iJRASET

International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6290

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

Artificial Immune System based uncloneable Device Signature for Node Authentication IOT

Uttam Singh[1], Sohit Agarwal[2]
[1]M.Tech Scholar, [2]Professor, Computer Science and Engineering
Suresh Gyan Vihar University, Jaipur

Abstract—In order to realize true potential of ubiquitous computing and Internet of things establishment of Trust is very essential especially in Machine to machine communication. Devices should possess ability of mutually authenticating themselves. The aim of this paper is to develop artificial immune system algorithm based Device Authentication Scheme. The proposed scheme is deployed at Fog level.

Index Terms— Internet of Things, Security, cryptography, Bio inspired algorithms, Device Authentication.

I. INTRODUCTION

The realization of web4.0 is possible only because of Internet of Things(IOT). IOT is also referred as Machine to Machine communication. IOT is master technological network of all networks. The aim of IOT is to create cyber-physical systems by connecting devices, industrial or domestic to network. IOT enables the devices to perform more than their capabilities and hence converts them into smart devices. The connection of devices to the internet enables them to make intelligent decisions by mutual interaction with little or no human interaction. IOT will soon take us to a world where everyday appliances such as AC, TV ,door locks , coffee brewers can perform their task as soon as they sense us. The commercial capabilities of IOT has already been explored. Accenture for better performance, security and consultancy. Rolls Royce, a British manufacturing firm uses IOT based sensors in their jet engines for continuous diagnosis to prevent catastrophic failure[2]. International Data Cooperation (IDC) published a report in 2013 stated that the number of connected devices or IOT devices are expected to reach 41 billion by 2020 with a predicted market share of $8.9 trillion dollars [3]. The application areas of IOT are mentioned in Fig 1.1.
IOT has a three layered architecture [4] as described below:

A. Perception Layer

Perception layer is the bottom layer and is also known as Sensor Layer. The main objective of this layer is to connect devices or things into IOT network and simultaneously collect process and transmit the information associated with these devices. The information is deployed through smart devices like RFID, sensors, actuators etc.

B. Network Layer

Network layer is the middle layer of IOT architecture and can be called Transmission Layer. This is the most important layer as it receives the processed information from the perception layer and appropriately transmits it to devices and applications through the interfaces and gateways in IOT network. The layer integrates devices like hub, gateways, cloud computing platforms and communication protocols and technologies like Bluetooth, Wi-Fi, Long-Term Evaluation (LTE) etc to transmit information in the heterogeneous network.

C. Application Layer

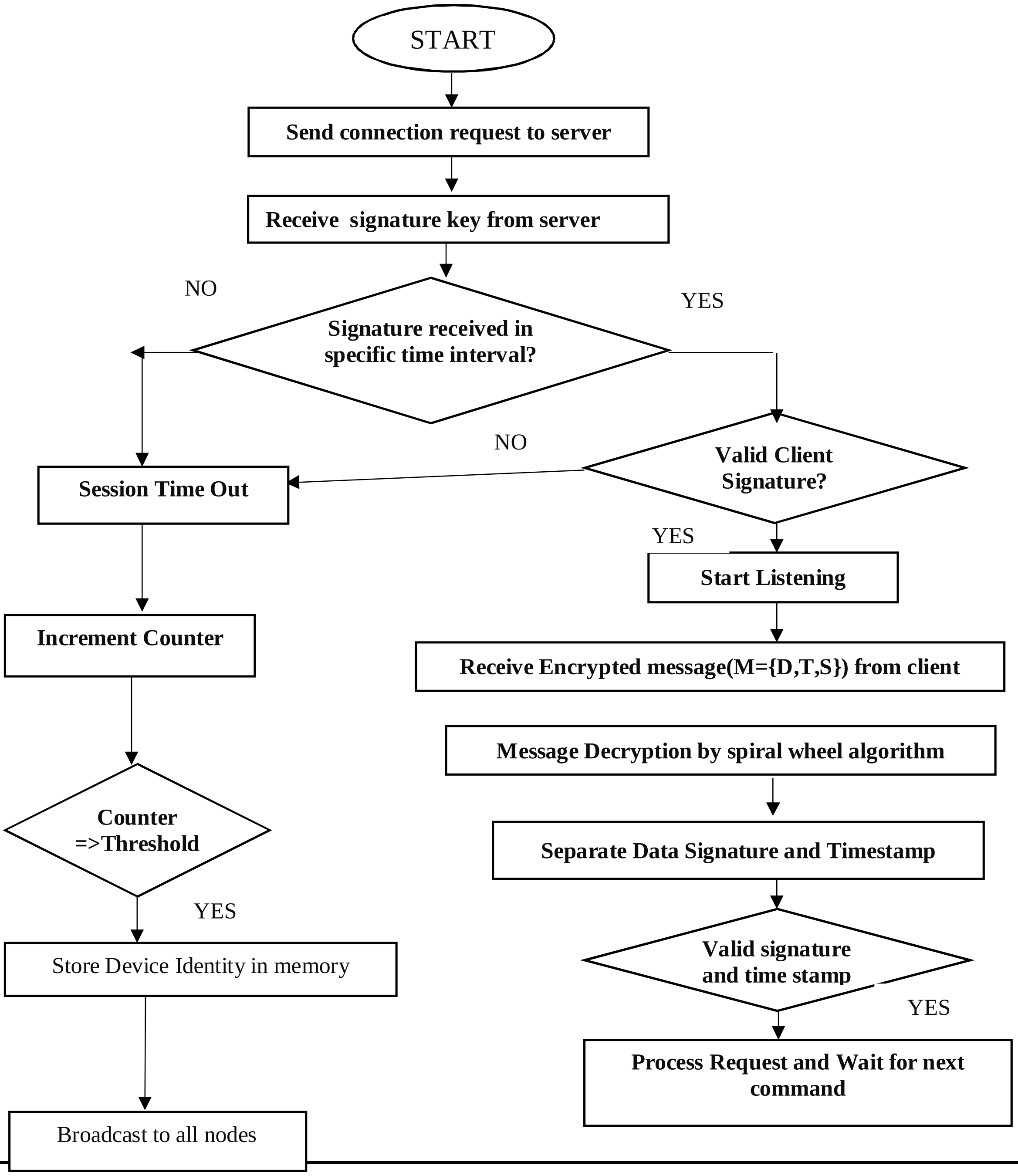
This is the top most layer of IOT architecture and delivers services in various fields like environmental monitoring, healthcare. etc. In other words application layer interacts with the user and provides him the necessary data.

Data confidentiality [5] prevents unauthorized disclosure of data and usually results from legislative measures. It consists of a set of rules and regulations which limit the access of information and keeps it concealed from outsiders. Appropriate methods like data encryption, password protection, and biometric authentication should be employed to prevent unintentional disclosure of data.

Identification[6] ascertains that only legitimate users and devices are connected to IOT network. Authentication ensures that the data transmitted in the network as well as the devices or applications requesting the data are genuine. However, designing an efficient authentication and identification mechanism for numerous and diverse devices in an IOT network is a challenging task.

Minimum Power Consumption and light weight computations [7] :IOT devices are expected to be lightweight and are often deployed in environments where charging may not be available. Thus the security protocols should not drain the device's battery. Similarly complex cryptographic algorithms cannot be applied on the IOT devices due to limited memory.

To manage the aforementioned security goals of IOT Fog computing paradigm is employed [8]. Cisco introduced the term Fog computing for the first time in 2012[9].Despite considerable differences the fog computing and edge computing are often quoted interchangeably [10]. Fog computing shifts the focus from a centralized cloud host to the network end device. The concept of fog computing is


START
Send connection request to server
Receive signature key from server
NO
YES
Signature received in specific time interval?
NO
Valid Client Signature?
Session Time Out
YES
Start Listening
Increment Counter
Receive Encrypted message(M={D,T,S}) from client
Message Decryption by spiral wheel algorithm
Counter =>Threshold
Separate Data Signature and Timestamp
YES
Store Device Identity in memory
Valid signature and time stamp
YES
Process Request and Wait for next command
Broadcast to all nodes

eliminating the dedicated resources for utilizing cloud services such as channel establishment and simultaneously increasing placement of intelligent resources at the end of network or the cloud edge[12]. The obvious advantage of fog computing is close availability of computing and storage resources to nodes. Furthermore fog computing architecture takes cumulative input from near organizations or end users and edge devices. The cumulative effort may be incurred in various forms such as management, configuration, communication and control. Edge computing technology is the extension of the cloud concept to the network edge[13]. The differentiating factor between cloud computing and fog computing is overdependence of cloud services on high internet bandwidth and geographically large scale organizational system. Fog services are much closer to the end-users, with dense geographical distribution, and much better support for mobility[14].

The aim of this research paper is to demonstrate a device authentication algorithm based on artificial immune system. Device Authentication is important to truly realize the concept of Machine to machine communication.

II. METHODOLOGY

Artificial Immune System is a pattern recognition technique which draws its analogy from the human immune system. The vital characteristics of human immune system mainly of memorization and self-learning are exploited by artificial immune systems to detect pattern inherent in information. The aforementioned algorithm is employed in intrusion detection and communication networks. The whole concept of Artificial immune system revolves around the point of identifying changes or deviation from normal conditions.

TABLE 2.1
ANALOGY BETWEEN IMMUNE SYSTEM
AND OUR PROPOSED ALGORITHIM

	Immune System	**Proposed Approach**
	Pathogen	Malicious node
	Antigen	Timestamp
	Immunological memory	EEPROME of NodeMCU(Fog Node)
	Antibodies	Security protocol on server
	Device	Cells
	Innate immune system	Primary security algorithm
	Adaptive immune system	Secondary security algorithm

The mechanism of our body which defends us against diseases is the immune system, It is a highly complex system, which is made up of enormous number of cells and proteins . These cells and proteins work collectively to defend our body from pathogens. Any foreign substance is termed as pathogen . Thus a pathogen can be any bacteria, fungus or virus which may result in infection. Lipids and proteins are essential components that make up a pathogen. Our immune system is able to differentiate between a body cell and a pathogen due to different formation structure of these proteins. Antigens are molecules that are found on the surface of pathogens and are specific to that pathogen. Any foreign molecule or foreign substance that can trigger a specific immune response against it is term as an antigen. The human immune system combats pathogen with two classified defense mechanisms, namely nonspecific immune defenses and specific immune defenses. Innate defense is another term used to denote nonspecific immune system defense. The functioning of innate immune system starts as soon as any antigen is detected in the body. This defense mechanism cannot exactly recognize the type of foreign particle but takes a generalized countermeasure. Immunological memory is an important aspect of specific or adaptive immune system. The immunological memory provides an amazing capability of storing information related to a pathogen so that it can quickly eliminate it next time it enters the body.

The analogy of our proposed approach with immune In our proposed approach malicious nodes are modelled as pathogens. Antigenic property of the pathogens is timestamp and server/servers acts as antibody. Devices are modelled as cells.

The aim of antibodies is to detect intrusion by noticing change in surrounding environment. When server receives connection request from client it sends it a signature code and waits for response. If a valid signature code arrives within a threshold time interval , server starts listening. The process flow of system is shown in Fig 2.1.

On the other hand if the arrived signature is invalid or the arrival time exceeds the threshold time limit, the client is treated as suspicious and artificial innate system algorithm starts working by closing session and incrementing the counter. If counter also exceeds the threshold value artificial adaptive immune system algorithm comes into play and stores the signature of suspicious node in artificial immunological memory which is EEPROME of Node MCU. And the same is communicated to all other server nodes.

However if the client is authorized, it sends encrypted message to the sever . The encrypted message consists of three parts action, device signature and timestamp. The server decrypts the message and separates the three parts of message. The required action is performed in favorable situations. The encryption and decryption of performed by our novel wheel algorithm.

A. Equations

Let M[] denotes Mac address of machine and T[] denotes system time acquired from RTC module in the format DD:MM;YYYY:hh:mm. Equation (ii) denotes shuffling of device signature D[] but keeping first character constant. Further shuffling od device signature is represented by equation(iv).Equation(iii) denotes calculation of midpoint of device signature D[].The final encrypted device signature is represented as EnDS[] in equation(v).The received signature is decrypted only if conditions of equation(vii) are fulfilled. The decryption process is represented by equation (v),(vi)and (vii).

$$\mathrm{D[\,]=M[\,]+T[\,]}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \ldots\text{(i)}$$

$$\mathrm{D[i]}=\sum_{i=0}^{len} \mathrm{D}[i+2] \qquad \text{(ii)}$$

$$p=\begin{Bmatrix} \frac{len+1}{2} & len = 2n+1 \\ (len/2)+1 & len = 2n \end{Bmatrix} \qquad \text{(iii)}$$

Encryption

$$\mathrm{D[i]}=\sum_{0}^{len} \mathrm{D}[len-i] \qquad \text{(iv)}$$

$$\mathrm{EnDS[i]}=\sum_{i=0}^{i<len} \mathrm{D}_{len}\,, \mathrm{D}_{len-len+1,}\mathrm{D}_{len-1,}\mathrm{D}_{len-len+2,}\mathrm{D}_{len\frac{1}{2},}] \quad \text{(v)}$$

T_0 = *Time at which Connection request received by server*

T_r = *Time at which device signature received by server*

$$\Delta T = T_r - T_0 \qquad \text{(vi)}$$

$$\text{If} \quad \Delta T \leq T_{th} \quad \text{perform signature decryption}$$

Decryption

$$\mathrm{DrDS[i]}_1 = \sum_{i=len}^{c} \mathrm{EnDS}[i+2] \qquad \text{(v)}$$

$$\mathrm{DrDS[i]}_2 = \sum_{i=c}^{0} \begin{Bmatrix} \mathrm{EnDS}[i-1] & , i = len \\ \mathrm{EnDS}[i-2] & , otherwise \end{Bmatrix} \qquad \text{(vi)}$$

$$\mathrm{DrDS}= \mathrm{DrUstr}_1 + \mathrm{DrUstr}_2 \ = \mathrm{D[\,]=M[\,]+T[\,]} \qquad \text{(vii)}$$

III. RESULTS

The hardware configuration of computer utilized for the project are Quad Core Intel(R)Core(TM)i3-5005U CPU @2.10 GHz processor , 2 GB RAM , Windows10 operating system. The hardware configuration of ESP 826612E Node MCU are 16 bit RISC Hz processor with 80 MHz processing speed , 32 KB RAM and Arduino based 32 bit microcontroller.

Microsoft Visual Studio 2015 and Arduino IDE are software platforms utilized for the development of project. The programming languages used are C# programming language (.Net Framework), and Embedded C.

Fig represents the developed Graphical User Interface and Fig3.1 and hardware circuit is represented in Fig 3.2. represents results. The developed system is successfully able to differentiate between authentic node and malicious nodes by artificial immune system based device signature.

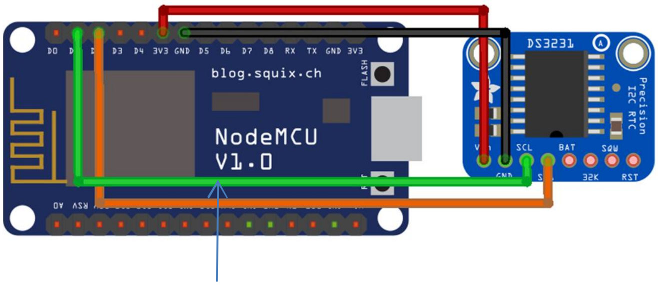


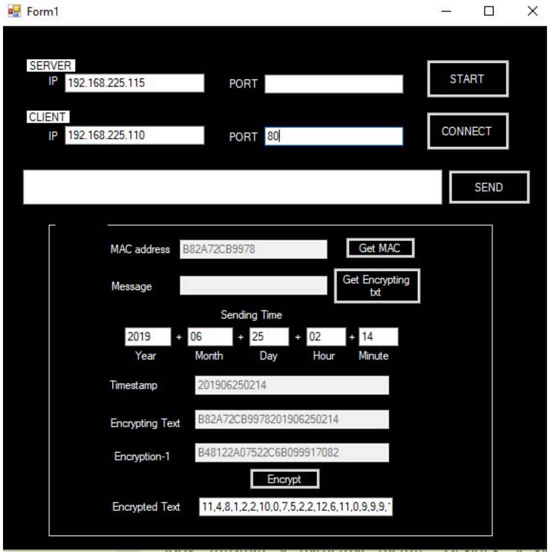
Fig 3.2 Circuit Diagram

IV. CONCLUSION

The device authentication scheme developed is deployed in real time and is both lightweight and robust. Another advantage of using the proposed approach is that the device signature is dynamic so frequency analysis attack is not possible in the node. The node is also protected from Middle Man attack. Thus the proposed scheme is ideal for device authentication in fog computing environment.

V. FUTURE SCOPE

In future the author plans to implement the developed algorithm in conjunction with machine learning to enhance artificial immunological memory.



SERVER
IP 192.168.225.115 PORT

CLIENT
IP 192.168.225.110 PORT 80

MAC address B82A72CB9978

Message

Sending Time
2019 + 06 + 25 + 02 + 14
Year Month Day Hour Minute

Timestamp 201906250214

Encrypting Text B82A72CB9978201906250214

Encryption-1 B48122A07522C6B099917082

Encrypted Text 11,4,8,1,2,2,10,0,7,5,2,2,12,6,11,0,9,9,9,

Fig 3.2 GUI of developed application

REFERENCES

[1] M. Saadeh, A. Sleit, M. Qatawneh and W. Almobaideen, "Authentication Techniques for the Internet-of-Things: A Survey", DOI 10.1109/CCC.2016.22, IEEE Internet of Things Journal.

[2] https://www.rtinsights.com/rolls-royce-jet-engine-maintenance-iot.

[3] IoT Analytics, "Why the internet of things is called internet of things: Definition, history, disambiguation," https://iot-analytics.com/internetof-things-definition/, 2014.

[4] S. Agrawal and M.L. Das," Internet of Things – A Paradigm Shift of Future Internet Applications", 978-1-4577-2168-7,2011 IEEE.

[5] N. Sklavos and I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations",978-1-5090-2914-3/16, 2016 IEEE.

[6] N. Sklavos, P. Souras, "Economic Models and Approaches in Information Security for Computer Networks", International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January, pp. 14-20, 2006.

[7] http://www.itu.int/osg/spu/publications/internetofthings/. (as on 19 Sep 2011)

[8] M. Katsaiti, A. Rigas, I. Tzemos, N. Sklavos, "Real-World Attacks Toward Circuits &amp; Systems Design, Targeting Safety Invasion", proceedings of the International Conference on Modern Circuits and Systems Technologies (MOCAST"15), Thessaloniki, Greece, May 14-15, 2015.

[9] R. T. Tiburski, L. A. Amaral, E. D. Matos, D. F. G. de Azevedo and F. Hessel, "Evaluating the Use of TLS and DTLS Protocols in IoT Middleware Systems Applied to E-health", 978-1- 5090-6196-9, 2017 IEEE.

[10] K. Gama, L. Touseau and D. Donsez, “Combining heterogeneous service technologies for building an Internet of Things middleware”, Computer Communications, Volume 35, Issue 4, 15 February 2012, Pages 405-417, ISSN 0140-3664.

[11] Q. Jing, A. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[12] R. Tiburski, L. Amaral, E. Matos, and F. Hessel, “The importance of a standard security architecture for SOA-based IoT middleware,” IEEE Communications Magazine, vol. 53, no. 12, pp. 20–26, Dec 2015.

[13] Li. Peng, A.Hu, J. Zhang, Y.Jiang, J.Yu, and Y. Yan, “Design of a Hybrid RF Fingerprint Extraction andDevice Classification Scheme”, IEEE Internet ofThings Journal,2018.

[14] M. N. Aman, K. C. Chua , B. Sikdar, “Physical Unclonable Functions for IoT Security”,IEEE,2016.