www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-9, Issue-1, February 2021
Research Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

A Secure Light Weight Authentication Protocol for Wireless Sensor Network in Internet of Things

M.M. Nareshbabu[1*], A.S.N. Chakravarthy[2], C. Ravindranath[3]

[1]Dept. of Computer Science & Engineering, JNTU Kakinada, Kakinada, India
[2]Dept. of Computer Science & Engineering, JNTU Kakinada, Kakinada, India
[3]Dept. of Computer Science & Engineering, Christ University, Bengaluru, India

[*]*Corresponding Author: itsnaresh4u@gmail.com, Tel.: +91-99591-92472*

Received: 10/Feb/2021, Accepted: 20/Feb/2021, Published: 28/Feb/2021

***Abstract*—** With the advancement of cloud and Internet of Things (IoT) technology, mobile phones, RFID systems and wireless sensor networks can be integrated to form heterogeneous systems to execute smarter applications. However, data exchange between remote cloud and sensor node via internet poses critical security challenges. The major challenge is the authentication and key exchange among the communication agents. In addition, resource constrained devices such as RFID tags, sensors in WSN and IoT integration (WSNIT) would require robust and light weight authentication schemes. To combat these issues, we establish in this paper a first of its kind of a WSN security protocol in IoT, which is light weight and resistant to cryptographic attacks.

***Keywords*—** Internet of Things, Cloud Authentication, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor networks (WSN) offer a virtual digital layer which senses the critical information from the physical world and submit it to storage system for remote processing and data analysis. Internet of Things (IoT) results in embedding of computational competence in all kinds of resource constrained devices like RFID tags, mobile devices etc. and allows these devices to connect to WSN and access the critical data stored in the sensors.

II. MOTIVATION AND PROBLEM STATEMENT

The amalgamation of IoT and WSN (WSNIT) [1,2,3] is in a promising stage and industry giants like IBM, H.P has started initial research on WSNIT. In china, IBM developed a smarter app called 'A Smarter Planet', which is built on top of sensors to deliver reliable Internet-based information from intelligent water management system and weather forecast systems to farmer's mobiles through Internet (SMS).

In order to allow safe exchange of critical data between WSNIT and various online social networks and to link the aggregated data from sensor nodes with web services based on SOAP, demands for stringent authentication system that is robust and light weight. Hence, we intent to come up with a light weight and cryptographic attack resistant authentication scheme in order to reap the maximum benefits from WSNIT.

III. WSNIT SYSTEM

As shown the fig 1, the data from sensors of WSN which is deployed in real time applications is transmitted to remote cloud servers via middle servers comprises of internet, computing and processing resources.

A. Communication Agents of WSNIT

WSNIT consists of three communication entities i.e. remote Cloud (C), middle server (M) and WSN (S) having identities ID_c, ID_m and ID_s respectively. During the initialization stage of the system, C and M shares a symmetric key 'm' and M and S share 'k' securely. Cloud and Middle server are private and not accessible to outside world. The WSN and middle server exchanges data via public Internet. we are elucidating the protocol diagrammatically. The protocol runs from top to bottom and from left to right.

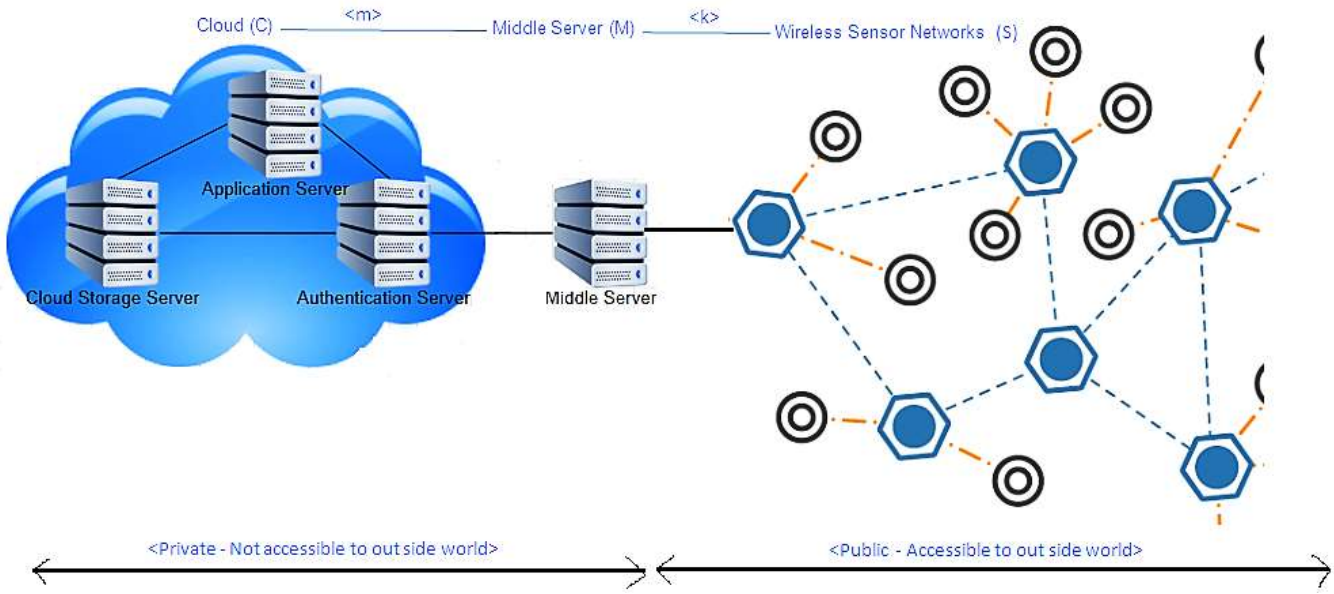

Fig. 1. Graphical view of WSNIT.

IV. WSNIT AUTHENTICATION PROTOCOL

Table 1. Proposed Protocol

Cloud (C)	Middle Server (M)	WSN (S)
Generate a random number R_c $\{R_c\}$ →		
	$M1 = R_c \oplus h(ID_s \oplus ID_m \oplus k)$ $\{M1\}$ →	
		$R_c = M1 \oplus h(ID_s \oplus ID_m \oplus k)$ Generate R_s $R2 = R_s \oplus h(k \oplus R_c \oplus ID_s \oplus ID_m)$ $M2 = h(ID_m \oplus ID_s \oplus R_c \oplus R_s \oplus k)$ ← $\{M2, R2\}$
	$R_s^* = R2 \oplus h(k \oplus R_c \oplus ID_s \oplus ID_m$ $M2^* = h(ID_m \oplus ID_s \oplus R_c \oplus R_s^* \oplus k)$ Check $M2^* = M2$, M Authenticates S Generate R_m $M3 = h(ID_m \oplus R_m \oplus R_c \oplus R_s)$ $R3 = R_s \oplus h(R_c \oplus ID_m \oplus k)$ $R4 = R_m \oplus h(R_s \oplus R_c \oplus ID_m \oplus k)$ ← $\{M2, M3, R3, R4\}$	
$Rs^* = R3 \oplus h(Rc \oplus IDm \oplus k)$ $Rm^* = R4 \oplus h(Rs^* \oplus Rc \oplus IDm \oplus k)$ $M3^* = h(IDm \oplus Rm^* \oplus Rc \oplus Rs^*)$ $M2^* = h(IDm \oplus IDs \oplus Rc \oplus Rs^* \oplus k)$ if $M2^* = M2$ and $M3^* = M3$ C authenticates M and S. Generates a session key S.K. $M4 = h(IDm \oplus Rm^* \oplus m) \oplus S.K$ $M5 = h(IDm \| m \| S.K \| Rm^*)$ $M6 = h(IDs \oplus k \oplus Rs^*) \oplus S.K$ $M7 = h(IDs \| k \| S.K \| Rs^*)$ $\{M4, M5, M6, M7\}$ →		

	$S.K^* = M4 \oplus h(IDj \oplus Rm \oplus m)$ $M5^* = h(IDj \| m \| S.K^* \| Rm)$ If $M5^* = M5$, C is authenticated by M {M6, M7} →	 $S.K^* = M6 \oplus h(IDj \oplus k \oplus Rs)$ $M7^* = h(IDj \| k \| S.K \| Rs)$ If $M7^* = M7$, C is authenticated by S.

V. SECURITY ANALYSIS

Table 1. Parameters available to an attacker

Equation Accessible to an Attacker (E) via internet	Values known to 'E'	Values not known to 'E'
$M1 = R_c \oplus h(ID_s \oplus ID_m \oplus k)$	None	ID_s, ID_m, k
$M2 = h(ID_m \oplus ID_s \oplus R_c \oplus R_s \oplus k)$	None	ID_m,,ID_s, R_c, R_s, k
$R2 = R_s \oplus h(k \oplus R_c \oplus ID_s \oplus ID_m)$	None	ID_m,,ID_s, R_c, k
$M6 = h(ID_s \oplus k \oplus R_s) \oplus S.K$	None	ID_s, k, R_s. Hence unable to get S.K.
$M7 = h(ID_s \| k \| S.K \| R_s)$	None	ID_s, k, S.K., R_s

In our proposed scheme, the keys shared among C, M and S i.e k, m are assumed to be shared securely and it is impossible for an attacker 'E' to intercept. As shown in the table, even though the symmetric keys k and m are leaked out, in order to perform impersonation, MiM attacks, 'E' requires one or more 128 bits long random numbers and identities i.e ID_s, ID_m, ID_c, R_c, R_s, S.K. It is computationally impossible for 'E' to guess these values in real polynomial time. Therefore, we can conclude that, our scheme resists all major cryptographic attacks.

VI. CONCLUSION

In this manuscript, we have proposed and analysed first of its kind of secure and light weight authentication protocol for the amalgamation of WSN and IoT. We have designed the scheme using only light weight hash (SHA-2) and XOR operations. As shown in table 2 and discussed earlier, our scheme is attack resistant, due to the fact that, the attacker must guess one or more unknown variables of 128 bit length (which is computationally impossible) to succeed in any attack.

REFERENCES

[1] Daniel G., Sergio L., Federico B., Nik B., Eleana A.,"The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments". *Springer book: Internet of Things and Inter-cooperative Computational Technologiesfor Collective Intelligence* , Vol **460**, **2013**

[2] Andrew W., Anurag A., Li X.,. 2014, "The Internet of Things—A survey of topics and trends" *Springer journal of Information Systems Frontiers*. Mar **2014**.

[3] John L., Hua Z., Zhihong L., Xiangcheng W., Yuhong C., "The Wireless Sensor Network Security Protocol Research in Internet of Things". *Advances in Intelligent and Soft Computing* Vol **149**, pp **241-247**, **2012**.

AUTHORS PROFILE

Mr. Naresh Babu M. M. received his M.Tech degree from VIT University, Vellore, India. Currently he is pursuing Ph. D. in the Department of C.S.E., Jawaharlal Nehru Technological University Kakinada, Kakinada, A.P., India. He has published papers in various International journals and conferences. His areas of current research include Networks, Mobile Security & Cryptography.

Dr. A. S. N. Chakravarthy is currently working as Professor, Dept. of Computer Science & Engineering, Coordinator MOOCs & Skill Development Centre, Jawaharlal Nehru Technological University Kakinada, Kakinada, A.P., India. He has 62 papers published in various International journals and conferences. His research areas include Networks, Security & Cryptography, Biometrics, and Digital Forensics. He is Editorial board member for various International Journals.

Dr. C. Ravindranath received the Ph.D degree in Electrical and Computer Engineering from University of Texas at San Antonio(USA). He is currently the principal of Trinity Institute of technology & Research, Bhopal, India. He is reviewer of IEEE, SPIE and Elsevier. He was post research fellow at University of Texas at San Antonio (USA). He has published large number of research papers in the reputed International/National journals and conference proceedings. He has two patents in Digital Image Security. His areas of current research interest include System Security, Multimedia Processing, Information Assurance and Applied Statics.

