ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

Hash Authentication Using IoT

Ruchi Sharma

Department of Electrical and Electronics Engineering, Vivekananda Global University, Jaipur, India

Email ID: sharma.ruchi@vgu.ac.in

ABSTRACT:A key principle when delivering the Internet of Things as a service is secure authentication when exchanging data between sender and receiver nodes. Hash algorithms may provide such a framework for IoT based applications to authenticate themselves. The new NIST-standardized safe hash-algorithm methodology is SHA-3. SHA-3 is entirely apt to ensure authentication for a transaction between sender and recipient. The paper presents a novel signature generation technique based upon SHA-3. Under this authentication scheme two of the common IoT communication models for publishing subscribe and request response are examined. The transmitter produces a specific hash code for the data it is about to send. The hash code acts as the transaction's authentication token. For both simulated communication models, mechanisms for the sender receiver interaction are integrated into the system codes. The system architecture controls the receiver's contact with the cloud, too. This interaction ensures that the protocols and api(s) offered by cloud service providers are correctly authenticated and these protocols are also incorporated into the simulation. Both the cloud services used in the network architecture, i.e. cloud messaging as a service, and cloud database as a service ensure verification of the sender's identity. In this way a blanket authentication scheme for the IoT architectures described above is set up.

KEYWORDS: Cloud, Hash Signatures, IoT, Publish-Subscribe, Request-Response, Remote Messaging, Sensors, Web Servers

I. INTRODUCTION

The number of active IoT devices is expected to reach 10 billion by 2020, which is expected to rise to a massive 22 billion by 2025. This shows the possibilities of the Stuff Internet. One such IoT tool, raspberry pi, is a low-cost, portable computer capable of making the Internet of Things more accessible to developing countries. It is a computer capable of serving as both the end node in an IoT network and a small IoT network analytical machine and central server. It offers language support for the python programming. There are two common models of IoT communication, namely subscribe publishing and request response. This paper takes into consideration subscribe publish model with an MQTT broker. Under this model an MQTT broker serves as a server, and the clients are both the publisher and the user. A broker keeps a list of the topics to which different publishers publish information. A customer subscribes to a subject of interest, and can get updates from the broker asynchronously. A publisher will be a hardware sensor which sends sensed data. A subscriber would be a computer which processes the received data further. A publish subscribe architecture is useful for remote communication, where the network bandwidth is restricted and a light code footprint is required.

This is also useful when in a heavy traffic environment there are many nodes which send and receive data. At the other hand, the request response communication model is a tried and tested model which works well in a low traffic environment. Publish subscribe model is asynchronous while the response model for requests is synchronous. Thus publishing subscribe model is versatile and the message can remain in the broker's message queue for some time while the receiver is busy, for a restricted memory broker it is vulnerable to memory buffer overflows. On the plus side, vital data would be available in the broker for publish subscribe model that is implemented in highly sensitive applications even when the receiver is busy. However, in a crucial application for a request response model, there is the risk of unproductive pinging between the recipient and the sender to keep up-to-date continuously. Request response model is therefore a good option for low traffic, non-critical setting, so it is simpler to set up.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

Nevertheless, authentication of the obtained data is a primary task in both the publisher subscriber and request response communication models. SHA-3 (Keccak) offers a safe method to establish a unique data transaction signature, a unique hash-code for this transaction. SHA-3 is the latest of the hash algorithms standardized by the National Institute of Technology and Standards (NIST). Consider X1 and X2 as two messages which produce H (X1) and H (X2) when applying a hash function. With the birthday paradox, a hash collision (theoretically) may be created in O(2n/2) attempts for a n bit hash code. Nonetheless, in practice it is important that the hash algorithm makes such a hash collision (which would compromise the hash algorithm) incredibly difficult to obtain. Hence the option of SHA-3 which is the most stable hash algorithm currently in use. SHA-3 is built with a sponge. It has an absorption step in which it reads in and processes data. It has then a squeezing step in which the output of the hash code is generated.
In the current times an integration of the IoT system with the cloud is indispensable. If the receiver machine needs to communicate some vital information to some remote client, say an android device, a cloud messaging service may help send an acceptable notification. At the same time, the device can upload necessary data to a cloud database. Then, this data can be further analyzed to identify trends that provide insights into the specific study area. The system architecture discussed in the paper takes into account cloud integration and secure authentication in cloud interaction.

II. LITERATURE REVIEW

The Internet of Things (IoT) presented a groundbreaking opportunity to develop powerful industrial systems and applications by exploiting the growing ubiquity of RFID and cellular, mobile and sensor devices. In recent years, a large variety of industrial IoT applications have been developed and deployed. This paper discusses existing IoT research, key enabling technologies, major IoT applications in industries, and describes research trends and challenges, in an attempt to understand the growth of IoT in industries. A significant contribution of this study paper is that it thoroughly sums up the latest state-of - the-art IoT in industries[1]. The Internet of Things (IoT) has drawn considerable attention to work over the last year. IoT is seen as part of the Internet of the future which will contain billions of intelligent' things' that interact. The Internet's future will be comprised of heterogeneously linked devices that will further expand the world's boundaries with physical entities and virtual components. The Internet of Things (IoT) will add new capabilities to the linked devices. The concepts, architecture, basic technologies, and IoT implementations are regularly checked in this study[2]. Communications on the Internet of Things (IoT) are considered a component of the new generation of wireless communication networks. As such, IoT represents a term leading to various design strategies to achieve specific efficiency and performance goals. Base stations must be able to provide an expanded range in that case for a large number of low data rate nodes. On the other hand, IoT nodes must be low-cost devices with limits on the total available power (i.e. powered battery) and processing capacity[3]. This paper offers an overview of the Internet of Things (IoT) with a focus on technology enabling, protocols, and implementation issues. The IoT is allowed by the latest advances in RFID, smart sensors, networking technologies and protocols on the Internet. The basic concept is to have smart sensors work directly to create a new class of apps, without human intervention. The present Internet, Web, and Machine-to-Machine (M2 M) technology transition can be seen as the first step of IoT. The IoT is expected to bridge diverse technologies in the coming years to allow new applications by linking physical objects together to support intelligent decision-making[4]. The Internet of Things (IoT), also called the Internet of All or the Digital Internet, is a modern concept of technology conceived as a global network of computers and devices capable of communicating with one another. The IoT is regarded as one of the most important areas of emerging technology and is attracting significant interest from a wide variety of sectors. This article describes five IoT technologies necessary for the delivery of effective IoT-based products and services and addresses three IoT categories for business applications used to maximize the value of the customers[5]. Ubiquitous sensing provided by technology from the Wireless Sensor Network (WSN) cuts through many areas of modern life. This includes the opportunity to assess, infer and appreciate environmental measures, ranging from fragile ecologies and natural resources to urban environments. The prevalence of such devices in a communicating-actuating network produces the Internet of Things (IoT), in which sensors and actuators integrate seamlessly with the world around us, and the knowledge is exchanged across channels to build a common operating picture (COP). Encouraged by the recent adoption of a range of wireless technologies such as RFID tags and built-in sensor and actuator nodes[6]. This paper thus offers a detailed overview of the technologies, protocols, and architecture supporting an urban IoT. The paper will also present and discuss the technological approaches and best practice recommendations implemented in the Padova Smart City project, a proof-

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

of-concept installation of an IoT island in the city of Padova, Italy, conducted in cooperation with the municipality [7]. The Internet of Things (IoT) is making digital devices the main building blocks in the creation of ubiquitous cyber-physical digital frames. The IoT has various areas of use including health care. With exciting technical, economic and social opportunities, the IoT movement is redesigning conventional health care. This paper analyses developments in IoT-based healthcare technology and reviews state-of - the-art IoT-based healthcare solutions network architectures / platforms, implementations and industrial patterns. This paper also analyzes different IoT protection and privacy functions, including protection specifications, threat models, and health care taxonomies[8]. With the emergence of smart homes, smart cities, and smart infrastructure, the Internet of Things (IoT) has emerged as an field of incredible influence, opportunity, and growth, with Cisco Inc. predicting 50 billion connected devices by 2020. Some of those IoT tools, however, are easy to hack and compromise. These IoT devices are usually limited in their processing, storage, and network bandwidth, and are thus more vulnerable to attacks than other endpoint devices such as smartphones, tablets, or computers. We present and assess global security issues for IoT in this document[9]. This paper discusses first the relationship between cyber-physical systems and IoT, both of which play important roles in the realization of an intelligent cyber-physical environment. Thereafter, emerging architectures, enabling technologies, and IoT security and privacy issues are discussed to enhance understanding of state-of - the-art IoT growth. This paper also examines the relationship between IoT and fog / edge computing, in order to analyze the fog / edge computing-based IoT, and address problems in fog / edge computing-based IoT. Finally, many implementations are discussed, including the smart grid, smart transportation and smart cities, to illustrate how fog / edge computing-based IoT is to be applied[10].

III. METHOD

In this paper the general architecture of the device considered for simulation 1. Here, an IoT node that has a sensor built on it is the sending computer. A sensor is an electronic tool used in the real world to detect various quantities, such as temperature, humidity, and distance etc. The receiver is an IoT device which receives these measurements and is able to process and manipulate the data. In comparison to the sender it is a fairly (computationally) efficient Linux-based computer which can be controlled. Any programmable computer (such as Arduino) may serve as a transmitter. It is the sender's duty to provide authenticity to the data using the SHA-3 based signatures. As such it is the recipient's duty to check the validity of the received data. This is also the duty of the receiver to determine if essential data have been received and to submit correct notification to a remote client system. Such important alerts are sent through the cloud messaging service. The obtained authentic data is also added to a cloud database. Data can be obtained from one or more transmitters and can be processed for further review in the cloud database. An architecture of communication enables the connection between sender and recipient.

SHA-3 based unique signatures for a transaction:

The message sent by the sender is from the form (hash code, data) where the' hash code ' acts as the specific data transaction signature, and the' data' in the simulation is the distance measured by the ultrasonic sensor Using the SHA-3 algorithm it produces this 512 bit hash code. The hash code is a feature of the data (distance) to be sent, and the receiver machine's specific serial hardware Id. Within the simulation the receiver's special serial Id (raspberry pi) is hard-coded into the system code of the sender. The specific serial Id of Pi can be accessed on the computer from,, /proc / cpuinfo. It means that in addition to the protection provided by the SHA-3 algorithm, the specific hardware characteristics of any chosen IoT node (and previously known to other nodes in the network) are used for authentication. The receiver machine's unique serial Id is appended to the distance data, and the SHA-3 hash for this string is determined. This hash serves as a special signature for the transaction's authentication. Many transactions would of course have different signatures.

Raspberry Pi:

On Ubuntu 18.04 (bionic beaver) a raspberry pi client (with raspbian OS) is set up with a static ip configured in the /boot / cmdline.txt file and the default gateway added for lanaccess. Wifi information are configured in the wpasupplicant.conf file in the /etc / wpa supplicant directory and ssh is activated. A gui login into pi is rendered using VNC server on pi and remmina on 18.04. Figure 1 shows the function of Raspberry Pie.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

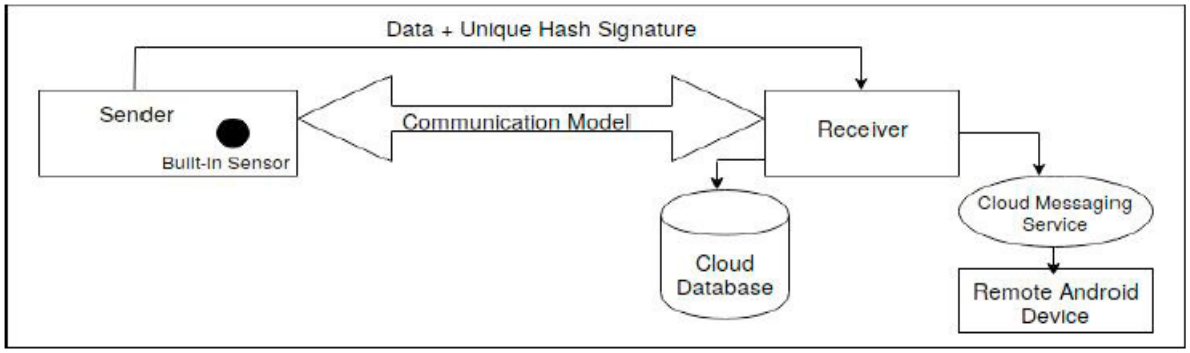

Fig.1: The Figure Portrays the Function of Raspberry Pie

Ultrasonic Sensor (HC-SR04):
The ultrasonic sensor is mounted on raspberry pi. Pi conveniently offers python to interact with the ultrasonic sensor as a programming language. For this interaction, a pre-installed python library for pi called RPi. GPIO assists. Using the sensor, it is then possible to record a distance measure of a nearby object using some basic programming.
Broker (for Publish Subscribe Architecture):
On the raspberry pi, Mosquitto-mqtt is set up as a broker. On port number 1883 the broker listens to incoming client requests.
Firebase Cloud Messaging for Android:
The program is ready to deploy to an android device after configuration. An Android emulator with Android 9. + (Google Play), API 29, 1080 xxhdi 1920 resolution, x86 CPU with available Play Store, which supports at least Android Jelly Beans is used for testing purposes. Following the successful launch of the android application on the device, a new token is created to allow the remote device to receive push notification. This token is retrievable from the running operation logcat. If the token is retrieved it can then be used to send push alerts to this android device across platforms.

IV. CONCLUSION

The paper addresses a blanket authentication scheme that applies to cloud-based services in order to publish subscribe and request response based IoT architectures. In all these communication models the authentication of da ta in the interaction between the sender and the recipient is assured by the use of the state-of - the-art SHA-3 algorithm. This process generates a specific signature between the sender and the receiver for any data transaction. Authentic checked data obtained by the recipient will be further processed while the inauthentic data is discarded. The connection between the recipient and the cloud is protected through the frameworks the cloud service providers provide. A push notification is successfully delivered via a cloud messaging service to the remote client device through a unique authentication token created during the initial handshake between the user and the service. Updates made by the receiver to the cloud database for checked authentic data obtained from the sender are also authenticated by using a private key that was created during the initial cloud database setup. This is an effective and state-of - the-art blanket authentication method that can be implemented into the real world.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*. 2014.
[2] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, 2015.
[3] F. Gregorio, G. González, C. Schmidt, and J. Cousseau, "Internet of Things," in *Signals and Communication Technology*, 2020.
[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, 2015.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

[5] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, 2015.
[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, 2013.
[7] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, 2014.
[8] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, 2015.
[9] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, 2018.
[10] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, 2017.

- K Deepika, N Naveen Prasad, S Balamurugan, S Charanyaa, "Survey on Security on Cloud Computing by Trusted Computer Strategy", International Journal of Innovative Research in Computer and Communication Engineering, 2015
- P Durga, S Jeevitha, A Poomalai, M Sowmiya, S Balamurugan, "Aspect Oriented Strategy to model the Examination Management Systems", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 2, February 2015
- RS Venkatesh, PK Reejeesh, S Balamurugan, S Charanyaa, "Further More Investigations on Evolution of Approaches and Methodologies for Securing Computational Grids", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 1, January 2015
- V M Prabhakaran, S Balamurugan, S Charanyaa, "Developing Use Cases and State Transition Models for Effective Protection of Electronic Health Records (EHRs) in Cloud", International Journal of Innovative Research in Computer and Communication Engineering, 2015
- VM Prabhakaran, S Balamurugan, S Charanyaa, " Entity Relationship Looming of Efficient Protection Strategies to Preserve Privacy of Personal Health Records (PHRs) in Cloud", International Journal of Innovative Research in Computer and Communication Engineering, 2015
- Vishal Jain, Dr. Mayank Singh, "A Framework to convert Relational Database to Ontology for Knowledge Database in Semantic Web", "International Journal of Scientific & Technology Research (IJSTR), France, Vol. 2, No. 10, October 2013, page no. 9 to 12 , having ISSN No. 2277-8616.
- Vishal Jain, Dr. Mayank Singh, "Architecture Model for Communication between Multi Agent Systems with Ontology", International Journal of Advanced Research in Computer Science (IJARCS), Vol. 4 No.8, May-June 2013, page no. 86-91 with ISSN No. 0976 – 5697.
- Vishal Jain, Dr. Mayank Singh, "Ontology Based Information Retrieval in Semantic Web: A Survey", International Journal of Information Technology and Computer Science (IJITCS), Hongkong, Vol. 5, No. 10, September 2013, page no. 62-69, having ISSN No. 2074-9015, DOI: 10.5815/ijitcs.2013.10.06.