Dynamic Device Signature for Intrusion Prevention in Fog based IoT.

Khushboo Tak, Dr.Rakesh Rathi

M.Tech Scholar, HOD of Computer Science and Engineering of Govt. Engineering College Ajmer
Computer Science and Engineering,
Govt. Engineering College, Ajmer, India

Abstract: The aim of our project is to develop a lightweight robust node authentication algorithm called 'Dynamic Device Signature (DDS)'to ensure data integrity in Fog based IoT networks. The proposed algorithm prevents security breaches by preventing malicious nodes from entering the network. When Fog node receives a connection request it sends a DDS request to the client node. The client node prepares its dynamic device signature using a random key and sends it to the fog node. If fog node receives a valid device signature in specified time duration then access rights are provided to the client, else the rights are denied. The signature is called dynamic as it changes with every time instance to beat frequency analysis attack. Once the node is verified it can communicate with fog node in encrypted messages. The proposed algorithm will not only reduce latency but will also reduce computational burden on fog layer. It can compete against various attacks such as MITM (Man in the Middle), Device Impersonation, Packet Modification and Eavesdropping etc.

Index Terms **- Internet of Things, Device Fingerprinting, Fog Layer, IoT security.**

I. INTRODUCTION

Internet of Things is the master technological networks of all networks. Internet of Things will connect devices which we use every day such as Television, Air Conditioner even door locks to the network or digital world [1]. The concept of IoT is already being used by many reputed companies such as Rolls Royce, Accenture and many others [2]. IoT will create a new age of automation. Each year the number of connected devices is growing at an enormous rate and it is predicted that the number of connected devices will reach 41 billion [3].

Internet of Things has a three-layered architecture with the three layers being Perception layer, network layer and application layer [4]. This architecture is represented in Fig 1.1. In order to truly realize the true potential of IoT efficient security protocols are very important because IoT devices are expected to share lot of sensitive data related to a everyday life of user [5]. Thus, data confidentiality is very important in IoT environment. The aim of IoT is realized by Ubiquitous Computing as shown in Fig 1.1. Ubiquitous computing advocates that processing can take place in any device, at any place and at any time in all format and network [6].

User Identification and authentication is another important security goal of Internet of Things [7].User Identification ensures that only legitimate users are able to access the network. User Authentication has remained a prime research concern over the past few years. However, much less attention is focused on device authentication. To deal with the previously mentioned security objectives of IoT Fog computing worldview is utilized [8]. Cisco presented the term Fog computing without precedent for 2012[9].Despite extensive contrasts the fog computing and edge computing are frequently cited reciprocally [10]. Fog computing shifts the concentration from a brought together cloud host to the system end gadget. The idea of fog dispensing with the devoted assets for using cloud administrations, for example, channel foundation and at the same time expanding position of smart assets toward the finish of system or the cloud edge[12]. The conspicuous preferred position of fog computing is close accessibility of computing and capacity assets to hubs. Moreover fog computing design takes aggregate contribution from close associations or end clients and edge gadgets. The total exertion might be acquired in different structures, for example, the executives, arrangement, correspondence and control. Edge computing innovation is the expansion of the cloud idea to the system edge [13]. The separating factor between distributed computing and fog computing is overdependence of cloud benefits on high web transfer speed and topographically huge scale authoritative framework. Fog administrations are a lot nearer to the end-clients, with thick geological circulation, and much better help for mobility [14].

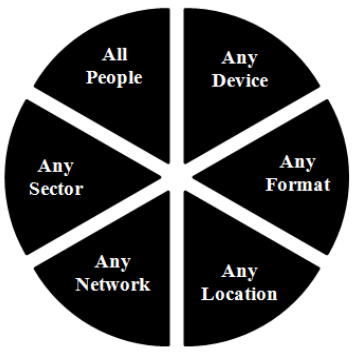


Fig 1.1: Ubiquitous Computing

II. RESEARCH METHODOLOGY

The aim of this research is to develop an autonomous device authentication algorithm that can be implemented at Fog layer. The algorithm has been designed by considering the lightweight computational abilities and limited processing power requirements for Internet Of Things. The algorithm generates A Dynamic Device Signature which is used to provide access right to the device. The signature is named Dynamic as it changes with every time instant to combat the well-known IoT attacks namely Dictionary attack, Side Channel attack , Frequency Analysis attack etc. The adopted server, client and threat model is discussed in section 2.1. The proposed algorithm and consequent sequencing of operations is discussed in section 2.2.

2.1 SYSTEM MODEL

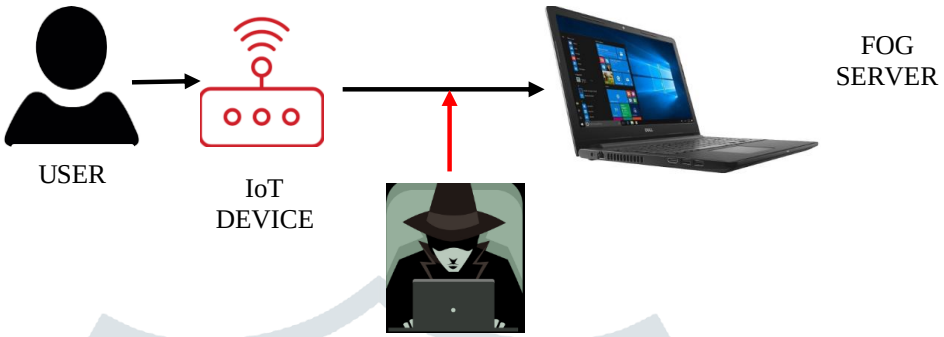


Fig 2.1: System Model

The system model is represented in Fig 2.1 . User interacts with the IoT device. The IoT device captures user's request and sends it to Fog server for further processing. Before processing the request the server must authenticate the IoT device without user intervention as threat is supposed to be present in form of security breaches.

2.1.1 Characteristics of IoT Device : The IoT device is analogus to a Dumb device with network connecticity . It has limited storage and processing power. In the proposed system ESP826612E NodeMCU is the IoT device.

2.1.2 Characteristics of Fog Server :The Fog server has advanced resources than the IoT device and monitors the activities of all devices .In the proposed approachFog server is represented by a PC.

2.1.3 Threat Mode : An attacker or hacker is supposed to evaesdrop on the communication between IoT device and Fog Server. The attacker has comparable or even higher resources than Fog Server. The attacker can introduce a malicious node in the system by blocking or sending death to the actual device and cloning its IP and Mac Address. The security is breached completely if Fog Serever authenticates the malicious node and process its requests.

2.1.4 Characteristics of User : The user leads a modern lifestyle with a significant degree of automation and connected things. The user wants his privacy to be protected but at the same time doesnot want to invest much time and thoughts in complicated security protocols.

The developes device aurthentication algorithim doesnot bothers user to enter extra security codes such as One Time Passwords for authenticating device.

2.2 PROPOSED ALGORITHIM

The schematic and sequential steps of the proposed algorithm are shown in Fig 2.2. The entire process can be divided into three steps as discussed below.

2.2.1 Handshake Session: The IoT device sends a request for connection to the server at time T=T_0 . This connection request reaches the server at time T=$T_0 + t$. As the request is received the server starts the handshaking window which remains active till time T=$T_0 + t + t_1 + t_2$.

2.2.2. Dynamic Device Signature Generation: The device prepares a time dependent random key when server requests the dynamic device signature. Firstly device acquires the system time and computes its sum till a single digit number is achieved. This single digit number is the key (k_i). Ten physical device identification numbers are present in the database. As per k_i the subsequent physical device identity is chosen which is called Device id (I_D). In the next step timestamp is acquired in the form of DD:MM;YYYY:hh:mm which is called (S_t). The Device id (I_D). and timestamp (S_t).is concatenated to form device signature (DS) at T=$T_0 + t + t_1$. A novel Helicoid Encryption is applied on the signature. The encryption procedure of Helicoid algorithm is represented by equations. Firstly the central plane (CP) of string is computed by equation 2.1. Starting from this Central plane the characters are shifted cyclically as per equation 2.2.Equation 2.3 represents the encrypted dynamic device signature (ES) which is sent to server.

2.2.3 Session Start : The received encrypted dynamic device signature is decrypted only if the signature arrives within the hand shake window i.e. on or before T=$T_0 + t + t_1 + t_2$. If the signature reaches with delay one more attempt of handshake is given else access is denied. The idea behind applying the time constraint on handshake window is that if signature reaches with considerable delay then it means it was modified or the requesting node does not know the exact processing steps and hence the signature is achieved by manipulation.

If the signature reaches in the specified time interval then it is decrypted by Helicoid decryption and identity of device is extracted. In case of valid identity communication is initiated and access rights are granted. Simultaneously a

Session window is started. The communication can last till the session window is open i.e. T=T_S. In case of session timeout the device is again asked for signature.

$$CP=\begin{cases}\frac{L+1}{2} & L=2n+1\\ (L/2)+1 & L=2n\end{cases} \quad (2.1)$$

$$E[i]=\sum_0^L E[L-i] \quad (2.2)$$

$$ES[i]=\sum_{i=0}^{i<len} E_L, E_{L-L+1}, E_{L-1}, E_{L-L+2}, E_{L\frac{1}{2}}] \quad (2.3)$$

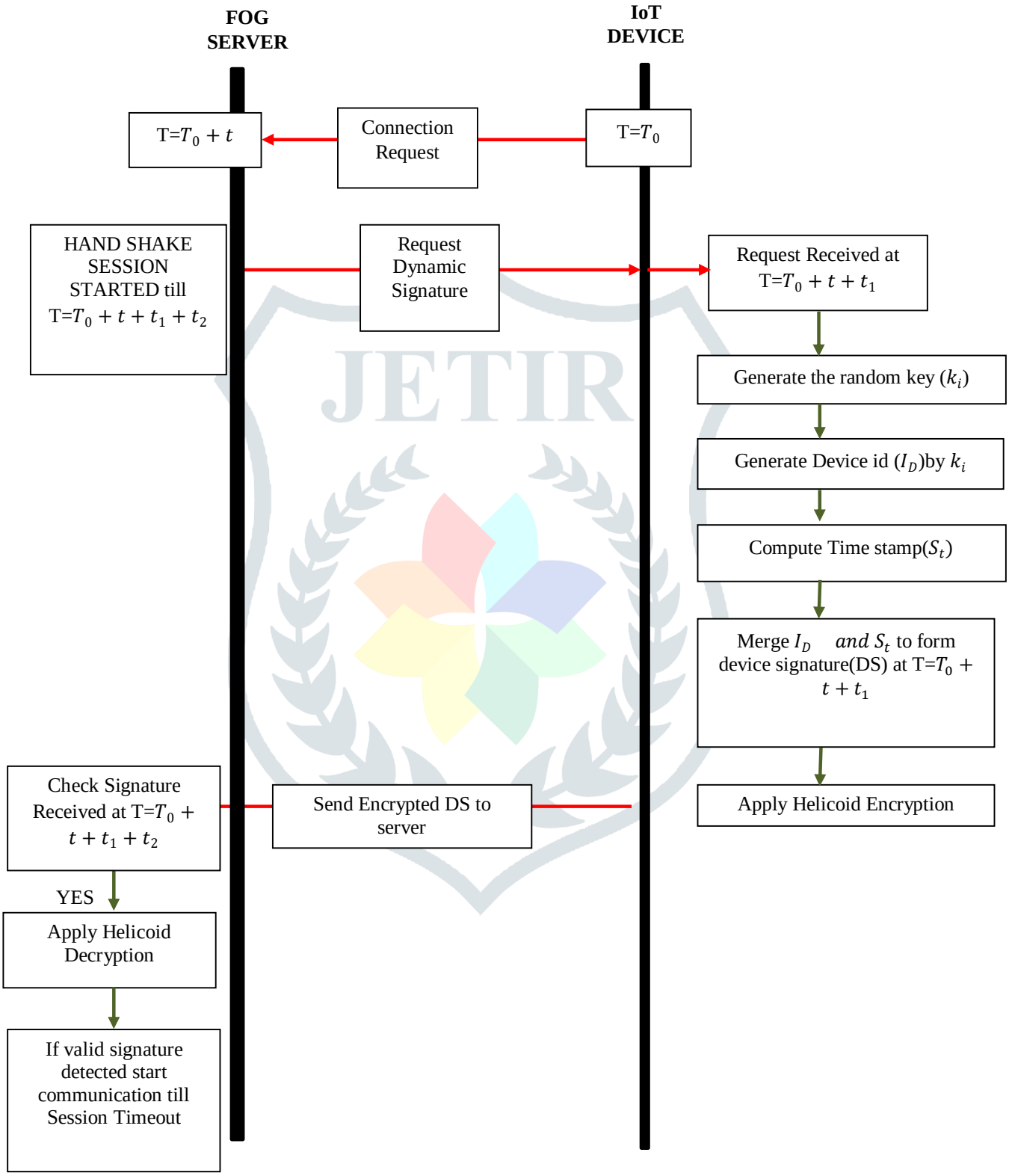
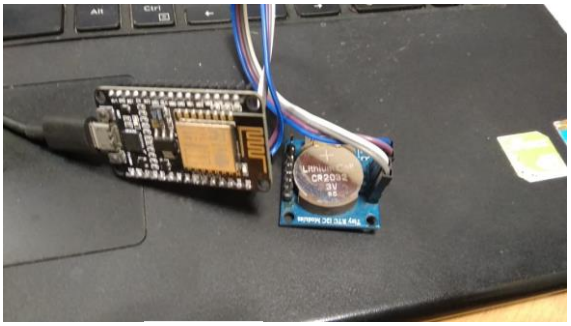


Fig 2.2: Process flow of proposed algorithm.

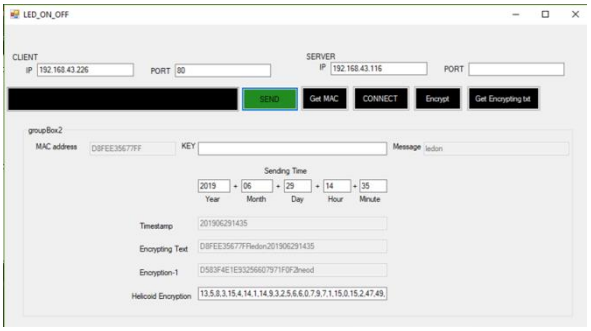
III. RESULTS AND DISCUSSION

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 3.1(a) denotes the used components which are Node MCU ESP826612E and Real Time Clock (RTC) module. Fig 3.1(b) denotes the developed Graphical User Interface using socket programming in C#. Asynchronous programming is used in

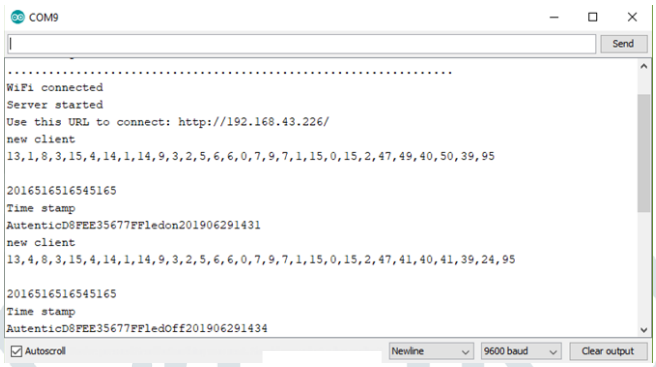
developing client and server socket for sending and receiving data. The IP address and port number of both client and server are entered in the respective textbox. The signature is extracted and sent for authentication. Fig 3.2 denotes the authentication of IoT device in case of receiving valid device signature.



(a)



(b)



(c)

IV. CONCLUSION

The proposed algorithm for automatic device authentication is lightweight yet efficient. The proposed algorithm can easily combat various attacks. As the key is generated randomly and dynamically the algorithm can beat dictionary and frequency analysis attack. The proposed algorithm also has high reliability against side channel attack. Thus it is advantageous in IoT environment deployment.

V. FUTURE SCOPE

In future the efficacy of the proposed algorithm should be tested in cloud computing environment. Different nature inspired algorithms such as Artificial Immune system can be applied to detect the intrusion behavior and block the attacker. The same can be achieved by integrating the developed algorithm with Machine Learning.

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] 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.