a Role Policy. The roles are created from policies under certain constraints specified in the policy documents already stored in the database. The I-RBAC framework describes the procedures of knowledge management and access decision. All the activities performed by the users and agents are stored in audit log as a corresponding access track function to further safeguard the multi-agent security. Authorization module is responsible for overall role assignment to get access to the shared resources under certain constrains at the beginning of the system. At runtime, the information of the roles with the changing task and role status is also recorded dynamically in the triplet store.

The following components form the core of the I-RBAC framework and authorization shown in the Figure 5.

- Policy Framework: It is designed as a separate module running on remote system. It helps in making access decision to the particular resources. Policies are defined using RDF/XML and are also residing on the same system.
- Agent Container (JADE server): It deals with the creation of agents and handles all the activities of the agents, like assigning different tasks to the agents, performing dynamic changes to the policies and granting permission to different agents.
- Logon Module (JADE-S server): It deals with the authentication of the users and agents. It provides additional security to the JADE agents along with the predefined security provided by JADE implemented with FIPA compliance.
- Database: It is a storage space for the I-RBAC states.
- Triplet Store: It is a storage space for ontologies in RDF/XML format.
- Authorization Module: It is responsible for the overall function of providing authorization to the authenticated users. This takes request from the user and finally respond back either with acceptance or rejection to the user request.
- User: An agent working on behalf of a user who wants to access certain resources.
- Policy Enforcement Agent (PEA): This agent is responsible to take request from the user along with the credentials of the user and pass them to the other corresponding agents like PDA.
- Policy Decider Agent (PDA): This agent takes request from the PEA and asks PIA for policies to decide the access to the certain resources and sends back the response to the PEA.
- Policy Interpreter Agent (PIA): This agent is a part of the Interpretation Module and performs interpretation task upon the policies to transform them into rules about the specific users and tasks.
- Interpretation Module: This module is designed to tackle the transformation of policies into an access control list (ACL) format which are further used by authorization module and corresponding agents.
- Admin Agent: This agent is administrating the overall activities of the agents.
- Administrator: It is a user that is responsible for the providing updated policies into the system.

All the users in the organization are assigned roles based upon their tasks in the domain. The administrator defines the access control policies for user roles. The user requests an access to a particular resource to complete the assigned task and this request goes through a series of steps as shown in the Figure 5. Agents in the system work together for handling this request on the basis of changing policies and complete the process of granting/denying access privileges to the requested user. There are different roles according to different tasks. This makes the system and access control policies dynamic and flexible.

1) I-RBAC STATES FORMATION

The I-RBAC framework mainly focuses on the process of role discovery i.e. role engineering and role assignment

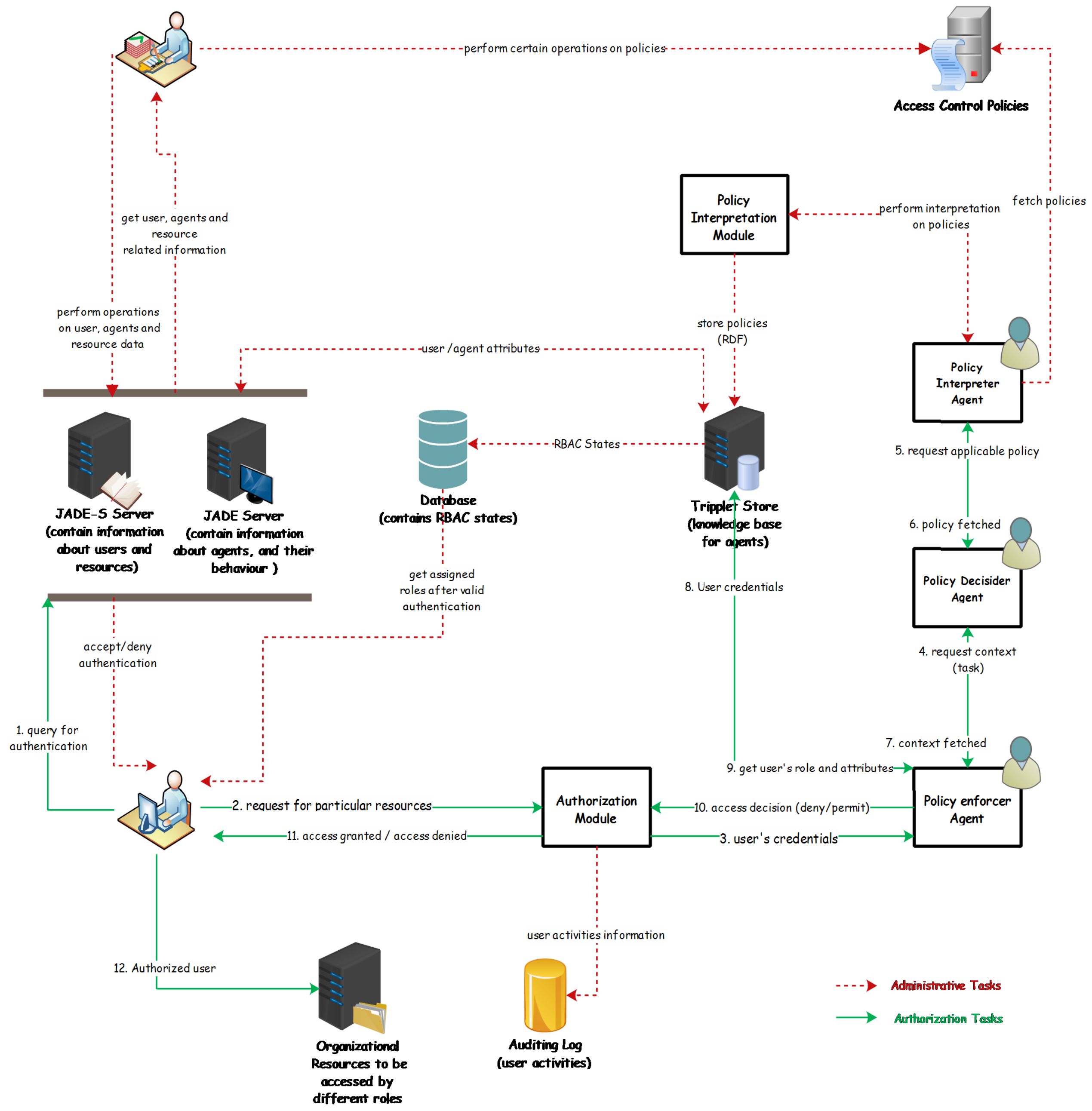
perform certain operations on policies
Access Control Policies
fetch policies
perform interpretation on policies
Policy Interpretation Module
get user, agents and resource related information
perform operations on user, agents and resource data
store policies (RDF)
user /agent attributes
Policy Interpreter Agent
RBAC States
JADE-S Server (contain information about users and resources)
JADE Server (contain information about agents, and their behaviour)
Database (contains RBAC states)
Tripplet Store (knowledge base for agents)
5. request applicable policy
6. policy fetched
Policy Decisider Agent
get assigned roles after valid authentication
8. User credentials
accept/deny authentication
4. request context (task)
1. query for authentication
7. context fetched
9. get user's role and attributes
2. request for particular resources
Authorization Module
10. access decision (deny/permit)
Policy enforcer Agent
11. access granted / access denied
3. user's credentials
user activities information
12. Authorized user
Administrative Tasks
Authorization Tasks
Organizational Resources to be accessed by different roles
Auditing Log (user activities)

FIGURE 5. I-RBAC framework implementation scenario.

through role mining. The functionality of these processes is described below as flow chart in the Figure 6 that describes the process of role discovery from a given policy text file as input that contains information about the organizational policies and user roles (e.g., policy documents). Algorithm 1 provides a generic algorithm for role engineering (Role creation) process. After pre-processing of the input policy file, features (rules) are extracted from a policy file that describe which organizational role can be performed having some specific rights (group of permissions). These extracted features further become input for role generating, role hierarchy optimization and role classification algorithms. The final output of this phase is candidate role list (business roles). These roles are to be assigned to users based on their profile and designation assignments.

The candidate business roles list helps system administrators to choose a suitable role and assign it to the user. In the process of role assignment, every user is assigned a single business role i.e. job title. Whenever the user is assigned a new task within organizations or across the organization, there is need to map her role accordingly. Therefore, in this process input is a role list and assigned set

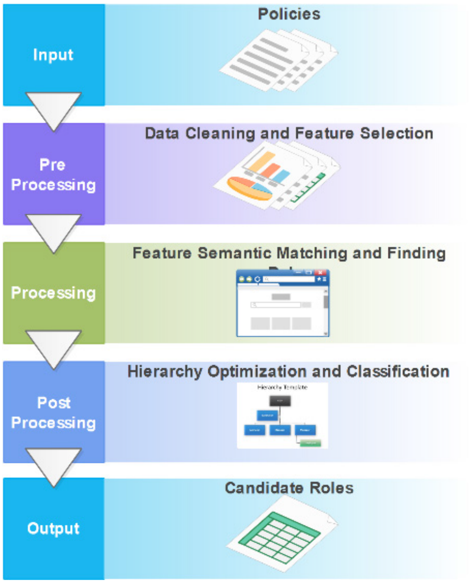
Input
Policies
Pre Processing
Data Cleaning and Feature Selection
Processing
Feature Semantic Matching and Finding Roles
Post Processing
Hierarchy Optimization and Classification
Output
Candidate Roles

FIGURE 6. Role engineering process.

Algorithm 1 Role Creation

```
Input: Policy File (PF)
Output: Candidate Role List (CRL)
begin
    read (PF)
    $cleanedPF = cleanData(PF)$
  $extractedFeatures = selectFeature(cleanedPF)$
      namedroles
      $= semanticMatch(extractedFeatures)$
    $hierarchy = concludeHierarchy(namedRoles)$
    $CRL = classifyRoles(extractedFeatures)$
end
```

of tasks to a user taken from task profile and user profile. Finally, I-RBAC states are generated using different policy ontology mapping/matching, and role mapping algorithms. Figure 7 describes over all flow of role assignment process. Algorithm 2 provides a generic algorithm for role mining and role assignment process. Role assignment algorithm is dynamically started each time a user is assigned a different task. It maps user and task profiles to know the exact access permission requirements of the task. It then matches these requirements with candidate role list and finds the best matching role (using relevant ontology). The one or more matched roles are dynamically assigned to the user through user role assignment process (URA) that are needed to complete an assigned task. The changes are updated in the proposed I-RBAC model as new I-RBAC states that become active for user to perform new actions.

B. RESULTS

Experiments are performed on the proposed I-RBAC model to measure its performance. The evaluation of access control models is mostly performed by calculating their runtime for a number of data elements used in the model. Most of the times, these data elements are permission assignments [51]. Comparative evaluation with other models is usually not performed due to the fact that each model uses different number of data elements, so the comparison becomes meaningless. The I-RBAC model uses task and task-role elements which are not part of the core RBAC standard and do not exist

Algorithm 2 Role Assignment

```
Input: CRL, Task Profile(TP), User Profile (UP)
Output: RBAC states[...]
begin
  read (CRL, TP, UP)
  proposedRoles[ ]
      $= getRole(roleMapping(CRL,$
          $matchPolicy(CRL,mapPolicy($
          $UP,TP))))$
    $URA = proposedRole[1|2..|n]$
    I-RBAC[ ]
      $= updateUserProfile(U,R,T, URA, RTA, TPA)$
end
```

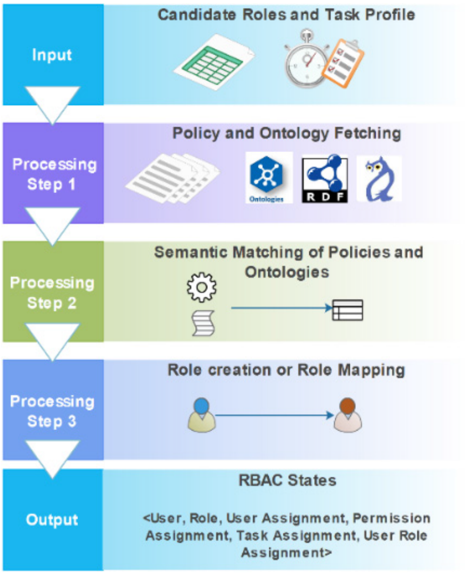
Input
Candidate Roles and Task Profile
Processing Step 1
Policy and Ontology Fetching
Ontologies
RDF
Processing Step 2
Semantic Matching of Policies and Ontologies
Processing Step 3
Role creation or Role Mapping
Output
RBAC States
<User, Role, User Assignment, Permission Assignment, Task Assignment, User Role Assignment>

FIGURE 7. Role mining and role assignment.

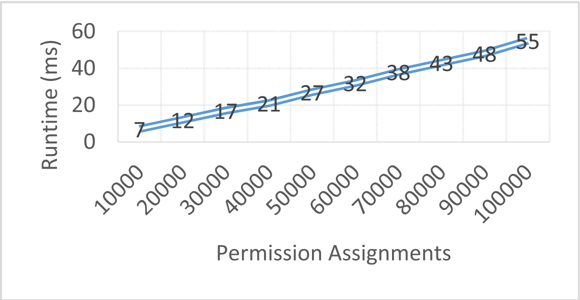

FIGURE 8. Runtime with varying number of permission assignments.

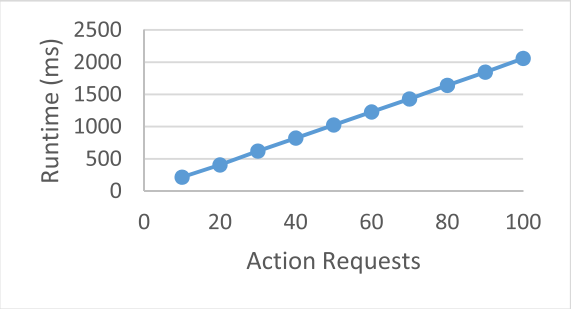

FIGURE 9. Runtime of concurrent action requests.

in most of the other models. Permission assignments are the access control rules that need to be evaluated on every access request. Evaluation of the large number of permission assignments may affect the performance of an access control model. The proposed I-RBAC model is executed using large set of permission assignments and other data elements related to components of the I-RBAC model to measure its performance. Permission assignments are gradually increased from 10000 to 100000 to measure the changes in runtime of the model. The number of roles used for the experiments are 1300 as described in the dataset of roles provided by Standard Occupational Classification (SOC), USA [47]. Different types of nested queries and subqueries are executed, and their average runtime is calculated to determine the performance of the I-RBAC model. The Figure 8 shows runtime of the I-RBAC model using different number of permission assignments. It shows that runtime is linear for very large number of permission assignments, thus resulting in computational complexity of O(n). Execution time for different number of action requests is also calculated and its results are presented in the Figure 9 which again shows a linear runtime trend. These results show that the I-RBAC model can be effectively used with large number of permission assignments and many concurrent user requests.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have focused on the need for a security mechanism that can support today's dynamically changing environments and presented our proposed I-RBAC model and framework which fulfills these requirements. The proposed access control framework provides an approach to solve the issue of security in distributed environments through intelligent multi-domain access control. The proposed I-RBAC framework is a general multi-agent system based on RBAC for providing access to organizational assets with semantic roles. Semantic roles are actually the occupational titles from different organizations. The concepts of task-dependent roles activation and deactivation are introduced by associating them with certain attributes of user, roles, actions and objects. Likewise, the concepts of monitor agents are presented that are actually a group of agents to handle a certain activity in the whole I-RBAC multi-agent framework. These activities are role creation, role mining and role assignment depending upon the associated task information about the user.

Furthermore, the concept of knowledge management through ontology for proposed model is introduced in order to achieve dynamicity and scalability. The security policy is also considered in the ontology of the model for defining and enforcing dynamic access control rules having sets of tasks, types of permissions from a set of actions and objects. In this model, agents can handle dynamic role assignment under certain specified role constraints in the reformed policy. Our proposed I-RBAC framework uses real world dataset for creating roles with business semantics. The ontologies have abilities to reason and help in access control decision making and also provide semantic interoperability. Generality for handling multiple domains is added through business roles class. Intelligent agents provide the dynamicity and can acquire the changed environments. The formal description of the model and a prototype implementation architecture of our framework has also been presented and tested with large data. The experiments used up to 100,000 permission assignments (access control rules) for business roles from different domains (like we chose our academic departments, finance department, taxation department, private banks and life insurance organizations, police department, smart city project's department. etc.) to perform collaborative tasks in distributed environment. The experimentation was performed up to 100 concurrent action requests. The results of these experiments validated the proposed framework for such large data in terms of linear runtime (in fact, less than 60 ms with 100,000 permission assignments and around 2000 ms for 100 concurrent action requests).

The acquired knowledge by the core ontology of the I-RBAC model is based upon latest version of SOC (Standard Occupational Classification) List [47]. This list reached to 1300 occupational/business roles up till now. However, in futue, if the list is more refined then I-RBAC core ontology can be improved which will subsequently result in fine-grained access control features in order to assign more precise roles. Moreover, although we tested our model for large enough permission assignments and concurrent action requests, it needs testing on even larger scale with different scenarios which is our plan for the future.

REFERENCES

[1] H. Huang, F. Shang, J. Liu, and H. Du, "Handling least privilege problem and role mining in RBAC," *J. Combinat. Optim.*, vol. 30, no. 1, pp. 63–86, Jul. 2015.

[2] P. Samarati and S. C. de Vimercati, "Access control: Policies, models, and mechanisms," in *Proc. Int. School Found. Secur. Anal. Design*, 2000, pp. 137–196.

[3] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Trans. Inf. Syst. Secur. (TISSEC)*, vol. 4, no. 3, pp. 224–274, Aug. 2001.

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

[5] L. Fuchs, G. Pernul, and R. Sandhu, "Roles in information security—A survey and classification of the research area," *Comput. Secur.*, vol. 30, no. 8, pp. 748–769, Nov. 2011.

[6] A. Colantonio, R. Di Pietro, and N. V. Verde, "A business-driven decomposition methodology for role mining," *Comput. Secur.*, vol. 31, no. 7, pp. 844–855, Oct. 2012.

[7] A. Colantonio, R. Di Pietro, A. Ocello, and N. V. Verde, "A formal framework to elicit roles with business meaning in RBAC systems," in *Proc. 14th ACM Symp. Access Control Models Technol.-SACMAT*, New York, NY, USA, 2009, pp. 85–94.

[8] I. Molloy, H. Chen, T. Li, Q. Wang, N. Li, E. Bertino, S. Calo, and J. Lobo, "Mining roles with semantic meanings," in *Proc. 13th ACM Symp. Access Control Models Technol.-SACMAT*, New York, NY, USA, 2008, pp. 21–30.

[9] A. Colantonio, R. Di Pietro, A. Ocello, and N. V. Verde, "A new role mining framework to elicit business roles and to mitigate enterprise risk," *Decis. Support Syst.*, vol. 50, no. 4, pp. 715–731, Mar. 2011.

[10] S. N. Chari, I. M. Molloy, and Y. Park, "Role mining with user attribution using generative models," U.S. Patent 8 983 877, Mar. 17, 2015.

[11] Z. Xu and S. D. Stoller, "Algorithms for mining meaningful roles," in *Proc. 17th ACM Symp. Access Control Models Technol.-SACMAT*, New York, NY, USA, 2012, pp. 57–66.

[12] A. Colantonio, R. Di Pietro, A. Ocello, and N. V. Verde, "Mining business-relevant RBAC states through decomposition," in *Proc. IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2010, pp. 19–30.

[13] B. Mitra, S. Sural, J. Vaidya, and V. Atluri, "A survey of role mining," *ACM Comput. Surv. (CSUR)*, vol. 48, no. 4, pp. 1–37, Feb. 2016.

[14] N. Badar, J. Vaidya, V. Atluri, N. V. Verde, and J. Warner, "Using classification for role-based access control management," *Int. J. Technol. Policy Manag.*, vol. 16, no. 1, p. 45, 2016.

[15] J. Hu, K. M. Khan, Y. Zhang, Y. Bai, and R. Li, "Role updating in information systems using model checking," *Knowl. Inf. Syst.*, vol. 51, no. 1, pp. 187–234, Apr. 2017.

[16] R. Ghazal, A. K. Malik, N. Qadeer, and M. Ahmed, "Intelligent multi-domain RBAC model," in *Proc. Innov. Solutions Access Control Manage., IGI Global*, 2016, pp. 66–95.

[17] D. Wu, X. Chen, J. Lin, and M. Zhu, "Ontology-based RBAC specification for interoperation in distributed environment," in *Proc. Asian Semantic Web Conf.*, 2006, pp. 179–190.

[18] E. J. Coyne, "Role engineering," in *Proc. 1st ACM Workshop Role-Based Access Control*, 1996, p. 4.

[19] M. Frank, A. P. Streich, D. Basin, and J. M. Buhmann, "A probabilistic approach to hybrid role mining," in *Proc. 16th ACM Conf. Comput. Commun. Secur.-CCS*, New York, NY, USA, 2009, pp. 101–111.

[20] S. Oh and S. Park, "Task-role-based access control model," *Inf. Syst.*, vol. 28, no. 6, pp. 533–562, 2003.

[21] B. Wang and S. Zhang, "An organization and task based access control model for workflow system," in *Advances in Web and Network Technologies, and Information Management*. Berlin, Germany: Springer, 2007, pp. 485–490.

[22] R. A. Zuniga and S. Festin, "A design for task-role based access control for personal health record systems," *Philippine Eng. J.*, vol. 38, no. 1, pp. 27–38, 2017.

[23] X. H. Le, T. Doll, M. Barbosu, A. Luque, and D. Wang, "An enhancement of the role-based access control model to facilitate information access management in context of team collaboration and workflow," *J. Biomed. Informat.*, vol. 45, no. 6, pp. 1084–1107, Dec. 2012.

[24] Y. Asim, A. K. Malik, W. Naeem, S. Rathore, and B. Raza, "Community-centric brokerage-aware access control for online social networks," *Future Gener. Comput. Syst.*, to be published.

[25] W. Bai, Z. Pan, S. Guo, and Z. Chen, "RMMDI: A novel framework for role mining based on the multi-domain information," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Jun. 2019.

[26] W. Sun, S. Wei, H. Guo, and H. Liu, "Role-mining optimization with separation-of-duty constraints and security detections for authorizations," *Future Internet*, vol. 11, no. 9, p. 201, Sep. 2019.

[27] W. Sun, H. Su, and H. Liu, "Role-engineering optimization with cardinality constraints and user-oriented mutually exclusive constraints," *Information*, vol. 10, no. 11, p. 342, Nov. 2019.

[28] X. Ma, R. Li, and Z. Lu, "Role mining based on weights," in *Proc. 15th ACM Symp. Access Control Models Technol.-SACMAT*, New York, NY, USA, 2010, pp. 65–74.

[29] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," *J. Mach. Learn. Res.*, vol. 3, pp. 993–1022, Mar. 2003.

[30] M. Rosen-Zvi, C. Chemudugunta, T. Griffiths, P. Smyth, and M. Steyvers, "Learning author-topic models from text corpora," *ACM Trans. Inf. Syst. (TOIS)*, vol. 28, no. 1, pp. 1–38, Jan. 2010.

[31] I. Molloy, Y. Park, and S. Chari, "Generative models for access control policies: Applications to role mining over logs with attribution," in *Proc. 17th ACM Symp. Access Control Models Technol.-SACMAT*, 2012, pp. 45–56.

[32] M. Kuhlmann, D. Shohat, and G. Schimpf, "Role mining–revealing business roles for security administration using data mining technology," in *Proc. 8th ACM Symp. Access Control Models Technol.-SACMAT*, New York, NY, USA, 2003, pp. 179–186.

[33] F. De La Prieta, S. Rodríguez-González, P. Chamoso, J. M. Corchado, and J. Bajo, "Survey of agent-based cloud computing applications," *Future Gener. Comput. Syst.*, vol. 100, pp. 223–236, Nov. 2019.

[34] H. Idrissi, M. Ennahbaoui, E. M. Souidi, A. Revel, and S. Elhajji, "Access control using mobile agents," in *Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS)*, Apr. 2014, pp. 1216–1221.

[35] G. Navarro, J. Borrell, J. A. Ortega-Ruiz, and S. Robles, "Access control with safe role assignment for mobile agents," in *Proc. 4th Int. Joint Conf. Auto. Agents Multiagent Syst.-AAMAS*, 2005, pp. 1235–1236.

[36] A. Moreno and D. Isern, "Accessing distributed health-care services through smart agents," in *Proc. 4th IEEE Int. Workshop Enterprise Netw. Comput. Health Care Ind. (HealthCom)*, Nancy, France, 2002, pp. 34–41.

[37] A. Upadhyay and M. Rai, "Application of mobile agents for security using multilevel access control," *Int. J. Tech. Res. Appl.*, vol. 2, no. 4, pp. 225–230, Jul./Aug. 2014.

[38] D. Isern and A. Moreno, "Distributed guideline-based health care system," in *Proc. 4th Int. Conf. Intell. Syst. Design Appl., (ISDA)*, 2004, pp. 145–150.

[39] C. Santos-Pereira, A. B. Augusto, R. Cruz-Correia, and M. E. Correia, "A secure RBAC mobile agent access control model for healthcare institutions," in *Proc. 26th IEEE Int. Symp. Comput.-Based Med. Syst.*, Jun. 2013, pp. 349–354.

[40] O. Chira, C. Chira, T. Roche, D. Tormey, and A. Brennan, "An agent-based approach to knowledge management in distributed design," *J. Intell. Manuf.*, vol. 17, no. 6, pp. 737–750, Dec. 2006.

[41] D. Schmidt, R. H. Bordini, F. Meneguzzi, and R. Vieira, "An ontology for collaborative tasks in multi-agent systems," in *Proc. ONTOBRAS*, 2015.

[42] M. Viroli, A. Omicini, and A. Ricci, "Infrastructure for RBAC-MAS: An approach based on agent coordination contexts," *Appl. Artif. Intell.*, vol. 21, nos. 4–5, pp. 443–467, Apr. 2007.

[43] A. P. Marikkannu, J. Adri Jovin, and A. T. Purusothaman, "FaultTolerant adaptive mobile agent system using dynamic role based access control," *Int. J. Comput. Appl.*, vol. 20, no. 2, pp. 1–6, May 2011.

[44] I. Saenko and I. Kotenko, "Genetic algorithms for role mining problem," in *Proc. 9th Int. Euromicro Conf. Parallel, Distrib. Netw.-Based Process.*, Feb. 2011, pp. 646–650.

[45] I. Saenko and I. Kotenko, "Using genetic algorithms for design and reconfiguration of RBAC schemes," in *Proc. 1st Int. Workshop AI Privacy Secur.*, 2016, p. 4.

[46] *O*NET OnLine*. Accessed: Aug. 13, 2018. [Online]. Available: https://www.onetonline.org/

[47] *2018 Standard Occupational Classification System*. Accessed: Mar. 13, 2019. [Online]. Available:https://www.bls.gov/soc/2018/major_groups.htm

[48] G. Singh and V. Jain, "Information retrieval (IR) through semantic Web (SW): An overview," 2014, *arXiv:1403.7162*. [Online]. Available: https://arxiv.org/abs/1403.7162

[49] D. Schmidt, R. Basso, C. Trojahn, and R. Vieira, "Matching domain and top-level ontologies exploring word sense disambiguation and word embedding," in *Proc. Ontol. Matching (OM ISWC Workshop)*, 2018, p. 1.

[50] *Wordnet*. Accessed: Feb. 10, 2019. [Online]. Available: https://wordnet.princeton.edu

[51] Y. Liu, T. Zhang, Z. Liang, H. Ji, and D. L. McGuinness, "Seq2RDF: An end-to-end application for deriving triples from natural language text," in *Proc. 17th Int. Semantic Web Conf.*, 2018.

[52] M. Wooldridge, *An Introduction to Multiagent Systems*. Hoboken, NJ, USA: Wiley, 2009.

[53] T. Farrenkopf, M. Guckert, and N. Urquhart, "AGADE using personal preferences and world knowledge to model agent behaviour," in *Proc. Int. Conf. Practical Appl. Agents Multi-Agent Syst.*, 2015, pp. 93–106.

[54] G. Santos, T. Pinto, H. Morais, T. M. Sousa, I. F. Pereira, R. Fernandes, I. Praça, and Z. Vale, "Multi-agent simulation of competitive electricity markets: Autonomous systems cooperation for European market modeling," *Energy Convers. Manage.*, vol. 99, pp. 387–399, Jul. 2015.

RUBINA GHAZAL received the M.S. degree in computer science from the University of Agriculture, Faisalabad, Pakistan, in 2004. She is currently pursuing the Ph.D. degree in computer science with COMSATS University Islamabad (CUI), Islamabad, Pakistan. She has been an Assistant Professor with the University Institute of Information Technology, Pir Maher Ali Shah Arid Agriculture University, Rawalpindi, Pakistan, since 2006. She was a Lecturer with the University of Agriculture Faisalabad, from 2002 to 2005. Her research interests include role-based access control, multiagent systems, and semantic Web technologies.

AHMAD KAMRAN MALIK received the M.S. and M.Sc. degrees in computer science and the Ph.D. degree from the Vienna University of Technology (TU-Wien), Vienna, Austria. He is currently an Assistant Professor with COMSATS University Islamabad (CUI), Islamabad, Pakistan. He has published numerous research articles in international journals and conferences. His current research interests include data science, information security, access control, and social network analysis.

NAUMAN QADEER received the B.Sc. and M.Sc. degrees in computer science from Bahauddin Zakariya University, Multan, Pakistan, in 1998 and 2001, respectively, and the M.S. degree in computer science from the University of Agriculture, Faisalabad, Pakistan, in 2004. He was a Lecturer with the University of Agriculture, from 2002 to 2005. He has been a Lecturer with the Federal Urdu University for Arts, Science, and Technology, Islamabad, Pakistan, since 2005. His research interests include multiagent systems, robotics, image processing, and deep neural networks.

BASIT RAZA received the Ph.D. degree in computer science from International Islamic University, Islamabad, Pakistan, in 2014. He is currently an Assistant Professor with the Department of Computer Science, COMSATS University Islamabad (CUI), Islamabad. He has published a number of conference and journal articles of international repute. His research interests include database management systems, security and privacy, data mining, data warehousing, machine learning, and artificial intelligence.

AHMAD RAZA SHAHID received the Ph.D. degree in computer science from York, U.K., in 2012. During the Ph.D. degree, he was involved in automatically building a WordNet for four languages, namely, English, German, French, and Greek. After the Ph.D. degree, he has been involved in the areas of computer vision and pattern recognition, machine learning, and natural language processing. He is currently an Assistant Professor with the COMSATS Institute of Information Technology, COMSATS University Islamabad, Islamabad, Pakistan. He was involved in a few of the problems that include cancer detection, pedestrian detection, driver fatigue detection, and data mining.

HANI ALQUHAYZ received the bachelor's degree in computer science and the master's degree in information systems management from King Saud University and the Ph.D. degree in computer science from De Montfort University, U.K. He is currently an Assistant Professor with the Computer Science Department, College of Science, Majmaah University, Saudi Arabia. His research interests include wireless security, scheduling, image processing, the IoT, security and privacy, data mining, machine learning, and artificial intelligence. He has authored several papers in high-impacted journals such as IEEE ACCESS, *Sensors*, and *Wireless Communications and Mobile Computing*.