HBAC: An access control over Semantics-enabled Smart Grids to enable energy-efficiency and lifetime optimization

Isma Farah Siddiqui, Asad Abbas, Scott Uk-Jin Lee
Dept. of Computer Science & Engineering, Hanyang University, Ansan, South Korea
isma2012,asadabbas,scottlee@hanyang.ac.kr

Abstract—**Smart grid is deployed with Information and Communication (ICT) technologies using numerous IoT devices. IoT devices are durable and ensures semantic enriched data transformation to smart grid repository. To this extent, devices are utilized with initial installed configurations as smart grid do not have a re-enforcement control over IoT devices. As a result, device may get overloaded with inefficient throughput and huge energy consumption. In this paper, we present a Handshake Based Access Control (HBAC), which re-enforce custom defined configurations over IoT devices. Our proposed mechanism allows smart grid to deploy optimized policy modules over IoT devices. The case study presented in this paper elaborates significance of optimization over device lifetime and energy consumption.**

Keywords-component: Smart Grid; IoT; Handshake Based Access Control (HBAC); ICT.

I. INTRODUCTION

The concept of smart grid is designed to meet auto-facilitation of electricity units in terms of reliability, energy efficiency, integrated communication with sensing measurements, self-healing and fault detection mechanism. Data digitization has given modern aspects i.e. advanced control and self-optimizing decision support to smart grid computing. The phenomena of Internet of Things (IoT) consists of large number of devices connected together. Data generated at nodes is acquired using a machine interpretable format and can be utilized for a meaningful processing to knowledge base repositories. ICT-based IoT devices are programmed to synchronize device performance with smart grid using consistent multithreaded approaches. Semantic grid collaborates smart grid with IoT devices, and facilitates with applicable coalition scenario in between [1].

Semantics-enabled smart grid is a notable utilization of semantic web technologies. The framework being used to process IoT datasets through semantic grid is Resource Description Framework (RDF). Fine grained data is received in device type format at an IoT device buffer and transformed to RDF format. The semantic grid data in RDF format is stored in their respective repositories [2].

Access control mechanism controls activity of a subject which performs some operation to an object. The mechanism is further categorized in Access Control List (ACL), Attribute Based Access Control (ABAC), Policy Based Access Control (PBAC), Role Based Access Control (RBAC), and Capability based access control (CapBAC) [3]. ACL grants access rights to specific subjects but become complex when number of resources and subjects increases. ABAC resolves role explosion issues but do not define whether an attribute is within the domain or outside the domain. PBAC grants access to multiple systems but limited to specific resource only. Extending to that, RBAC grants rights to roles and subjects to roles but lead to role explosion when resources increases and do not discuss multiple subjects. Finally, CapBAC grants customized access control over IoT devices without any limit of things (subjects and resources) but do not deal with data transformation between a subject-to-object (RDF enabled access control approach) and subject-to-subject (IoT enabled access control approach).

When a device unit generates dataset, the originated data is transformed into RDF format within the transformation channel. Data is stored in RDF data repository, from where smart grid can access and process it in an efficient way as seen from Fig. 1. In the current scenario, IoT devices are handling large amount of data input. Smart grid is a case sensitive phenomena and a single misshape could lead to disastrous circumstances i.e. improper data input due to device runtime durability issue or inappropriate power consumption issues. Furthermore, IoT devices are not programmed to re-enforce configurations in between large scale operations and a mechanism to synchronize data between smart grid and devices is unavailable due to independent working medium of RDF access control and IoT access control. As a result, garbage data can be stored in repository with large amount of indexing and sorting issues and device durability is decreased with a huge power loss in such a smart grid scale.

To solve above mentioned deficiencies, we propose Handshake Based Access Control (HBAC) which integrates access control mechanisms in between RDF enabled access control and IoT enabled access control. Main contributions of this paper are:

- A handshake mechanism of RDF enabled access control to IoT enabled access control.
- RDF analytics based reinforcement of IoT device configurations.
- Energy efficient and optimized throughput policy enforcement to IoT devices.

The rest of the paper is organized as follows. Section II presents related work. Section III provides proposed approach. Section IV elaborates architectural details with case study. Finally, section V concludes paper along with future work.

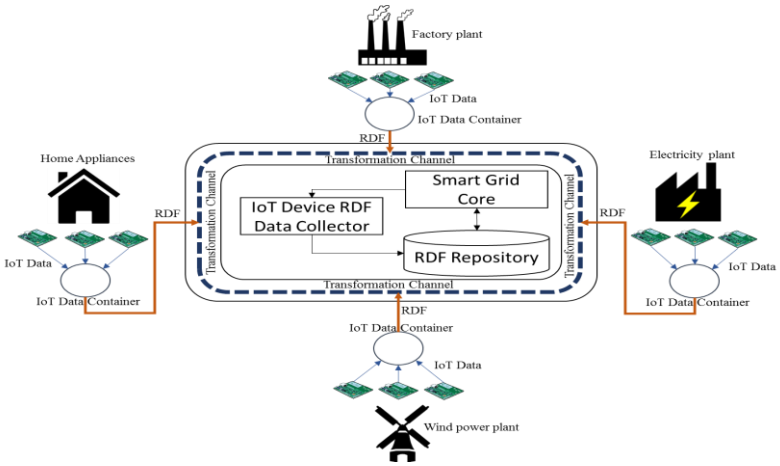

Figure 1. Semantics-enabled Smart Grid integrated with IoT devices

II. Related Work

Since IoT devices started being deployed over grids, researchers are giving their valuable input. Initially, Jabłońska [4] discussed IoT devices over smart grid but how the data is processed from device to a repository is not discussed. Later, Aitor [2] discuss accessing and processing data to RDF repository in smart grid environment but lack IoT devices contribution in it. Xiang Su [5] discussed IoT data transformation from SenML to RDF as an efficient mechanism, but is limited to only SenML enabled devices and do not transform IoT capability control to RDF. Semantic data provisioning provides a basic mechanism of storing IoT data directly into RDF database but does not discussed access controls and data transformations which results in experimental issues [6].

IoT devices and smart grid are not connected with a same medium. Therefore, smart grid needs a mechanism to enforce changes to IoT devices. Grid core is only aware of RDF based access control policies i.e. ABAC and RBAC and do not interpret CapBAC, which is IoT based access control policy. In order to convey an interpretable enforced message, a Handshake Based Access Control (HBAC) is proposed in this paper.

III. Proposed Approach

A. *Handshake Based Access Control (HBAC)*

Smart Grid Core (SGC) dispatches an enforcement message to ABAC/RBAC policy module, attributes and roles are verified over their respective environment and role store containers. Policy Information Point (PIP) serves as a source of roles and attributes. It is a backup service to an enforcement request for information about any missing roles and attributes. Policy Decision Point (PDP) evaluates policy application of smart grid core request and return an enforcement authorization decision. Policy Enforcement Point (PEP) receives the authorization decision and deploy access control authorization and enforcement over resource. PEP further communicates enforcement ruling to handshake layer as seen from Fig. 2.

Handshake Based Access Control (HBAC) includes default CapBAC policy module. Source values stored in PIP, PEP and PDP are override with a policy prefix change. RBAC/ABAC data (subject-to-object) is transformed to CapBAC data (subject-to-subject) and become ready to dispatch as HBAC instance as depicted in Fig. 3.

IV. Architecture of a Semantics-enabled Smart Grid with HBAC support

Fig. 4 presents architectural details of a semantics-enabled smart grid with added HBAC support. An IoT device sends generated data through a network path to IoT device RDF container. At that time, data format is observed as raw IoT device format. IoT device RDF layer linker converts raw data format into RDF format. RDF formatted data is dispatched to transformation channel. RDF data is collected at IoT device RDF Data Collector unit. This unit identifies data format and store it to RDF repository.

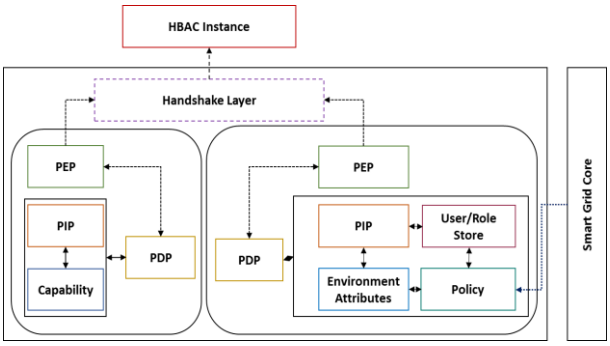

Figure 2. Handshake Based Access Control (HBAC)

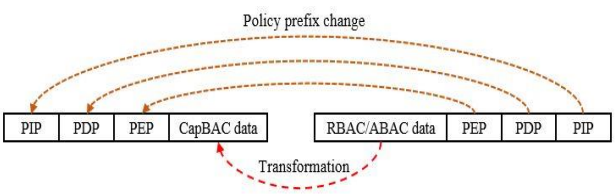

Figure 3. Internal Mechanism of HBAC Layer

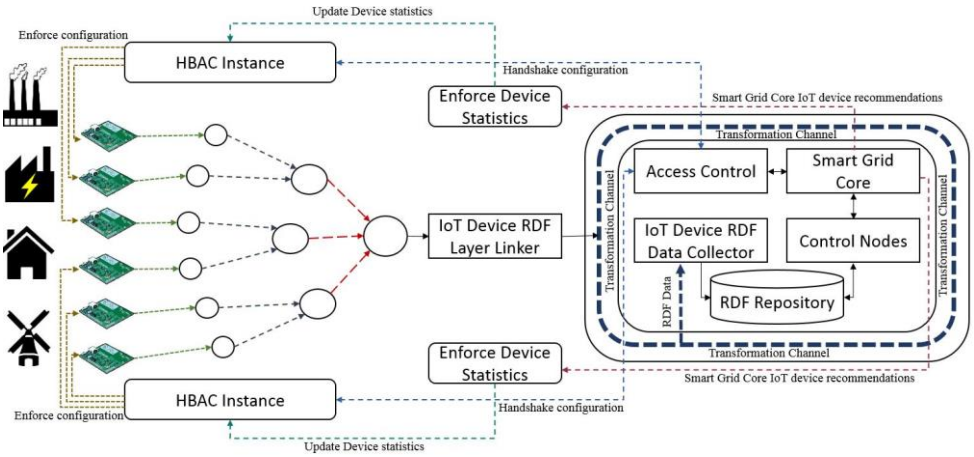

Figure 4. Architecture of Semantics-enabled Smart Grid with HBAC Support

SGC access RDF data through control nodes module. SGC do not access repository directly but process distributed jobs through control nodes. Data analytics is also managed by control nodes. Analytics includes: 1) IoT devices data transformation statistics 2) Power consumption of entire process, and 3) Data availability.

IoT devices integrity and availability is a prime concern of smart grid. In order to ensure optimized performance, smart grid analyzes IoT data stored in repository. RDF data includes IoT device ID, information processed through IoT device and power consumption with working rate/second. Through analytics, smart grid become aware of lifetime including throughput and energy being consumed by a specific IoT device.

As shown in Fig. 4, SGC identifies overburdened IoT device through data analytics. The sole purpose is to increase lifetime with optimized energy consumption and throughput. SGC dispatches enforcement module consisting of two parts:

1) Access control policy, and

2) Enforce IoT device module.

Access control policy is processed through an access control module and dispatched to HBAC instance container. Enforce device module includes the enforcement configuration to deploy over targeted IoT device. Policy is dispatched to enforce device statistics module which enforce IoT device model configuration properties in method and dispatch to HBAC instance. HBAC instance includes the enforcement method and access control policy for IoT device, which after integration are further dispatched to concerned IoT Device. IoT device gets refurbished and optimized over defined configuration.

V. CONCLUSION

IoT devices in a smart grid plays a vital role in routine operations processing. With the passage of processing timeline, an IoT device becomes inefficient and may consume more than usual energy resources. The communication medium between an IoT device and smart grid is not same and it is difficult to optimize a device's lifetime with its optimized energy consumption. In this paper, we have presented a Handshake Based Access Control (HBAC), which communicates between smart grid cores and deploys enforced configurations for optimized throughput utilization and remove energy consumption overhead from IoT devices.

In the future, we plan to explore direct and indirect RDF transformations over smart grid and enforcement policy issues within it.

REFERENCES

[1] S. Karnouskos, "The cooperative internet of things enabled smart grid." In Proc of the 14th IEEE international symposium on consumer electronics (ISCE2010), June. 2010.

[2] A. Pena, and Y. K. Penya, "Distributed semantic repositories in smart grids." In Proc of 9th IEEE International Conference on Industrial Informatics (INDIN 2011), IEEE, 2011.

[3] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," in Journal of Mathematical and Computer Modelling, Vol. 58. No. 5, pp. 1189-1205, 2013.

[4] M. R. Jabłońska, "Internet of things in smart grid deployment." Rynek Energii 2 (2014): 111.

[5] S. Xiang, H. Zhang, J. Riekki, A. Keränen, J. K. Nurminen, and L. Du, "Connecting IoT Sensors to Knowledge-based Systems by Transforming SenML to RDF." Procedia Computer Science 32 (2014): pp. 215-222.

[6] A.I. Maarala, S. Xiang, and J. Riekki. "Semantic data provisioning and reasoning for the Internet of Things." Internet of Things (IOT), 2014 International Conference on the. IEEE, 2014.