Pratibha International Interdisciplinary Journal – Vol. 01, Issue 01, April-June 2025. ISSN-XXX-XXX

Trustworthy Computing in the Dynamic IoT Cloud Resort to Resource and Role Hierarchy Based Access Control Model

Dr. Shilpa B. Sarvaiya[1]
[1]Department of MCA, Vidya Bharati Mahavidyalaya, Amravati
Corresponding author: sarvaiya.shilpa@gmail.com

****

ABSTRACT

A provider of cloud computing services that offers public cloud solutions can expand its offerings to the Internet of Things (IoT) sector by allowing third parties to utilize its infrastructure. This enables the integration of IoT data and/or computational components that function on IoT devices. In this paper, we consider the issues of reliable computing for the dynamic IoT Cloud using Role based access control model. The access control model serves as the essential element in reliable computing. Over the past several decades, numerous access control models have been created, and of all these models, the role-based access control (RBAC) model is the most commonly implemented in businesses and various organizations. Here, first, we introduce the vertical and horizontal computing structures in the extended IoT Cloud where IoT devices, Edge, Fog, and Cloud are integrated in a layered infrastructure. Then we design a framework and mechanisms for performing trusty computing making use of the vertical IoT Cloud to secure the IoT Cloud in vertical and horizontal computation structures. Specifically, we discuss a general trusty computing pattern in the IoT Cloud using RRBAC. Our model offers greater extensibility, flexibility, and adaptability. Our theoretical analysis result show that this model can effectively provide dynamic and secure access control model.

Keywords:IoT, IoT Cloud, Edge Computing, Fog Computing, Access Control, Role-based control model (RBAC).

****

Introduction

The technologies associated with the Internet of Things (IoT) are advancing at a swift pace. Current estimates suggest that there are tens of billions of physical devices linked to the Internet, and this figure continues to increase rapidly. Numerous applications for IoT are currently under development. With the growing number of deployments of IoT systems and variations of IoT applications, IoT computing structure is becoming increasingly complex. To support real-time big data analytics for processing data generated by IoT devices in the physical world, the research community has explored the vertical data/computing structure, which spans from IoT devices to edge gateways, to fog networks, and to the clouds. The paths for data/computation could be pre-built statically or established dynamically. Also, dynamically arising tasks demand discovery and cooperation of IoT capabilities in the neighbourhood in real time, which implies the need for edge based horizontal data/computation structure in the IoT Cloud. Security is an important issue in the IoT Cloud infrastructure. With various computing scenarios in the IoT world, there are different issues related to security and trustworthy computing. When dynamic data/computing flow structures are considered, the security of the system becomes more challenging [1]. In this paper, we consider the methods for achieving trustworthy computing in the vertical and horizontal IoT infrastructure resort to RRBAC (Resource and Role hierarchy Based Access Control) model. Role-based access control (RBAC), this policy is very simple to use. In RBAC roles are assigned by the system administrator statically. In which access is controlled depending on the roles that the users have in a system. Access control is the most fundamental component in trustworthy computing. Many access control models have been extensively investigated in the literature and they can be used in IoT Cloud. However, due to the large number of IoT resources and their diverse properties, privilege assignment could be an issue.

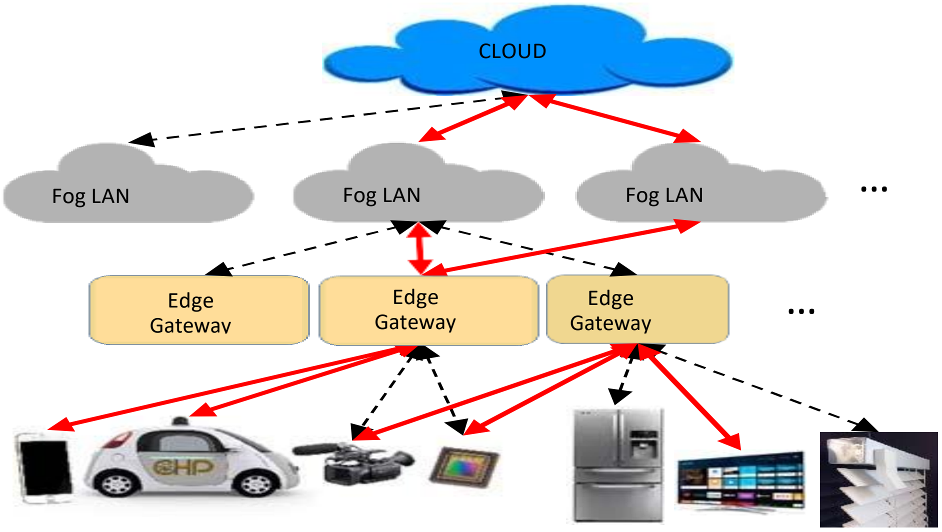
We consider the resource hierarchy to organize the IoT resource and use an RRBAC (Resource and Role hierarchy Based Access Control) model for access control in IoT Cloud. Another issue in the IoT Cloud is its open and dynamic nature. We discuss the general framework for performing trustworthy computing in the vertical IoT Cloud and use two examples, intrusion detection and certificate authority, to illustrate the idea. In any IoT Cloud computation, in the vertical or horizontal structures, there will be information flow through a sequence of computing resources, which may be trustworthy under the potentially untrustworthy IoT Cloud infrastructure. The rest of this paper is organized as follow. In Section 2, we discuss the IoT cloud infrastructure and the vertical and horizontal computation structures in this infrastructure. Section 3 discusses the trustworthy computing issues in IoT cloud and how to perform trustworthy computing in the vertical IoT cloud structure. An advanced access control and policy specification model is introduced in Section 4 for IoT cloud with high mobility. Section 5concludes the paper.

IOT Cloud Infrastructure

IoT devices are being deployed at an increasing rate. A majority of these IoT devices are sensors and they continuously generate a large amount of data [2]. Generally, IoT devices have limited computing power and storage space, and require power management to prolong their battery lives. Thus, they are not suitable to store and process the data continuously generated by themselves. Cloud provides enormous computing and storage capacities which offers an effective and economic platform for IoT data processing and storage. However, the centralized nature of the cloud data centres brings potential concerns for IoT computing. The wide-area network (WAN) bandwidth is limited and transferring the large amount of data from the IoT devices to the cloud can causes severe latency. With the increasing number of IoT devices, the WAN can be highly congested, further causing delays. Many IoT systems collect data for real-time decision making, and the significant latency can make the decisions meaningless. To resolve the network latency problem, edge and fog computing solutions have been proposed for the IoT cloud. Edge and fog computing take the computation away from the central cloud to the edge [3, 4]. Edge nodes generally serve as the gateway for the IoT devices and can perform some preliminary computations. Fog Computing is coined by CISCO, which is a mini-scale cloud that sits beneath the Cloud and much closer to the edge [5]. In this section, we discuss two IoT cloud computing structures, vertical and horizontal, that make use of the extended IoT cloud infrastructure.

Vertical IoT Cloud Infrastructure

Due to the limited computing resources on the edge nodes and fog LANs, they cannot always stand alone to perform all the computations on the continuous data streams from the IoT devices. Thus, the layered infrastructure, from IoT devices, to the edge gateways, to the fog LANs, and to the cloud should be integrated to provide real time and powerful computation for the IoT systems. This “vertical IoT cloud computing structure” is depicted in Figure 1. Continuous data generated from the IoT devices are streamed to the edge, fog, and cloud. Computations are decomposed such that preliminary decisions can be made on the nearby edge nodes and fog LANs. The cloud can handle intensive computations and globalized data processing. The layered vertical IoT cloud could have static or dynamic data/computation structures. In a static setting, the IoT devices are connected to a specific edge gateway. Each specific edge gateway is connected to a specific fog LAN. The fog LAN then connects to a specific cloud. However, a static configuration could incur resource underutilization, have unbalanced load, and be prone to single-point failures. Thus, it is frequently desirable to have dynamic IoT cloud configurations. The dynamic vertical IoT cloud structure is illustrated in Figure 1, where the black dotted lines are the default connections and the red lines represent the dynamically selected connections for non-dedicated data and computation flow paths.



◄- - - - -►
Default infrastructure link

◄━━━►Horizontal Edge-to-Edge connections

Figure1: Vertical IoT Cloud Computing Structure.

Horizontal IoT Cloud Infrastructure

In the vertical IoT cloud, we consider the dynamics in forming the data/computing flow paths for processing the continuous IoT data streams. However, there are additional dynamics in the IoT cloud. Many existing IoT systems, such as smart homes, smart buildings, smart manufacturing, etc., are built statically. These systems consider a set of pre- selected IoT devices at known locations and control devices to perform some predefined tasks and handle some anticipated events. In order to make the best use of the available IoT capabilities, we need to consider handling dynamically arising tasks in IoT systems. Service computing techniques, including IoT service discovery and composition can be used to dynamically discover and compose IoT capabilities to handle the dynamic tasks, and this has to be done by nearby IoT resources and in real time. We consider an edge-centric horizontal IoT cloud computing structure for peer-to-peer IoT service discovery, composition, and execution. The horizontal edge structure cannot standalone either. For example, in order to perform access control during service execution, we may need the assistance of the higher-level computing resources, including the fog and cloud. Figure 2 shows the edge-centric horizontal IoT cloud structure in the extended IoT cloud infrastructure. In figure 2, where the black dotted lines are the connections and the green lines represent horizontal edge-to-edge connections. Between dedicated data and computation flow paths.

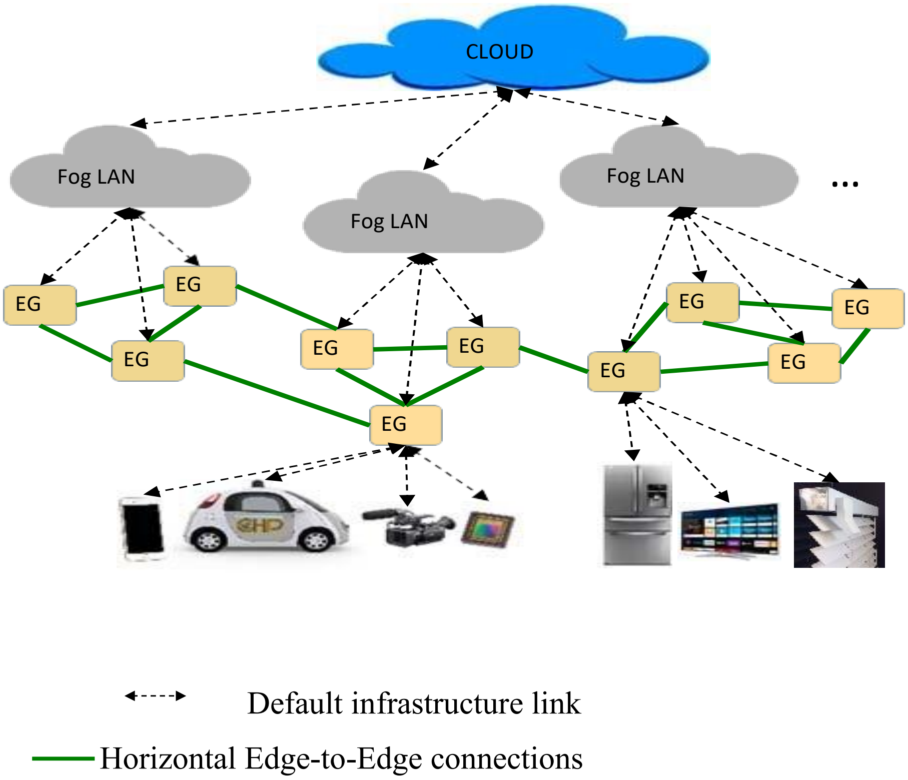

CLOUD
Fog LAN
Fog LAN
Fog LAN
...
EG
EG
EG
EG
EG
EG
EG
EG
EG
EG
EG
Default infrastructure link
Horizontal Edge-to-Edge connections

Figure 2: Horizontal Edge-Centric IoT Cloud Structure

Trustworthy Computing by IoT Cloud Infrastructure

Security is an important issue for IoT cloud, especially in dynamic IoT computing structures. In any system, access control is the basis for security protection, which involves tasks such as identity management, authentication, authorization, policy specification [6]. Thus, we have to rely on the vertical IoT cloud computing structure to support trustworthy computations. In this section, we introduce the basic framework for IoT Cloud computing model. The central idea is to use the vertical IoT-Cloud structure to support the security related computations that cannot performed by the IoT devices alone [7]. We use intrusion detection as an example to show the structure of the frame work, which is illustrated in figure 3. An IoT device does not have sufficient power to perform intrusion detection computation, so it passes its traffic data to the edge node [6]. The edge node hosts a learnt model for intrusion detection that is specific for the local domain. It takes the traffic data and determines whether there is an intrusion. The edge node also passes the traffic data up. At the fog node, incremental learning is performed to add the new traffic data as the training input to further enhance the intrusion detection model. At the cloud node, a globalized analysis is performed on traffic data from different sources to greatly enhance the learning effects. Whenever the model has relatively significant changes, it is passed down to the edge node to improve its intrusion detection capability. Many other trustworthy computing tasks can be executed in the IoT cloud using the framework. For example, consider the access control mechanism in the IoT cloud. Generally, authentication and authorization are performed by a Certificate Authority (CA). The CA hosts the access control policies. Upon authentication, the access rights for a user are provided as a signed certificate (token) and passed back to the application representing the user. But policy hosting and policy validation can be computing and memory intensive. Thus, we decompose the CA task in the IoT cloud. An important question for the trustworthy computing model given in Figure 3 is whether we can trust the edge and fog nodes. The edge node may return an opposite decision for intrusion detection or grant permission to an illegitimate access, which makes the trustworthy computing un-trustable. Note that it is more likely that we can harden the security of one centralized node to perform trustworthy computing tasks. But there are a large number of edge nodes and hardening the security for all of them at the same level as a central node will be infeasible. The probability of one of these edge nodes being compromised can be very high. Thus, additional mechanisms are desirable to ensure that the security related computations are performed in a more trusted manner. We can use hierarchical CAs and let the higher level CAs monitor the behaviors of low level CAs by sampling their decisions. The validation data can be passed directly from the data source. Also, replication with majority voting can also be used to ensure robustness and trustworthiness of the trustworthy computing tasks. To achieve security and trustworthy computing in IoT systems, we need to first consider the insufficient computing power needed for these computations. Thus, we need to make use of the vertical IoT computing infrastructure to perform trustworthy computing for IoT devices. How to decompose the specific trustworthy computing tasks and allocate them to the computing resources along the vertical IoT cloud structure is application dependent. We discuss the general framework for performing trustworthy computing in the vertical IoT cloud and use two examples, intrusion detection and certificate authority, to illustrate the idea. Also, the trustworthiness and robustness of the computing resources in the IoT cloud can be a concern and we consider some common solutions that is Permission Management, Integrated data provenance and Information flow control based on the IoT Cloud for performing trustworthy computing securely under the potentially untrustworthy IoT cloud infrastructure.

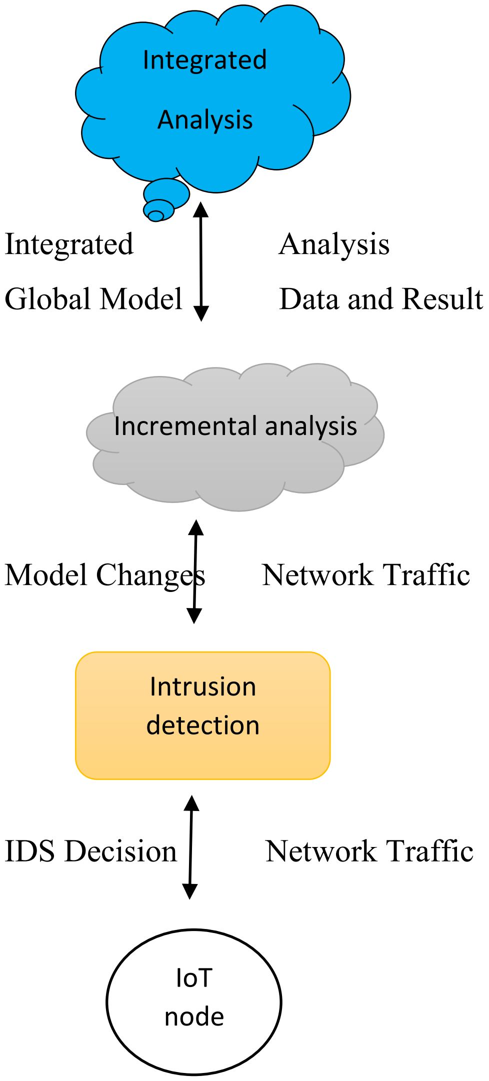


Figure 3: Trustworthy Computing Model in the IoT Cloud

Access Control Model for Dynamic IoT Cloud

As discussed in Section 3, access control is the most fundamental component in trustworthy computing. Many access control models have been developed in the past three decades and among all these models, role-based access control (RBAC) models [8] are most widely used in enterprises and other organizations. Role-based models can greatly cut down the cost for policy specification. Furthermore, the role hierarchy within RBAC offers a natural depiction (role hierarchy) of the user structure within an organization. Each role accurately reflects the responsibilities and authority associated with the user in the designated position. The RBAC model emphasizes the creation of a hierarchy among subjects to minimize the complexity involved in specifying and managing access rights; however, it does not apply the same principle to objects (i.e., the resources that need to be accessed). In the context of IoT cloud, there exists a vast array of resources.If permissions have to be assigned for individual IoT resources to roles, permission assignment and management can have a very high complexity, likely to be infeasible [9]. RBAC model also has limitations in highly open environment where no role hierarchy can be formulated [10] In RBAC, the only alignment required for interoperation is to map the roles from one domain to another and role mapping techniques has been well explored [11]. For interoperation in ABAC, we need to align the attributes as well as the values for the attributes. If two systems do not have equivalent attributes, it is impossible to align them. We had extended the RBAC model and created the RRBAC (Resource and Role hierarchy Based Access Control) model [12] to circumvent the problems in RBAC and ABAC discussed above. Similar to role hierarchy, IoT resources can be organized in a hierarchy and permissions can be assigned based on the resource hierarchy. By providing resource hierarchy as a part of the access control model, we can greatly simplify access rights assignments using the resource groups and privilege inheritance concept on the resource hierarchy. The high level RRBAC model is formally specified in Section 4.1. For the dynamic and open IoT systems, we develop a “resource role hierarchy” based access control model to support easy policy specification. An entity in the system can build a resource role hierarchy to specify its view of the other entities in the system without knowing the specific entities. We integrate the RBAC model with RRBAC so that access control policies can be specified based on the relative role hierarchy and resource hierarchy [13]. When a dynamic IoT network is formed, the other entities are mapped to the relative role hierarchy of entity based on their attributes. The attribute values are obtained by mining the societal databases and social networks. The resource role hierarchy concept is presented in Section 4.2.

Role-Based Access Control Model (RBAC)

Role-Based Access Control approach (RBAC), a policy mechanism defined roles and privileges. This approach scales better than other models. However, when talking about a huge number of devices, managing roles for individual entities the possibility of grouping sensors and assigning roles to those that have the same rights is a good solution for this problem. For providing access rights to user it is important to know the user’s responsibilities assigned by the organization. RBAC try to reduce the gap by combining the forced organizational constraints with flexibility of explicit authorizations [14]. RBAC mostly used for controlling the access to computer resources. RBAC is very useful method for controlling what type of information users can utilize on the computer, the programs that the users execute, and the changes that the users can make. In RBAC roles for users are assigned statically, which is not used in dynamic environment. It is more difficult to change the access rights of the user without changing the specified roles of the user. RBAC is mostly preferable access control model for the local domain. Due to the static role assignment it does not have complexity. Therefore, it needs the low attention for maintenance [15, 16]. Role is nothing but the abstractions of the user behaviour and their assigned duties [17].

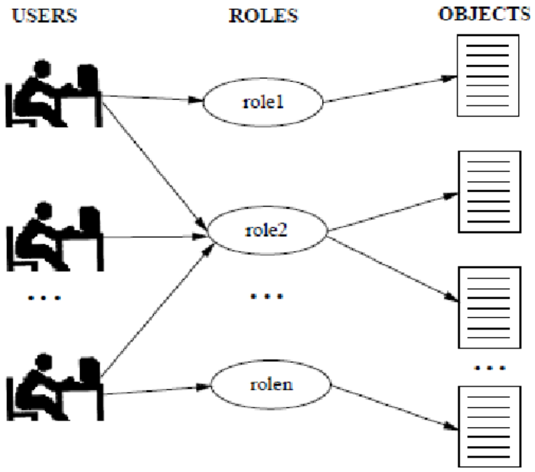


Figure 4: Access Control Model of Role-Based

Essentially, role-based access control policies must identify the roles present within the system. A role can be described as a collection of responsibilities and actions linked to a specific work activity. In an access control security model, a role is viewed as a job-related access right that can be assigned to authorized users within an organization. This enables authorized users to fulfill their associated responsibilities. [16, 17].

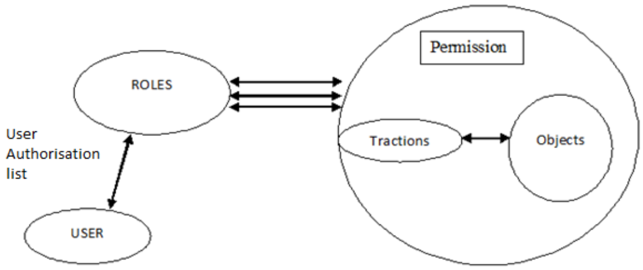
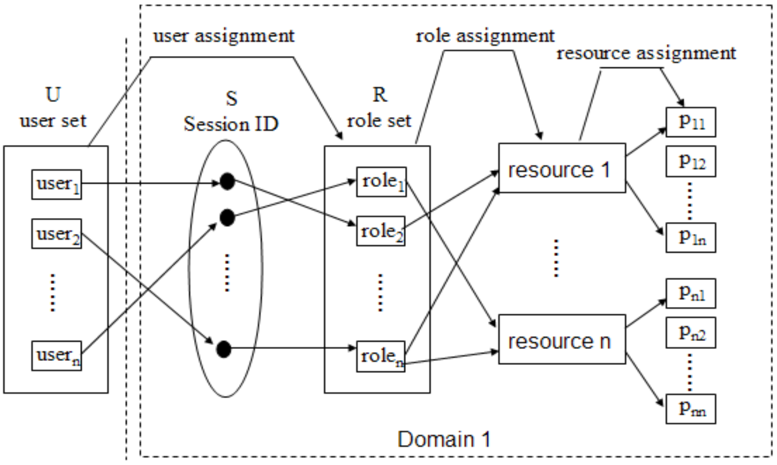


Figure 5: A Mapping of User-Role-Permission

A permission p is a pair < trans, objset >, where trans represents the transaction that executes on the set of objects that is objset. Consider **P** indicate the universal set of permissions, **Trans** indicate the universal set of transactions, and Obj indicates the set of objects.

Resource and Role Hierarchy Based Access Control (RRBAC)

The big difference between RRBAC and RBAC is that RRBAC can support open and distributed environments. RRBAC is suitable for multiple security domains with different applications. Figure 6 is the structure graph of RRBAC model. From Figure 6, the users are distributed anywhere, in a school, in a company etc. In every security domain, the administrator is charge of managing the sessions and roles. Usually, the sessionIDs are randomly generated as a procedure for a user to perform actions. The roles are man-made according to the registration of the resources. The resources are also distributed. After a resource registers and passes the examination, it can become a legitimate resource. Surely, a valid resource is treated as a part of the domain [18].



.

Figure 6: Diagrammatical Representation of RRBAC model

Conclusion

Here we discuss a framework and corresponding techniques, such for performing reliable computing using edge-centric vertical Cloud computing structure for IoT Cloud. The main Contribution of this paper is to propose a flexible Resource and Role Hierarchy Based Access Control (RRBAC) model for the open and dynamic Cloud environment. Working from the traditional RBAC model, the proposed RRBAC model is more extendable, flexible and adaptive, and stays isolated. Role-based models can greatly cut down the cost for policy specification. Access Control is the process or mechanism for giving the authority to access the specific resources, applications and system. Access control defines a set of conditions or criteria to access the system and its resources. In Role Based model creates different authorities' permissions by assigning access rights to specific roles or jobs within the company then role-based access control assigns these roles to users, it is effectively implemented in an organization because files and resources are assigned according to the roles. Assigning roles to the user was done by the system administrator. In, this, Roles are assigned affected to each resource. For example, roles can decide a resource to be used at certain times of the day. RRBAC allow the data owners to use the trust evaluation to decide to save their data in the IoT the primary contribution of this paper is to comprehend the trust models that allow owners and roles to assess the trustworthiness of specific roles and users within the RBAC system. Cloud. RRBAC model provides a flexible approach for many security domains. RRBAC facilitates various forms of resource sharing within an open distributed environment. Consequently, the RRBAC model offers a self-adaptive framework that is sufficiently flexible to be integrated with any distributed and dynamic policy, employing a strategy that is dynamic, robust, and highly scalable.

Acknowledgement:

At the outset, I thank God, the Almighty, for the blessings he has sprinkled on me. It is his supremacy and kindness that has supported me to step forward. I thank **Dr. Dinesh N.Satange**, Research Supervisor, Assistant Professor Narsamma Hirayya Arts Commerce and Science College, Kiran Nagar Amravati for his guidance and undivided support throughout this research paper.

I sincerely thank **Dr. Raosaheb Shekhawat**, President of Vidya Bharati Shaikshanik Mandal, Amravati for their support and cooperation.

I am extremely thankful to **Capt. Dr. Mithilesh M. Rathore**, Vice-President of Vidya Bharati Shaikshanik Mandal, Amravati

I am deeply grateful to **Dr.Pradnya S. Yenkar, Principal** of Vidya Bharati Mahavidyalaya, Amravati for always encouraging me to reach the best of my capabilities.

I express my deep gratitude towards to my Family for their love, unwavering support, trust and encouragement.

Declaration of conflict of interests

In Role-Based Access Control (RBAC), conflicts of interest are addressed through Separations of Duties (SoD) mechanism, which ensure that users are not granted access to roles or permissions that could lead to a conflict. This is typically achieved by either preventing users from holding conflicting roles simultaneously (Static SoD) or limiting the simultaneous use of conflicting roles during a single session (Dynamic SoD).

Plagiarism statement (Mandatory)

I , Dr. S.B. Sarvaiya declared research paper entitled “Trustworthy Computing in the Dynamic IoT Cloud Resort to Resource and Role Hierarchy Based Access Control Model” is the own and original work. The work embodied in this research paper has not been submitted earlier to any university/institution for any publication.

References

[1] I-Ling Yen, Farokh Bastani, San-Yih Hwang,” Trustworthy Computing in the Dynamic IoT Cloud”, IEEE Conference on Information Reuse and Integration for Data Science 2018 IEEE.

[2] J.Gertner,” Behing GE’s vision for the industrial Internet of Things”, 18 June 2014. [Online] Available:https://www.fastcompany.com/3031272/can-jeff-immelt-really-make-the-world-better

[3] M. Satyanarayanan, P. Bahl, R. Caceres and N. Davies, "The case for VM-based cloudlets in mobile computing," IEEE Pervasive Computing, vol. 8, no. 4, p. pp. 14–23, 2009.

[4]D. Willis, A. Dasgupta and S. Banerjee, "Paradrop: A multi- tenant platform for dynamically installed third party services on home gateways," in ACM SIGCOMM Workshop on Distributed Cloud Computing.

[5]L. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," in Computer Communication Review, 2014.

[6]D. Privitera and H. Shahriar, "Design and development of smart TV protector," in National Cyber Summit, 2018.

[7]F. Turkmen and B. Crispo, "Performance evaluation of XACML PDP implementations," in ACM CCS Workshop on Secure Web Services, 2008.

[8]R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role- based access control models," IEEE Computer, vol. 29, no. 2, pp. 38-47, 1996.

[9]E. Yuan and J. Tong, "Attribute based access control (ABAC) for web services," in IEEE International Conference on Web Services, 2005.

[10]C. Hu, D. Ferraiolo, D. Kuhn, A. Schnitzer, K. Sandlin, R. Miller and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," in NIST Special Publication 800-162, 2014.

[11]B. Shafiq, J. Joshi, E. Bertino and A. Ghafoor, "Secure interoperation in a multidomain environment employing RBAC policies," IEEE TKDE, vol. 17, no. 11, pp. 1557- 1577.

[12]N. Solanki, Y. Huang, I.-L. Yen, F. Bastani and Y. Zhang, "Resource and role hierarchy based access control for resourceful systems," in CompSAC, 2018.

[13] Xingdong Li, Zhengping Jin “Resource and Role Based Access Control Model”, 3rd International Conference on Mechatronics and Industrial Informatics (ICMII 2015).

[14] Bokefode Jayant.D., Ubale Swapnaja A,Apte Sulbha S,Modani Dattatray G,” Analysis of DAC MAC RBAC Access Control based Model for Security”, International Journal of Computer Applications (0975-8887) Volume 104-No.5,October 2014.

[15] Zhuo Tang, Juan Wei, Ahmed Sallam, Kenli Li, and Ruixuan Li,” A New RBAC Based Access Control Model for Cloud Computing Springer-Verlag Berlin Heidelberg 2012.

[16] Yizhu Zhao, Yanhua Zhao, Hongwei Lu,” A flexible role-and resource-based access control model”, International Colloquium on Computing, Communication, Control, and Management 2018 ISECS

[17] H.L.F.Ravi Sandhu, Edward J.Coyne and C.E. Youman. Role-based Access Control Models.IEEE Computer, 29 February 1996.

[18] Nidhiben Solanki,Yongtao Huang,I-Ling Yen,Farokh Bastani,Yuqun Zhang,”Resource and Role Hierarchy Based Access Control for Resourceful Systems, International Conference on Computer Software and Applications 2018 42nd IEEE.