Antimmuno Protocol : A Novel Model for Security Concerns in Multi-hop IoT Routing

Prakash Chandra Sahoo and Pralipta Samal

Department of Computer Science Engineering, Trident Academy of Technology, Bhubaneswar, Odisha, India

prakashsahoojobs@gmail.com

Abstract—The aim of the proposed research model is to examine the a new technology for reducing security threats in multi-hop iot networks by using antigen and immunology principles. Various types of threats and the methods to counteract them has been discussed in the said research paper. Antigen uses special modules to counteract the malicious spywares and help in restoring the sound health of an IoT based network.

Keywords— Antigen, Immunology, Malware, IoT Security, Multi-hop routing, Jamming, Cloning,

1.INTRODUCTION

Internet of Things (IoT) has recently gained much of attention as the technology grows at a faster rate and is reaching the hands of billions. IoT would be the future of technology where M2M and D2D communication among smart devices would increase at a sharp rate. This paper addresses an security protocol technique where the systems are smart enogh to fight external threats in a similar manner analogous to the immune system of human body . [1]-[4]

2.TYPES OF THREATS IN MULTI-HOP IOT ROUTING

Sl No.	Type of Threat	Antimmunology in Causal Study
1	Evesdropping	Encryption applied prior to stealing by the attacker
2	Hyperactive	Applied especially in medical environment
3	Imitative	Alternation is done in holistic cleaning if the threat
4	Inneruptive	Attacker uses cloning the source, so anti-spoofing program is run
5	Routed-Diversive	Blind-signature based program is run by the group for restricting sensitive information
6	Blocked-Chain	Trojan worms are made to dissolve at the destination before the attack
7	Affricative	Jamming procedure is started by the source which secure the firewall
8	Congregative	Malicious malware are packed as bunched spam and disintegrated by cryptographic techniques.

Table -1 – Details of Various security threats and measures taken by the proposed system.

Security threats have been challenge for wireless systems. When we consider IoT there has been a tremendous increase in its application in recent years.

It is roughly estimated that by 2025 the devices using iot would be 2.5 billion. This creates and psychological impact on the programmers to device iot based solutions. When we consider the protocols for designing systems to make security attacks invincible, various protocols have been suggested.prop indication process for multi-hop IoT networks is a challenge which is overcome by using the immunology computer science principle. [5]-[8]

3.ANTIMMUNO PROTOCOL : COMBINATION OF ANTIGEN AND IMMUNOLOGY

STEPS	MULTI-HOP IOT ROUTING PARAMETERS	ANTIGEN PROTOCOL

1	**Website Module**	• Weaker passwords elimination is guaranteed.
2	**Encryption/Decryption**	• Implementation of strong password with special characters & numerals needed .
3	**Network-security Services**	• Fuzz flow minimization.
4	**Transportation Cryptology**	• End-to-End encryption for D2D communication.
5	**Authorization Concern**	• Customer return feedback at user level is obtained.
6	**Cloud-security Networking**	• Defenseless structures of API are highly reduced.
7	**Mobile-security Networking**	• Week pass-codes of mobile is re-written by device
8	**Insufficient Security Configurability**	• Extending passwords to 32 characters after authentication access.
9	**Firmware of D2D/M2M**	• Dynamically updating of existing applications to suit antigen protocol.
10	**Physical point-to-point security**	• External I/O hardware ports control on hand-held devices like USB-ports.

Table – 2 – Addressing multi-hop IoT routing by Antigen Protocol.

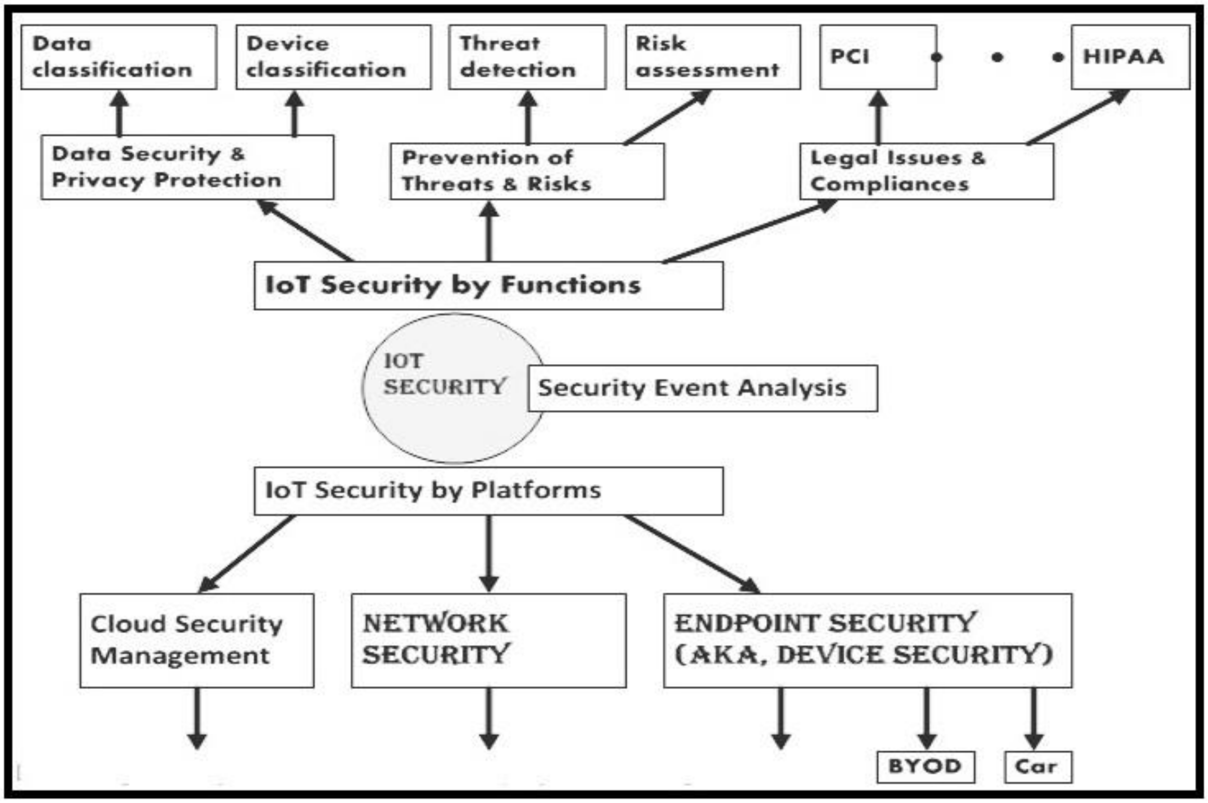
Data classification
Device classification
Threat detection
Risk assessment
PCI
HIPAA
Data Security & Privacy Protection
Prevention of Threats & Risks
Legal Issues & Compliances
IoT Security by Functions
IOT SECURITY
Security Event Analysis
IoT Security by Platforms
Cloud Security Management
NETWORK SECURITY
ENDPOINT SECURITY (AKA, DEVICE SECURITY)
BYOD
Car

Figure 1- Summary of IoT Security Event Analysis.

Antigen : It is aspecial protocol designed to ensure thee smart behavior of the network , and develop a self-fighting strategy to the threat.

Immunology:

STEPS	MULTI-HOP IOT ROUTING PARAMETERS	IMMUNOLOGY PROTOCOL
1	**Website Module**	Utilizing new dynamic languages like Kotlin in device depended platforms similar to amazon web services (AWS)
2	**Encryption/Decryption**	Cloud computing assisted error correction based on deep learnling
3	**Network-security Services**	Filling proper stacked layer-to-layer open source interconnection at network level
4	**Transportation Crptology**	Enabling superlative encryption on the basis of source request
5	**Authorization Concern**	Hyper-interactive domain name server (DNS) for self-correcting firewall hacks
6	**Cloud-security Networking**	Iterative repeat request (IRQ) levels set by the cloud security provider.
7	**Mobile-security Networking**	OTP based password resetting in portable device appliances (PDAs)
8	**Insufficient Security Configurability**	Fingerprint based Biometric authentication in smart hand-held devices (SHHDs)
9	**Firmware of D2D/M2M**	Confutative hardware-interfacing in near-field cellular integrated networks .
10	**Physical point-to-point security**	Anti-Malware self-repetitive iteration initiated as soon as the threat is detected at primary source.

Table – 3 – Addressing multi-hop IoT routing by Antigen Protocol.

Steps to be followed in Antimmuno protocol in counteracting security threats in multi-hop IoT networks must include scalability in testing, holistic edged technology and smart encryption in primary stage. The secondary stage must inculcate system versatility, full-life likelihood algorithm based support . This large haul weakens the attackers trying to break the barrier with explicit ownership

6. SCOPE FOR REAL-TIME APPLICATION

Immunology protocol uses fair-usage mechanism for establishing safe techniques of malware detection. The security threats in an unambiguous environment could be detected by self correcting structure of the intelligent network. The future indices that may be used for its advanced application are D2M (Devices to Machine), CISCOT (Internet of Thing based CISCO systems , WSW (World Size Web). The services must be consumer oriented, economical and user-friendly.

REFERENCES

[1] Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[2] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Network Journal., vol. 54, no. 15, pp. 2787–2805, Oct 2010

[4] Caiming Liu ; Yan Zhang ; Huaqiang Zhang , "A Novel Approach to IoT Security Based on Immunology" IEEE 2013 Ninth International Conference on Computational Intelligence and Security.

[5] Yanbing Liu ; Yao Kuang ; Yunpeng Xiao ; Guangxia Xu, "SDN-Based Data Transfer Security for Internet of Things",IEEE Internet of Things Journal, Year: 2018 , Volume: 5 , Issue: 1

[6] Mikael Asplund ; Simin Nadjm-Tehrani, “Attitudes and Perceptions of IoT Security in Critical Societal Services”, IEEE Access Year: 2016 , Volume: 4

[7] Peng Hao ; Xianbin Wang ; Weiming Shen, “Equivalence A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication”, IEEE Access Journal, Year: 2018 , Volume: 6

[8] Anne H. Ngu ; Mario Gutierrez ; Vangelis Metsis ; Surya Nepal ; Quan Z. Sheng, “ IoT Middleware: A Survey on Issues and Enabling Technologies”, IEEE Internet of Things Journal, Year: 2017 , Volume: 4 , Issue: 1

[9] Ramya Ranjan Choudhury, “A Network Overview of Massive MIMO for 5G Wireless Cellular: System Model and Potentials” , International Journal of Engineering Research and General Science, Volume 2, Issue 4