International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Applications, Attacks and Authentication Schemes for Future IoT

M. Savitha , M. Senthilkumar

Abstract: ***The internet has gently penetrated and completely mushroomed in to our entire life activities. Still we give the impression to be extremely unimaginable about real fact for the reason that we are overflowing with the need for internet. This evolution has ended up in the necessity of extensive technological advancement. One among them is the concept of Internet of Things (IoT). IoT is a framework of computing appliances that are interrelated with the purpose of exchanging data over the network. Internet of Things is a structure in which day by day gadgets have turned up shrewder which in turn makes it possible for the each day operations to be smart and communications to be instructive. Any significant influence in the progress of the Internet of Things is essentially the consequence of the deeds that work together for a superior outcome conducted in various domains like social science, electronics, informatics and telecommunications. Consequently, this broad range of applications of IoT causes enormous volume of data sharing which in turn distributes the confidential data pertaining to the users. Hence the need for authentication of IoT devices is of significance to defend against the security attacks. In this paper, a detailed survey of Internet of Things which offers a comprehensive focus on the theory, architecture, applications and related research is presented.***

Keywords: Internet of things, biometric, security, RFID, authentication, bio-inspired.

I. INTRODUCTION

A world deprived of internet is almost impractical to be imagined. The significance of internet in our daily life is analogous to oxygen for the world of technology. Being contented without internet is absolutely a tougher task for maximum of the people nowadays. Even the plainest happenings like entertainment and communication depend severely on the internet. Grounded on its definition, the internet is the technology that links various users and computers. But in the current scenario, internet merely does not connect the computers. It also connects the people, organisations, industries, culture, art and so many as depicted in Fig 1. Based on the requirements of the entities associated in the internet, it has varied applications. Thus the worth of internet in our existence matters. This evolution has ended up in the need for wide-range of technological progression. Internet of Things (IoT) is considered to be one of the vital aspects of this development.

Internet of Things denotes the stern connectivity existing amongst the physical and digital world [1].

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Mrs. M. Savitha*, Research Scholar , Department of Computer Science, Government Arts College, Udumalpet- 642 126, India.
Dr. M. Senthilkumar , Assistant Professor, Department of Computer Science, Government Arts and Science College, Avinashi- 641 654, India

Internet of Things is defined as the assembly of two aspects. Former element is the Internet which is termed as the networks of networks that could link billions of users through certain standard internet protocols [2].By means of various technologies; it connects enormous count of people, institutions, organisations, businesses and so on. The later element is the Thing, which fundamentally refers to the gadgets that get transformed to entities of intelligence [3]. The Internet of Things is an innovative model which is swiftly attaining concentration in the contemporary world of wireless telecommunications. The fundamental notion of this thought is the ubiquitous existence of a diversity objects like Radio-Frequency IDentification (RFID)tags, mobile phones, actuators, sensors, etc., that are capable of getting communicated with one another and also liaise with their neighbours with the intention of attaining collective objectives [4].

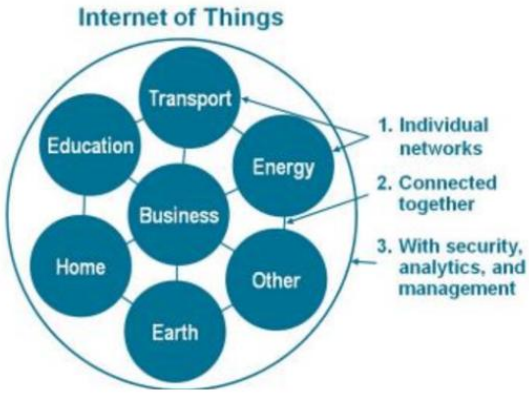

Fig 1. IoT regarded as network of networks [adapted from 10]

IoT signifies a ground-breaking evolution of the conceptualization of internet from a communication means from man-to-man into all-to-all framework [5]. Subsequently this growth and usage would produce colossal security hazards and challenges. It's a real challenge to secure Internet of Things (IoT) systems due to its manifold spots of vulnerability. In IoT, the recent outbreak of hackings and security breaches has revealed obvious vulnerabilities. More precisely authentication, privacy, information gathering and maintaining and access control are turning in to crucial processes to be operated and maintained [6]. Accordingly, IoT is a desirable and guaranteeing platform for the hackers to implement their unethical activities and progress their range of network expansion [7, 8]. Based on the application field, the necessities for security comprises of all the security needs such as authentication, confidentiality, availability, Integrity and so on [5].

Utilising the prevailing network organisation, the smart devices could be accessed and managed remotely that permits a direct incorporation with the physical world, the computing systems. This provision lessens further the human interaction,

And enhances precision and effectiveness too which give rise to the economic assistance. Thus, the smart devices in IoT facilitate the day-to-day life of people [12].The Authentication structure for the applications of IoT is illustrated in Fig. 2 in which various smart devices like actuators ND sensors are implemented. The smart devices are linked with the Internet by means of their adjacent gateway node (GWN). Different kind of end users like doctors and smart home users could have a direct access of the real-time data from certain IoT devices via the GWN for which authorization is provided to the users[11].

In the procedure of authentication of IoT devices, Bio-features act as the appropriate vital tool. In this approach of Biometric authentication, physical traits of the users like fingerprints, eyes, face or electrocardiogram and behavioural characteristics such as voice, signature etc., are employed as means of securely accessing a system, as an alternative for the PINs or passwords [9].

For IoT devices several authentication approaches grounded on bio-inspired features were proposed so far. These methodologies execute two categories of authentication functions in which either (1) the users are authenticated for the mobile devices to be accessed or (2) the users are authenticated for accessing remote servers by means of their mobile devices. The major difficulties that the biometric-based authentication schemes undergoing are (a) by what means an authentication system could be designed, which is exempted from susceptibilities that can be made use by the hackers and (b) in what way to assure that the biometric reference templates of the users are not negotiated by a hacker at the remote server level or device level.

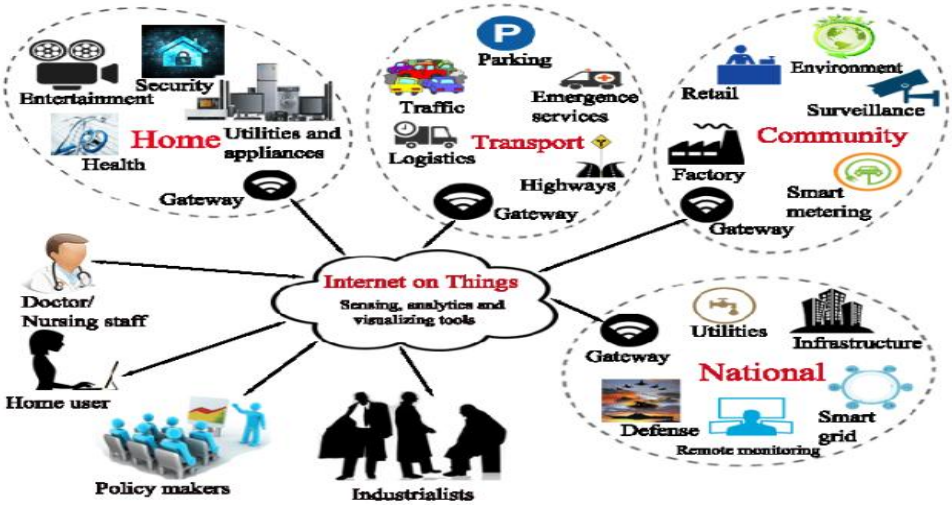

Fig 2. Authentication structure for the applications of IoT [adapted from 11]

Architecture of IOT

IoT architecture is the framework of plentiful components which includes sensors, protocols, actuators, cloud services, and layers.

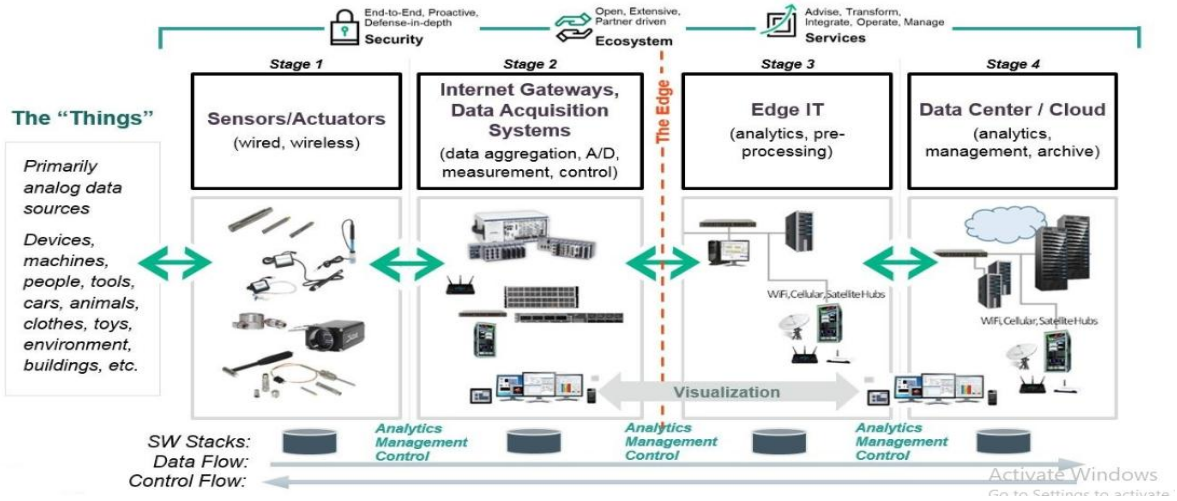

Fig 3.Architecture of IoT solutions [adapted from 13]

In the architecture of IoT, there exists four different phases. Principally, three IoT architecture layers exists as listed below:

1. The client side termed as IoT Device Layer
2. Operators on the server side which is called the IoT Getaway Layer
3. A pathway for connecting clients and operators called IoT Platform Layer

The architecture of IoT comprises of 4 Stages as mentioned below:

1. Sensors and actuators
2. Internet getaways and Data Acquisition Systems
3. Edge IT
4. Data centre and cloud

In stage 1, the purpose of sensors is to translate the information acquired in the external world into the form of data that is suitable for processing. Actuators are utilised to interfere the physical actuality, for instance adjusting of room temperature. In stage 2, the significant purpose is to deal with the massive volume of information gathered in the prior stage and compress it to the best format suitable for further assessment. Furthermore the needed transformation in terms of structure and timing occurs in this phase. In stage 3, the data that is organized is sent to the world of IT where the edge IT systems implement the improved analytics and pre-processing indicated as technologies of visualisation and machine learning. In Stage 4, the actual process occurs in the cloud or data center and thus the data from various different sources are involved for a comprehensive investigation.

IoT Applications

Out of the wide range of possible IoT applications, only a meagre volume is utilised in our society. As represented in Fig 4, the major domains of vital applications include:

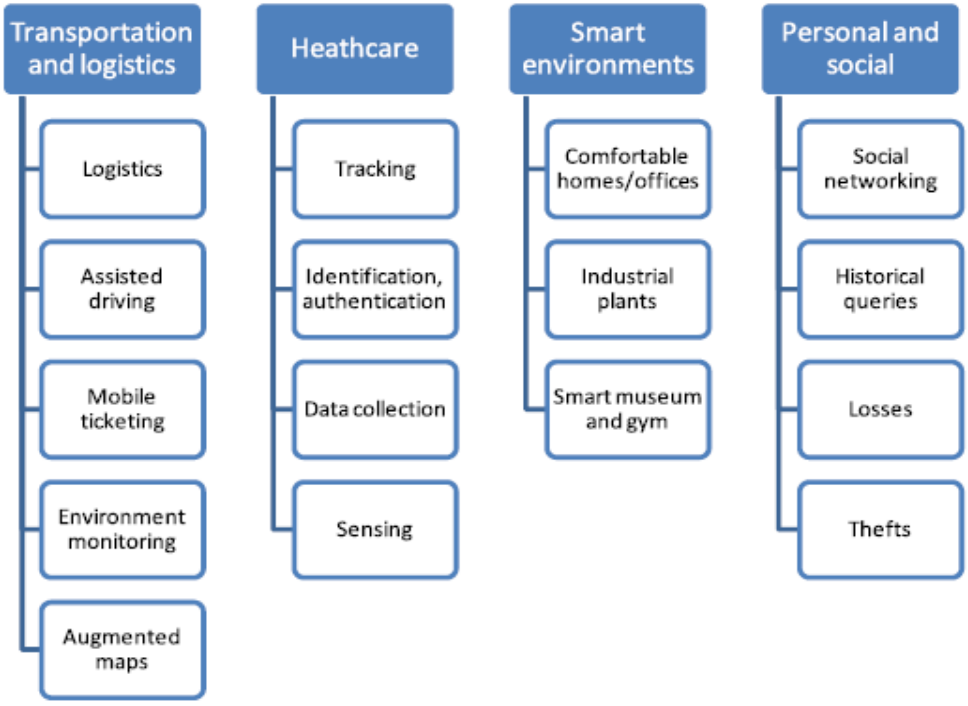

Fig 4. Areas of IoT applications [adapted from 1]

1. Transportation and Logistics
2. Healthcare
3. Smart environments
4. Personal and Social

In the field of transportation, most of the vehicles are emerging with associated sensors, processing power and actuators. Likewise in logistics, the goods transported and the roads are also furnished with sensors and tags to transmit vital information regarding various aspects to facilitate their movement. In the domain of healthcare, significant activities performed are identification and authentication of people, objects and people tracking and so on. In the smart environments, the usage of IoT makes things easier and life comfortable. In personal and social domain, support the users to communicate with others in an attempt to construct social relationships [1]. Thus the applications of IoT is realised in wide spectrum of life activities.

Security in IoT

IoT is rapidly developing among several commercial and industrial domains. With this growth, there is also a parallel upsurge in the number of devices that are interconnected and multiplicity of IoT applications. On the other hand, IoT methodologies are not still established enough and consequently there are huge volume challenges yet to be beaten up [21]. One among the highly crucial issues is the concept of security. Owing to the assortment of the appliances and multiplicity of communication protocols in the IoT framework, and also because of different services provided and a variety of interfaces, implementation of security aspects grounded on the conventional IT network solutions is not applicable [22].

There is enormous count of devices and massive number of sensors that are interconnected over network and the principal aspect is that their number is shooting up in a daily basis.

Secured and reliable connection is expected for all of those devices [23]. Majority of the internet linked devices are not furnished with effective security procedures and are susceptible to different security concerns such as privacy, trust and confidentiality.

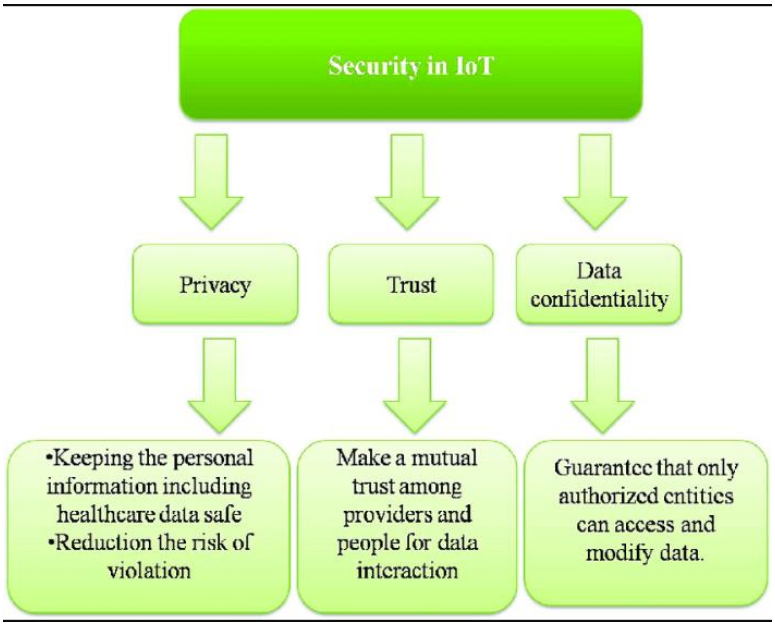

Fig 5. IoT Security features [24]

In IoT all the entities associated in the network offer facilities that are from anywhere at any time. In consequence, certain level of security measures are necessary for the network to be protected against the vulnerable acts. Since many of the organisations and industries are implementing IoT technologies, an ingenious IoT architecture including a full-fledged structure of security is expected. However, since the IoT devices are restrained in the usage of resources and intended to utilise less power together with the delivering of all the necessary functions, security is been considered as the least preferred attribute. But then as the IoT devices that are inadequately secured act as the gateway for the malicious attacks by permitting the intruders to access the resources, IoT security is unavoidable. Appliances such as gateways, transceivers etc., exploit the absence of encryption, feeble passwords and so on. It is absolutely a challenging task to devise a common solution for IoT security because of the broad range of explicit IoT operating systems custom configurations and versions of firmware. Moreover, bombarding variety of IoT devices and IoT applications also develops still more difficulties [21].

RFID, nanotechnology, embedded system technology, and sensor technology are the fundamental technologies holding IoT and hence the major challenge sprouts out from the assembly of IoT framework. The architecture of IoT is classified in to three different layers as sensing layer, transportation layer and application layer [25]. The security issues pertaining to each of these layers in IoT are listed out in Table1.

Table 1.Security challenges in IoT architectural layers

Layers of IoT	Challenges in Security
Sensing	Interception, Interruption, uniform coding for RFID, modification, conflict collision for RFID and so on.
Transport	WLAN application disputes, DOS/DDOS attacks, connectivity problems, forgery/middle attack, heterogeneous network attacks and so on.
Application	Integrity of Data, privacy, authentication, Information availability, middleware security etc.

IoT devices are subjected to security issues from different direction like software attacks, Physical attacks, cryptanalysis attacks and so on [26]. The concepts related to these attacks are discussed and listed out in Table 2.

Table 2.Security challenges in IoT devices

Challenges	Process of attack	Security needs	Cases
Software attacks	Utilize susceptibilities present in the system in the course of its own communication interface and malicious code is inserted.	Appropriate updating of antivirus	Trojan horse, worms
Physical attacks	Corrupt the hardware and other components.	Tamper resistance	Reconstruction of Layout
Cryptanalysis attacks	Breaching the encryption by acquiring the cipher text.	Secured encryption pattern	Known-plaintext attack
Environment attacks	By means of retrieving the encryption information, The encryption key of the device could be detected by the attacker	Secured encryption strategy	Side channel attack, Timing attack,
Man in the Middle	In case the data is not encrypted, an eavesdropper sense the transmitting network silently and may steal or modify the transmitted information	Encryption	Alteration and eavesdropping
Imitation	In spoofing, a malicious node imitate some other devices and initiate attacks in order to either distribute malware or steal data. Cloning duplicate the data	Identity based authentication protocols.	Cloning and Spoofing
DoS	Data packets are either modified or else resent again and again on network by the attacker.	cryptographic techniques and authenticity	UDP flooding
Fabrication	The authenticity of the information is moved. The attacker inject false data and which could damage the information authenticity	Data authenticity	SQL injection

II. RELATED RESEARCH

Majority of the disagreements and critique with regard to IoT are autonomy, privacy, security and control. Much of research work has been done by numerous researchers focusing these issues and quite attractive outcomes have been achieved and registered in literature.

The Internet of Things: A survey, presented byLuigi Atzori et. al.,[1] offers a survey on Internet of Things. In this paper various sights of the concepts of IoT model and the technologies that makes it possible are discussed in a completely elaborate manner. Various domains of the applications of IoT are also listed and explained with suitable instances. The issues that remain open to be solved are also listed which enables the researches for future work to be conducted in that route.

Flexible Certificate Revocation List for Efficient Authentication in *IoT* proposed by Li Duan et.al.,[14] discusses about the variance existing between RAM consumption and bandwidth which becomes a crucial issue for IoT in public key infrastructure (PKI) based authentication. To overcome this issue, two new CRL protocols of lightweight and with utmost agility which are grounded on generalized Merkle hash tree and Bloom filter were proposed in this research work.

Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks submitted by Mohammad Wazid et.al., [12] designed a novel secured three factor lightweight authentication approach for the remote users in HIoTNs termed as the User Authenticated Key Management Protocol (UAKMP).Password, personal biometrics and smart card are the three different traits applied in UAKMP. In this paper, the security aspect is assessed comprehensively in the Real-Or-Random (ROR) model and Automated Validation of Internet Security Protocols and Applications tool.

Multimodal Biometric Authentication In IoT: Single Camera Case Study offered by Nemanja Maček et.al.,[15], presented an alternative approach for multimodal biometrics. The authentication methodology which makes use of iris and face samples from superior quality camera is discussed in this paper. The effectiveness of the proposed technique is analysed experimentally employing CASIA databases. In spite of the benefit of lesser storage space, the downside of this approach is the retrieval of privacy concerns and iris biometrics on templates stored

Analysis of Authentication Techniques in Internet of Things (IoT) by Mohammed El-hajj et.al.,[5] presents a detailed analysis and sketched out the various authentication approaches proposed by several researchers. This paper also studies and compares the prevailing protocols for authentication and discusses about their corresponding merits and demerits

Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends by Mohamed Amine Ferrag et. Al.,[9] abridges the issues that obstructs the progress and implementation of biometrics models in huge measure which encompasses the physiological and behavioural aspects of human beings. This paper also presents various data mining and machine learning methods utilised by authorization and authentication methods meant for mobile IoT appliances.

(WIP) Authenticated Key Management Protocols for Internet of Things by Celia L et. al., [16] submits an interactive key management protocol and a non-interactive key management protocol in order to reduce the expenses of communication over IoT since efficient and secure key management for IoT authentication is the primary requirement for the operations to be handled in a secured manner Lightweight PUF-Based Authentication Protocol for IoT Devices by Yilmaz et.al., proposed a lightweight PUF-based authentication protocol. This protocol was executed on a wireless sensor network built employing Zolertia Zoul re-mote. Exploiting the configuration of server-client, the operations of the proposed approach was established. Employing DTLS handshake protocol and UDP, the usage of memory and utilisation of power were projected

DTLS based Security and Two-Way Authentication for the Internet of Things by T. Kothmayr et.al., [18] proposed for the Internet of Things, the fully operated two-way authentication security approach. The security scheme grounded on RSA algorithm. The approach is framed to function in the communication stacks which provide UDP/IPv6 networking for Low power Wireless Personal Area Networks

Secure Authentication Protocol for IoT Architecture by Sahu et.al., proposed a a smart home on the basis of IoT architecture in which the IoT smart Hub interact with the cloud together with the smart gadgets and home devices. Since there lies the higher chance for hacking and attacks being smart phone and cloud are involved, a a secure authentication protocol for assuring security is also proposed in this paper

A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Generation Computer Systems by Amin et.al., [20] developed Light Weight Authentication Protocol for IoT-enabled Devices in Distributed Cloud Computing Environment. The security challenges in Multiserver cloud environment are put forward by this work and designed a framework suitable distributed cloud environment and also an authentication protocol is proposed employing smartcard.

Table 3.Analysis of existing research work

Year	Authors	Ref No.	Methodology	Goal
2013	T. Kothmayr, C. Schmitt, W. Hu, M. Br, G. Carle	[18]	Grounded on RSA and operate on the framework of a system architecture and the scheme's feasibility	authentication security scheme for the Internet of Things constructed to operate on standard communication stacks that present UDP/IPv6 networking for Low power Wireless Personal Area Networks (6LoWPANs)
2015	Amin, R.; Biswas, G. P.	[30]	*BAN* logic for security validation and *AVISPA* security tool	mutual authentication and a secure session key agreement property
2016	Nemanja Maček et.al	[15]	Photometric and geometric methods like Gabor filtering and fiducial point localization to create biometric templates for identifying and authenticating the user	Multimodal biometric authentication using face and iris biometric traits
2017	Ahmed, M.E.; Kim, H.	[27]	SDN infrastructure that gather the statistical data regarding traffic flow maintained at every SDN-enabled switch	To identify the malicious packets on the given network path with higher precision rate by overcoming the drawbacks of ADSs which is based on sampling-based anomaly detection approaches
2017	Sahu, Amiya Kumar, Suraj Sharma, Deepak Puthal, Abhishek Pandey, and Rathin Shit	[19]	Secure authentication protocol connecting IoT smart Hub and smart phone which in turn linked with the cloud	Providing secured smart home based IoT architecture
2017	T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng	[29]	Symmetric encryption scheme using secret keys produced by chaotic systems for data transmissions in smart home systems	To assure authenticity and data integrity using energy-efficientcommunication protocol for SHSs
2017	Mohammad Wazid et.al	[12]	User authenticated key management protocol with smart card, password, and personal biometrics	Secure lightweight three-factor remote authentication scheme for HIoTNs
2017	Sravani Challa eta	[11]	Implemented with NS2 simulator and tested with Burrows-Abadi-Needham logic and automated validation of Internet security protocols	Signature-based authenticated key establishment scheme for IoT

2018	Aman, M.N., Basheer, M.H. and Sikdar, B	[28]	Physically unclonable functions and the features of wireless signal from an IoT device	Two-factor authentication protocol for protecting the IoT systems against spoofing and other types of attacks
2018	Amin, R., Kumar, N., Biswas, G.P., Iqbal, R. and Chang, V	[20]	BAN logic model and AVISPA tool with informal cryptanalysis in Distributed Cloud Computing Environment	authentication protocol employing smartcard
2018	Yilmaz, Yildiran, Steve R. Gunn, and Basel Halak	[17]	Physically unclonable functions implemented on a wireless sensor network created by utilising Zolertia Zoul re-mote substantiated in a server-client configuration	Secure authentication for IoT devices having limited resources
2018	Celia, L. and Cungang, Y	[16]	Interactive key management protocol and a non-interactive key management protocol	Reduce the communication cost of IoT by providing an authenticated channel through pairwise key generation and rekeying schemes for IoT devices
2018	Li Duan et.al	[14]	Lightweight CRL protocols on the basis of generalized Merkle hash tree and the Bloom filter	To provide a balance between bandwidth and RAM consumption together with security aspects in controlled IoT environment
2019	Sathyadevan, S., Vejesh, V., Doss, R., & Pan, L	[9]	Authentication provided in advance of offering access to the gateway services for the middleware servers or edge/sensor nodes by Port guard tool	Securing the services running in the gateway from external attackers

III. CONCLUSION

The ubiquitous nature of Internet has revealed that it has intertwined in all our day-to-day activities from communications that happens at a virtual level to social interactions. The emergence of Internet of Things has complemented internet by making the interactions possible amongst the humans and things which. At this point of discussion, it is vital to mention that IoT has to be well thought-out as the fundamental fragment of the prevailing world of internet. In the current scenario, heavy focus is paid by the researchers on the IoT authentication processes since universal need of IoT gives way for more options for authentication associated challenges and vulnerabilities which in turn keeps the possibilities of various types of attacks in a broader spectrum. Keeping all these issues in mind, this paper focuses on the complete analysis and survey of IoT and its related concepts. It also presents an elaborative analysis of the existing research work concentrating on authentication for Internet of Things including bio-inspired features

REFERENCES

1. L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/ j.comnet.2010.05.010
2. Somayya Madakam, R. Ramaswamy, SiddharthTripathi, Internet of Things (IoT): A Literature Review, Journal of Computer and Communications,2015, 3, 164-173
3. Shashank Agrawal, Dario Vieira, A survey onInternet of Thing, Abakós, Belo Horizonte,v. 1, n.2, p. 78 – 95, maio 2013 – ISSN:2316–9451.
4. D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.
5. Mohammed El-hajj et.al., Analysis of Authentication Techniques in Internet of Things (IoT),Conference Paper · October 2017 DOI: 10.1109/CSNET.2017.8242006
6. L. Kai Zhao, "A Survey on the Internet of Things Security," Computational Intelligence and Security, vol. 9, pp. 663 - 667, 2013.
7. Granjal, J., Monteiro, E., & Silva, J. S., " Security for the internet of things: a survey of existing protocols and open research issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.
8. Sathyadevan, S., Vejesh, V., Doss, R., & Pan, L., Portguard - an authentication tool for securing ports in an IoT gateway, in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) pp. 624-629., Kona, HI, USA, 2017.
9. Mohamed Amine Ferrag et. Al., Authentication and Authorization for Mobile IoT Devices UsingBiofeatures: Recent Advances and Future Trends, Hindawi, Security and Communication Networks, Volume 2019, Article ID 5452870, 20 pages
10. Dr Mahdi H. Miraz et.al.,A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT), Conference: 2015 Internet Technologies and Applications (ITA), September 2015, 10.1109/ITechA.2015.7317398
11. Sravani Challa etal., Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications, IEEE Access PP(99):1-1 · March 2017, 10.1109/ACCESS.2017.2676119
12. Mohammad Wazid et.al., Design of Secure User Authenticated Key Management Protocol for Generic IoTNetworks, IEEE INTERNET OF THINGS JOURNAL, Article · December 2017, DOI: 10.1109/JIOT.2017.2780232
13. JR Fuller, Practice Director, IoT, Wipro Limited The 4 stages of an IoT architecture, Internet article, May 26, 2016
14. Li Duan et.al.,Flexible Certificate Revocation List for Efficient Authentication in IoT, Proceedings of the 8th International Conference on the Internet of Things, p. 7. ACM, 2018.
15. Nemanja Maček et.al.,Multimodal Biometric Authentication In Iot: SingleCamera Case Study, The Eighth International Conference on Business Information Security(BISEC-2016), 15th October 2016, Belgrade, Serbia
16. Celia, L. and Cungang, Y., 2018, July. (WIP) Authenticated Key Management Protocols for Internet of Things. In 2018 IEEE International Congress on Internet of Things (ICIOT) (pp. 126-129). IEEE.
17. Yilmaz, Yildiran, Steve R. Gunn, and Basel Halak, Lightweight PUF-Based Authentication Protocol for IoT Devices, 2018 IEEE 3rd International Verification and Security Workshop (IVSW), pp. 38-43. IEEE, 2018
18. T. Kothmayr, C. Schmitt, W. Hu, M. Br, G. Carle, DTLS based Security and Two-Way Authentication for the Internet of Things, no. May, 2013.
19. Sahu, Amiya Kumar, Suraj Sharma, Deepak Puthal, Abhishek Pandey, and Rathin Shit. Secure Authentication Protocol for IoT Architecture, International Conference on Information Technology (ICIT), pp. 220-224. IEEE, 2017.

20. Amin, R., Kumar, N., Biswas, G.P., Iqbal, R. and Chang, V., 2018. A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Generation Computer Systems, 78, pp.1005-1019
21. Mikhail Gloukhovtsev, IoT Security: Challenges, Solutions & Future Prospects, Knowledge Sharing Article © 2018 Dell Inc. or its subsidiaries.
22. M.b. Mohamad Noor and W.H. Hassan / Current research on Internet of Things (IoT) security: A survey, Computer Networks 148 (2019) 283–294
23. Mirza Abdur Razzaq et.al., Security Issues in the Internet of Things (IoT): A Comprehensive Study, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017
24. Sabrina Sicari, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, Volume 76, 15 January 2015, Pages 146-164
25. Alma Oracevic et.al., Security in Internet of Things: A Survey, 978-1-5090-4260-9/17 ©2017 IEEE
26. K. Laeeq and J. A. Shamsi. A Study of Security Issues, Vulnerabilities, and Challenges in the Internet of Things. In Securing Cyber-Physical Systems. Taylor and Francis. Oct 2015.
27. Ahmed, M.E.; Kim, H. DDoS Attack Mitigation in Internet of Things Using Software Defined Networking. In Proceedings of the 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), San Francisco, CA, USA, 6–9 April 2017.
28. Aman, M.N., Basheer, M.H. and Sikdar, B., 2018. Two-Factor Authentication for IoTWith Location Information. IEEE Internet of Things Journal, 6(2), pp.3335-3351.
29. T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2707489
30. Amin, R.; Biswas, G. P. (2015): A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, vol. 36, pp. 58-80.

AUTHORS PROFILE

Savitha M is currently pursuing research in the Department of Computer Science, Government Arts College, Udumalpet, Tirupur, India. She received her B.Sc(Maths) from PKR ARTS College for Women, Gobichettipalayam, India and M.C.A from PSGR Krishnammal College for Women, Coimbatore,India. She obtained M.Phil., PKR ARTS College for Women, Gobichettipalayam, India . She has 1 International Journal and 5 Conference publications to her credit.She is currently focusing on IoT..

Senthilkumar Maruthamuthu is currently working as Assistant Professor in the Department of Computer Science, Government Arts and Science College, Avinashi, Tirupur, India. He received his B.Sc. from Bharathiar University, Coimbatore, India and M.C.A from Bharathidassan University, Tiruchirappalli, India. He obtained M.Phil., from Manonmaniam Sundaranar University, Tirunelveli, India. He completed Ph.D., in Anna University, Chennai, India. He has more than 21 years of teaching and research experience. He has 14 International Journal and 5 Conference publications to his credit. He is a Reviewer for reputed International Journals. His field of specialization is Wireless Communications. He is currently focusing on IoT, Big Data and Cloud Computing.