Attribute - Semantic Based Access Control Policy Model for IoT

Arun Murugesan, Balamurali Saminathan, Maheswari Kanapathy

Abstract: ***Internet of Things (IoT) devices under cloud assistance is deployed in different distributed environment. It collects sensed data and outsources the data to remote server and user for sharing. As IoT is used in important fields like healthcare, business and research, the sensed data are sensitive information which needs to be protected. Encryption is usual technique to protect data from adversaries. A fine grained access control is essential for heterogeneous device involved social network. The existing access control policies were defined for predefined identity and role which needs to be changed in dynamic situations. Moreover, all the necessary policies cannot be defined in advance and new policies were demanded for new situational context. To solve these issues, this work design a model which calculate final trust value based on semantic information dynamically referring to ontology. a access control policy is also designed on semantic role of the device. The semantic technology is used for high level reasoning of the context situation.***

KeyWords: ***Fog computing, Access control, IoT, Semantics, Ontology, Attribute***

I. INTRODUCTION

The Cloud computing model is concerned with security at both producer and consumer end. The providers expect that their resources and services are used by authorised users and the same way the consumers expect their data to be safe and securely maintained. Generally, a centralised access control mechanism practice large number of authorizing rules with increase in resource, user and services.

Today's cloud environment includes thousands of physical and virtual machines are added and removed. So the existing enterprise access control mechanism does not scalable for public internet. The new access control mechanism should support multi tenants, scalable and independent of network characteristics such as topology, decoupling, routing and addressing [1].

One of the most emerging technology is Internet of Things (IoT) which include both living and non living things in a network. The new system has the ability to sense the information, process it and take decision on it. The devices involved in IoT network are resource constrained(less storage and memory capacity) and edge devices . The IoT integrates WSN technology for digital interface with real world [2]. IoT environment with interconnected hero type of objects provide location and analytic details for data processing. IoT differs from WSN in providing the internet to nodes. A sample of IoT interconnection with its objects is shown in Figure 1.

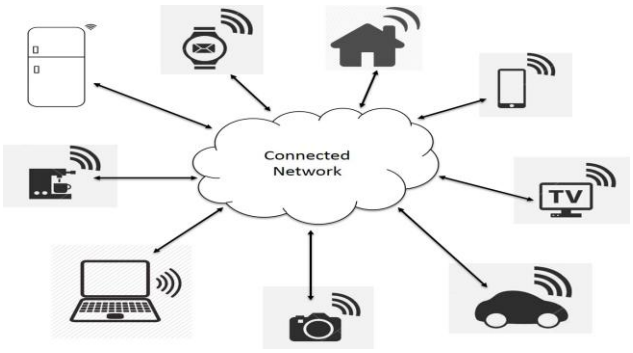


Figure 1: IoT with Connected Entities

The very essential security aspect of IoT is device authorization and authenticating them with an identity [3]. The resource constrained IoT devices are supported by Cloud for storing and computing process. But the existing cloud environment is prone several security issues for collecting and sharing of data between users. As IoT is mostly applicable in dynamic environment such as smart home, in which users enter and leave frequently transactions with identity lead to privacy breach [4].

IoT connects objects with sensors for sensing data used for sharing, monitoring and managing. IoT network model has three layers such as perception layer, transport layer and application layer [5]. The sensors in the perception layer sense the information and send to application layer through internet. The sensor nodes are deployed in an environment which is not under human control so highly vulnerable to malicious attacks [6]. The IoT are emerging trend of internet which support low latency, mobility and geographically distributed resources. The IoT's form fog nodes which are assisted by cloud. The un trusted cloud practices many cryptographic techniques for data confidentiality. Now the security should be ensured in a three layer architecture i.e user-fog-cloud [7].

IoT security requirements:

IoT paradigm is more useful in real time monitoring purpose such as smart home and patient health care sectors. So, eradicating the security problems gains more importance. Privacy violation, illegal accessing of content and hacking cameras are some of dangerous threats[8].The IoT environment becomes more and more complex in addition of devices. This complex network and terminal devices faces worse privacy issues such that securing personal health histories, official documents are challengeable [9]. Various issues to which IoT is prone is shown in Figure 2.

Revised Manuscript Received on December 16, 2019.

***** Correspondence Author

Mr. Arun Murugesan*, Deaprtment of Computer Applications, Kalasalingam Academy of Research and Education, Krishnan koil. India.

Dr. Balamurali Saminathan, Deaprtment of Computer Applications, Kalasalingam Academy of Research and Education, Krishnan koil. India.

Dr. Maheswari Kanapathy, Deaprtment of Computer Applications, Kalasalingam Academy of Research and Education, Krishnan koil. India.

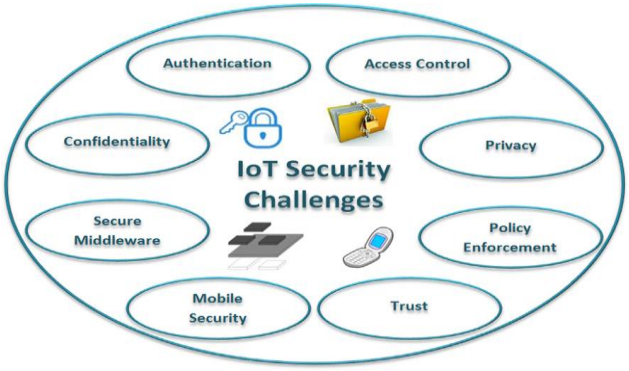


Figure 2: Main security issues in IoT[9]

The main aim of this work is to provide dynamic and scalable solution to privacy issues.

II. MATERIALS AND METHODS

A. Access control rules

Access control rule allow the resource owners to pose access conditions to users upon their resources. Only eligible users are authorised and granted rights to access. The access control and granting depends on the role of the user [10]. Wang et. al. [11], expressed that similar to cloud, the devices also include sensitive information, business decisions for e.g personal data, correspondence mail, contact information, credit card and credentials, business planning corporate agreements and location details. When this data need to be stored in fog nodes , the communication with the encrypted data is followed for data confidentiality[12].

B. Access control models

The three broad categories of access control models for cloud computing: (1) Role-based models; (2) Attribute-based encryption models and (3) Multi-tenancy models.
Role-based access model (RBAC)
In role based RBAC model, the privilege is based on the users role and least permission for their job or task is given [13]. The role decides the link relation between subject and object. In IoT the terminal node in perception layer is sensor or device. In distributed environment, multilevel access control on the resource is dynamic and only for permitted time [14].

In the work of [15], the author proposed temporal-RBAC (TRBAC) model, in which the role can be enabled and disabled dynamically based on the request. But in the work [16], it is argued that some roles need to be static and stay always and they proposed generalized TRBAC (GTRBAC) in which role is activated instead of enabling.

C. Attribute based access model (ABAC)

In ABAC model, the subject and object entities are related based on the characteristic attributes associated with them. The permission is granted based on attribute values. Attributes can also hold data that mean any restrictions on user [17][18]. ABAC is flexible and scalable for fine grained access control in complex system like Internet of Things. A fine grained access model with key based is suggested in [19] where the users are provided with private keys to encrypt and decrypt the attribute values of the objects.

III. MULTI-TENANCY MODEL

In this model, control policies are defined for a group of Virtual machines as tenants. The capturing of physical characteristics is difficult as this type of multi tenancy is prone to side channel attacks [20]. The communication between this multiple tenants through covert channel are interfered, the information is tapped [21].

In RBAC, permissions are created for each role but the best way is to define common policies for the resources. And the resources can be defined with characteristic attributes for validating against the policies. Access rules are lightweight, access rules are generalized and managed centrally [22].

A. Attribute based methodology

Finding out the trusted sensor nodes in IoT environment is important research topic. The trust nodes are decided based on the context information and the recommendations from other nodes. In an efficient trust system, the information are shared very securely. The proposed system suggests a dynamic way of authorizing and filters out illegal request and also trap the misuse of permitted rights. When the request is forwarded to cloud through gateway, the cloud uses context information to validate the trust value of the requestor. The request that satisfy the threshold fixed, are forwarded for further validation by the cloud. Final trust value is calculated with attribute values referencing the policies, the authorized device are allowed to communicate with other device for service till the allotted time.

IV. SEMANTICS IN IoT ENVIRONMENT

A. Semantic relation between entities

Nowadays, Semantics are highly involved in dynamic web applications so that domain conceptualization is accounted in data model. It is very important to take decision on entity interrelations. In this paper, we present model for accurate decision making, considering semantic relations among entities in domains of access control either subject or object [23].

B. The Trust Model

Employing semantics, each entity in this model can have a trust value to reject or accept collaboration with other entity. These entities are modelled using ontology in subject, object and action domain with semantic interrelations using OWL (Ontology Web Language). The semantic relation information between the users are used for expressing authorization rules[24][25].
In the Ontology, the devices of IoT environment is represented by class Device. The class Category represent the class of authorization. This is based on the semantic relationship. The class TrustValue gives degree of trust. It takes any float value between 0 and 1. The following are methods used

initialTrustValue: The trust managers assign initial trust to new entry
hasDirectTrust: The degree of trust gained during validation
hasRecTrust: opinion value from other device about the device on validation

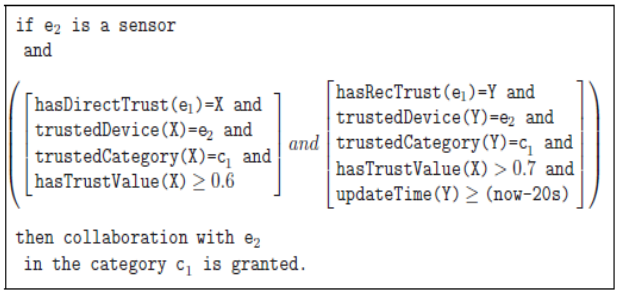
trustRelated: The semantic relation between two categories of trust

C. Semantic policies

The policies are defined based on contexts as high level abstracted model. This approach describes the contexts and their classification so that conflicts between policies can be traced out.

Security rule to design policies.

The policies are described in the SWRL (Semantic Web Rule Language). This language is used to process and to query ontologies. Suppose that entity e1 request for collaboration with entity e2 in the trust category c1. A rule for e1 can be represented as:



When the rules are satisfied, the entity is ready for collaboration.

The trust value is calculated as given in equation (1). Suppose device e1 put request for entity e2. The e1 evaluate trust value for e2 on referring to other entities. The other entity who give opinion is ei. T (ei, e2, c1) is direct value on e2 by ei under c1 category. T (e1, ei, c1) is trust value of e1 on e2 under c1

$$T_{infer}(e_1, e_2, c_1) = \frac{\sum_{i=1}^{n} T(e_i, e_2, c_1) \times T(e_1, e_i, c_1)}{T(e_1, e_i, c_1)} \quad (1)$$

The trust value is taken as a attribute value and used in attribute based access control method. The trust manager updates the trust value with time [26].

V. LITERATURE SURVEY

The existing access control solutions are meant for non resource constrained system whereas IoT environment entities are resource constrained which seek cloud for resource sharing. Also the system here involves communication between end users and heterogeneous devices

Banerjee et al. [27] proposed symmetric key based authentication for wireless sensor networks. They use pairwise key distribution. Chan-Perrig-Song et al. [28] proposes a random key scheme with self recovery but the system is not scalable and need large memory space.

The author of [29] proposed multitenant access model in which addition and removal of tenants are attempted. Almutairi et al [30] proposed a multi-tenant multi-cloud environment in which virtual resource manager, RBAC are implemented. Both inter cloud and intra cloud operations are involved.

The paper [31] is designed as Policy Update Attribute Based Encryption model support policy updates and attributes addition and revocation. This method provides fine grained access control mechanism on cipher texts.

Yeh et al. [32] proposed a WSN protocol using Elliptic Curve Cryptography (ECC). ECC performs better because of small key size. In [33], access token is provided to access a resource by resource manager. In IoT like decentralised environment, the server grants the token. Guoping et al. [34] have used Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models and proposed a system that use context information and produced very efficient access control mechanism on internet objects.

VI. PROPOSED ATTRIBUTE - SEMANTIC ROLE BASED CONTROL

The access control mechanism is to control any subject accessing the object, so that resource use is restricted from illegal use and managed effectively. Attribute Base Access Control (ABAC) is fine grained as it considers the attributes that include information about role, identity and also sensitive information.

A. *The Definition of ABAC*

Here this paper formally defines the (basic) ABAC policy:

Definition 1. IoT entities: Let U be User (i.e. mobile users, computers, client, etc.), R be Resource and E be the Environment. User request certain resources. Subject takes action and acts on Resources. Environment is context information for making a policy rule at instant system time.

Definition 2. Attributes (A): The attributes may be of users, resources and environments.. Attributes include identity, name, role, location, data, time etc. Attribute Authority is responsible to the define and management of the attributes of users, resources and environment.

$A = I_i = \{identity, name, role, date, time, location, ...\}$

where i is the attributes defined in the Internet of Things for ith object

B. Workflow of proposed model

The system is proposed to validate a client request based on attributes which is rich in context information. This context information is used for trust value calculation. The trust value is validated against a access control policy. The context information and the access control policy is enriched with semantic knowledge extracted from domain ontology.design a access control policy. Following are the steps followed by the proposed system.

1. Using the usual credential of username and password the IoT device enter the social network.
2. The IoT device requestor put a request to the cloud for a resource access.
3. The device holds attributes with information about location, ip address , internet type etc.
4. Local trust value is calculated on aggregating the context values.
5. The data from the mobile device is send to IoT Gateway.

6. IoT Gateway check with minimum threshold value
7. The Gateway forward the request to cloud when it meets the threshold.
8. On adding the semantic trust value to local trust, the Cloud calculates the final trust value.
9. Referring to the other necessary context value and the access control policies, the device is authorized and permitted based on the privileged rights.
10. If the final trust value meets the predefined threshold, cloud

"permits the request"
Else
"deny the request"

Initially the gateway itself has to get connected to the cloud on permission through valid credentials. The request accepted by the cloud is send back to the gateway which forwards the same to IoT destination node on creating CoAP (Constrained Application Protocol) message. The rights to access a resource are decided on referring to policies based on role of the requestor. The proposed model suggest a semantic relation based role so that it is fine grained and exist for all the time. This semantic relation is grasped from ontology which is conceptualization of a domain.

C. Access control policy with READ/WRITE or CONTROL permission

Any device can access the resource only based on the rights permitted by the cloud. The device with READ permission cannot WRITE or CONTROL the sensor data. When the granted permission is WRITE or CONTROL, the device can change the content and also can have control over it for example using Smartphone. The rights are assigned by the cloud based on the final trust value meeting the threshold value. For very minimum trust value, the request is declined by the cloud. The basic architecture of the proposed system is shown in the Figure 3

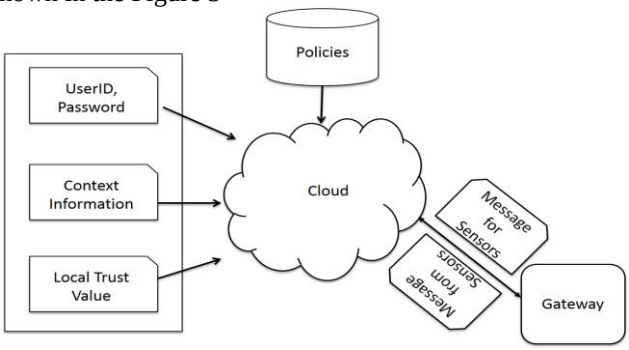


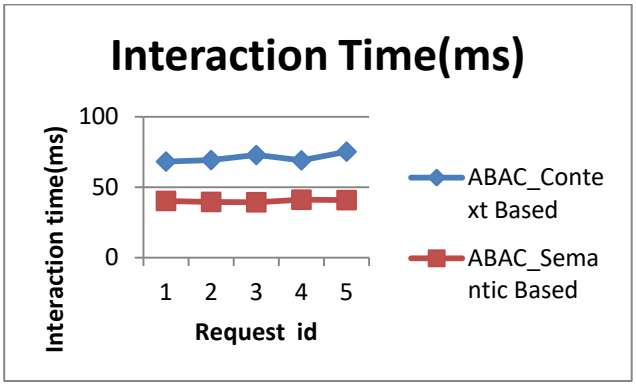
Figure 3: Interaction between IoT gateway and Cloud

VII. PERFORMANCE EVALUATION

The proposed system is evaluated on measuring the response time for completing a request.

A. *Implementation details:*

An Android application in Java 1.7 SDK and Android Platform act as a mobile client. The context information from sensors is fed to the application and calculate initial trust value. The application receives the context information from sensors and evaluates the initial trust value.. Google Cloud service and Android tablet of Memory: 2 GB is used. Gateway's are identified using IP and MAC address. An Android tablets is used as a portable clients in the implementation



The context values considered are Location(latitude, longitude), Internet Information(MAC and IP addr.), Time(Date ,Time). Threshold of semantic based trust value is 0.8(the maximum range of the value falls in the range[0..1]. Initial trust value initialized to 0 and Threshold local trust value is 50.

Client-Cloud Interaction Time: The interaction time is the time between the mobile client and Google cloud service granting permission. The policy entities are expressed as rules .The interaction time between the device and the cloud is repeatedly measured for five consecutive requests because Users can get response in real time if the verification tool can detect fault when the fault-causing rule is added to the policy, rather than after all the rules of the policy has completed.

The quality of the access control model depends on fault finding when a conflict occurs with a request validation. The redundant rule also affect the policy rule performance as the runtime constitutes the total checking of the rule set. The rule set must be defined for all the possibilities of test case in a domain. The graph in the figure infers that the ABAC model with trust value calculation based on context information alone shows variation in runtime but the proposed semantic based ABAC mode is consistent runtime. Also, the validation of attribute based request on semantic policies occupy very less interaction time of response between the mobile client and cloud in IoT environment.

VIII. CONCLUSION

For many organizations working with dynamic and huge pool of data, protecting and sharing of the data has become very challenging due to crypto attacks and various security risks. The risk of allowing the illegal intruders to share the information is defended by identifying them. For this, the proposed system believe on the contextual information about the users such as when, where, who and why need the information. There is also necessity of controlling the whole process dynamically. The request is also validated with the attributes collected. The proposed (Attribute Based Access Control) ABAC design semantic based information which gives more conceptualised description about the user. The policies are semantically designed based on the role, description and relationship between entities extracted from ontology. Untrusted request are denied when evaluated against policy rules. The evaluation takes place at both device and cloud level. So the proposed system is more reliable and reduces risk even if some of the environmental factors are matched. The true relation based rights are permitted for the IoT entities as the system is designed on semantic domain relationship.

In future, the system can be extended to next level security

on having he user's request history and designing fine grained policies. The proposed system implementing in real social network with heterogeneous devices is needed to study the other factors such as trust.

REFERENCES

1. Natarajan Meghanathan ,"REVIEW OF ACCESS CONTROL MODELS FOR CLOUD COMPUTING", ICCSEA, SPPR, CSIA, WimoA – 2013,pp. 77–85, 2013
2. Manrique JA , Rueda-Rueda JS , Portocarrero JM . Contrasting internet of things and wireless sensor network from a conceptual overview. In: Proceedings of the 2016 Âfieee international conference on internet of things (iThings)
3. Kolias C , et al. DDOs in the iot: mirai and other botnets. Computer 2017;507:80–4 .
4. Saputro N, Yurekli AI, Akkaya K, Uluagac S. Privacy preservation for IoT used in smart buildings. Hu F. Security and privacy in internet of things (IoTs): models, algorithms, and implementationsPublisher: CRC Press; Chapter: 7.
5. L. Atzori, A. Iera, G. Morabito. The internet of things: A survey. Computer Networks. 54, 2787-2805 (2010).
6. A. Mnif, O. Cheikhrouhou, M. Ben Jemaa. An ID-based user authentication scheme for Wireless Sensor Networks using ECC. In Proc. Microelectronics (ICM), Hammamet, 1-9 (2011).
7. Yi, S.; Li, C.; Li, Q. A Survey of Fog Computing: Concepts, Applications and Issues . In Proceedings of the 2015Workshop on Mobile Big Data, Hangzhou, China, 21 June 2015; pp. 37–42, doi:10.1145/2757384.2757397
8. Rahul Godha and Sneh Prateek. Home Automation: Access Control for IoT Devices. International Journal of Scienti_c and Research Publications (IJSRP), 4(10), 2014.
9. Yuanjun Song. Security in Internet of Things. PhD thesis, Royal Institute of Technology, 2013
10. Qin, L., Atluri, V.: Concept-level access control for the semantic web. In: ACM Workshop on XML Security, Fairfax, VA, USA (2003) 94–103
11. Yong Wang, Jinpeng Wei, and K. Vangury. Bring your own device security issues and challenges. In 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), pages 80{85. IEEE, jan 2014.
12. Yi, S.; Li, C.; Li, Q. A Survey of Fog Computing: Concepts, Applications and Issues. In Proceedings of the 2015Workshop on Mobile Big Data, Hangzhou, China, 21 June 2015; pp. 37–42, doi:10.1145/2757384.2757397
13. V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data," Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89-98, 2006
14. G. Zhang, J. Tian. An extended role based access control model for the Internet of Things. In Proc. ICINA, Kunming, V1-319 (2010).
15. D. Nurmi, R. Wolski, C. Grzegorczyk, S. Soman, L. Youseff and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," Proceedings of the International Symposium on Cluster Computing and the Grid, pp. 124-131, 2009
16. B. Shafiq, J. B. D. Joshi, E. Bertino and A. Ghafoor, "Secure Interoperation in a Multi-domain Environment Employing RBAC Policies," IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 11, pp. 1557-1577, Nov. 2005
17. Q. Han, J. Li. An Authorization Management Approach in the Internet of Things, (2012
18. K. Yang and X. Jia, "Attribute-based Access Control for Multi-Authority Systems in Cloud Storage," Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems, pp. 536- 545, 2012.
19. T. Ristenpart, E. Tromer, H. Shacham and S. Savage, "Hey, You, Get off my Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199-212, 2009
20. Globus, http://www.globus.org/, last accessed: November 9, 2012
21. W. Xiaopeng, L. Junzhou, S. Aibo and M. Teng, "Semantic Access Control in Grid Computing," Proceedings of the 11th International Conference on Parallel and Distributed Systems, vol. 1, pp. 661- 667, July 2005
22. Ann Cavoukian, Michelle Chibba, Graham Williamson, and Andrew Ferguson. The Importance of ABAC: Attribute-Based Access Control to Big Data: Privacy and Context. Technical report, The Privacy and big Data Institute, 2015.
23. Mohsen Taherian , Rasool Jalili, and Morteza Amini ,"A Semantic-Aware Ontology-Based Trust Model for Pervasive Computing Environments", C. Rong et al. (Eds.): ATC 2008, LNCS 5060, pp. 47–59, 2008
24. Patel-Schneider, P., Hayes, P., Horrocks, I.: OWL: Web Ontology Language Semantics and Abstract Syntax, W3C Recommendation (2004)
25. Hayes, P., Horrocks, I., Patel-Schneider, P., Boley, Tabet, S., Grosof, B., Dean, M.:SWRL: A Semantic Web Rule Language Combining OWL and RuleML (2004)
26. Mohsen Taherian, Rasool Jalili, and Morteza Amini," A Semantic-Aware Ontology-Based Trust Model for Pervasive Computing Environments", ATC 2008, LNCS 5060, pp. 47–59, 2008.
27. S. Banerjee, D. Mukhopadhyay. Symmetric key based authenticated querying in wireless sensor networks. In Proc. first Int. Integrated internet ad hoc and sensor networks.ACM, New York, NY, USA, 1223-1227 (2006)
28. H. Chan,A. Perrig. Security and privacy in sensor networks.Computer, 36, 103-105 (2003)
29. C. L. Dumitrescu and I. Foster, "GRUBER: A Grid Resource Usage SLA Broker," Euro-Par 2005, LNCS 3648, pp. 465-474, 2005
30. Abdulrahman Almutairi ; Muhammad Sarfraz ; Saleh Basalamah ; Walid Aref ; Arif Ghafoo," A Distributed Access Control Architecture for Cloud Computing",**:** IEEE Software ,Volume: 29 , Issue: 2 , March-April 2012
31. B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, and T. Freeman, "A Flexible Attribute Based Access Control for Grid Computing," Journal of Grid Computing, vol. 7, no. 2, pp. 169-180, 2009.Computer
32. H. L. Yeh, T. H. Chen, P. C. Liu, et al. A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography, Sensors, 11, 4767-4779(2011).
33. Jaehong Park and Ravi Sandhu. Towards usage control models: beyond traditional access control. In Proceedings of the seventh ACM symposium on Access control models and technologies - SACMAT '02, pages 57{64, New York, New York, USA, jun 2002. ACM Press
34. Guoping Zhang and Jiazheng Tian. An extended role based access control model for the Internet of Things. In 2010 International Conference on Information, Networking and Automation (ICINA), volume 1, pages V1{319{V1{323. IEEE, oct 2010.

AUTHORS PROFILE

Mr. M. Arun, Assistant Professor, Department of Computer Applications, Kalasalingam Academy of Research and Education have more than 12 years of Teaching Experience. He completed his Under Graduation in Computer Applications at Madurai Kamarajar University and Post Graduation in Computer Applications at Anna University, His Major research area is Network Security

Dr. S. Balamurali, Senior Professor, Department of Computer Applications, Kalasalingam Academy of Research and Education, he has more than 30 years of Teaching Experience, he has completed his Under graduate in Mathematics in PSG College of Arts and Science, Post Graduate in Statistics in PSG in College of Arts and Science and Doctoral Degree from Bharathiar University in the field of Statistics, His current area of Research is Statistics, Data Mining, Network Security. He has more than 200 publications in International Journals. He is acting as a reviewer for more than 20 peer reviewed journals.

Dr. K. Maheswari received her B.sc (Computer Science) from Madurai Kamaraj University and MCA. M.Phil. from Bharathidasan University. She has completed her Ph.d at Bharathiar University. She is currently working as an Associate Professor in the Department of Computer Applications, Kalasalingam Academy of Research and Education. She has 23 years of teaching experience. She has presented research papers in several national and international conferences. She has published many research papers in various international journals. Her research interest is VoIP , network security and Data Mining.