Security framework for heterogeneous IoT application environment

Vinod Kumar Mahor*
Directorate of ICT, Research CenterImarat(RCI),
Hyderabad,Telangana, India

Santosh Satnami
Directorate of ICT, Research CenterImarat(RCI),
Hyderabad,Telangana, India,

Tilak Sarmah
Directorate of ICT, Research CenterImarat(RCI),
Hyderabad,Telangana, India,

Abstract: Internet of Things(IoT) enables the real-world objects to interconnect with the help of internet and exchange the data and commands. The adaptation space of IoT is rapidly increasing and spreading across number of fields like smart home, smart office, automobile, smart grid, surveillance, industry 4 0 etc [1, 2] The device deployment scenario and interaction path between user and device varies from application to application. In this paper, we have classified heterogeneous IoT applications based on the interaction path between user and devices. For each class, we have proposed the type and category of authentication required along with suitable cryptographic primitives to meet authentication requirements. We have classified the authentication and access control schemes proposed in literatures so far based on authentication factors, type and categories We also suggest the level for deploying the authentication rules and logics in heterogeneous IoT environment.

Keywords: Group Authentication, User authentication, IoT Security, IoT Application security, Device authentication, Message authentication

I. INTRODUCTION

Internet of Things connects the physicals world to the abstract information world and enables users to gather information from physical environment with the help of different IoT devices called Things and connectivity to internet. The user can also give commands to and execute actions on actuator type IoT devices. Usually the real-world data are acquired by the different type of sensors mounted on IoT devices and for warded to gateway which in turn sends it to the user or server or cloud or another IoT device based on architecture and deployment as depicted in Figure 1. The messages exchanged between IoT device anduser/server can be of type unicast, multicast or broadcast. Usually user or device sends message to another device in IoT environment. But in many cases the same messages needs to be sent to set of devices. But due to resource constrained network environment of IoT, forming a group of receiving devices and sending the message to that group proves more bandwidth efficient and energy saving than sending messages one by one to individual devices. This type of message communication is called multicasting [3]. As the application areas of IoT is increasing, the heterogeneity in device deployment and interaction path between user and device is increasing. This creates a challenge for designing a suitable and effective security solution. Communication environment of IoT is hostile and heterogeneous, and hence it is more vulnerable to various attacks like eavesdropping, replay, masquerading, message modification etc. which can result in jeopardizing of the complete function of system. Also, when the data collected by IoT devices are stored in the server or cloud may be sensitive and its access needs to be controlled only to its intended receivers and no one else. Different security mechanisms like user authentication, device authentication, message authentication, fine grained access control are adopted to provide security at different layers in IoT architecture [4]. point-to-point authentication using message authentication code(MAC) can be applied for unicast communications. But this mechanism does not suite therequirement of multicast communication as any of the group member possessing the shared key can forge the message and pretend as original sender and hence fails to provide source authentication. On the other hand, use of public key and signature based schemes provides source authentication but they have high computation and communication cost which makes it unsuitable for constrained environment.

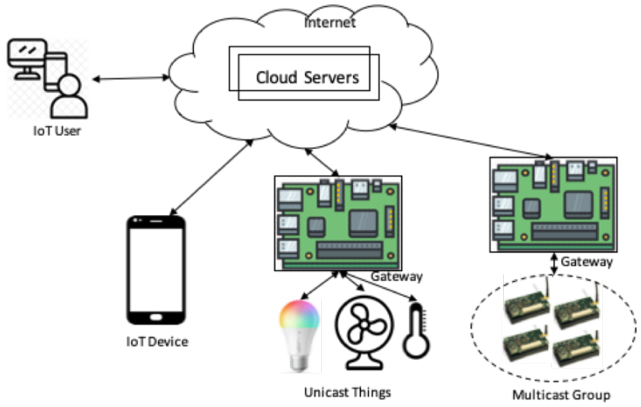


Figure 1: IoT connectivity scenarios.

The rest of the paper is organized as follows: Section II covers the survey of literatures relevant to our work. Section III briefly describes various terms used in the context of IoT security. In section IV we provide the taxonomy of different user and device authentication schemes in resource constrained IoT scenario. In section V, we define five classes for IoT applications and suggest authentication requirements along with suitable primitives. Section VI concludes our research article.

II. LITERATURE SURVEY

Several user and device authentication schemes for IoT have been published in literatures [5,6,7,8,9,10,11]. User authentication schemes provides authentication between user and IoT device or user and cloud server [5]. Other than communication between user and server/device, IoT also supports message exchange between two or more devices (i.e. Between sensors, actuators, gateway etc.) which requires device to device authentication. Apart from this, in sever al IoT applications, one message is multicast to set of devices. The authentication in this case is done using multicast authentication schemes. Multicast authentication schemes for resource constrained environments can be divided into three categories i.e. public key based, symmetric key based and one time signature based[12].

In[13], Luket.al. described seven important properties of multicast authentication 1. Resistance against node compromise, 2. Low computation overhead, 3. Low communication overhead, 4. Robustness to packet loss, 5. Immediate authentication, 6. Messages sent at irregular times, 7. High message entropy. Not all the schemes proposed for multicast authentication, meets all of these properties.

Public key based schemes are costly in terms of computationand communication and are not suitable for resource constrained devices. But now due toimprovement in the capabilities of IoT devices like smart phones, sensor nodes etc. and efficient implementation of public key cryptographic algorithms, has created new motivation for researchers to apply public key based schemes to resource limited applications [8, 9, 10] Most of the ID based authentication schemes requires computing bilinear maps which are very computation intensive and not good for resource constrained IoT devices. Yao et.al.[12] proposed very efficient public key based multicast authentication scheme based on Nyberg's accumulator. Computation overhead of fast one-way Nyberg's accumulator is verylow compared to signature based schemes (ECC or RSA). In many IoT applications, the nodes need to be clustered in to groups and the communications happens between members of the group. Authentication of nodes in the group is required to enable secure communication among them. So, sending individual authentication request from each device in the group will result in heavy traffic congestion and may also degrade performance of authentication server.Hence several group authentication schemes were proposed [14, 15, 16, 17]. These schemes utilized different underlying mathematical primitives like Paillier threshold cryptography, Lagrange interpolation formula, ECC etc. and have different pros and cons.

III. IOT SECURITY CONTEXT

Here, we have briefly described various security concepts used in context of IoT.

User authentication: When user tries to access data stored on the server by IoT deviceor try to execute command on some IoT device, the identity and genuinity of user verifiedbeforeallowinghisaccessintothesystem.

Device authentication: The IoT devices are usually deployed in unsecured environment where these devices can be physically captured, cloned and tempered by adversaries. Hence before allowing the new device to join the network and participate in communication, it is necessary to authenticate the genuinity of device.

Unicast authentication: In IoT system, when a message containing data or commandis exchanged between two devices or between a device and a user, it is called unicast communication. In this case, the authentication verifies genuinity of message source or integrity of the message.

Multicast authentication: Many times in IoT system, multiple nodes are grouped together to achieve common goal and one message is sent to set of nodes at the same time. Multicast authentication is adopted to secure the multicast messages exchanges between IoT devices and Gateway. It provides the authenticity of received data and it is known as multicast authentication.

Group Authentication: This one is totally different from traditional one-to-one or multicast authentication. It is applicable to the IoT application scenario where communication happens within a group of devices and there are multiple provers and verifiers within the group.

Fine grained access control: Once the user or device is successfully authenticated, the access to services, data or action needs to be controlled as per the user's access privileges. There are many ways to enforce the controlled access like Access Control List (ACL), Role Based Access Control (RBAC), Identity Based Access Control(IBAC) etc. But for data sensitive IoT applications, it is required to control the access of data, action or service at granular level which is called FGAC.

A. Security Primitives

We have considered following security primitives as part of proposed security framework. Several security schemes have been designed and published in literatures using these primitives to meet different aspects of security for IoT systems. Table 1 describes the applicability of authentication schemes designed using below mentioned primitives for user and device authentication in IoT.

Public Key Encryption (PKE): The security schemes designed based on PKE like RSA, ECC, Chaotic map and Elgamal are computationally intensive compared to symmetric key based schemes. Although lightweight PKE based authentication schemes have been proposed [5] which can be applied in IoT environment which is not extremely resource constrained.

Hash-XOR: Computing hash function is highly efficient compared to public key encryption and decryptions and computation time of XOR is almost negligible. So, security schemes designed using only cryptographic hash function and XOR operations are extremely efficient and suites IoT environment.

Threshold Cryptography: In multicast and group based communication, the message is protected by a key which can be recovered only when number if nodes (determined by threshold) having part of secret, collaborates. Secret sharing scheme, Nyberg one way accumulator and paillier threshold cryptography are the foundation for several multicast and group authentication schemes.

Physical Unclonable Function(PUF): Authenticating a device is key challenge if it's physical security is not ensured i.e. the device can be captured and cloned by adversary. In this case PUF helps to uniquely authenticate the device by generating unique digital fingerprint based on physical characteristics of the electronic chip.

IV. IOT AUTHENTICATION SCHEMES-TAXONOMY:

To provide security to the IoT systems deployed in different scenarios, various user and device authentication and access control schemes have been proposed in literatures [12,14,15,16,17]. Authors have classified authentication schemes proposed so far with respect to factors for user authentication, category for device authentication and underlying cryptographic primitives. The Figure 2 depicts the classification of IoT authentication schemes.

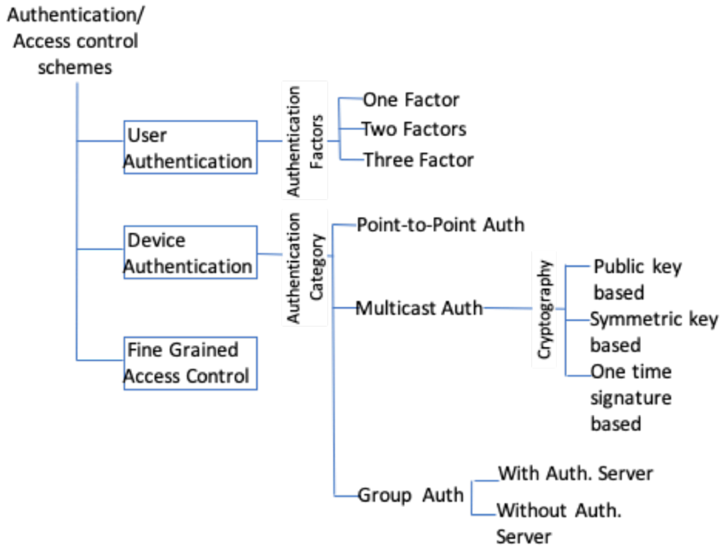


Figure 2: IoTAuthenticationandAccessControlSchemes-Taxonomy

V. CLASSIFICATION OF IOT APPLICATIONS:

The design of any IoT system depends on its intended application and operating environment. The range of IoT application varies from very simple to extremely complex. In simple application scenario, there are few sensor nodes collects some environmental data and sends it to the user by connecting to internet using wireless communication protocol. But in extremely complex application scenario, there can be thousands of sensing nodes with heterogeneous communication protocols and also involving edge and cloud servers. The complex IoT application may also include set of devices which are grouped to perform common function. In a group, the devices coordinate with each other and perform local processing of data before sending it to the server. Here, we classify the IoT applications based on the interaction path between user and IoT devices which is pictorially represented in figure-3. We have defined the five classes of internet connected IoT applications inwhich any IoT application with similar user-device interaction scenario can be categorized.

Presumptions:

- It is presumed that all the IoT devices connects to internet either directly or through Gateway node. The user also needs to connect to internet in order to interact with any IoT device and no direct access to IoT device is allowed to any user.
- It is also presumed that IoT device are resource constrained device in terms of compute, network bandwidth, storage and power [18] The Gateway node has better resources compared to IoT devices.
- User may use Desktop, Laptop or mobile device to access the IoT application.

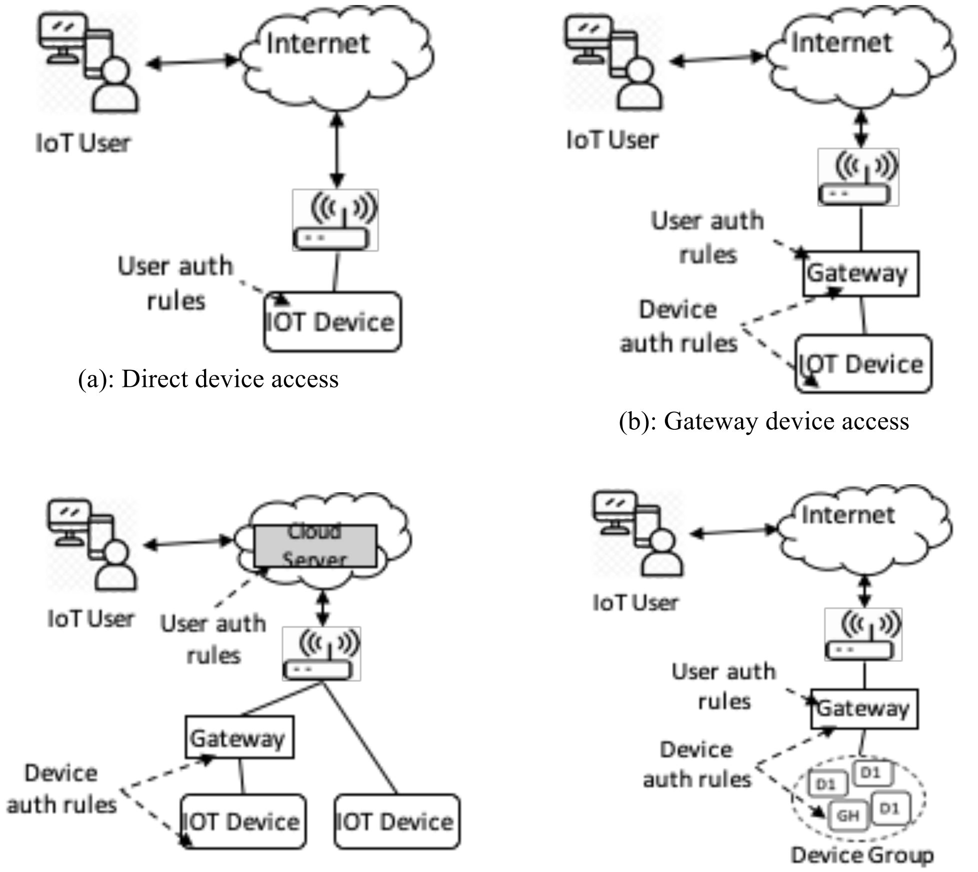
Class-1: Direct device access: In this class of IoT applications, the IoT device areconnected to internet with public identity like public IP or Through proxy and the user candirectly access the device to read data or to send command. In this case, any authentication or access control rules are implemented at device level itself.

Class-2: Gateway device access: In this case, the IoT things are connected to gateway node using local interface or short range protocols like BLE, NFC, LoRaPAN (IEEE 802.15.4) etc. The interactions of these devices with internet happens only through gateway node and user cannot have direct access to the device. Authentication and Access control rules are implemented at gateway node.

Class-3: Cloud device access: The IoT devices either directly or through gateway readsand writes their data to designated cloud server with the help of APIs. The user can neverhave direct access to any device and can only access relevant data from the cloud servers. Here, all the authentication and access control policies are implemented at cloud server. This is widely deployed class of IoT applications.

Class-4: Device group access: Many IoT applications requires to group similar IoT devices (devices doing similar activity for particular function) so that the devices can coordinate with each other or a command can be sent to group of devices simultaneously. Usually in this case, for every group there is one node designated as group head. The authentication can be handled by group head or by separate authentication server. So, in this class, the authentication and access control rules are implemented at group head or authentication server.

Class-5: Hybrid access: If any IoT application, requires the combination of any two or more of the above described class, it comes under hybrid class and the device access rule and access control policies will be implemented as per the original class under this hybrid.



(a): Direct device access

(b): Gateway device access

(c): Direct device access

(d): Device group access

Figure 3: Four classes of heterogeneous IoT applications

The Table 2 describes the type of authentication applicable to different classes. It also describes where and on which entity, the authentication and access control rules to be implemented with respect to all five classes.

Class	Auth entities	User Auth Rules on	Device Auth rules on	Suitablesecurityprimitives	
				User auth	Device auth
Class -1	User↔ Thing	Thing	Not Applicable	ECC[19], Hash-XOR[20], ChebyshevChaotic Map[7]	Not Applicable
Class -2	User↔Gateway, Gateway ↔Thing	Gateway	Gateway+ Thing	U2F[21], ECC[19], Hash-XOR[20]	PUF[22], Lattice[23], Lightweight PKE[5]
Class -3	User↔CS, CS↔Gateway	CS	Gateway+ Thing,CS+ Gateway	ECC[19], ChebyshevChaotic Map[7]	Lattice[23],LightweightPKE [5]
Class -4	User↔GH	GH	Thing↔GH, GH↔Auth Server	ECC[19], Hash-XOR[20], ChebyshevChaoticMap [7]	Multicast authentication: Public Key[8,9,10], Secret Sharing[24], Nyberg's Accumulator[12] GroupAuthentication: [14,15, 16,17,25]
Class -5	Combination of (Thing/ Gateway/ Cloud Server/ Group head)	Depends on Hybridization	Depends on Hybridization	ECC[19], Hash-XOR[20], Chebyshev Chaotic Map[7]	Depends on Hybridization

Table 2: Level of deploying authentication logic and suitable security primitives for different application classes

Notations: Following notations have been used to represent entities in the Table-1
GH: Group Head, *PUF*: Physical Unclonable Function, *CS*: Cloud Server, *PKE*: Public Key Encryption

VI. CONCLUSION

The applications of IoT is rapidly spreading in almost every aspect of life and many have been proven extremely fruitful. All of these applications may result in to disaster if no proper security has been implemented. This paper helps to classify any IoT applicationbased how the user interacts with IoT device or access the data. Based on this classification, the proper authentication and access control mechanism can be framed based on suitable security primitives.

REFERENCES

[1] S.Aheleroff, X.Xu, Y.Lu, M.Aristizabal, J.PabloVelásquez, B.Joa, and Y.Valencia,"Iot-enabled smart appliances under industry 4.0:Acase study,"*Advanced Engineering Informatics*, vol. 43,p. 101043,2020. [Online]. Available:https://www.sciencedirect.com/science/article/pii/S1474034620300124

[2] I.Lee and K.Lee,"The internet of things (iot): Applications, investments, and challenges for enterprises,"*Business Horizons*,vol.58,no.4,pp.431–440,2015.[Online].Available: https://www.sciencedirect.com/science/article/pii/S0007681315000373

[3] P.Porambage, A.Braeken, C.Schmitt, A.Gurtov, M.Ylianttila, and B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for iot applications, "*IEEE Access*,vol.3,pp.1503–1511,2015.

[4] D. Singh, P. Pal, M. Mishra, A. Lamba, and S. Swagatika, "Security issues in different layers of iot and their possible mitigation,"052020.

[5] N.Li, D.Liu, and S.Nepal,"Lightweight mutual authentication for iot and its applications, "*IEEE Transactions on Sustainable Computing*,vol.2,no.4,pp.359–370,2017.

[6] C.-I. Lee and H.-Y. Chien, "An elliptic curve cryptography-based rfid authentication securing e-health system, "*International Journal of Distributed Sensor Networks*, vol.11,no.12,p.642425,2015. [Online]. Available: https://doi.org/10.1155/2015/642425

[7] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things," *IEEE Internet of Things Journal*, vol. 5,no.4,pp.2884–2895,2018.

[8] D.Malan, M.Welsh, and M.Smith,"A public-key infrastructure for key distribution in tiny os based on elliptic curve cryptography,"in *2004 First Annual IEEE Communications Society Conferenceon Sensor and AdHoc Communications and Networks, 2004.IEEESECON2004.*,2004,pp.71–80.

[9] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks'," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4554–4564,2009.

[10] S. Yamakawa, Y. Cui, K. Kobara, and H. Imai, "Lightweight broadcast authentication protocols reconsidered," in *2009 IEEE Wireless Communications and Networking Conference*,2009,pp.1–6.

[11] M. T. Hammi,B. Hammi,P.Bellot,and A. Serhrouchni,"Bubbles of trust: A decentralized block chain-based authentication system for iot," *Computers & Security*,vol.78,pp.126–142,2018. [Online]. Available:https://www.sciencedirect.com/science/article/pii/S0167404818300890

[12] X.Yao, X.Han, X.Du,and X.Zhou,"A lightweight multicast authentication mechanism for small scale iot applications," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3693–3701,2013.

[13] M. Luk, A. Perrig, and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication,"in *Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks*. New York, NY, USA: Association for Computing Machinery,2006,p.147–156.[Online].Available:https://doi.org/10.1145/1180345.1180364

[14] N. Mehta, P. Jadhav, P. Lupane, P. Honrao, and P. Mahalle, "Group authentication using paillier threshold cryptography," in *2013 Tenth International Conference onWirelessandOpticalCommunicationsNetworks(WOCN)*,2013,pp.1–4.

[15] S.Li, I.Doh, and K.Chae,"A group authentication scheme based on lagrange interpolation polynomial," in *2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing(IMIS)*, 2016,pp.386–391.

[16] C. Wan, A. Hu, and J. Zhang, "An elliptic curve based message source authentication protocol for group communication," in *2010 International Conference on Electrical and Control Engineering*, 2010,pp.373–375.

[17] L.Harn, "Groupauthentication,"*IEEETrans.Comput.*,vol.62,no.9,p.1893–1898, Sep.2013.

[Online].Available:https://doi.org/10.1109/TC.2012.251

[18] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N. B. Carvalho, "Challenges in resource-constrained iot devices: Energy and communication as critical success factors for future iot deployment,"*Sensors*,vol.20,no.22,2020.

[19] B.Hammi, A.Fayad, R.Khatoun, S.Zeadally, and Y.Begriche, "A lightweight ecc-based authentication scheme for internet of things(iot),"*IEEE Systems Journal*,vol.14,no.3,pp.3440–3450,2020.

[20] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment,"*IEEE Journal of Biomedical and Health Informatics*, vol.22,no.4,pp.1310–1322,2018.

[21] H.Luo, C.Wang, H.Luo, F.Zhang,F.Lin, and G.Xu,"G2f: A secure user authentication for rapid smart home iot management," *IEEE Internet of Things Journal*,pp.1–1,2021.

[22] B.Kim, S.Yoon, Y.Kang, and D.Choi,"Puf based iot device authentication scheme,"in*2019 International Conference on Information and Communication Technology Convergence(ICTC)*,2019,pp.1460–1462.

[23] J.Hoffstein,J.Pipher,andJ.H.Silverman,"Ntru:Aring-basedpublickeycryptosystem," in *Algorithmic Number Theory*.Berlin, Heidelberg: Springer BerlinHeidelberg,1998,pp.267–288.

[24] O.Bamasag and K.Y.Toumi,"Efficient multicast authentication in internet of things,"in *2016 International Conference on Information and Communication TechnologyConvergence(ICTC)*,2016,pp.429–435.

[25] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold cryptography-based group authentication (tcga) scheme for the internet of things (iot)," in *2014 4th InternationalConference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems(VITAE)*, 2014,pp.