International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Securing the IOT Devices with Artificial Immune System

Bhagya Shree, Suman Bhakar

Abstract*: Security is the main concern for IOT devices as are expected to share a lot of crucial information about the user and his surroundings. The traditional security mechanisms are ineffective against sophisticated and advanced security attacks such as Man in the Middle Attack, Denial of Service attack, Identity cloning. Different solutions have been proposed for user authentication. Device authentication is crucial in IOT environment and cannot be neglected. Despite this device authentication has not gained equal attention from the research community. The aim of this research is to develop a lightweight and robust device authentication algorithm by Artificial Immune System to ensure data integrity in IoT networks. The concepts of Artificial Immune system are utilized for generating a non-redundant device signature which is used to differentiate between authentic and malicious nodes. The device signature is generated dynamically and is non reusable. This property makes the proposed algorithm secure against numerous high-level attacks such as frequency analysis attacks, Man in the Middle attack, side channel attacks, Denial of Service attack. The developed algorithm is tested in real time and prevents malicious nodes from entering the network. In addition to being immune against the high level attacks the proposed algorithm functions with low communication cost. The proposed algorithm can be used for providing security in IOT devices with limited battery life and processing power such as IOT enabled and remotely deployed Wireless Sensor Networks for forest fire detection, power plant monitoring , remote military applications and many others.

Keywords* : Artificial Immune System, Device Authentication, Internet of Things, Security.

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. 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 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[1]. 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 [2].

IoT needs to address the security in the designed system i.e. the most important concerns. Efficient data communication demands high-level security from random cyber-attacks. Attacks such as Sybil, eavesdropping, message modification, traffic analysis and Denial of Service (DoS) etc. are harming the people and institutions by obtaining their access information as well as gain financial benefits [3]. The exponential growth of IoT attracts the cyber-attackers with more number and in complex manner. It becomes sophisticate to breach the security with new tools [4]. Classification of attacks in IOT is shown in Fig 1. Advanced security services like applied cryptography and trusted computing have not grown considerably as compared to usage of smart devices in every day applications. Economic aspects of device such as cost, market etc. along with restricted computing power are main restrictions towards achieving robust security solutions [5]. Digital assaults are recorded consistently, essentially because of the inadequately anchored applications, administrations, and gadgets [6]. Due to the above-mentioned reasons For past years the research community has remained highly interested in the concept of Internet of Things. It has received much attention from both industrial and academic organizations. Security and privacy issues are the important research targets [7]. Kumar and etal[8] proffers a novel approach for protecting data by integrating RSA algorithm and steganography technique. The paper also points high efficiency of RSA algorithm for data security. Cheng and etal[9] proposed a Bloom Filter as a Lightweight countermeasure For MitM attack is proposed.

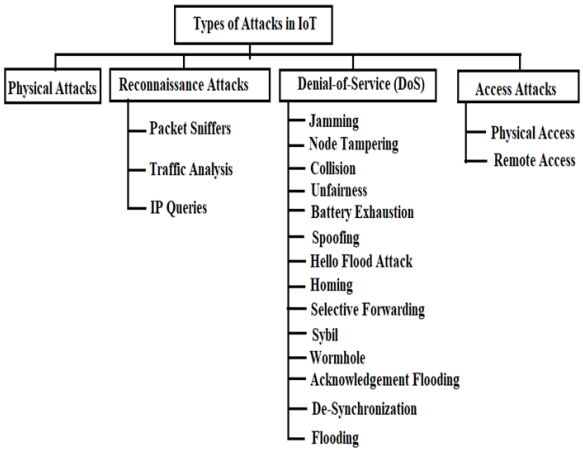

Fig 3: Classification of IOT Devices[10]

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

Bhagya Shree*, Pursuing Post Graduation student, computer science program, Rajasthan college of Engineering for women's, Jaipur.

Suman Bhakar, Assistant Professor, Cumputer Science Department, Rajasthan College of Engineering for Women, Jaipur.

It has been found from the literature that very few research works exists for securing device to device communication without human intervention. The aim of the research paper is to design a novel and unique algorithm as signature for data encryption/decryption for solving the Man-in-the-Middle attack and data authentication

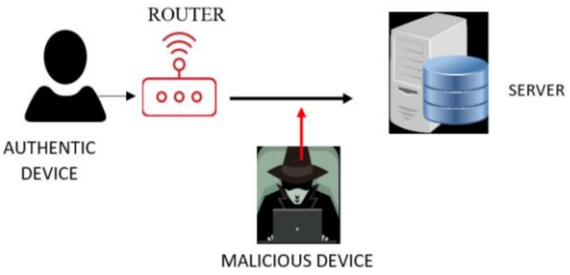

Fig 2: System model

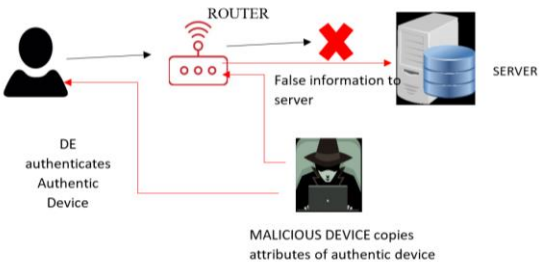

Fig 3: Threat model

II. PROPOSED ALGORITHIM

A. Threat Model

The threat model consists of three entities namely authentic device, malicious device and server. The malicious device eavesdrops on communication between authentic device and server. The malicious node can also deauthorize the authentic node and connect to server by cloning its attributes as shown in fig 1.

Table-II Analogy of proposed system with Artificial Immune System

SNO	Immune System	Analogy in Proposed Approach
1	Pathogen	Malicious node
2	Antigen	Device Signature
3	Immunological memory	EEPROME of NodeMCU(Fog Node)
4	Antibodies	Security protocol on server
5	Device	Cells
6	Innate immune system	Primary security algorithm
7	Adaptive immune system	Secondary security algorithm

B. Proposed Scheme

In this research an algorithm for autonomous device authentication is proposed. The proposed algorithm utilizes the computational abilities of Artificial immune system. The analogy of our proposed approach with AIS is shown in Table I. In the proposed approach malicious nodes are modelled as pathogens. Antigenic property of the pathogens is device signature. Server/Servers acts as antibody. Devices are modelled as cells. The proposed approaches utilize the self and non-self-detection paradigm of the immune system. The process starts with creation of self-nodes or self-antigen set. The self-antigen set is the collection of valid device signature at a particular instant of time for the authentic node. When server receives connection request from client, it checks for the device signature. If a valid signature code arrives within a threshold time interval, server starts listening. On the other hand, if arrived signature is invalid or the arrival time exceeds the threshold time limit, the node is treated as suspicious and artificial innate system algorithm starts working by the 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 the user. The details of the proposed algorithm are mentioned below

C. Initializing Population

In the first step initial population of authentic nodes or self-nodes. The initial population is denoted by set P. Each node (N_i) in the population can be identified by ten unique features (F_(〖jN〗_i)).

$$p \subseteq N_i \quad (1)$$

$$N_i \subseteq F_j \qquad 1 \leq j \leq 10 \quad (2)$$

D. Initializing Population

The self-antigen set is created by the self-nodes. The self-antigen set comprises of the command (C) and the device signature. The device signature is created by following steps:

Step 1 : Count =1
Step 2 : Get timestamp(TS[]) in DDMMYYYYhhmm format.
Step 3: for i=1; i≤ lenghth(TS) ; i++
S= S+TS[i]
Step 4: do while S/10 != 0
for i=1; i≤ lenghth(S) ; i++
S= S+S[i]
Step 5: if count <=1
Extract the feature 〖F=F〗_s
Step 6 if count >1 && mod(count,2)=0
Extract the feature F=F_s-1
Else if count >1 && mod(count,2)=0
Extract the feature 〖F=F〗_s+1
Step 7 : Prepare the request to be sent to server
R=[C, F]
Step 8 : count=count+1

It can be observed that the antigen property changes with timestamp and each session.

E. Initializing Population

In this session server receives connection request from the node. The server separates the command and the feature. If the feature is valid at the given time then communication is started and action is taken.

F. Initializing Population

However, if valid signature is not valid then the request is not processed and server waits for next command. If again valid device signature is not encountered then Adaptive immune system becomes active.

G. Initializing Population

The adaptive immune system blocks the device and sends the notification to the user.

III. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed algorithm of Dynamic Device Signature is successfully deployed in real time IoT environment. Node MCU is the IoT device and PC is the fog server. User can send two commands, which are, processed they as 'LEDOFF' and 'LEDON'. Fig 3 denotes the used components which are Node MCU ESP826612E and Real Time Clock (RTC) module. Fig 5 denotes the authentication of IoT device in case of receiving valid device signature.

Fig 4 denotes the developed Graphical User Interface using socket programming in C#. Asynchronous programming is used in developing client and server socket for sending and receiving data. The IP address and port number of both client and server are entered in the respective textbox. The signature is extracted and sent for authentication.

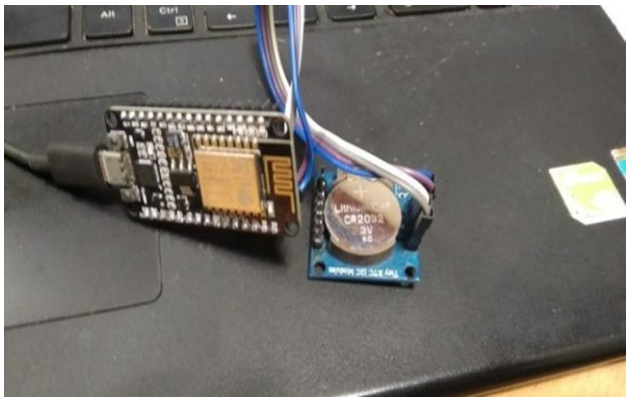

Fig 3: Node MCU ESP826612E and Real Time Clock (RTC) module

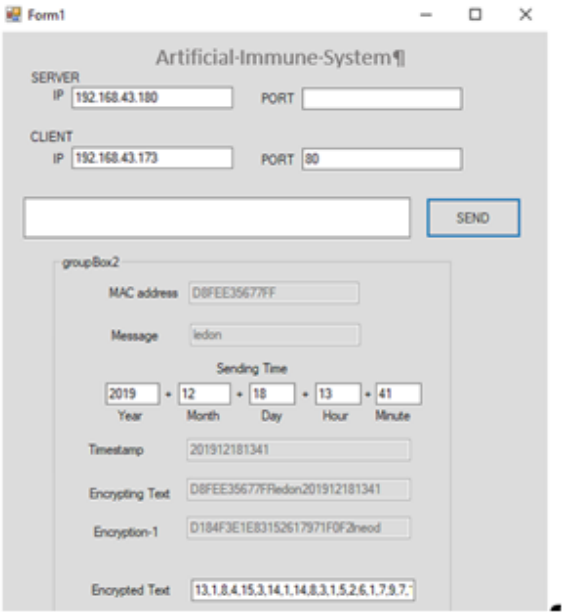

Fig 4: Node MCU ESP826612E and Real Time Clock (RTC) module

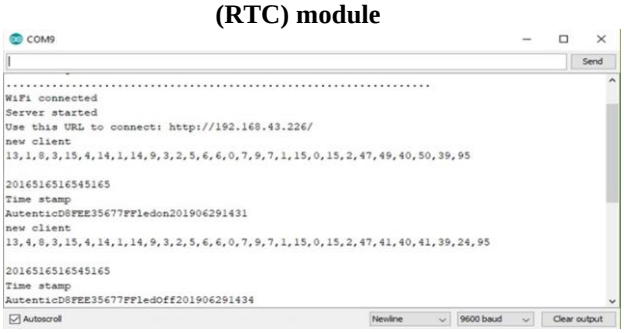

Fig 5 Output window

The performance of the system is characterized based on two factors namely communication overhead and communication cost. Communication overhead is defined as number of messages exchanged during the authentication process. Communication cost is defined as number of data bits exchanged during the authentication process. Fig 6 shows the comparison of proposed algorithm (DDS)with the PAS algorithm[11], which is based on Physically unalienable Functions for device authentication. Communication overhead and communication cost obtained in the proposed algorithm is 3 and 272-300 bits respectively, which is a significant improvement over previous research.

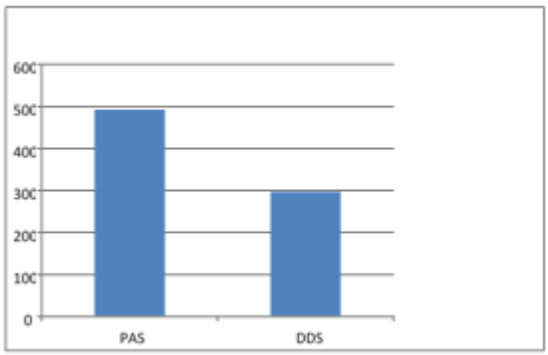

Fig 6: Performance Analysis

IV. CONCLUSION

In this research a device authentication algorithm is developed by artificial immune system. The algorithm generates a dynamic and non-redundant device signature. The proposed algorithm functions with a communication cost of 270-300 bits and communication overhead of 3 messages. Communication cost and overhead in the proposed algorithm is much lower than previous approaches such as PAS.

FUTURE WORK

In future the author plans to implement the developed algorithm in conjunction with machine learning to enhance artificial immunological memory. Future work can be carried on the authenticity of the system to get rid of the unknown users try to fetch the data. More functionality in the algorithm to make it reliable and user-friendly can also be added such as biometric features

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 & 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. I.Makhdoom, M. Abolhasan, and R.Liu," Anatomy of Threats to The Internet of Things", IEEE Communications Surveys & Tutorials,2018.
11. M. A. Muhal, X. Luo, Z. Mahmood and A. Ullah, "Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things," 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), , 2018, pp. 160-165

AUTHORS PROFILE

Bhagya Shree, is a pursuing post graduation student within the computer science program from Rajasthan college of engineering for women's, in Jaipur. She has completed her graduation in computer science from Rajasthan college of engineering for women's at Rajasthan technical university.In her graduation,She has completed her project in Desktop Management Through Android,And Online Auto Marketing Sales. She has done her internship from HCL Training $ Staffing,Manesar and she had completed her Training in Java and Oracle.In her Post Graduation,She had made her dissertation on programming and self stabilization for wireless sensor networks. she had given her participation in DST sponsored national conference On 'Environmental Protection".currently,she is doing her research in internet of things.she has good experience in internet security.

Suman Bhakar, is Assistant Professor in Cumputer Science Department in Rajasthan College of Engineering for Women Jaipur. She received her Ph.D. degrees in computer science from the Manipal University Jaipur Rajasthan, India in 2019.She received her Master degree in computer science department from the university of chennai,Tamil Naidu,2015 And She had made her project in clustering of Uncertainity Data.. She had completed her Bachelor degree from Rajdhani Institute Of Technology And Management,jaipur.Her Research interests include Augmented reality, image processing,Security.She has good knowledge in java.She has paricipant on several seminar on security.she has good experience in artificial intelligence.She had made several project on image processing.In her PHD,She has made project based on Glyph Detection Through Augmented Reality.