Improved Security and Efficiency with Time Based Tokenized System & COAP for Internet of Things (IOT)

[1]Shivani Bilthare, [2]Ashok Verma
[1,2]Dept. of Computer Science & Engineering, GGITS, Jabalpur, Madhya Pradesh, India

Abstract

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has interconnections through the physical, cyber and social spaces. Most of devices among them are resource constrained. During the interaction between devices, IoT gets suffered from severe security challenges. Security of resource constrained networks becomes prime important. Many existing mechanisms give security and protection to networks and systems but they are unable to give fine grain access control. In this work, focus is on enhancing the performance of the IoT system with high security and least usage of the resources on the constrained devices i.e. the load related with security is kept on the servers which are high resource oriented. Performance of CoAP based framework is enhanced and compared with existing security CoAP implementations. Test results shall be compared for communication overhead and authentication delays.

Keywords

IoT, Cloud Computing, Security, Constrained Application Protocol, Resource Management, Token System

I. Introduction

The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society.

The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.

When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a smart grid, and expanding to the areas such as smart cities.

"Things," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental / food / pathogen monitoring or field operation devices that assist firefighters in search and rescue operations. Legal scholars suggest looking at "Things" as an "inextricable mixture of hardware, software, data and service". These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include home automation (also known as smart home devices) such as the control and automation of lighting, heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer / dryers, robotic vacuums, air purifiers, ovens or refrigerators / freezers that use Wi-Fi for remote monitoring.

As well as the expansion of Internet-connected automation into a plethora of new application areas, IoT is also expected to generate large amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IoT is one of the platforms of today's Smart City, and Smart Energy Management Systems.

The concept of the Internet of Things was invented by and term coined by Peter T. Lewis in September 1985 in a speech he delivered at a U.S. Federal Communications Commission (FCC) supported session at the Congressional Black Caucus 15th Legislative Weekend Conference.

II. Cloud Computing

Cloud computing is a collection of technologies that allow IT resources to be virtualized, used on an on-demand basis and delivered via the Internet as services. Cloud computing can be considered a new computing paradigm in so far as it allows the utilization of a computing infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. It is sold on demand, typically by the minute or the hour; it is elastic - a user can have as much or as little of a service as they want at any given time and the service is fully managed by the provider. Because of the it's features of greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention.

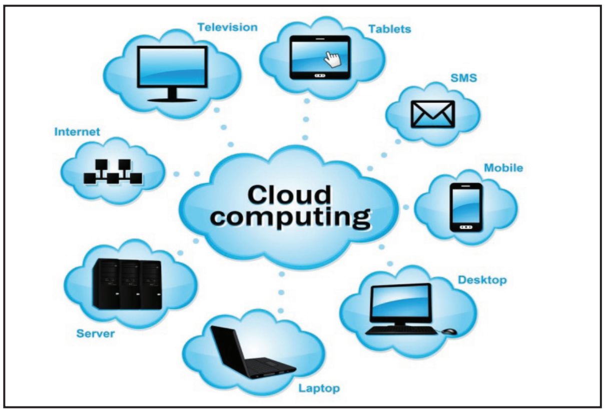

Fig. 1: Cloud Computing

Cloud Computing can be classified into 4 types on the basis of location where the cloud is hosted:-

A. Public Cloud

A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. It is owned by a cloud provider selling cloud services and, by definition, is external to an organization.

B. Private Cloud

A private cloud a proprietary network or a data center that supplies hosted services to a limited number of people. It may be managed either by the organization or a third party, and may be hosted within the organization's data center or outside of it.

C. Community Cloud

A community cloud is somewhat similar to a private cloud, but the infrastructure and computational resources are shared by several organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization.

D. Hybrid Cloud

A hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables interoperability.

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure resources, application platform and software as services to the consumer.

1. Software-as-a-Service

SAAS is defined as a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network. Also known as "on demand" software, it is the most mature type of Cloud Computing because of its high flexibility, proven support services, enhanced scalability, reduced customer maintenance, and reduced cost due to their multi-tenet architectures. It is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

2. Platform-as-a-Service

PAAS provides infrastructure on which software developers can build new applications or extend existing applications without requiring the need to (purchase development, QA, or production server infrastructure. It is a model of software deployment where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

3. Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

The cloud platform is used in this project is IBM Bluemix. It is an open standard, cloud based platform for building, managing and running applications of all types (web, mobile, big data, new smart devices, so on).

This work is providing solution for following main issues in the constrained devices over IoT:

- The main objective of this work is to discuss, analyze & provide high security in Internet of Things in order to make the data and devices attached to the IoT.
- It provides the detailed discussion of the security issues might be caused on the Internet of the things and devices attached.
- It also discusses the problem faced in providing security over the IoT as the devices connected to it are mostly resource constrained.
- The dissertation is oriented majorly on the security of IoT and performance degradation caused due to application of the security measures.

It also considers the various security algorithms applied over IoT devices their pros & cons, issues raised and discussed and provide a high performance solution to the problems raised.

III. Existing System

Internet of Things (IoT) is growing as an attractive system paradigm. There is a lot of hype around the internet of things (IoT) and it continues to evolve as authors move beyond humans talking to machines. IoT has interconnections through the physical, cyber and social spaces. Things used in IoT are sensors and actuators, mechanical devices and networking includes gateways, wireless infrastructure. Most of devices among them are resource constrained. During the interaction between devices, IoT gets suffered from severe security challenges. Complicated network produces potential vulnerabilities referred to heterogeneous devices, sensors and backend systems. So to realize the dream of internet of things secured device to device communication is expected. Security of resource constrained networks becomes prime important. Many existing mechanisms give security and protection to networks and systems but they are unable to give fine grain access control. In this work, we focused on CoAP based framework to give service level access control on resource constrained devices. It gives fine grain access control on a per service basis. ECDSA is used to improve privacy of the system. Performance of CoAP based framework is compared and analyzed with existing security solutions. Test results are presented which shows that communication overhead and authentication delay are less than the existing system. Hence security performance of system gets improved. The goal is to present comprehensive security framework for low power networks consist of resource constrained devices according to M. B. Tamboli and D. Dambawade [1].

The Internet of Things (IoT) comprises a complex network of smart devices, which frequently exchange data through the Internet. Given the significant growth of IoT as a new technological paradigm, which may involve safety-critical operations and sensitive data to be put online, its security aspect is vital. This paper studies the network security matters in the smart home, health care and transportation domains. It is possible that the interruption might occur in IoT devices during operation causing them to be in the shutdown mode. Taxonomy of security attacks within IoT networks is constructed to assist IoT developers for better awareness of the risk of security flaws so that better protections shall be incorporated by M. Nawir, A. Amir, N. Yaakob and O. B. Lynn [2].

Internet of Things (IoT) paradigm involves new characteristics, techniques and threats that cannot be completely taken into consideration through the traditional formulation of security problems. The IoT calls for a new paradigm of security, which will have to consider the security problem as a comprehensive approach including the new actors and their interactions. Biologically inspired models for security have been more flourishing to put up the wonderful defense in securing ad hoc networks. Because of the features of ad hoc network, they require a strong, decentralized security mechanism. The similarities between the biological phenomenon's and the operations of the network make bio inspired approach an interesting field for research. In this paper R. Banu, G. F. A. Ahammed and N. Fathima explore various biologically inspired approaches to security in IoT and significant findings as well as a brief illustration of research gap for various robust and computationally efficient security techniques in IoT as suggested by R. Banu, G. F. A. Ahammed and N. Fathima [3].

Event-triggering (ET) is an up-and-coming technological paradigm for monitoring, optimization, and control in the Internet of Things (IoT) that achieves improved levels of operational efficiency. This paper first defines the envisioned ET architecture for the IoT domain. It then classifies and reviews the various different ET approaches obtained from the available literature for the three phases of ET, namely behavior modeling, event detection, and event handling. Thereafter, a novel data-driven technique is developed to address all three phases of ET in an efficient and reliable manner. Finally, the applicability of the proposed data-driven technique is showcased in a real-world public transport scenario, demonstrating a substantial improvement in energy and spectrum efficiency compared to existing periodic techniques by P. Kolios, C. Panayiotou, G. Ellinas and M. Polycarpou [4].

Today in the current global scenario, the prime question in every girl's mind, considering the ever rising increase of issues on women harassment in recent past is mostly about her safety and security. The only thought haunting every girl is when they will be able to move freely on the streets even in odd hours without worrying about their security. This paper suggests a new perspective to use technology for women safety. "848 Indian Women Are Harassed, Raped, Killed Every Day!!" That's a way beyond HUGE number! G. C. Harikiran, K. Menasinkai and S. Shirol propose an idea which changes the way everyone thinks about women safety. A day when media broadcasts more of women's achievements rather than harassment, it's a feat achieved! Since we (humans) can't respond aptly in critical situations, the need for a device which automatically senses and rescues the victim is the venture of our idea in this paper. G. C. Harikiran, K. Menasinkai and S. Shirol propose to have a device which is the integration of multiple devices, hardware comprises of a wearable "Smart band" which continuously communicates with Smart phone that has access to the internet. The application is programmed and loaded with all the required data which includes Human behavior and reactions to different situations like anger, fear and anxiety. This generates a signal which is transmitted to the smart phone. The software or application has access to GPS and Messaging services which is pre-programmed in such a way that whenever it receives emergency signal, it can send help request along with the location co-ordinates to the nearest Police station, relatives and the people in the near radius who have application. This action enables help instantaneously from the Police as well as Public in the near radius who can reach the victim with great accuracy [5].

Network Security is one of the important concepts in data security as the data to be uploaded should be made secure. To make data secure, there exist number of algorithms like AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm) etc. These techniques of making the data secure come under Cryptography. Involving lnternet of Things (IoT) in Cryptography is an emerging domain. IoT can be defined as controlling things located at any part of the world via Internet. So, IoT involves data security i.e. Cryptography. Here, in this paper we discuss how data can be made secure for IoT using Cryptography by S. Kulkarni, S. Durg and N. Iyer [6].

The paper presents a survey and analysis on the current status and concerns of Internet of things (IoT) security. The IoT framework aspires to connect anyone with anything at anywhere. IoT typically has a three layers architecture consisting of Perception, Network, and Application layers. A number of security principles should be enforced at each layer to achieve a secure IoT realization. The future of IoT framework can only be ensured if the security issues associated with it are addressed and resolved. Many researchers have attempted to address the security concerns specific to IoT layers and devices by implementing corresponding countermeasures. This paper presents an overview of security principles, technological and security challenges, proposed countermeasures, and the future directions for securing the IoT as per R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan [7].

Internet of Things (IoT) involves creating network of everyday items embedded with electronics, software and network connectivity. In this way, users are empowered with possibility to communicate with devices, in order to control them or retrieve necessary information. Data security in IoT is one of substantial issues. This paper explores security protocols provided by communication technologies used in IoT such as: RFID, Bluetooth, Wireless network and ZigBee. Also, it presents issues which can arise in practical appliance. Finally, M. Grabovica, S. Popić, D. Pezer and V. Knežević give overview, summary and comparison of advantages of described technologies by M. Grabovica, S. Popić, D. Pezer and V. Knežević [8].

Internet of Things (IoT) is growing as an attractive system paradigm. There is a lot of hype around the internet of things (IoT) and it continues to evolve as we move beyond humans talking to machines. IoT has interconnections through the physical, cyber and social spaces. Things used in IoT are sensors and actuators, mechanical devices and networking includes gateways, wireless infrastructure. Most of devices among them are resource constrained. During the interaction between devices, IoT gets suffered from severe security challenges. Complicated network produces potential vulnerabilities referred to heterogeneous devices, sensors and backend systems. So to realize the dream of internet of things secured device to device communication is expected. Security of resource constrained networks becomes prime important. Many existing mechanisms give security and protection to networks and systems but they are unable to give fine grain access control. In this work, authors have focused on CoAP based framework to give service level access control on resource constrained devices. It gives fine grain access control on a per service basis. ECDSA is used to improve privacy of the system. Performance of CoAP based framework is compared and analyzed with existing security solutions. Test results are presented which shows that communication overhead and authentication delay are less than the existing system. Hence security performance of system gets improved. The main goal of authors work is to present comprehensive security framework for low power networks consist of resource constrained devices.

Algorithm & Protocols Used in Existing System

- LAN based mapping of the IoT
- CoAP (Constrained Application Protocol)
- Kerberos
- ECDSA (Elliptical curve Digital Signature Algorithm)

A. Requirements in Existing System

Objective of existing system is to improve the authentication and to get fine grain access control. Communication overhead, authentication delay, computational complexity of the security system should be low to improve security performance. In their work authors have used Ticket System, which is useful to distinguish authenticated user from intruder. So, only valid devices should be allowed to communicate with access control services. In order to enhance the privacy of communication, advanced encryption schemes should be used. Ac- cess methods and rules could be changing with authentication policies. These can be changes according to conditions like position, sensor data, power source, time, quantity, complexity etc. The goal is to present comprehensive security framework and to give fine grain access control per services.

B. Proposed Architecture of the Existing System

Proposed framework uses CoAP, Kerberos and ECDSA solutions to create low power security platform for main server. Architecture is shown in Figure.

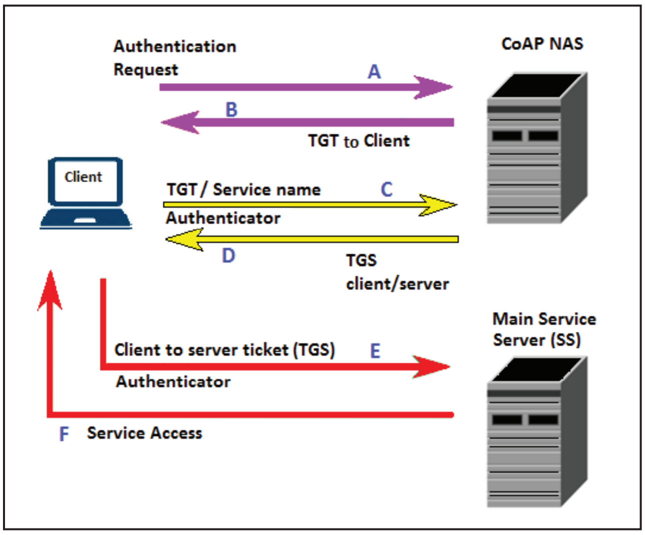

Fig. 2: Proposed Framework Architecture

In Figure 2, the client wants to access services on Main server. So it has first undergone security check at CoAP NAS. New user has to make registration first. Existing user made login and ready to get ticket if login details matched with the stored one (A). Ticket (TGT) is send back to client (B). Now client send request to access particular services along with ticket (TGT) to CoAP NAS (C). If it has valid ticket then CoAP NAS grant the request and returns ticket (TGS) for requested service. Using TGS, client send request for service access situated on main server (E).
After verifying TGS, main server gives reply to Client (F). Whole process is explained briefly in subsection C and D of section III. RMI (Remote Method Invocation) is used here to start the services. Kerberos approach provide authentication by generating ticket for valid user. Authentication service [.well- known/auth] must exist on CoAP server [11]. CoAP server must be able to perform login and logout correctly. On successful login it should generate ticket and on logout should delete it.

IV. Problem Statement

This work is focusing on developing an algorithm that will enhance the performance & security of the IoT system.
Since IoT system is used by many resource constrained devices therefore this work will provide the least usage of the resources on the constrained devices.

V. Proposed Work

In this work, we provide a detailed discussion of the Internet of Things, Cloud Computing, security issues, issues raised when application of the security algorithms is done, resource management, load transfers over high resource devices and enhancing the performance with high security over the IoT devices.
The proposed system is improving the performance of the existing system further by making the following modifications in algorithms and flow of processing:

1. User will input authentication details
2. These will be forwarded to a server residing in the nearest vicinity
3. The server will authenticate the user details and on success will generate a timestamp & a key as in Kerberos security, which will send the same to the user.
4. Server will also generate a random time interval based on the frequency of the use by the user and will keep the same with it.
5. Unlike existing system, key shall not be generated every time user accesses the server, but will be verified.
6. The new key shall be re-generated once the random time interval shall expire.
7. This will reduce the network traffic and load on server and hence will reduce the performance overheads
8. In place of ECDSA, we propose to apply an encryption mechanism to reduce the space requirement and processing time requirement on resource constrained devices.

VI. Conclusion

Internet of Things (IoT) is growing as an attractive system paradigm. IoT has interconnections through the physical, cyber and social spaces. Most of devices among them are resource constrained. During the interaction between devices, IoT gets suffered from severe security challenges. Complicated network produces potential vulnerabilities referred to heterogeneous devices, sensors and backend systems. Security of resource constrained networks becomes prime important. Many existing mechanisms give security and protection to networks and systems but they are unable to give fine grain access control. This work is proposing to provide an implementation and verification of the security and performance over the IoT.

References

[1] M. B. Tamboli, D. Dambawade,"Secure and efficient CoAP based authentication and access control for Internet of Things (IoT)," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, pp. 1245-1250, 2016.

[2] M. Nawir, A. Amir, N. Yaakob, O. B. Lynn,"Internet of Things (IoT): Taxonomy of security attacks," 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, pp. 321-326, 2016.

[3] R. Banu, G. F. A. Ahammed, N. Fathima,"A review on biologically inspired approaches to security for Internet of Things (IoT)," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, pp. 1062-1066, 2016.

[4] P. Kolios, C. Panayiotou, G. Ellinas, M. Polycarpou, "Data-Driven Event Triggering for IoT Applications," In IEEE Internet of Things Journal, Vol. 3, No. 6, pp. 1146-1158, 2016.

[5] G. C. Harikiran, K. Menasinkai, S. Shirol,"Smart security solution for women based on Internet of Things (IOT)," International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, pp. 3551-3554, 2016.

[6] S. Kulkarni, S. Durg, N. Iyer,"Internet of Things (IoT) security," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 821-824, 2016.

[7] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan,"Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, pp. 336-341, 2015.

[8] M. Grabovica, S. Popić, D. Pezer, V. Knežević,"Provided security measures of enabling technologies in Internet of Things (IoT): A survey," Zooming Innovation in Consumer Electronics International Conference (ZINC), Novi Sad, pp. 28-31, 2016.