I J C T A, 10(9), 2017, pp. 501-510 ISSN: 0974-5572

Enhanced Identity Management and Security in IoT backing with Cloud using ICAC

Ajinkya S. Shewale* and Sandeep G. Sutar**

ABSTRACT

The integration and amalgamation of all communication systems is the purpose of the Internet of Things. This makes by itself an interesting challenge when toting new things and enabling new amenities on the internet. Expanding the IPv6 protocol suite with higher address space and defining innovative capabilities restoring end to end connectivity also end to end service. IPv6 makes feasible the new conception of spreading Internet of Everything. IPv6 has been intended to offersafe communication to user and mobility for all devices attached to the user. Thereby user can constantly be connected. This describes the key challenges, how they have been solved with IPv6, finally presents the future works and vision that describes the roadmap of the Internet of Everything in order to reach a device access controlling interoperable, trustable, mobile, distributed, valuable and powerful enabler for emerging applications such as smarter cities, human dynamics, cyber-physical systems, smart grid, green networks, intelligent transport systems and ubiquitous healthcare.

Index Terms: Access control,Internet of things, IPv4, IPv6, Smart cities.

1. INTRODUCTION

Research of Internet of Things environment are collected on the smart objects, i.e., small and highly constrained devices in terms of memory ability, computation ability, energy autonomy, and communication abilities. These types of things are used by some several technologies.Barcode for the simple identification of a resource is the most technology for identify the things (e.g., product identifier) and Quick Response (QR) or matrix barcodes for the extended identification of a resource (e.g., plain text and Universal Resource Locators (URLs)), Radio Frequency Identification (RFID) is used for digital identification of resources with abilities for various resource identification, identification out of line of sight, and extended identification abilities. Last but not list, Near Field Communication (NFC) for the digital identification of resources through personal devices such as smart phones and the formation of peer-to-peer (P2P) communications.

In order to backing all the unindustrialized Internet-enabled devicesIPv6 spreads the addressing space. For providing secure communication to users and mobility for all devices committed to the user IPv6 is planned so that users can constantly be associated. To figure the Internet of Things IPv6 topographies what have made it possiblelinking all the objects. The integration and unification of all communications systems that surround us is the goal of Internet of things. Henceforth, the systems can get control and access to the other systems in order to deliver ubiquitous communication and computing with the purpose of defining a new generation of amenities.

For the Internet of ThingsIPv6 is assumed the most proper technology.It provides scalability, flexibility, open, tested, extended, ubiquitous, and end-to-end connectivity. But it is not viable for all the things and resources integrated into the Internet of Things ecosystems to be accompanying with protocols intended

* Computer Science and Engineering ADCTE, Ashta India, *Email: ajinkyashewale29@gmail.com*

** Computer Science and Engineering ADCTE, Ashta India, *Email: sutarsandeep07@gmail.com*

with the considerations ofdevices with higher abilities. Mobility-aware solutions increase the connectivity and enhance adaptability to changes of location and infrastructure. Internet of Things is enabling a new generation of dynamic ecosystems in environments such as smart cities and hospitals.

With currentinternet infrastructure dynamic ecosystems wants ubiquitous access to Internet, seamless handover, flexible roaming policiesand an interoperable mobility protocol. One of main requirements for mobility management in dynamic ecosystems is integration and interoperability with existing infrastructure, meanwhile mobile nodes need the ability to use other networks during roaming. For this, it is important to offer a highly compatible solution with available access points, routers and networks.

For the success of the Internet of ThingsIPv6 based solutions are key enablers. The mobility, security is a high necessity for the IoT. This close bondamong the cybernetic and physical world enabled by the Internet of Things carries with it vulnerabilities in terms of security and privacy. Since vulnerability is now not simply limited to the hardware of our computer. Security is also an inherent necessity for the mobility management. Since this offers the ability to convey traffic to a new address and claim the identity of a node. So, mobility opens high number of vulnerabilities for the man in the middle attacks, identity sup plantation, and data integrity. The described evolution from the Internet of Things towards a ubiquitous and mobile Internet is having influence in several application areas and market sectors. In clinical environments security is a major requirement.

Internet of Things is considered the major communication improvements in recent years. It offers the basis for development of supportive services and applications. Extensive research using this concept in different areas such as building automation, Intelligent Transport Systems is being conducted.

2. RELATED WORK

This work has described the key components to reach the evolution of connectivity, reliability and support for heterogeneity, security and mobility. This section describes the ongoing and future works to continue improving the potential of the IoT and its application in eHealth/mHealth and emerging areas such as Smart Cities.

The public IPv4 address space managed by IANA (http://www.iana.org) has been completely depleted by Feb 1st, 2011. This creates by itself an interesting challenge when adding new things and enabling new services on the Internet. Without using public IP addresses, the Internet of Things capabilities would be greatly reduced.

Dynamic ecosystems require ubiquitous access to Internet, seamless handover, flexible roaming policies, and an interoperable mobility protocol with the existing Internet infrastructure. These features are challenges for Internet of Things devices due to their constraints. The work presented in [1, 2] analysis of the requirements, desirable features, existing solutions and proposes, on the one hand, detection of movement direction for IEEE 802.15.4 radios to offer a fast handover, and on the other hand, an efficient solution for constrained environments compatible with IPv6-existing protocols, i.e., Mobile IPv6.

Internet of Things is considered one of the major communication advances in recent years, since it offers the basis for the development of cooperative services and applications. Extensive research using this concept in different areas, such as building automation, Intelligent Transport Systems, and in particular for healthcare, is being carried out. For example, its potential for mobile health applications has been reported in [3, 4], showing its potential identification capacities for drug identification, and its communication capabilities in offering ubiquitous therapy by providing wireless and mobility capabilities for personal devices and smart objects, in addition to allowing the collection of data anytime and anywhere.

The Internet of Things (IoT) [5], or Machine-to-Machine (M2M), is one of the main drivers for the evolution of the Internet towards the Future Internet.

Nowadays, sensors, actuators and devices (so-called things), are connected to the Internet through gateways and platforms such as Supervisory Control and Data Acquisition platforms (SCADAs), panels, and brokers. These gateways and platforms break the end-to-end connection with the Internet. For that reason, this initial approach is defined as an Intranet of Things [6].

The Intranet is being extended to smart things [7] with a higher scalability, pervasiveness, and integration in to the Internet Core. This extension is leading to reach a real IoT, where things are first class citizens in the Internet, and they do not need to relay any more on a gateway, middleware, proxy, or broker.

In addition to the physical devices, IoT is also enriched with the cybernetic resources and Web-based technologies. For that purpose, IoT is enabled with interfaces based on Web Services such as Restful architecture and the novel protocol for constrained devices Applications Protocol (CoAP) [8]. These interfaces enable the seamless integration of the IoT resources with information systems, management systems, and the humans. Reaching thereby a universal and ubiquitous integration among human networks (i.e., society), appliance networks, sensor networks, machine networks, and, in definitive, everything networks.

IoT offers several advantages and new capabilities for a wide range of application areas. For example, now a days IoT is finding applications for the development of Smart Cities, starting with the Smart Grid, Smart Lighting and transport with new services such as Smart Parking and the Bicycle Sharing System [9] for building sustainable and efficiently smart ecosystems.

IoT started focusing on building blocks such as Radio Frequency Identification (RFID), due to its capabilities of identifying the uniqueness of an object in the world. After that initial approach, the technology evolved and the IoT was not much more a metaphor for RFID capabilities, else it was feasible that the devices such as sensors and appliances were connected to the IoT. Thereby, it was giving birth to smart things and smart objects concepts, as an evolution of the devices located at the Wireless Sensor Networks(WSN) with IPv6 connectivity through protocols such as the mentioned 6LoWPAN [10].

3. PROPOSED SYSTEM

In above figure 1, The Heterogeneous devices are connected with the application framework for communication. Application framework collects the information from devices and stores in the cloud. And

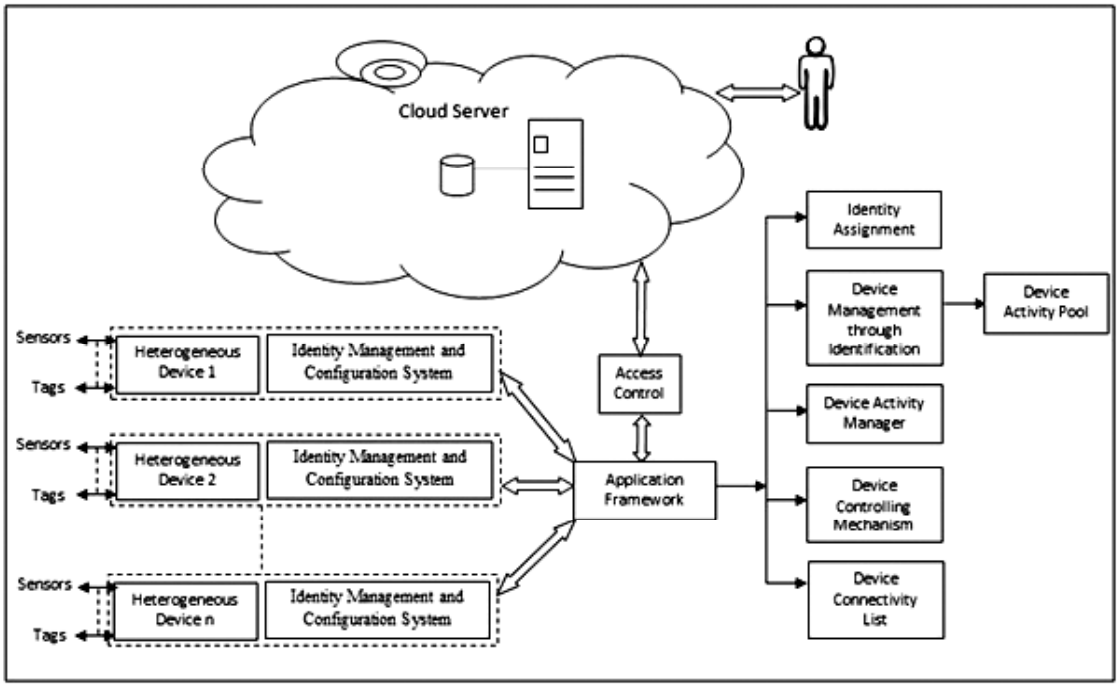

Figure 1: System Architecture

cloud user can access the information. Application framework does Identity assignment, Device management through Identification, Device activity management, Device Controlling, Manage list of connected device.

3.1. Our proposed system can be divided into following modules

3.1.1. Identity management and configuration system

There is difference between addresses and identifier of devices. Addresses determine the communication endpoint within a certain system. Followings are the aspects considered in Identity Management and Configuration System.

1. Identity is assigned by the IP and identity assignment algorithm, an IP address is needed to establish a connection between devices.
2. Device can have its address changed as per the ad-hoc Basis. Addresses need not be permanent.
3. A new device can take the address of a previous device. A device can have more than one IP address.
4. Mapping between identifier and addresses allows layer of indirection. This enables configurations like several identifiers pointing to one address.

HETEROGENEOUS DEVICES

IoT devices are any kind of device connected to Internet. Such as servers, laptops, and personal computers, to emerging devices such as smart phones, smart meters, sensors, identification readers, and appliances. Here designing a mechanism for IoT to allowing communication among very heterogeneous devices connected via a very wide range of networks through the Internet infrastructure.

3.1.2. Access control

Access Control is the important security mechanism is used to enhance security policy for autonomous domain in cloud system. By using access control, guarantee security, privacy, integrity of information and user confidentiality achieved higher .The maximum number of the IoT applications need to take into considerations the support of mechanisms to carry out the authentication, authorization, access control and key management.

The classic authentication mechanisms (ex.: login /password) is not directly work in the IoT. Objects have to afford some sort of lightweight token or certificate for an authentication where no user (providing a password) is involved. For stronger authentication means of individuals usually combine two or multiple factors.

Algorithm–

Identity-driven capability-based access control scheme:

There is concurrent communication of more than one device in IoT in private or public domain. Successful IoT communication and computing includes sharing of pool of resources/ devices in a flexible way. For this purpose, there is a need of secure access of resources. Least privilege is important to establish secure communication between multiple devices, and services with access control and authorization in IoT. The idea of capability for access control is stretched where the identities of the involved devices are entrenched in the access capabilities. Identity-driven capability-based access control scheme presented in this contribution helps to assuage issues related to complexity, and dynamics of device identities. This is implemented for WIFI, and results less scalability issues and better performance analysis compared with other access control schemes.

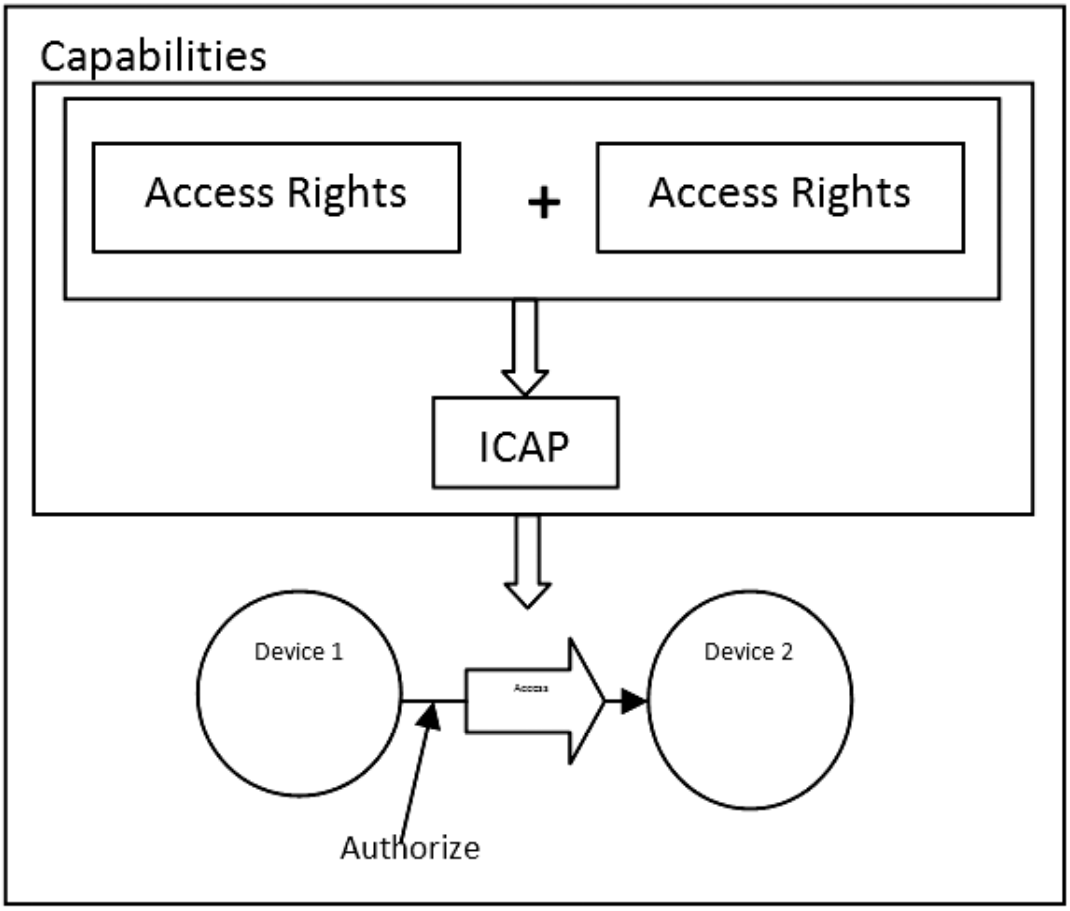

Figure 2: Identity Driven Capability Structure

Proposed Identity-driven Capability-based Access Control (ICAC scheme):

The capability terms a set of access rights for devices. Devices which may also contain security attributes such as access rights or other access control data. Identity-based Capability (ICAC) structure is shown in Figure 2 with how capability is used for access control.

ICAP is represented as below

ICAP = (ID, AR, Rnd) Where,

- ID = Device Identifier.
- AR = Set of access rights for the device with device identifier as ID.
- Rnd = Random number to prevent forgery and is a result of one way hash function as given in equation below,

$$Rnd = f(ID, AR).$$

Where f is publicly known algorithm based on public key crypto system to avoid the problem of key distribution. When the device accepts access request with the capability, one way hash function is run to check the Rndcontrary to tampering. If the integrity of the capability is maintained, then access right is granted. Capability structure adapted in this is showed in Figure 2. This capability is not kept centrally on a particular device. Each device has its own capability which is verified by each access. First, both the devices get connected to ad-hoc network and then an identity is generated for these devices based on media access control address for unique identification. After this, the connection requests are sent, and the connection is established. The access rights are decided and capabilities are created for these devices. The capabilities

are exchanged with a message digest. SHA-1 message digest is used to check the tampering or imitation of capability.

3.1.3. Application framework

Identity and Resource Management–

In identity management module device identity is given by considering a staggering variety of identity and relationship types, according to certain object identity principles:

- Object's identity is different as identity of its underlying mechanisms. The x-ray machine in radiology department have an IP address, but it has its own identity to discriminate it from other machines.
- Object can havemultiple temporary identities and also have one core identity.Hospital can become meeting place for a health conference after a fire.
- Object can classify itself usingits specific features or identity. Virtual food identifies itself by ingredients and quantity.

Device Activity Manager

As per the suspicious activity pool, devices are managed and controlled alarm will be raise when a suspicious thing happens to the device in IoT. E.g. suppose activity pool having rule that camera should not be open if any device raise request in IoT for open the camera, system will raise the alarm.

Device Controlling Mechanism

Here IPv6 features used to joining all the objects and form the IoT. To accomplishgoal of IoT i.e. integration and unification of all communications systems that surrounds. Following are the functionalities by device control mechanism.

1) The system gets an access control of devices in the IoT network for provide easy communication.
2) The purpose using access control is to transfer and receive data from heterogeneous device to cloud server.

Resource List

Resource list contains all devices list with identification proofs.

4. RESULT AND DISCUSSION

4.1. Execution Time

Device Connected	Execution Time
Raspberry Device	2000
DESKTOP-F97HI2F	4000
SAI-PC	4500

Figure 3a: Device Connection Time

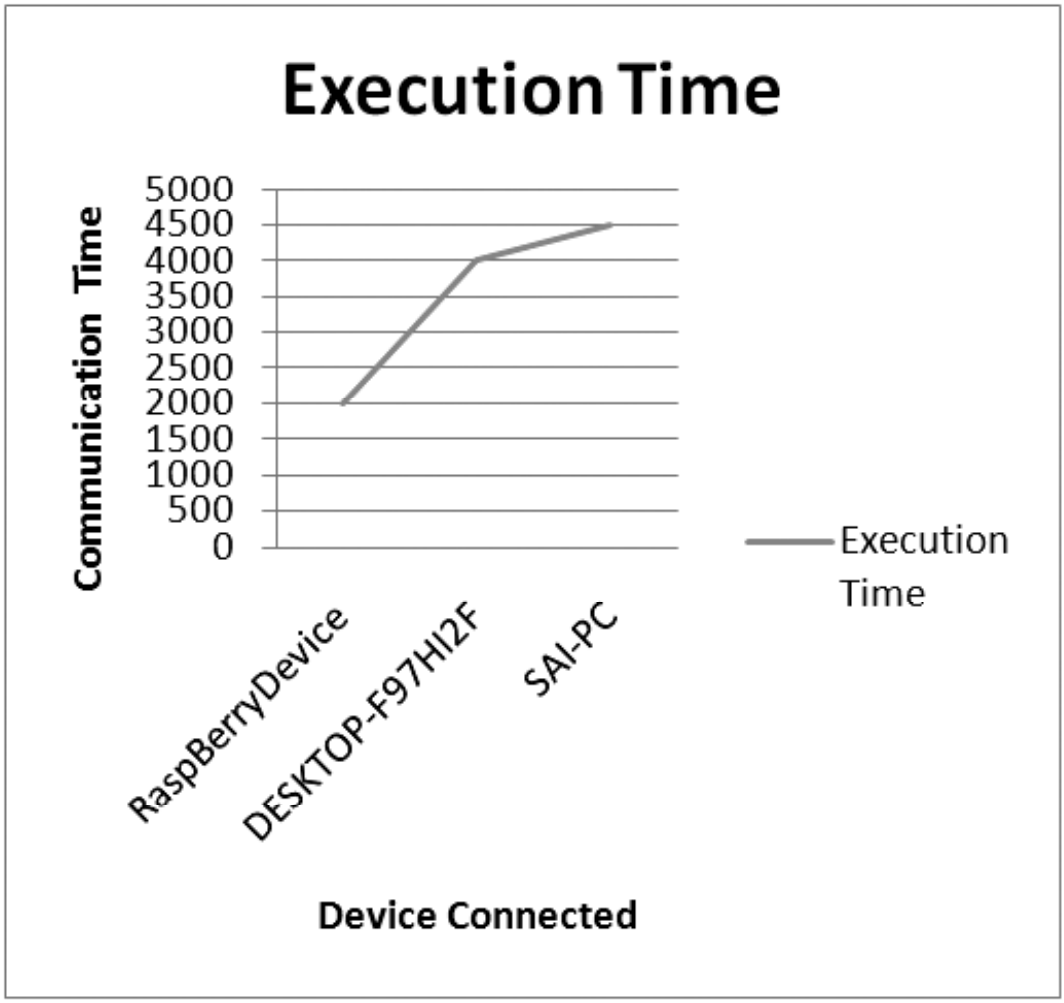

Figure 3b: Device Connection Time Graph

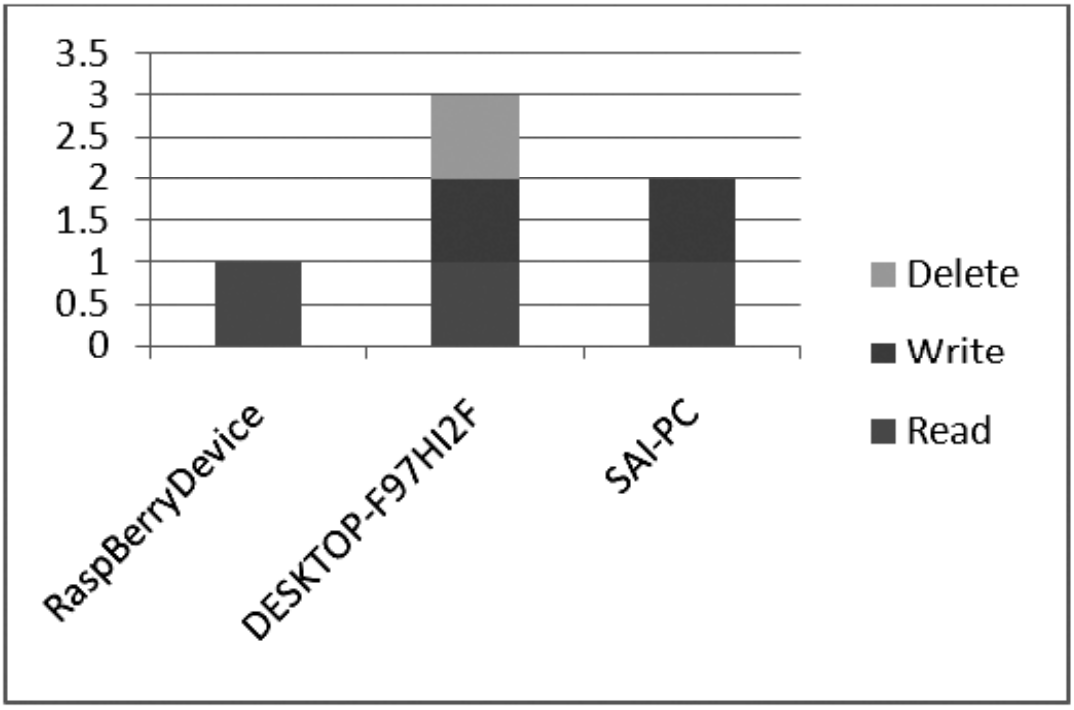

Figure 3c: Device Access Rights

Device Name	Read	Write	Delete	Status
Raspberry Device	yes	No	no	Write/Delete Blocked
DESKTOP-F97HI2F	yes	Yes	yes	Full Access
SAI-PC	yes	Yes	no	Delete Blocked

Figure 3d: Device Access Rights Status

4.2. Comparison of Different Access Control Algorithms

Table 4.2. Comparison of Different Access Control Algorithm

Algorithms	*Generic*	*Scalable*	*Granular*	*Delegation*	*Time Efficient*	*Security*
ICAC	Yes	Yes	No	Yes	Yes	Yes
ACL	Yes	No	No	No	No	No
RBAC	No	No	Yes	Yes	No	No
CWAC	Yes	No	Yes	No	No	No

Table 4.2. Show the comparison of these access control algorithms.This comparison is grounded on functional parameters such as generic nature, scalability, granularity, delegation, time efficiency and security. State of the art for authentication and access control shows that there is no integrated protocol for authentication and access control. Goal is to achieve mutual identity establishment, i.e. authentication and once authenticated access control will take place. In this paper proposes a new method of authentication of devices also access control for the IoT resources using key approach with scalability and less memory requirements. The most important design issue of IoT is the mobility of heterogeneous devices and proposed scheme works efficiently for this purpose.

4.3. Performance of Administration Utility under Heavy Usage

Following tableshows the performance benefit of the interpretation of the devices.

Table 4.3.a
Performance of Administration Utility under Heavy Usage

Administration Utility	*Time in Sec*	
	Old	*New*
Real	0.07	0.05
User	0.06	0.05
System	0.01	0.01

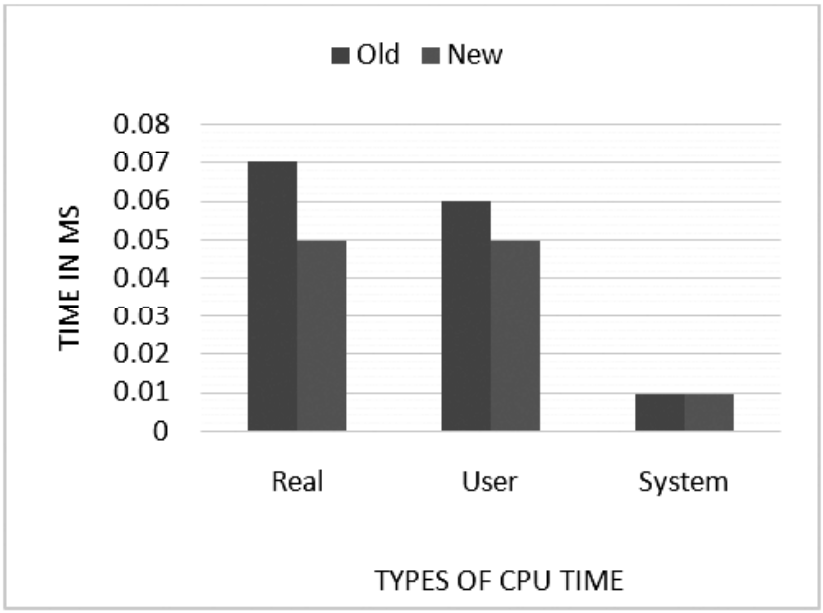

Figure 4: Performance of Administration Utility under Heavy UsageTime

It represents the time took to enable a policy through the administration utility. The rule set that was used contained a combination of available Devices in network. Here is amassive difference in running times of the two versions.

4.4. Synthetic Benchmark

It permits producing different types of workloads to encounter a precise sub-system of the hardware under test. CPU, Memory I/O, Disk I/O, and Network I/O are the main constituents that we want to test in this part of the experiments.

CPU-The results show different test cases.

Table 4.4.a
Test Cases for CPU Benchmark

CPU Benchmarking	
Execution Time	*Power Consumption*
434.074	1.4140
446	1.4054

However, thecontainer engine introduces a negligible impact on the CPU performance, with a percentage difference in the order of 2.67%.

Memory I/O - For testing memory performance. Same as tothe CPU case, native and container performance can be considered comparable with a max percentage difference of 6.04% during the memory test cases.

Table 4.4.b
Test Cases for Memory Benchmark

Memory Benchmarking			
	Average Speed		*Power Consumption*
598.22	70.93	601.55	2.2314
562.05	70.43	570.51	2.2478

5. CONCLUSION

Summary of this is, one vision of the future is that IoT becomes a utility with increased sophistication in sensing, actuation, communications, control and in creating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. Due to the large scale of devices new research problems will arise. The connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security. In addition to the support of the addressing, IPv6 offers the possibility to provide a scalable security and mobility.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] A. Abbasi and H. Chen, "CyberGate: A System and Design Framework for Text Analysis of Computer Mediated Communication," MIS Quarterly, vol. 32, no. 4, pp. 811-837, 2008.

[3] A. Abbasi, H. Chen, S. Thoms, and T. Fu, "Affect Analysis of Web Forums and Blogs Using Correlation Ensembles," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1168-1180, Sept. 2008.

[4] A. Abbasi, H. Chen, and A. Salem, "Sentiment Analysis in Multiple Languages: Feature Selection for Opinion Classification in Web Forums," ACM Trans. Information Systems, vol. 26, no. 3,article no. 12, 2008.

[5] S. Argamon, C. Whitelaw, P. Chase, S.R. Hota, N. Garg, and S. Levitan, "Stylistic Text Classification Using Functional Lexical Features," J. Am. Soc. Information Science and Technology, vol. 58, no. 6, pp. 802-822, 2008.

[6] P.V. Balakrishnan, R. Gupta, and V.S. Jacobs, "Development of Hybrid Genetic Algorithms for Product Line Designs," IEEE Trans. Systems, Man, and Cybernetics, vol. 34, no. 1, pp. 468-483, Feb. 2004.

[7] H. Cui, V. Mittal, and M. Datar, "Comparative Experiments on Sentiment Classification for Online Product Reviews," Proc. 21st AAAI Conf. Artificial Intelligence, pp. 1265-1270, 2006.

[8] F. Fleuret, "Fast Binary Feature Selection with Conditional Mutual Information," J. Machine Learning Research, vol. 5, pp. 1531-1555, 2004.

[9] I. Guyon, J. Weston, S. Barnhill, and V. Vapnik, "Gene Selection for Cancer Classification Using Support Vector Machines," Machine Learning, vol. 46, pp. 389-422, 2002.

[10] I. Guyon and A. Elisseeff, "An Introduction to Variable and Feature Selection," J. Machine Learning Research, vol. 3, pp. 1157- 1182, 2003.

[11] M. Hall and L.A. Smith, "Feature Subset Selection: A Correlation Based Filter Approach," Proc. Fourth Int'l Conf. Neural Information Processing and Intelligent Information Systems, pp. 855-858, 1997.

[12] M. Hu and B. Liu, "Mining and Summarizing Customer Reviews,"Proc. ACM SIGKDD, pp. 168-177, 2004.

[13] V. Ng, S. Dasgupta, and S.M.N. Arifin, "Examining the Role of Linguistic Knowledge Sources in the Automatic Identification and Classification of Reviews," Proc. Conf. Computational Linguistics, Assoc. for Computational Linguistics, pp. 611-618, 2006.

[14] B. Pang, L. Lee, and S. Vaithyanathain, "Thumbs Up? Sentiment Classification Using Machine Learning Techniques," Proc. Conf. Empirical Methods in Natural Language Processing, pp. 79-86, 2002.

[15] B. Pang and L. Lee, "A Sentimental Education: Sentimental Analysis Using Subjectivity Summarization Based on Minimum Cuts," Proc. 42nd Ann. Meeting of the Assoc. Computational Linguistics, pp. 271-278, 2004.

[16] W. Bian and D. Tao, "Harmonic Mean for Subspace Selection," Proc. 19th Int'l Conf. Pattern Recognition, 2008.

[17] D. Tao, X. Li, X. Wu, and S.J. Maybank, "Geometric Mean for Subspace Selection," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 31, no. 2, pp. 260-274, Feb. 2009.

[18] D. Tao, X. Li, X. Wu, and S.J. Maybank, "General Averaged Divergence Analysis," Proc. Seventh IEEE Int'l Conf. Data Mining, pp. 302-311, 2007.

[19] T. Zhang, D. Tao, X. Li, and J. Yang, "Patch Alignment for Dimensionality Reduction," IEEE Trans. Knowledge and Data Eng., vol. 21, no. 9, pp. 1299-1313, Sept. 2009.

[20] I. Hemalatha1, Dr.G.P.S.Varma2 and Dr.A.Govardhan3 "Feature Relation Networks for Sentiment Detection in Messages "International Journal for Resear ch in Science & Advanced Technologies Issue-3, Volume-2, 044-046.

[21] Ahmed abbasi, Stephen France, Zhu Zhang, and Hsinchun Chen, Fellow, "Selecting Attributes for Sentiment Classification Using Feature Relation Networks" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 3, MARCH 2011.