Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

A review for IOT authentication – Current research trends and open challenges

Mihir Mehta [a,*], Kajal Patel [b]

[a] Gujarat Technological University, India
[b] VGEC – Chandkheda, India

ARTICLE INFO

Article history:
Received 9 October 2020
Accepted 27 October 2020
Available online xxxx

Keywords:
IOT
Authentication
Authorization
Encryption
Spoofing attack
MITM attack

ABSTRACT

Internet of things is becoming the prime technology currently. By the utilization of IOT, different types of gadgets can interface, link and dialogue data without any interruption. IOT brings intelligence and automation in different areas like agriculture, transportation, industry, health and many more. The end point intention of the IOT operations is to extend opulence and productiveness of the stakeholders. IOT composition includes different sensors and other things which are associated with the web. As Web is open architecture, it lay out favourable ground to Intruders for performing different kinds of security threats. Security and Protection are the symbolic point of view for IOT system. IOT gadgets have limitation in terms of storage and also computational efficiency. So, existing traditional approaches can not be deployed directly into IOT Network. Confidentiality, Integrity and Authentication are pillars for IOT Security. Among them, Authentication service is prime nature because it validates identity of gadgets into the network. If Authentication approach is not secured enough than adversary can gain network control and also can launch various other kinds of attacks into the network. In this review article, a detailed analysis of the security related challenges specially related to Authentication and source of threats in IOT applications is discussed. A brief comparison of recent advancements in various domains of IOT Authentication security is also summarized with suggested enhancements. After doing critical review of existing algorithms; we have derived research gap which can provide opportunity for doing research work in IOT Authentication domain.

1. Introduction

The Internet of Things is a network consists of different kinds of Sensors, Actuators and other small gadgets. These gadgets are associated to the Web and exchange information without human mediation. Currently, there are many application areas for IOT. Some of them are Smart Home, Smart Agriculture; Smart city, Health-care and Manufacturing. For example IOT is very much useful in Health care sector for providing treatment into rural areas where there is a lack of infrastructure and also very much limited medical professional are available. IOT is also useful for monitoring patients continuously when they are at the home. Medical Professional if found some medical emergency based on observed parameters than immediate help is possible to the patient in critical situation. So, like this; IOT offers services into various sectors also. The components which make IOT are: Sensor, Aggregator, Transmission channel, Outer utility and Decision trigger. A sensor is an electronic service that examinations physical attributes. The function of aggregator is to oversee and amass the information. Transmission channel gives a uni-directional or bi-directional way through which data can fly. Outer service is gear or programming item which can be gotten from other third party stakeholders. Examples are different Cloud services or databases for storage purpose and so on. A decision trigger produces the last yield expected to satisfy the needs or explanations of the users. [1].

1.1. Composition of Internet of things

There are many point of mind for IOT Architecture especially for number of layers. However many of researches agree on three lay-

[*] Corresponding author.
E-mail address: mihir_mehta@gecg28.ac.in (M. Mehta).

https://doi.org/10.1016/j.matpr.2020.10.859
2214-7853/© 2020 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

Please cite this article as: M. Mehta and K. Patel, A review for IOT authentication – Current research trends and open challenges, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2020.10.859

ers IOT Architecture. They are: Perception layer, Network layer and Application layer [2].

Perception layer: It is first layer in IOT composition. The role of this layer is to collect and send data to the Network layer. It collects the data from sensors which are attached to the various IOT gadgets. There are various types of sensors which sense different physical properties. It also does some initial processing on collected data [2].

Network layer: It is the layer placed in between of three tiers in IOT composition. The role of this layer is to route and transmit the data received from Perception layer. Data may be passed by using Web as a media. Various protocols used at this layer are Bluetooth, Zigbee, Wi-fi [2].

Application layer: It displays applications to end stakeholders for specialized ambition. For example, Smart Home application, Smart City application. The application layer process the data received from Network layer and produces end result according to purpose of specific IOT application [2].

1.2. Security challenges for IOT

Unlock Composition: In IOT, all gadgets are associated to the Web and it is exposed structure. So it raises a risk for different cyber Threats [3].

System barriers: IOT gadgets have limited processing power, CPU, energy and computational resources. Because of these barriers existing traditional security methods can not be deployed in IOT architecture directly [3].

Lack of grades: Different IOT gadgets are fencing to grading. All IOT gadgets are a standalone skeleton consisting hardware, firmware and correspondence associate. It is a key to apply security at the plan stage, consists of secure code, and direct exhaustive examination in the time of the assembling process. However there is no sensible approach to institutionalize and actualize these different security methods on each gadget [3].

Inadequate trust and Coherence: Bundle of gadgets is connected to the web. So it is approximately not feasible to check that all gadgets have relevant protections arranged and is updated with the latest security spots. Only single endangered link in the network provides entry in other gadgets to adversary. So, to check the trust and data coherent from every IOT gadget is crucial [3].

Software Weakness: Large numbers of gadgets are linked with the web. So it is very much problematic to review that all gadgets have relevant defends set up and is updated with a new security spots. Only single weak link in the system permits access of all other gadgets to aggressor. So, to validate the trust and data credibility from every IOT gadget is exclusively necessary [3].

Unconfident Network Interfaces: Unconfident network interfaces to IOT gadgets can allow different attacks like brute force attack, password stolen attack. Example: adversary ready to sign in to application using various credentials supported brute force threat may get right of policy-making attributes and private data. Adversary also can change the passwords of lawful users [3].

1.3. Security threat model for IOT

IOT Applications can be categorized into following three layers. (1) Perception layer (2) Network layer (3) Application layer.

1.3.1. Security issues at sensor layer

Node Capture attack [4]**:** an IOT application contains few low energy knobs such as sensors and actuators. These knobs are susceptible to a spread of attacks by the attackers. The adversary may attempt to catch or supplant the genuine knobs within the IOT system with a malignant knob. This malignant may seem as in the context of the network yet it is constrained by the attacker.

Malicious code injection attack [4]**:** Attacker injects some malicious code in the memory of the knob. Regularly, in IOT gadgets software updates via air as interface. So it provides gateway to attacker to inject malicious code. Attackers can get access of complete IOT system because of this threat.

Side channel attacks [4]**:** The smaller scale structure of processors, electromagnetic transmission and their energy utilization uncover secret information to attackers. Side channel attacks may be supported by power consumption, timing attacks or electromagnetic attacks.

1.3.2. Security issues at network layer

Phishing site attack [4]**:** Adversary expect that at least few of the IOT gadgets from the network become victims of this attack. Main aim behind this attack is to theft credentials of legal users by directing them to phishing web pages. After acquiring credentials, attackers can get access of IOT network and can launch further attacks also.

Access attack [4]**:** In this kind of attack unauthorized person gets access of the network. Attacker continues to remain undetected within the network for long duration. The aim of this kind of attack is to theft valuable data instead of to cause damage to the network.

DOS/DDOS attacks [4]**:** In this type of attacks, the adversary jams the objective servers with an enormous number of undesirable fake requests. This keeps the objective server from ordinary-working, thereby disrupting services to legal users. If there are various sources used by the adversary to jam the objective server, then such kind of attack is called as DDOS or distributed denial of service attack.

Routing attacks [4]**:** Petty nodes try to redirect the data traffic and modifies routing path for data. Sinkhole attack is example of such routing attack in which an opponent broadcasts a man-made shortest routing path and attracts nodes to route traffic through that path.

1.3.3. Security issues at application layer

Data Theft attack [4]**:** IOT applications deals with a confidential and private data. The data in transit is at high risk for attack in comparison with the data which is in rest. The privacy of the user also can be compromised if data theft attack occurs in the network. Data Encryption, Authentication, Trust Management techniques can be applied for security against such attacks.

Sniffing attack [4]**:** The attackers may use various sniffing tools to monitor network traffic flow. Based on traffic monitoring, adversaries also can get some sensitive and confidential information about users and network. By using these information, further attacks on network is also possible.

1.4. Why Authentication?

Confidentiality, Integrity and Authentication are three pillars for IOT Security. Confidentiality provides protection when data transmits on the media by using Encryption. Integrity offers service of security against data modification by using message digest approach. However, Authentication validates the identity of entity distinctly in a system and based on that offers access to the permissible entity. If there is a proper authentication approach deployed in the network, it prevents from various security threats like Replay attack, Impersonation attack, Key stolen attack [5]. If we do not deploy authentication method perfectly into the system then private credentials like key value, password can be captured by adversary and it can further ruin to the system or user by launching other security threats by utilizing stolen information. Because of that, Authentication is the prime security attribute for IOT system. Based on authentication; different gadgets can exchange data with each and every one and also can receive the information with the trust in system. So, Authentication is the prior and first important step for setting up safe and reliable communication among various IOT gadgets/users in the system. Authentication is attractive and favoured approach now a day for providing entry into the gadgets in IOT System [6].

2. Literature review

2.1. Comparison of existing authentication approaches for IOT

Authentication is security service which provides verification of identity of gadget/user in the network. It is very much important security pillar as malicious gadgets/users which are not legal gadgets; can damage the network and various attacks can be possible in the network.

Any of authentication algorithms from Literature review can be one of the following types.

Identity based authentication [7–11]: In this kind of authentication algorithm, one party presents information to another party for authentication. This schema can utilize one or a blend of hash, symmetric or asymmetric cryptography algorithms. However, most of these schemas require secret key, password or smartcard.

Token based authentication [12]: Gadget/user identity is verified by identification badge provided by a server like OAuth2 protocol. OAuth2 is a token based authentication and authorization open standard.

Physical Unclonable Function [9–10]: IOT gadgets face a few challenges for example, low energy, lack of computational resources, low storage capability. This shortage of assets confines for usage of conventional cryptography techniques on IOT gadgets. PUFs offers secure authentication without storing any cryptographic assets on the gadget. PUF is a circuit which gets a series of bits (Challenge) as Input and creates a string of bit (Response) as output. PUF based authentication works on this Challenge-Response model. So, gadget can be authenticated and verified dependent on reaction of challenge, which is given as input by server.

Context based Authentication [13–14]: It is the reconciliation of data about the physical context of a gadget to enhance verification process, collected features can be sent to other gadgets .where these provided features are processed to make determinations about the gadget's location and origin time of the message. This information can improve the authentication process Figs. 1-4.

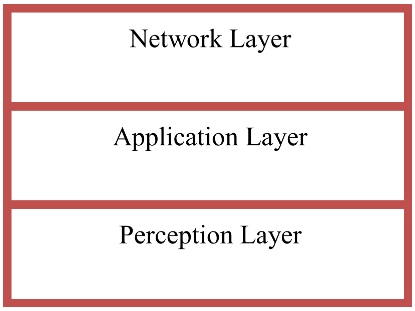

Fig. 2. IOT Architecture [2]

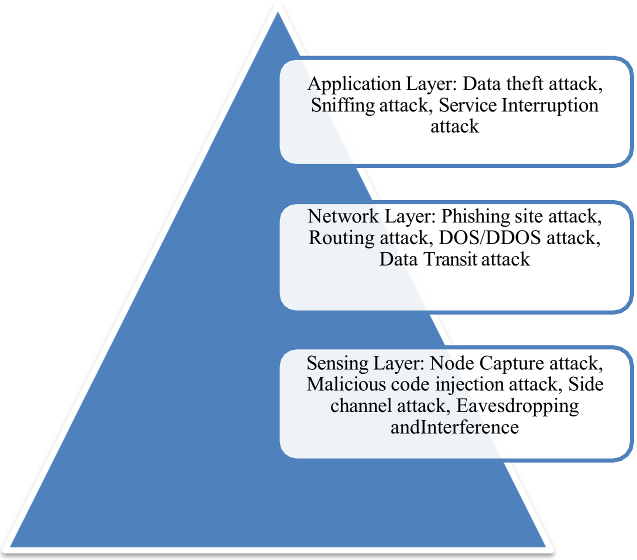
Application Layer: Data theft attack, Sniffing attack, Service Interruption attack
Network Layer: Phishing site attack, Routing attack, DOS/DDOS attack, Data Transit attack
Sensing Layer: Node Capture attack, Malicious code injection attack, Side channel attack, Eavesdropping andInterference

Fig. 3. IOT Threat Model [4]

Procedure based Authentication: This type of authentication generally includes One-way authentication or Two-way authentication (Mutually authentication). In One-way authentication, only one party will authenticate itself to another; while the other one will remains unauthenticated. In two-way authentication, both parties authenticate each other vice versa. So, it is also referred as Mutual authentication.

Identity based authentication approach is effortless and simple to execute. Credentials such as password, key value are stored into gadget memory for validating identity. So, it provides a way to Key stolen threat and Side channel threat. Token based authentication method provides prevention from threats such as key stolen attack.

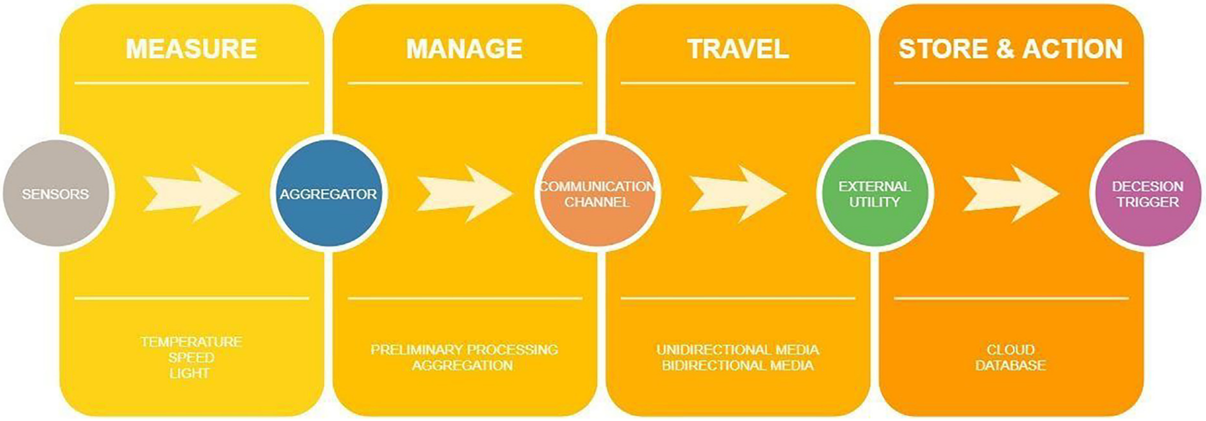

Fig. 1. IOT Components [1]

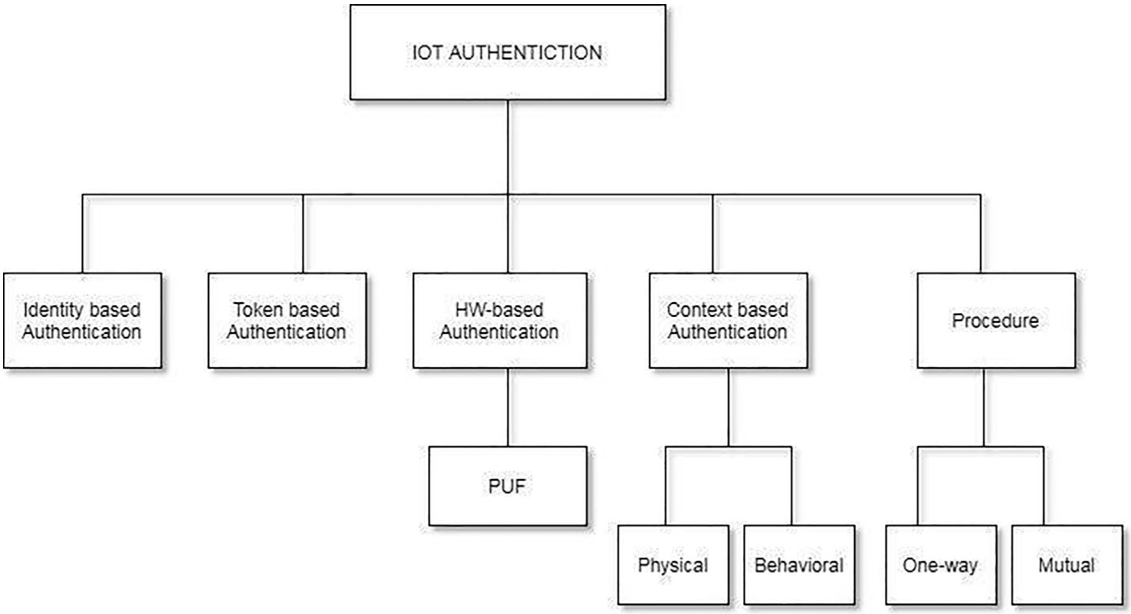
IOT AUTHENTICTION
Identity based Authentication
Token based Authentication
HW-based Authentication
Context based Authentication
Procedure
PUF
Physical
Behavioral
One-way
Mutual

Fig. 4. IOT Authentication approaches.

Because there is no requirement for storing any credential for validating identity of gadgets. Authentication is possible as a result of Access token. It is generated by AS- Authorization Server. But, this is yet susceptible to various threats like Token capturing and Replay threat. Recently, PUF is in fashion for achieving authentication for IOT gadgets. PUF does not require storing anything such as key value or password on gadget memory for checking authentication of entity. It is hardware based method for achieving authentication. It is depends on CRP- Challenge Response pair. We should apply Context based authentication with the integration of any discussed approach to enhance security in IOT system and to provide unambiguous way of identification for IOT gadgets Tables 1-3.

2.2. State of art

Network model named as Auth is suggested here for achieving authentication. Auth is locally consolidated and globally scattered approach [7]. Proposed Model caches the credentials of all joined gadget locally and also stores approaches for gadget access policy. PKI- Public Key Infrastructure [21] and digital certificate [21] based method is introduced here. Gadget authentication approach through transmission investigation is proposed for IOT [15]. Suggested method determines the type of the gadget and also the model of gadget by finding the matching of qualities derived from network traffic. Introduced method follows three steps. They are (1) Procurement of transmission Information (2) Derivation of transmission quality (3) Figuring out of Sameness by transmission quality. Secure User Authenticated Key Management Protocol (UAKMP) is proposed for clustered IOT system [8]. Suggested attributes for gaining authentication are password, individual biometrics and the client smart card. This method utilizes Cryptography message digest function in combination with Private Encryption/Decryption. UAKMP working is six steps. They are (1) Off line sensing knot admission (2) Admission of each entity (3) Entity sign in (4) Authentication and key understanding (5) Password change and biometric change (6) Newly added sensing knot placement [8].

Authentication method which depends on Physical layer attributes is suggested [13]. Physical layer authentication utilizes physical attributes such as Received signal quality (RSS) and Channel drive reaction (CIR). ML based perception is introduced here for achieving Physical Layer Authentication. Security approaches which are Token based are introduced with dynamic vitality security level trade off for IOT gadgets [12]. The point of view for vitality-quality scaling is introduced in the security domain, the aim behind that is that different piece of work and data require various levels of security. For authentication purpose, AS generates token and it is supplied to the client. So, in this approach there is no need to store resource owners' key value or password. Generated

Table 1
Authentication algorithm types comparison.

Identity-based Authentication	Tokenbased Authentication	Physical Unclonable Function based Authentication	Context based Authentication	Procedure based Authentication
Mutual unknown key, password	Apieceof data-Token	Hardware based approach, IC circuit mounted on chip based on challenge–Response pair.	Physical ambience or Behavioral ambience.	One-way Authentication or mutual authentication
Decisive Credential are stored at Internal memory of Device.	Token will be generated by AS for approaching resource.	No Cryptographic assets will be stored in memory. Challenge willbe hand over by server; device will compute response based on PUF and will provide it to server.	Ambience Information Like location, radio signal quality will be validated for authentication.	
KeyStolen attack, Password leakage attack, Side-channel attack, location spoofing attack is possible.	Replay attack, Man in the Middle attack, impersonate attack, DOS attack is possible.	Modelling attack, Man in the Middle attack is possible.	Modification attack, Interception attack is possible.	

Table 2
Literature Review Findings.

Sr. No.	Title	Main Idea/Contribution	Suggested Enhancement
1	Hokeun Kim et al. [7]	- PKI,Digital Certificate based authentication approach. - Auth(centrally database) storesthe information like credentials of registered Devices , access policies of its locally registered devices in its database.	- Security approach is based on centralized trust could leads to the issuesof a single point of Failure.
2	Hirofumi Noguchi, Misao Kataoka et al. [15]	- device identification strategy utilizes network information as common information that does not rely on the kind of devices and can be acquiring without any specific kind of Measurement equipment.	- Vulnerability assessment of a device can be done. - Constraint on communication can be applied for vulnerable devices.
3	MohammadWazid, Ashok Kumar Das et al.[8]	- User Authenticated key management protocol for H-IoT is suggested here. In suggested approach, IoT system can be categorized into different disunited clusters. - Cluster consists of CH, Sensing nodes and Gateway node. - Authenticationis achieved via Gateway node.	- Gate way node floods in required information in each deployed sensor knob' memory in advance for authentication purpose. - So, if node is compromised and stored details will be stolen than further attack is also possible.
4.	Ning Wang, Ting Jiang et al.[13]	- Physicallayer qualities of wireless media like Receive signal strength and channel impulse ratio parameters are utilized for authentication purpose.	- The link quality indicator (LQI) of the radio signal of the IoT device can also be considered as wireless fingerprints to check the current location of the IoT device.
5.	MuhammadNaveed Aman, Sachin Taneja et al [12]	- An essential stream in OAuth 2.0 can be depicted as: the customer passes an approval solicitation to the AS. The AS confirms the customer and dependent on result, sends an access token to the customer. the customer utilizes the given access token to confirm itself to the concerned asset server and customer can get to it. - The common point of vitality quality scaling is presented in the security space, in light of the examination that different assignmentsand information can require various degrees of security.	- If acknowledged token by AS is hijacked by any other device and then token used by the adversary for utilization of service than attack is also possible here. - Variable size PUF is suggested to use according to type of application. So how to categorize applications by iot device is a big question here.
6.	Prosanta Gope and Biplab Sikdar et al[9]	- lightweight and privacy- preserving two-factor authentication scheme for IoTdevices. - Two factors are (1) Secret shared key (2) PUF. - IOT Device sends request with device identity to the server. Server will generate Challenge and returns back to the IOT Device. IOT device will compute response for the given challenge and passes it back to the Server. Server will verify it, and bases on that generates session key.	- after one time authentication, if device becomes compromised, whole network security at higher risk and Physical attack, Key stolen attackwillalso becomes possible. Man in the Middle attackisalso possible in this suggestedPUF based authenticationby monitoring the communication between server and IOT device. Attacker will intercept and store exchanged CRPs. CRPs than can be used to perform Replay attack also.
7.	MuhammadNaveed Aman and Biplab Sikdaretal.[10]	- Two factor authentication(1) Device ID (2) PUF - Challenge – Response pair is used in PUF based approach after verifying device identity.	- -Intruder can intercept Challenge- Response between IOTdevice and Server andalso can store them. These CRPs' can be feed to the Machine learning algorithm and based on that other CRP also can be predicted.
8.	Yan Zhao, Shiming Li et al.[11]	- Authentication based on Password and Smart card	- -Proposed approach is vulnerable to Physical attack - –Side channel attack, Password leakage attackand Impersonation attack.
9.	Majid Alotaibi et al. [16]	- -biometric based user authentication and key agreement schema based on Symmetric cryptography. - based on User id and Password, Biometric password is generated for authentication purpose.	- -higher computational load and vulnerable to DOS and Password stolen attack.
10.	Zahoor Ahmed Alizai, NoquiaFateema Tarin et al.[14]	- multifactor authentication schema which is based on digital signature and device capability. - by the help of digital signature, both the device and server can authenticate each other.	- Proposed schema is required high computational load as for generating digitalsignature, asymmetric cryptography is involved. Device capability verification also requireslarger computational overhead and IOT devices are resource constrained. So, proposed schema is not suitablefor such devices. Also, it is vulnerable to Impersonation and DOS attack.

token explains the lifespan, overview and other access properties. In [9], lightweight & privacy-preserving multi authentication approach for resource embarrassed IOT gadgets has proposed by authors. Existing Identity based authentication method is susceptible to Physical attack and Side channel attack. So, for enhancing security of IOT, idea of two-factor authentication is discussed here. Proposed attributes are as follows (1) Secret shared key (2) PUF. In [10], authors outlined multi factor authentication method for IOT gadgets. IOT gadgets are easy target for launching Spoofing and Impersonation threat because of their minimum cost nature. So, for offering tight authentication authors have taken into point attributes PUF and gadget hardware fingerprints for authentication. In [11], authors described a secure and dynamic authentication method which is depends on Password and Smart card. Password based authentication method is susceptible for Password cracking attack. So, to offer tight security; Password based approach is together with smart card based approach. In [16], author proposed biometric based user authentication and key agreement method depending on Private cryptography. Author have explained multifactor authentication. Proposed approach is based on User id and password. Concept of biometric password is also introduced here. In [14], authors outlined a multifactor authentication approach which is based on attributes such as digital signature and gadget capability.

3. Research gap

Authentication provides the way for identification and distinguishing clients and gadgets in a network and conceding access to endorsed entity only. Authentication is approach to reduce too frequently occurring threats such as Replay attack, Impersonate attack Man in the middle attack, etc. The analysis of current Authentication methods derives the following conclusion:

Table 3
Attack Analysis from LR.

Sr. No.	Title	Layer	Key stolen attack/ Password leakage attack	Impersonation attack	Replay attack	DOSattack	Inter-ceptionattac k	MITMattack	Modeling attack	Spoofing attack	Physical attack- changing distance attack & same-device type attack
1	Hokeun Kim et al. [7]	A	0	0	0	1	1	0	N/A	0	0
2	MohammadWazid et al. [8]	A	0	1	1	0	0	0	0	0	0
3	Ning Wang etal. [13]	P	N/A	1	0	0	0	0	N/A	1	0
4	ProsantaGopeet al. [9]	A	1	1	0	0	0	0	1	0	0
5	Naveed Amanet al. [10]	A + P	1	1	0	0	0	0	0	1	0
6	Yan Zhao et al.[11]	A	0	1	1	0	0	0	N/A	0	0
7	Majid Alotaibiet al. [16]	A	0	1	1	0	0	1	N/A	0	0
8	NoquiaFateema Tarinet al. [14]	P	1	1	0	0	1	1	N/A	0	0
9	Sachin Tanejaet al. [12]	A	1	0	0	1	0	1	0	0	0

(a) Pinched verifier threat is feasible.
(b) Knob imprisonment attack is feasible.
(c) Replay attack and Denial of service is feasible.
(d) Snatched smart card threat and sensor knob spoofing threat is feasible.
(e) Physical threats like Location spoofing attack, changing distance attack is feasible.

In methods suggested from Literature; Gadget authentication for IOT system can be achieved by the help of Cryptography, Gadget characteristics, Gadget capability, Password & smart card. It has been no experimental work found which utilizes context data of a gadget such as geo-location data as one factor in multi factor authentication algorithms. Context data is prime attribute because if context data like location of a gadget will be modified by changing a gadget location from current location to remote location; it can lead to serious damage to machine functioning in industry application of IOT and also to humans' life. It also disobeys the fundamental concept behind authentication as fabrication threat will possible due to changing the gadget location. In IOT during authentication, there is a demand to validate the location of a gadget also together with gadget identity. So, this kind of designed authentication procedure also offers security against various types of physical attack if intruder generates false information by modifying gadget location. Also, currently there is a demand of designing authentication algorithm which also considers dynamic key generation according to session time for gadget conversation. Approach designed in this way also can provide security against key stolen attack very well. Confidentiality, Integrity and Authentication are significant elements for IOT Security. It has been no experimental work found which has considered at a same time on all these three security elements. This proposed way of multi-key based authentication; in which key will be generated dynamically according to session time for authentication can also be utilized for achieving confidentiality by encryption during data transmission. So, proposed approach can also provide protection against Interception attack, Replay attack.

(1) Most of the existing Authentication methods for IOT network use a single key based approach / password based approach to authenticate IOT gadget. From the literature survey we have analyzed that suggested types of the authentication are susceptible to the various threats like Key stolen attack, Side channel attack, MITM attack, Gadget cloning attack. If the password also not changed over the time, then also it is prone to Dictionary attack. And if the adversary has the shared key/password, an identical fake gadget also can be made. So, there is a need to work on authentication approach in which key value should be changed over the time. So, if adversary gets shared key than also he/she can not get access of the system and can not compromise with system security. We can provide security against MITM attack, Interception attack, Dictionary attack, Key stolen attack, Gadget cloning attack and Replay attack.
(2) IOT gadgets are kept in unlock and unrestricted places, which may reason them to be unsafe towards different Physical and cloning attack. So, it is significant that any security approach developed for IOT gadgets should not exclusively be best & proficient yet additionally can find any infringement of physical safety of IOT gadgets. In these kinds of screen play, a traditional identity based authentication approach, in which a pre-distributed confidential key is the one and only one factor for authentication, is not adequate for deriving solution for the security problems. This kind of authentication technique occasionally results in the ambiguous gadget identification in which gadget identity is only verified but the context information of gadget is not taking into consideration for authentication purpose. It may results to the numerous Physical attack, changing distance attack and location spoofing attack. So, for providing unambiguous identification of gadget and secure authentication of independent gadgets in an open and heterogeneous IOT system, novel and light weight technique is required. One kind of approach to solve such types of problem is to integrate information about the physical context of a gadget to enhance the authentication process.

4. Conclusion

In the universe of the IOT, plenty of gadgets are linked to the web. As we know that Web follows Open architecture. So, it provides a platform to an adversary for launching different kinds of security threats to the IOT system. Without proper security; applications of IOT can not be gain popularity and also they are not so much useful. So Security of IOT network is prime research direction currently. In this article; we have provided conceptual terminologies about IOT which consists of definition, architecture & challenges for security in IOT system. Then we outlined related research work which already has done by different research scholars in the field of IOT security. We have also made comparative study of some existing security methods. We have presented existing methods with their main idea and also we have suggested some suggestions for enhancement of IOT Security which can be done as future research directives. After presenting a comparative review of traditional authentication algorithms, we have identified a concrete research gap for efficient IOT gadget authentication on which there is a demand to work for enhancing security service for IOT.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Jeffry Voas, Bill Agresti "A Closer Look at the IOT "things" ", published by IEEE Computer Society, Vol. 20, Issue 30, Page No. 11-15, May2018.

[2] Vangelis Gazis Manuel Goertz Marco Huber Alessandro Leonardi . "IoT: Challenges, Projects, Architectures", presented at IEEE 18th International Conference on Intelligence in Next Generation Networks 2015.

[3] Sulabh Bhattarai and Yong Wang "End-to-End Trust and Security for Internet of Things Applications", published in IEEE Computer Society,2018

[4] Vikas Hassija, Vinay Chamolaet al. ,"A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", published in IEEE Access,2019

[5] Tarak Nandy, Norjihan Abdul Ghani and Sananda Bhattacharya," Review on Security of Internet of Things Authentication Mechanism", published in IEEE Access, Vol. 7, Page No. 151054- 151089,2019.

[6] Mardianabinti Mohamad Noor, Wan Haslina Hassan, "Current research on Internet of Things (IoT) security: A survey", published in ELSEVEIR Computer Networks, Page No. 283-294, 2019.

[7] HokeunKim and Edward A. Lee, "Authentication and Authorization for the Internet ofThings",published in IEEE Computer Society, 2017

[8] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, et al., Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks, published in IEEE Internet of Things Journal (2017).

[9] ProsantaGope, Biplab Sikdar, Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Gadgets, IEEE Internet Things J. (2018).

[10] Muhammad Naveed Aman, Mohamed Haroon Basheer, Biplab Sikdar, Two factor Authentication for IOT with Location Information, IEEE Internet Things J. (2018).

[11] Yan Zhao, Shimming Li, Liehui Jiang, "Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment", *WILEY Hindawai Security and Communication*, Networks (2018).

[12] Muhammad Naveed Aman, Sachin Taneja, et al., Token-Based Security for the Internet of Things With Dynamic Energy-Quality Trade-off, published in IEEE Internet of Things Journal (2018).

[13] Ning Wang, Ting Jiang, Shichaoly, et al., Physical-Layer Authentication Based on Extreme Learning Machine, published in IEEE Internet of Things Journal (2016).

[14] Zahoor Ahmed Alizai, Noquia Fatima Tareen, Iqura Jadoon, Improved IoT Gadget Authentication Scheme Using Gadget Capability and Digital Signatures, IEEE International Conference on Applied and Engineering Mathematics (2018).

[15] Hirofumi Noguchi, Misao Kataoka, and Yoji Yamato, "Gadget Identification Based on Communication Analysis for the Internet of Things", published in IEEE Access, Volume 7,2019.

[16] Majid Alotaibi, An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN, IEEE Access (2018).

Further Reading

[1] Jyoti Deogirikar and AmarsinhVidhate "Security Attacks in IoT: A Survey", presented at IEEE International conference on I-SMAC,2017

[2] Chang-le Zhong, Zhen Zhu and Ren-gen Huang "Study on the IOT Architecture and Access Technology", *presented at IEEE 16th International Symposium on Distributed Computing and Applications to Business*, Engineering and Science (2017).

[3] B.V. Santhosh Krishna, T. Gnanasekaran, A Systematic Study of Security Issuesin Internet-of-Things (IoT), presented at IEEE International conference on I-SMAC, 2017.