A Study of Authentication Protocols in Internet of Things

Amiya Kumar Sahu*, Suraj Sharma†, Shankar Sharan Tripathi‡ and Kamakhya Narain Singh§
*†Dept. of CSE, International Institute of Information Technology Bhubaneswar, India
‡Dept. of CSE, Sri Shankaracharya Engineering College, Bhilai, India
§School of Computer Application, KIIT Deemed to be University, Bhubaneswar, India
*Email: c117002@iiit-bh.ac.in, †suraj@iiit-bh.ac.in, ‡tripathi.shankar@gmail.com, §kamakhya.vphcu@gmail.com

***Abstract*—Internet of Things(IoT) is a promising technology in the current era, and security is one amongst the significant challenges in its success. The resource constraints in devices make the design and implementation of counter security mechanisms more challenging. Many attacks from an eavesdropper may endanger to authentication and lunch further attack to IoT systems. Hence, there is a need for an efficient authentication mechanism to withstand all possible known attacks. This study discusses the recent research on lightweight authentication protocols and compares them on various security parameters. In addition, the study also enumerates the various research issues related to the efficiency of authentication mechanisms in IoT. The study also discusses the possible solutions for authentication.**

***Index Terms*—Authentication, Internet of Things, IoT, Security, Protocol, Lightweight,**

In recent years, the Internet of Things has emerged as an attractive field of research due to its vast scale of applications. The objective of IoT is the seamless integration of both digital and physical objects in one overarching network that would lead to an intelligent and autonomous era of the Internet. However, the rapid growth of things connected to the Internet resulted in various challenges, such as energy management, scalability, interoperability, and security. Primarily, security is the main concern in the success of IoT, which influences other challenges in the field. It is even more challenging than other challenges in terms of a complex environment and resource-constrained IoT devices. Usually, tiny IoT objects are mostly run by battery power, possess a limited amount of primary memory and processing power. And, designing a security mechanism which can be fit into these tiny devices is a daunting task. As a result, many research solutions have been proposed in IoT security dealing with: key management, user authentication, device authentication, user access control, privacy preservation, and Identity Management.

The recent developments in security tools for network information gathering is making an eavesdropper a stronger adversary. Many attacks, such as Eavesdropping, Replay, Preplay, Reflection, Man-in-the-Middle, Denial of Service, Typing attacks, and Certificate Manipulation, are a serious threat to authentication in IoT enabled Systems. Moreover, designing and implementing a secure counter mechanism to mitigate the attacks are difficult as the target devices are resource constraint. Figure 1 shows the challenges faced by IoT and security categories. Researchers have proposed many protocols to mitigate attacks on authentication. Primarily, the protocols

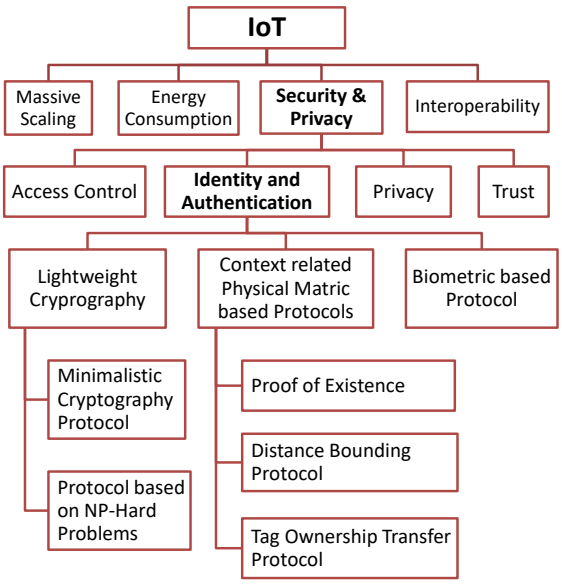

Figure 1: Challenges faced by IoT and security categories

are built on lightweight and low-cost encryption scheme. We, in this paper, specifically focused on the study of lightweight authentication protocols and testify them on various security parameters.

The rest of the paper is organized as follows: Section II describes the preliminaries of authentication, authentication in IoT and its various properties, Section III depicts the survey of authentication protocols in a tabular manner and section IV comprises open research issues in achieving lightweight authentication, future direction to solutions, and conclusion followed by references.

I. Preliminaries of Authentication

A. Authentication

Authentication aims to identify an entity (devices/users) within a communication network and does not allow access to an unauthorized entity. Authentication goes through two major steps: first, presentation of Identity, where a candidate has to submit their identity key for validation, second, the verification of that Identity in which the candidate has to provide proof

978-1-7281-6052-8/19/$31.00 ©2019 IEEE
DOI 10.1109/ICIT48102.2019.00045

of ownership of that identity key. Proof of ownership can be four types: something you know, something you possess, something you are, and something (context) related to you. Authentication mechanism can also be built upon two or more than two above factors.

Basically, the protocol design for authentication is based on answering three questions below[1]:

1) Assumptions: What are the keys already been established?
2) Session: How to generate a session key for communication?
3) Users: How many users will be served by the protocol?

Assumption: it is the base condition for a security mechanism to work and stand against various security attacks. It is assumed on three sharing mechanisms of keys: First, already have a shared-secret-key, Second, a requirement of off-line trusted server for sharing keys, Third, based on the requirement of an on-line server for sharing secret keys. Assumptions for security mechanism also essentially states the potential capabilities of an intruder.

Session: Session key generation is two primary sets of protocols, First, Key-Transport protocol where one of the principal generates and transport the key(s) to other principals in the communication, Second, Key-Agreement protocols where all principals input in a function to generate the session key. There is another way of session key generation. Hybrid session key generation protocol is also possible by harnessing the capabilities of both key-transport and key-agreement mechanism.

Users: Users may communicate point-to-point or may involve in multi-party communication. Thereby, user participation in a protocol is an essential factor for protocol design.

A scenario for the authentication requirement may come up with the permutation of the above three questions. So, the solution should firmly stand on the underlying assumptions. The assumptions also provide a reasonable key parameter to choose the security parameter for provable security.

B. Authentication in IoT

Authentication in IoT has two folds: user authentication and device authentication. And, the communication can be possible in three ways: User-User, Machine-Machine, Machine-User. Therefore, the device authentication mechanism in IoT is pretty challenging and different than the user-centric. In addition to this, the resource limitations in IoT objects make it more difficult.

The requirement of authentication is essential in all the three layers of Service Oriented Architecture (SOA) of IoT. In the Application layer, two scenarios may require authentication: First, a user needs to be authenticated before accessing and controlling a remote device, and Second, a user along with the associated IoT objects need to be authenticated before availing services from the cloud server. Similarly, the Network layer and Perception layer also requires authentication of nodes in their respective network to mitigate various attacks such as Sybil, wormhole, selective forwarding, tag cloning, spoofing, impersonation. Table I shows the possible attacks in the respective IoT layers of the SOA architecture.

Table I: Possible Attacks on IoT Layers

Layers	Attacks Possible in IoT
Application Layer	Replay, Preplay, Crypto attacks, Injection, buffer overflows
Network Layer	Sinkhole, False routing, Hello and session flooding, eavesdropping, Impersonation, Network protocol attacks
Perception/Physical Layer	Jamming, sybil, replay, Side Channel attack, Crypto attack

C. Authentication Properties

Figure 2 depicts the various security properties requirements for authentication. Three authentication properties, that is, Aliveness, Synchronization, and Message Agreement, are essential attributes which should be possessed by a typical security protocol. The Aliveness property guaranties the active participation, i.e., an intended communication partner has acted certain event. The synchronization property implies that all messages sent by communication partners in the system are indeed sent by them, and the order is also intact. Message agreement assures the message exchanged are in the agreed format between the communication partners. In addition, Secrecy of various message exchanged among the nodes is also an essential property. It would support other mentioned three security properties to hold. Cas Cremer et al. [2, 3] has devised a formal verification tool on the basis of these properties. The security properties of protocols can be verified by that tool. However, the preservations of these properties do not guarantee fool-proof protection from all security attacks. In addition to the security protocol, one should take care of implementation and constraints on which these properties would be tested.

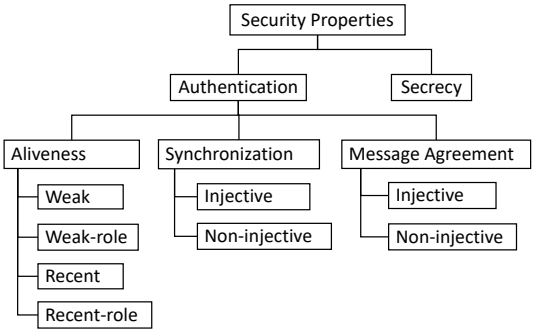

Figure 2: Security Properties

II. Lightweight Authentication Protocols

The Table II depicts the survey of recent papers on authentication, i.e., 2017-19. The survey specifically focused on lightweight protocol design, secure key establishment, and secure communication properties. It also differentiates the user centric authentication protocols from device centric.

Table II: Recent Research Work on Authentication

Ref.	Pub. Year	Layer	Key Establishment	Device Centric	User Centric	Protocol Type	Light weight	U2M	M2M	Security Objective	Domain	Tools Used	Objective
[4]	2019	N/W	KT	Y	Y	P2P	Y	Y	N	SC	Healthcare	AVISPA, BAN-logic	Mutual Authentication using XOR and one-way cryptographic hash function
[5]	2019	App	KA	N	Y	P2P	N	Y	N	SC	Healthcare	Scyther	Context based anonymous authentication scheme
[6]	2019	N/W	KA	N	Y	P2P	Y	Y	Y	SC	Fog Computing	AVISPA, NS2	user authentication scheme using XOR and one-way cryptographic hash function
[7]	2019	N/W	Hybrid	Y	Y	P2P	Y	N	Y	SC	WSN	Test-bed	key distribution algorithm is based on preexisting information to generate dynamic keys
[8]	2019	N/W	Hybrid	N	Y	P2P	Y	Y	N	SC	Smart Grid	Proverif	key establishment protocol for smart grid
[9]	2019	App	KA	N	Y	P2P	Y	Y	N	AC	Smart Home	AVISPA, BAN-logic	Mutual authentication and automated access control
[10]	2018	N/W	KT	N	-	P2P	Y	Y	Y	SC	Generic	Cooja	Security overhead abated
[11]	2018	N/W	-	Y	-	P2P	N	N	Y	AC	Vehicular N/W	MATLAB	Capacity based access admission control
[12]	2018	N/W	-	Y	-	P2P	N	Y	N	AC	Generic	AVISPA	Three factor Authentication
[13]	2018	N/W	-	Y	Y	P2P	-	N	Y	SC	Generic	MATLAB	Vulnerabilities mitigation for both IP or Non-IP devices
[14]	2018	N/W	-	Y	N	P2P	-	N	Y	SC	Generic	AVISPA	Security enhanced group based (SEGB)
[15]	2018	N/W	-	Y	N	P2P	-	N	Y	SC	Generic	NA	Secure N/W coding signatures
[16]	2018	App	-	Y	Y	P2P	Y	Y	N	AC	Smart Home	Test-bed	Authorization in an un-trusted Cloud Platform
[17]	2018	App	-	N	N	P2P	-	Y	N	AC	Cloud Multi Server	BAN-logic, AVISPA	Smartcard based Authentication protocol
[18]	2018	N/W	KA	Y	Y	P2P	-	N	Y	SC	Generic	NA	Mutual authentication
[19]	2018	N/W	-	Y	N	P2P	-	N	Y	SC	Generic	NA	Identity based Authentication protocol
[20]	2018	N/W	-	Y	N	P2P	-	N	Y	SC	VANET	NA	Certificate-less Authentication
[21]	2018	App	-	-	Y	P2P	-	Y	-	SC	5G Network	Scyther	Authentication protocol for a 5G user
[22]	2017	N/W	-	Y	-	P2P	N	N	Y	SC	Generic	NS3	Mutual authentication, three factor authentication
[23]	2017	N/W	KT	Y	-	P2P	N	Y	Y	SC	Generic	NA	Key management and Data integrity using AES based authentication
[24]	2017	App	KA	Y	-	P2P	Y	Y	N	AC	Generic	AVISPA	Lightweight Multi-factor Biometric authentication
[25]	2017	N/W	KA	Y	-	P2P	Y	Y	N	AC	WSN	AVISPA	Mutual authentication, biometic-hash based key agreement
[26]	2017	N/W	-	Y	-	P2P	N	N	Y	SC	WSN	NS2	Authentication scheme for multi gateway WSN
[27]	2017	N/W	-	Y	-	P2P	Y	N	Y	AC	Generic	C + +	Ultra weight RFID authentication protocol
[28]	2017	N/W	-	Y	N	P2P		Y	Y	AC	Medical	Cooja	Secured shared symmetric Key generated using Elliptic Curve Encryption SCheme
[29]	2017	App	KA	N	Y	P2P	-	Y	-	SC	Smarthome	Scyther	Secured shared symmetric Key between ISH and registred mobile user

Note: Y: Yes, N: No, N/W: Network, P2P: Point-to-Point, AC: Access Control, SC: Secure Communication, KA: Key Agreement, KT:Key Transport

III. Open Research Issues and Conclusion

Devising a secure and efficient authentication mechanism in IoT is more challenging due to its other facets such as heterogeneity in IoT devices, Scalability of the network, Interoperability amongst the devices. In addition, mobility of IoT devices would require a completely different strategy to deal with the requirement of authentication [7, 25, 26]. The context information of the mobile device, such as location, power status, active timestamps, and many more, could leverage the authentication mechanism. Nevertheless, the release of context information may be a threat to privacy. So, possibly a privacy-preserving context-based authentication mechanism is a help [5]. IoT enabled healthcare application very often require a distributed network access and cloud service. It would add value to healthcare service; However, authentication along with privacy is a significant challenge in this [4, 5, 28]. In a Vehicular ad-hoc network, or similar scenarios network may require more than one party communication at the same time. In that case, two-party authentication would be inefficient. There is a need for multi-party authentication and establishment of a conference key for a session. Many application in IoT are these days enabled with machine intelligence,i.e., IoT objects are acting autonomously. So, there is a need for device authentication before allowing them to access resources. Researchers are devising many device-centric security mechanisms where the device gets authenticated automatically. The advent of Quantum computer gave a boost to future computational capabilities. It may break all our standard security once it reaches to high bit processing capacity. There is a set of quantum secure algorithms that would still be secure. Basically, the security relies on the worst-case hardness of lattice-based NP-hard problems, such as Shortest Vector Problem, Shortest Independent Vector Problem, Shortest Integer Solution problem. Moreover, many exciting applications are also achievable using these lattice problems, such as Fully Homomorphic Encryption, Identity Based Encryption, Attribute-Based Encryption, Program Obfuscation, and many more.

Below are the weaknesses found in authentication mechanisms: 1. Many users logged in with same log-in identity problem and Stolen smart-card attack, 2. Node capture and node impersonation, 3. Bypassing Gateway, 4. Replay attack and forgery attack 5. Off-line password cracking attack.

This papers studied the authentication in IoT. It explained the preliminary of authentication, its challenges and layer-wise attacks on IoT systems. It explored the recent research on tackling authentication problem along with Its categorization. In the end, it discusses the current trend of various research issues and possible solutions related to authentication.

References

[1] *Protocols for Authentication and Key Establishment*. Springer-Verlag Berlin Heidelberg, 2012.

[2] Cas J. Cremers. The scyther tool: Verification, falsification, and analysis of security protocols. In *Proceedings of the 20th International Conference on Computer Aided Verification*, CAV '08, pages 414–418, Berlin, Heidelberg, 2008. Springer-Verlag.

[3] *Operational Semantics and Verification of Security Protocols*. Springer-Verlag Berlin Heidelberg, 2012.

[4] Ankur Gupta, Meenakshi Tripathi, Tabish Jamil Shaikh, and Aakar Sharma. A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks*, 149:29 – 42, 2019.

[5] Amel Arfaoui, Ali Kribeche, and Sidi-Mohammed Senouci. Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. *Computer Networks*, 159:23 – 36, 2019.

[6] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and Athanasios V. Vasilakos. Design of secure key management and user authentication scheme for fog computing services. *Future Generation Computer Systems*, 91:475 – 492, 2019.

[7] Samir Athmani, Azeddine Bilami, and Djallel Eddine Boubiche. Edak: An efficient dynamic authentication and key management mechanism for heterogeneous wsns. *Future Generation Computer Systems*, 92:789 – 799, 2019.

[8] Dariush Abbasinezhad-Mood, Morteza Nikooghadam, Sayyed Majid Mazinani, Abolfazl Babamohammadi, and Arezou Ostad-Sharif. More efficient key establishment protocol for smart grid communications: Design and experimental evaluation on arm-based hardware. *Ad Hoc Networks*, 89:119 – 131, 2019.

[9] Mohammed Alshahrani and Issa Traore. Secure mutual authentication and automated access control for iot smart home using cumulative keyed-hash chain. *Journal of Information Security and Applications*, 45:156 – 175, 2019.

[10] S. Shin and T. Kwon. Two-factor authenticated key agreement supporting unlinkability in 5g-integrated wireless sensor networks. *IEEE Access*, 6:11229–11241, 2018.

[11] Ming Tao, Kaoru Ota, Mianxiong Dong, and Zhuzhong Qian. Accessauth. *J. Parallel Distrib. Comput.*, 118(P1):107–117, August 2018.

[12] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo. Design of secure user authenticated key management protocol for generic iot networks. *IEEE Internet of Things Journal*, 5(1):269–282, Feb 2018.

[13] S.-K Choi, C.-H Yang, and J Kwak. System hardening and security monitoring for iot devices to mitigate iot security vulnerabilities and threats. *KSII Transactions on Internet and Information Systems*, 12:906–918, 02 2018.

[14] B. L. Parne, S. Gupta, and N. S. Chaudhari. Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network. *IEEE Access*, 6:3668–3684, 2018.

[15] Yi Tang Tong Li, Wenbin Chen and Hongyang Yan. A homomorphic network coding signature scheme for multiple sources and its application in iot. *Security and Communication Networks*, 2018.

[16] Bogdan-Cosmin Chifor, Ion Bica, Victor-Valeriu Patriciu, and Florin Pop. A security authorization scheme for

smart home internet of things devices. *Future Generation Computer Systems*, 86:740–749, 09 2018.

[17] Ruhul Amin, Neeraj Kumar, G.P. Biswas, R. Iqbal, and Victor Chang. A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment. *Future Gener. Comput. Syst.*, 78(P3):1005–1019, January 2018.

[18] Mohammad Nikravan, Ali Movaghar, and Mehdi Hosseinzadeh. A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks. *Wireless Personal Communications*, 99(2):1035–1059, 2018.

[19] O. Ruan, Y. Zhang, M. Zhang, J. Zhou, and L. Harn. After-the-fact leakage-resilient identity-based authenticated key exchange. *IEEE Systems Journal*, 12(2):2017–2026, June 2018.

[20] Pankoo Kim Sungbum Pan Haowen Tan, Dongmin Choi and Ilyong Chung. Secure certificateless authentication and road message dissemination protocol in vanets. *Wireless Communications and Mobile Computing*, (7978027):1–13, 2018.

[21] S. Sharma, S. Satapathy, S. Singh, A. K. Sahu, M. S. Obaidat, S. Saxena, and D. Puthal. Secure authentication protocol for 5g enabled iot network. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pages 621–626, Dec 2018.

[22] T. Qiu, X. Liu, M. Han, H. Ning, and D. O. Wu. A secure time synchronization protocol against fake timestamps for large-scale internet of things. *IEEE Internet of Things Journal*, 4(6):1879–1889, Dec 2017.

[23] Avijit Mathur, Thomas Newe, Walid Elgenaidi, Muzaffar Rao, Gerard Dooly, and Daniel Toal. A secure end-to-end iot solution. *Sensors and Actuators A: Physical*, 263:291 – 299, 2017.

[24] Parwinder Kaur Dhillon and Sheetal Kalra. A lightweight biometrics based remote user authentication scheme for iot services. *Journal of Information Security and Applications*, 34:255 – 270, 2017.

[25] Jangirala Srinivas, Sourav Mukhopadhyay, and Dheerendra Mishra. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. *Ad Hoc Netw.*, 54(C):147–169, January 2017.

[26] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, and Ashok Kumar Das. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment. *J. Netw. Comput. Appl.*, 89(C):72–85, July 2017.

[27] Masoumeh Safkhani and Nasour Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. *J. Supercomput.*, 73(8):3579–3585, August 2017.

[28] Zahid Mahmood, Huansheng Ning, Ata Ullah, and Xuanxia Yao. Secure authentication and prescription safety protocol for telecare health services using ubiquitous iot. *Applied Sciences*, 7(10), 2017.

[29] A. K. Sahu, S. Sharma, D. Puthal, A. Pandey, and R. Shit. Secure authentication protocol for iot architecture. In *2017 International Conference on Information Technology (ICIT)*, pages 220–224, Dec 2017.