International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

Secure Physical-Cyber-Social Convergence for the Internet of Things

Pranjal Chitte[1], Madhuri Chikhale[2], Pooja Gaikwad[3], Prajakta Khale[4]
Department of Computer Engineering, SND College of Engineering & RC, Yeola

***Abstract*-- The IoT is fastly relying on cloud computing and smart devices with sensors built in, in addition with thousands of applications to support them. In the world of Internet, IOT is one of the most important system model for interaction among different ubiquitous things. In this IOT plays an important role in interaction among the physical perception, cyber interaction & social correlations. While achieving all this, IOT is suffering from several security issues, so we need to find out the solution for security protection. In this paper, we design a system using U2IoT architecture (unit IOT & ubiquitous IOT). The homomorphism functions, directed path descriptors, & Chebyshev chaotic maps are jointly applied for mutual authentication. Many access authorities are assigned to achieve hierarchical access control. It also proof the accuracy of proposed APHA with the help of BAN logic. This is also applicable for other IoT application.**

***Keywords*- IOT, Security, authentication protocol, U2IoT architecture**

I. INTRODUCTION

The IOT technology comes from innovative developments and concepts in communication & information technology associated with ubiquitous connectivity, Pervasive computing & Ambient Intelligence. Basically IOT is considered as a network of networks containing anything such as sensors, physical objects, digital entities etc. The IOT has the purpose of providing an infrastructure facility the exchange of things in a secure & reliable manner. The global Internet-based technical architecture has an impact on the privacy & security of the involved stakeholders. Measures insuring the resilience to attack of architecture, data authentication, client privacy & access control need to be established.

This paper presents an overview of the security aspect of U2IoT architecture and recommended countermeasures. In particular, we review the functionalities for secure authentication. The remaining paper is organized as follows: Section I presents the literature survey and gives the progress in the field of IOT for different architecture. Section II gives introduction to proposed system architecture and authentication scheme. Section III shows the algorithmic strategies used. Finally, in section IV we draws a conclusion.

II. LITERATURE SURVEY

From the last few year, many industrial and academic project have been started to resolve the IOT issues like information disclosure security issue, malicious traceability issues and mobility object issues etc. In "**HIP security architecture for the IP based internet of things**" Meca et al. proposed a solution which is a compact combination and extension of HIP (Host identity protocol) and MIKEY (Multimedia Internet KEYing protocol) that enhance key management and secure network association. The self-governing multi-hop IP security architecture present favorable results compared to other IP based existing solution [2]. Raza et al. in "**Lithe: lightweight secure CoAP for the internet of things**" proposed a novel DTLS (Datagram Transport Layer Security) header compression scheme to reduce energy consumption by using the 6LoWPAN (IPv6 over low power wireless personal area network) standard and CoAP (Constrained Application Protocol) to provide protection for transmission of sensitive data. But it does not deploy Lithe in a real world IOT system with a real application scenarios [4]. In **"A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications."** Yao et al. design a message authentication code, this will be based on multicast authentication mechanism. It will be used for the small scale IOT application [6].

Despite vast literature were reviewed on some occasions and new secure communication have been proposed [1], [5], none of which considered the security and privacy issues of U2IoT as a whole system.

III. PROPOSED SYSTEM

Our proposed system works on the U2IoT architecture in which first U indicate unit IoT which refers to a basic network unit for a single application and second U indicate ubiquitous IoT which includes multiple applications within the centralized national management. Here we consider different scenarios in which multiple industrial IoT manages the corresponding unit IoT of different industries. The industrial IoTs are combined to form a national IoT to realize the interconnections.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

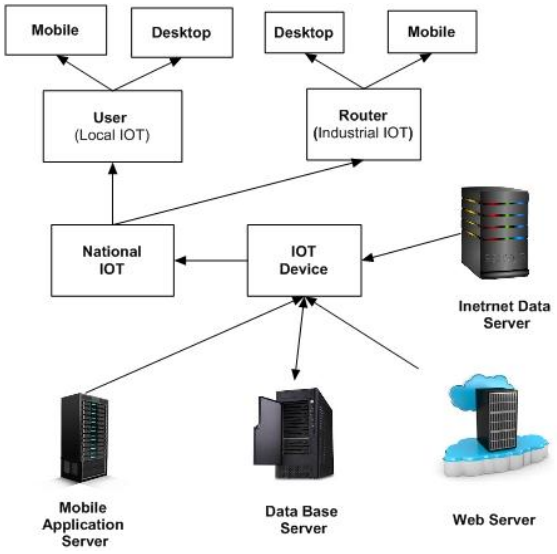

Figure 3.1: System Architecture

3.1 System Design

It is divided into following parts:-

1] Local IOT: It contains multiple unit IOT that means it is the collection of many unit IOT. Single application or multi-application can be established to compose a local IOT within a region.

2] Industrial IOT: As similar to local IOT it establishes different IOT frameworks but in a large level that is for an industry. It is the integration of multiple unit IOT's.

3] National IOT: The local IOT and industrial IOT comes under this national IOT. The national IOT have the authority to access both the local IOT and industrial IOT and can also manage multiple industrial data centres operations.

IOT device: It takes the data from the different level of IOT's to do the desired operation on it. The servers such as mobile application server, database server, web server are connected to the IOT device for authentication purpose.

The system architecture should fulfil the following prerequisite-

- Confidentiality, Integrity, and Availability
- Hierarchical access control
- Forward security
- Mutual authentication
- Privacy preservation

IV. ALGORITHMS

KNN Algorithm:

Central to many application involving moving objects is the task of processing K-nearest neighbor (KNN). The following important factor must be considered when designing method to process K-NN queries: 1) communication cost, 2) maintenance cost, 3) load balancing

1) *Communication cost :* To process k-NN queries in parallel with multiple servers may incur excessive data communication, which is very costly as compared with CPU cost.

2) Maintenance cost : The movements of the large number of objects lead to frequent updates to the indexes used for processing k-NN queries. So, the index structures must be designed for query processing that can be supported efficiently and updates can be handled simultaneously.

3) Load balancing : In actual,queries and the moving objects are usually non-uniformly distributed. So it is important to concentrate on storage of objects and distribution of query load to different nodes in the cluster to achieve good load balancing.

For each training example <p,f(p)>, add the example to the list of training examples.

Given a query instance pq to be classified,

_ Let p1,p2….pk denote the k instances from training examples that are nearest to pq .

_ And return the class of the k instances that represents the maximum of the k instances

V. CONCLUSION

In our paper, we reviewed different security strategies considered by previous researches for IoT systems. The primary need for any IoT security systems can be summarized as follows: 1. Authentication & Authorization 2.Data Privacy 3.Trust between involved parties .A secure aggregate authentication scheme that achieves end-to-end security under an adversary who does not learn any system secret. Our construction is efficient and supports iterative aggregation. we have proposed a scheme for thU2IoT architecture and also proved the accuracy of proposed system using BAN logic. The proposed scheme and homomorphism based Chebyshew chaotic maps, establishes trust relationships via the lightweight mechanisms and applies dynamically hashed values to achieve session freshness.

REFERENCES

[1] Bin Guo, Daqing Zhang , Zhiwen Yu , Yunji Liang, Zhu Wang & Xingshe Zhou. "From the internet of things to embedded intelligence." World Wide Web (2013) 16:399–420 DOI 10.1007/s11280-012-0188-y (2013): 400-420.

[2] Francisco Vidal Meca, Jan Henrik Ziegeldorf RWTH Aachen University,Pedro Moreno Sanchez, Oscar Garcia Morchon, Sandeep S. Kumar, Sye Loong Keoh Philips Research Eindhoven. "HIP security architecture for the IP-based Internet of Things." 2013 27th International Conference on Advanced Information Networking and Applications Workshops (2013): 1331-1336.

[3] Ning, Senior Member, IEEE, Hong Liu, Student Member, IEEE, and. "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things." IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 3, MARCH 2015 657 (2015): 657-665.

[4] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt. "Lithe: Lightweight Secure CoAP for the Internet of Things." IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013 (2013): 3711-3720.

[5] Thomas Kothmayr, Corinna Schmitt c, Wen Hub, Michael Brünig b, Georg Carle a. "DTLS based security and two-way authentication for the Internet of Things ." Ad Hoc Networks xxx (2013) xxx–xxx (2013): 1-14.

[6] Xuanxia Yao, Xiaoguang Han, Xiaojiang Du, Senior Member IEEE, and Xianwei Zhou. "A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications." IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013 (2013): 3693-3701.

[7] ZHANG-Tong, WU-Qi, LIU-Wen, CHEN-Liang. "Homomorphism Encryption Algorithm for Elementary Operations over Real Number Domain." 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover (2012): 166-169.