SURVEY REPORT ON ACCESS CONTROL AND AUTHENTICATION SYSTEM FOR INTERNET OF THINGS

Kuntal Shah[1], Chandresh Parekh[2]

[1] Student, M.Tech Cyber Security Raksha Shakti University, Ahmedabed,India
[2] Assistant Professor Telecommunication, Raksha Shakti University, Ahmedabad, India

ABSTRACT

Internet of Things is necessary part of everyday life. Compromise in the security of the Internet of Thing can create a disaster. To secure the Internet of Things, authentication and access control is important to establish secured communication between devices. Due to the unsecured authentication and access control system possibility of the attacks like eavesdropping, denial of service and replay attack has been increased. This survey paper focuses on different access control algorithms and their vulnerabilities. The difference between the security features of different algorithm is also discussed so that it will be helpful to the researcher to make a secured system according to their need.

Keyword: *- Internet of Things, Access Control, Authentication, Security Algorithm*

I. INTRODUCTION

The smart devices are now forming a new emerging world by establishing a new Internet-based information system and device service platform called the Internet of Things (IoT) [1]. As an emerging technology it is necessary that the, it should be secured at the time of the implementation [2]. The main attacks identified in the IoT are denial of service attack, man-in-middle attack, reply attack, Sink whole attack etc [2]. To make a secured system we have to pay attention on the P.A.I.N of the system it refers to the

1) PRIVACY: transferring message from source to destination can be easily intercepted by attackers and their data can be modified. Privacy refers to the system that the data cannot be accessed by the unauthorized parties. applied on storage of device. Simple solution for this is encryption/decryption mechanism.

2) AUTHENTICITY: End user should able to identify each other's identity to ensure that they are interacting with same entities that who they claim.

3) INTEGRITY: Message passing from source to destination should not alter; it should be received at receiver side same as that of sent at sender side. No intermediary hould change content of message while they are passing or on device.

4) NON-REPUDIATION: After the reception of the message the sender cannot able to decline that the massage is not sent by him/her. So to secure the IoT main two points to provide security from all attacks is by providing a good authentication and access control technologies [3][4] are known as the central elements to address the security and privacy problems in computer networks. They can prevent unauthorized users from gaining access to resources it prevents legitimate users from accessing resources in an unauthorized manner, and also enables legitimate users to access resources in an authorized manner [2]. This survey paper mainly gives information about the existing system for the access control and authentication and its relative pros and cones.

II. RELATED WORK

There is closely related work is done in [5] where security association takes place with increased communication overhead but in this the authentication system is not addressed. They have also introduced distributed access control solution based on security profiles but attack resistance is not explained. In [6], authors have presented Elliptical Curve Cryptography based authentication system but the major disadvantage is that they are not Denial of Service (DoS) attack resistant, because it does not define how the system establishes connection. In [7], authors have addressed the problem of secure communication and authentication based on the shared key and is applicable to limited location and cannot be used for wide area so the problem of scalability is present. It can address the peer-to-peer authentication but may not be able to extend in resource constrained environment. There has been lot of debate about which of the cryptographic primitives like Public Key Infrastructure (PKI) or symmetric crypto is suitable for the IoT [13]. Most of the researches are mainly focused in the area like Wireless Sensor Network (WSN) and its application. Many security mechanisms have proposed use of private key cryptography due to its faster result. But in this main problems are P.A.I.N and also Scalability and memory requirement to store keys that makes the system inefficient to heterogeneous devices in IoT but the public key cryptography based solution overcomes these challenges with high scalability, low memory requirements [2] and no requirement of key pre-distribution infrastructure and also gives more privacy, authenticity, integrity and non-repudiation. In [8], authors have presented ECC based mutual authentication protocol for IoT using hash functions and then mutual authentication is achieved between terminal node and platform using secret key cryptosystem by introducing the problem of key management and its storage. Self- certified keys cryptosystem based distributed user authentication scheme for Wireless sensor network is presented in [9] where only user nodes are authenticated and is not lightweight solution for IoT. In [10], author presents authentication with parameter passing during handshake. Handshake process is much time consuming and also based on symmetric key cryptography which consumes more memory for large size of prime numbers. Efficient identification system and authentication presented in [11] and it is based on the signal properties of node but is not suitable for mobile nodes. Direction of the signal is considered as parameter for node authentication but it takes more time to decide signal direction with more memory and computations involved. In [12], cluster based authentication is proposed which is most suited for futuristic IoT, but attacker can get hold of distribution of system key pairs and cluster key. Generation of random numbers and signatures will create considerable computational overhead and also consumes more memory resources. In [13] IECAC is more convenient to the secured access control and authentication system. The evaluation is shown in Table 1. Related work is summarized based on the parameters like mutual authentication, less memory requirement solution, attacks resistance, distributed nature and access control system.

From table 1, it is clear that, all existing solutions other than [13] for authentication and access control do not fulfill all requirements for IoT. In [13], authors have achieved mutual identity establishment i.e. authentication and once authenticated, access control will take place. It also proposes new method of authentication of devices and access control for the IoT using public key cryptographic approach with scalability and less memory requirements. Most important design issue of IoT is the mobility of heterogeneous devices and this scheme will work efficiently for this need.

TABLE-1: Evaluation Summery

Solutions	Parameters						
	Mutual Authentication	Less memory	Attack Resistance			Suitability for distributed Network	Secured Access control
			Eavesdropping	DOS	Reply		
5	N	N	N	N	N	Y	Y
6	Y	Y	N	N	N	Y	N
7	N	N	Y	Y	Y	N	N

8	Y	Y	Y	N	Y	Y	N
9	N	N	N	N	N	Y	N
10	Y	Y	Y	N	Y	N	N
11	Y	N	N	N	N	Y	N
12	Y	N	N	N	N	Y	N
13	Y	Y	Y	N	Y	Y	Y

[5] Ubiquitous access control in MAGNET, [6] ECC based authentication in RIFID, [7] Authentication Ad-hoc wireless network, [8] Authentication in IoT, [9] Authentication in WSN, [10] Progressive authentication in Ad-hoc Network, [11] Peer identification and authentication, [12] Authentication in Ad-hoc network [13] Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things.

I. CONCLUSION

This paper represents different types of the Access control system and its loop holes. It will help researcher and developers to make a secured IoT network which is less vulnerable and can provide better security to the system.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “*The Internet of things: a survey*,” Computer Networks, vol. 54, issue 15, 2010, pp 2787-2805.

[2] Jing Liu and Yang Xiao, and C. L. Philip Chen, “*Authentication and Access Control in the Internet of Things*”, 32nd International Conference on Distributed Computing Systems Workshops by Research Gate,2012.

[3] R. H. Weber, “*Internet of things – new security and privacy challenges*,” Computer Law & Security Review, vol. 26, issue 1, Jan. 2010, pp. 23-30.

[4] A. Vapen, D. Byers, and N. Shahmehri, “*2-clickAuth – optical challenge-response authentication*”, in: Proceedings of 2010 International Conference on Availability, Reliability and Security, 2010, pp. 79-86.

[5] D. M. Kyriazanos, G. I. Stassinopoulos and N. R. Prasad, "*Ubiquitous Access Control and Policy Management in Personal Networks,*" Mobile and Ubiquitous Systems: Networking & Services, 2006 Third Annual International Conference on, vol., no., pp.1-6, July 2006.

[6] S. I. Ahmed, F. Rahman and E. Hoque, “*ERAP: ECC based RFID Authentication Protocol*,” 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2008.

[7] D. Balfanz, D. K. Smetters, P. Stewart and H. C. Wong, “*Talking to strangers: Authentication in ad-hoc wireless networks”*, Network and Distributed Systems Security Symposium (NDSS), Feb 2002.

[8] G. Zhao, X. Si, J. Wang, X. Long and T. Hu, "*A novel mutual authentication scheme for Internet of Things*," sModeling, Identification and Control (ICMIC), Proceedings of 2011 IEEE International Conference on , vol., no., pp.563-566, 26-29 June 2011

[9] C. Jiang, B. Li and H. Xu, “*An efficient scheme for user authentication in wireless sensor networks*,” in: 21st International Conference on Advanced Information Networking and Applications Workshops, 2007, pp.438-442.

[10] R.R.S. Verma, D.O'Mahony and H.Tewari , "*Progressive authentication in ad hoc networks*,” Processing of Fifth European Wireless Conference, February 2004.

[11] T. Suen, A.. Yasinsac, "*Ad hoc network security: peer identification and authentication using signal properties*," Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC, vol., no., pp. 432- 433, 15-17 June 2005.

[12] L. Venkatraman and D.P. Agrawal, "*A novel authentication scheme for ad hoc networks,*" Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE, vol.3, no., pp.1268-1273 vol.3, 2000.

[13] Parikshit N. Mahalle , Bayu Anggorojati , Neeli R. Prasad and Ramjee Prasad , “*Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things*,”. In IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012). Taipei - Taiwan, September 24-27 2012.