Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 5, Issue 2, 2019
ISSN: 2455 – 7528

User and Device Authentication in IOT: A review

Uttam Singh
M.Tech Scholar
Computer Science and Engineering
Suresh Gyan Vihar University, Jaipur
uttam.singh0903@gmail.com

Sohit Agarwal
Assistant Professor
Computer Science and Engineering
SGVU,Jaipur
Sohit.agarwal@mygyanvihar.com

***Abstract*—The aim of this paper is to analyze previous researches for user and device authentication in IOT and suggest future research directions.**

***Index Terms*— Internet of Things, Security, cryptography, Bio inspired algorithims , Device Authentication.**

I. INTRODUCTION

TThe realization of web4.0 is possible only because of Internet of Things(IOT). IOT is also referred as Machine to Machine communication. IOT is master technological network of all networks. The aim of IOT is to create cyber-physical systems by connecting devices, industrial or domestic to network. IOT enables the devices to perform more than their capabilities and hence converts them into smart devices. The connection of devices to the internet enables them to make intelligent decisions by mutual interaction with little or no human interaction. IOT will soon take us to a world where everyday appliances such as AC, TV ,door locks , coffee brewers can perform their task as soon as they sense us. The commercial capabilities of IOT has already been explored. Accenture for better performance, security and consultancy. Rolls Royce, a British manufacturing firm uses IOT based sensors in their jet engines for continuous diagnosis to prevent catastrophic failure[2]. International Data Cooperation (IDC) published a report in 2013 stated that the number of connected devices or IOT devices are expected to reach 41 billion by 2020 with a predicted market share of $8.9 trillion dollars [3].

The world is advancing towards the master network of all networks, which is Internet of Things (IOT). It is called master network as it will have ability of connecting computers with everyday objects such as home appliance, vehicles etc. Such objects are defined as Smart Objects. Smart objects are capable of not only sensing objects around them but also interacting with them, to make collaborative decisions without human aid. These smart objects will have the ability to create independent social networks with other devices to track them with a unique digital identity [4]. For past years the research community has remained highly interested in the concept of Internet of Things. It has received much attention from both industrial and academic organizations. Security and privacy issues are the important research targets [5].Advanced security services like applied cryptography and trusted computing have not grown considerably as compared to usage of smart devices in every day applications. Economic aspects of device such as cost, market etc. along with restricted computing power are main restrictions towards achieving robust security solutions [6]. The privacy of the enormous number of objects is the major challenge which should be resolved for global acceptance of ubiquitous computing [7]. The end goal of Security is required with the end goal to effectively execute the productively algorithmic plans and conventions, in different gadgets, and in an incredible number of utilizations. In various cases, it isn't conceivable to receive IoT benefits at large scales. The convenience of IoT advances must be kept as high as could reasonably be expected. Toward this path, connected techniques must be produced, with the end goal to help heterogeneity and versatility, to keep clients obscurity and to deal with individual information security. Other than the convenience of the two applications and administrations, that IoT underpins, the test of security is likewise an incredible standard for trust, as one of the best needs for the clients is to have a high level of trust, while utilizing web based business, exchanges, discourse, content and some other method for correspondence in their ordinary "advanced life", Despite the fact that the expanded network of elective gadgets has expanded significantly the development of security and protection vulnerabilities. Digital assaults are recorded consistently, essentially because of the inadequately anchored applications, administrations, and gadgets [8]. Client end points are demonstrated likewise feeble and weak in terms of security.

As a matter of fact, the current security conventions are intended for utilization in daily chores and their usefulness depends upon noteworthy computing power, great memory assets, and power accessibility. Since the efficacy of these cryptographic models and security schemes are somewhat hazy, thorough and detailed investigation is required, with the end goal to be guaranteed, that they can be executed in the predefined assets of IoT [9] especially for the situation, of limited capacities of hand-held and convenient gadgets [10].

Likewise, other security administrations, for example, key administration, are growing up.
Also, the arrangement of another layer of security may produce an extra manufacturing or development cost and, contingent upon requirements of the ecological assets, but such expenses can't be permitted [11]. The transmitted information can be target of assaults and spy if proper security measures are not adopted. For example ensuring information secrecy and privacy in EMS situation is vital for empowering a solid comprehension of a patient's present life state Providing arrangements ready to relieve the security issues found in IoT middleware models is an essential assignment [12].Comprehending the challenges of communication enforced by Internet of things is highly imperative, While designing security frameworks so that they can operate in versatile systems. Essentially, challenges are identified with execution (i.e., reaction time), overhead, latency and packet loss.

eliminating the dedicated resources for utilizing cloud services such as channel establishment and simultaneously increasing placement of intelligent resources at the end of network or the cloud edge[12]. The obvious advantage of fog computing is close availability of computing and storage resources to nodes. Furthermore fog computing architecture takes cumulative input from near organizations or end users and edge devices. The cumulative effort may be incurred in various forms such as management, configuration, communication and control. Edge computing technology is the extension of the cloud concept to the network edge [13,15,16]. The differentiating factor between cloud computing and fog computing is overdependence of cloud services on high internet bandwidth and geographically large scale organizational system. Fog services are much closer to the end-users, with dense geographical distribution, and much better support for mobility [14,17,18,].

The aim of this research paper is to analyze previous researches in this domain and suggest possible research directions.

II. Literature Survey

Abdul Malik Ansari and Dr. Muzzammil Hussain, "Middleware Based Node Authentication Framework For Iot Networks",. IEEE ICIRCA 2018. In this paper, a light weight secure framework is proposed [19]. In this paper, a light weight secure framework for authentication, identity management, and a flexible trust management for secure and compatible communication channel among IoT devices is proposed. Various parameters like number of packets, average memory storage, number of nodes, and authentication are used to implement proposed technique. To evaluate and compare the results parameters like throughput, delay, bit error rate, and storage consumption are used. Results based on comparison demonstrate that the proposed technique works efficiently.

Chandrashekhar Guntuku and Syam Kumar Pasupuleti , "Secure Authentication Scheme for Internet of Things in Cloud",IEEE,2018 [20]. In the proposed scheme, authors use Chebyshev chaotic maps for authentication and elliptic curve cryptography for confidentiality and integrity. The authentication between the devices and cloud is achieved by using chebyshev polynomials and random numbers. The confidentiality and integrity of data during transmission can be achieved by Elliptical curve cryptography based encryption and hash functions. Through, security and performance analysis, the security and efficiency of proposed scheme is proved.

Muhammad Arif Mughal, Xiong Luo1, Zahid Mahmood and Ata Ullah, "Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things",IEEE International Conference on Smart Internet of Things,2018 [21]. This paper presents a PUF based Authentication Scheme (PAS) along session keying in order to ensure the secure interaction among smart devices in IoT. The authors also proposed the registration and authentication mechanism along with session keying based on challenge response pair. The secure command execution protocol among requesting devices, gateway and smart devices is also presented.

Yuesong Lin, Fuqiang Jiang, Zhu Wang and Zhuping Wang, "Research on PUF-based Security Enhancement of Narrow-Band Internet of Things", IEEE International Conference on Advanced Information Networking and Applications,2018 [22]. In this paper a summery analysis of the security risks in the NB-IoT network is given followed by chip binding and anti-counterfeiting technique by having the PUF integrated in the chip of the NB-IoT user equipment. Considering the low power requirement of NB-IoT, a secure communication protocol based on PUF is designed. Comparing with the PKI mechanism, the protocol simplifies the distribution of secret keys and certificates. Comparing with the TLS protocol, the proposed protocol simplifies the key agreement process and can still keep the high security level.

Linning Peng, Aiqun Hu, Junqing Zhang, Yu Jiang, Jiabao Yu, and Yan Yan, "Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme",, IEEE Internet of Things Journal,2018 [23]. In this paper, a lightweight PUF-based authentication protocol is proposed and implemented on a wireless sensor network constructed using the resource-limited IoT devices. The functionality of the proposed scheme was tested using a server-client configuration. Power consumption and memory utilisation of the proposed protocol were estimated and compared with the existing solutions, namely: DTLS (datagram transport layer security) handshake protocol and UDP (user datagram protocol).

Linning Peng, Aiqun Hu, Junqing Zhang, Yu Jiang, Jiabao Yu, and Yan Yan, "Design of a Hybrid RF Fingerprint

Extraction and Device Classification Scheme",, IEEE Internet of Things Journal,2018 [24]. This paper proposed a half breed grouping strategy by incorporating novel RF unique finger impression includes in a keen way and did broad investigations to assess the presentation. Four epic balance based highlights, specifically DCTF, recurrence balance, tweak counterbalance and I/Q balance include from CTF, were embraced and found successful in

Arsalan Mohsen Nia and Niraj K. [16] The paper expounds background of IOT and summarizes enabling technologies concerning security requirements of IOT system. The paper also establishes research challenges in security in IOT by analysing and comparing past researches and proffers directions for future research. In other words the paper demonstrates the need of defining principles and regulatory framework for establishing necessary high level security in IOT.

M. Radovan, B.Golub[18]The paper analyses trends in IOT technologies, in other words the paper analyses past, present and future of IOT technologies. The paper points Big Data as current trend in IOT, which is evident as today internet as approximately 8ZB published data. The paper also discusses impact of IOT in Industrial security and summarizes traditional and current changes in SCADA system. The paper also brings out the need of developing simpler and standard protocols for security issues in IOT system.

EdmundoMonteiro, Jorge Granjal and Jorge Sá Silva [19] The paper provides an extensive analysis of the available security protocols for protecting IOT communication and points out the future research challenges. The survey concludes that IP based technologies are essential for universally accepted applications for IOT.

Ankush B. Pawar and Dr.ShashikantGhumbre[20]It gives detailed analysis of IOT services and applications in medical field. According to the paper these applications can be divided into two categories, the single condition applications(applications used for monitoring a particular disease such as blood pressure, Glucose monitoring, ECG) and clustered condition applications(applications developed for managing multiple diseases for instance wheel chair management, rehabilitation system).In the later sections the paper discusses various security challenges associated with medical applications of IOT like access control privacy, trust, authentication policy enforcement and confidentiality and also discusses expediency of various cryptographic(AES,DES,RSA) and anonymization techniques . The survey concludes that RSA algorithm is an asymmetric algorithm or in other words it uses different keys for encryption and decryption thus, it provides superior protection against multiple attacks maintains data with more security.

Nisarg M. Vasavada, SwapnilBelhe, [22]The paper proposes a novel approach for power efficient IOT applications controlled by speech. The Automatic Speaker Recognition system is based on "Modified Vector Algorithm for Speaker Identification (MVA-SI)" .The MVA-SI precisely analyses the phones in the input speech and gives the input speech vectors significant Eigen values. Phones refer to consonants starting and vowels ending. Thus these are highly different from each other. The proposed system outperforms the traditional ASR system both in terms of Power efficiency and authenticity.

Q. Jing J. Lu D. Qiu, [23]The objective of this paper to deal with the security issues of Internet of things amidst all other challenges. IOT consist of three layers i.e. perception layer, transportation layer and application layer. The security concern related to every layer and the consequent solutions are discussed in this paper.WSN and RFID technology are used for perception layer with solutions that includes RFID Privacy Protection, Trust Management, Uniform Coding, and Conflict Collision for RFID. Trust Management of Nodes, Cryptographic Algorithms in WSNs, Secure Routing Protocols for WSNs, Key Management in WSNs are the technical solutions in WSN. The integration of RFID and WSNs i.e. RSN is also analysed after RFID and WSNs.

Matthew A. Crossman and Hong Liu[24]In this paper, the author has rooted superior, appropriate and user centric device authentication system for cloud services. The proposed method used is Near Field Communication (NFC) which allows Smartphone as authentication badge. The user needs to tap their phone close to NFC reader to achieve access rights. To ensure security of the key stored, additional techniques are used that includes application sandboxing and android key store system.

Once the authenticity and validity of the received fingerprint is confirmed, server authenticates the object. Physical state, transmitted state and location are the features used to define a unique fingerprint. Transfer learning is used to detect shared changes in fingerprints which can help to differentiate among usual changes and security attacks. The proposed method is unique and efficient as it has less computational requirements and because of stringer security framework for IOT environment.

Phillip H. Griffin[26]In this paper, biometric-based cryptographic techniques are explained to provide mutual, strong, multifactor identification and confidential communication in IOT. It provides security techniques that supports the aim of universal access i.e. users can authenticate their identities by selecting multiple choice options. With the help of BAKE (Biometric Authentication Key Exchange) protocol user credential are secured opposite Man-in-the-middle and phishing attacks. To ensure confidentiality, lightweight cryptographic algorithms are used which are appropriate to implement in resource constraint environment i.e. IOT for efficient execution. Thus, biometric based access control and BAKE can be used to maintain the security risk of malicious users in IOT. classifying ZigBee nodes. A smart hybrid classifier was designed to adaptively integrating features with the weights tuned to the channel conditions.

III. Result and Conclusion

From the extensive literature survey it can be concluded that security mostly in terms of user authentication has remained primary research domain. However the provided solutions cannot satisfy the constrained resources and power consumptions of IOT devices.

Physically Unclonable Functions (PUFs) have turned into an inexorably mainstream innovation for structure secure verification in these frameworks. PUF abuses the arbitrary elements of IC assembling procedure to create an assortment of crisscrosses. It creates diverse one of a kind test reaction sets to store in archive and after that utilization for secure relationship between the shrewd gadgets in IoT. Memory based and Analog electronic based PUFs are for the most part utilized for giving trustworthy security where MOS transistors based PUF accomplish a huge assortment of jumbles with littler sizes when contrasted with others.

PUF gadgets still have various remarkable unwavering quality and security issues which should be tended to before they can be received. One of the significant dependability issues is brought about by the maturing of CMOS transistors. This alludes to the slow debasement of incorporated circuits which can cause lasting changes in the electrical parameters of the CMOS gadgets (for example the limit voltage).Thus further research is expected to create lightweight ,uncloneable and stable gadget marks and same is point of our undertaking.

Conclusion

The device authentication scheme developed is deployed in real time and is both lightweight and robust. Another advantage of using the proposed approach is that the device signature is dynamic so frequency analysis attack is not possible in the node. The node is also protected from Middle Man attack. Thus the proposed scheme is ideal for device authentication in fog computing environment.

IV. Future Scope

In future the author plans to implement a device authentication scheme based on human immune system.

References

[1] M. Saadeh, A. Sleit, M. Qatawneh and W. Almobaideen, “Authentication Techniques for the Internet-of-Things: A Survey”, *DOI 10.1109/CCC.2016.22, IEEE Internet of Things Journal.*

[2]*https://www.rtinsights.com/rolls-royce-jet-engine-maintenance-iot.*

[3] IoT Analytics, “Why the internet of things is called internet of things: Definition, history, disambiguation,” https://iot-analytics.com/internetof-things-definition/, 2014.

[4] S. Agrawal and M.L. Das,” Internet of Things – A Paradigm Shift of Future Internet Applications”, 978-1-4577-2168-7,2011 IEEE.

[5] N. Sklavos and I. D. Zaharakis, “Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations”,978-1-5090-2914-3/16, 2016 IEEE.

[6] N. Sklavos, P. Souras, “Economic Models and Approaches in Information Security for Computer Networks”, International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January, pp. 14-20, 2006.

[7] “ITU Internet Reports 2005:The Internet of Things”. http://www.itu.int/osg/spu/publications/internetofthings/. (as on 19 Sep 2011)

[8] M. Katsaiti, A. Rigas, I. Tzemos, N. Sklavos, “Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion”, proceedings of the International Conference on Modern Circuits and Systems Technologies (MOCAST’15), Thessaloniki, Greece, May 14-15, 2015.

[9] R. T. Tiburski, L. A. Amaral, E. D. Matos, D. F. G. de Azevedo and F. Hessel, “Evaluating the Use of TLS and DTLS Protocols in IoT Middleware Systems Applied to E-health”, 978-1-5090-6196-9, 2017 IEEE.

[10] K. Gama, L. Touseau and D. Donsez, “Combining heterogeneous service technologies for building an Internet of Things middleware”, Computer Communications, Volume 35, Issue 4, 15 February 2012, Pages 405-417, ISSN 0140-3664.

[11] Q. Jing, A. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[12] R. Tiburski, L. Amaral, E. Matos, and F. Hessel, “The importance of a standard security architecture for SOA-based IoT middleware,” IEEE Communications Magazine, vol. 53, no. 12, pp. 20–26, Dec 2015.

[13] M. Yoon and J. Baek, “A Study on Framework for Developing Secure IoT Service”, 10.1007/978-981-10-0281-6_42, Advances in Computer Science and Ubiquitous Computing, Springer.

[14] T. Pultarova , “Ukraine Grid Hack Is Wake-Up Call For Network OperatorS”, E&T Magazine, Volume 11, Issue 01, February 2016,http://ieeexplore.ieee.org/document/7592621.

[15] https://www.gartner.com/newsroom/id/3598917.

[16] Ar. M. Nia and N. K. Jha “A Comprehensive Study of Security of Internet-of-Things” IEEE, 2016

[17] Y. Yang, L.Wu, G. Yin, L. Li and Hongbin Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things”, DOI 10.1109/JIOT.2017.2694844, IEEE Intenet of Things Jounal.

[18] M. Radovan and B.Golub, “Trends in IoT Security”, DOI: 10.23919/MIPRO.2017.7973624, IEEE, 2017

[19] J.Granjal, E. Monteiro and J. S.Silva “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues” IEEE, 2015 .

[20] A.B. Pawar and Dr.S. Ghumbre “A Survey on IOT Applications, Security Challenges and Counter Measures” IEEE, 2016.

[21] D.G. Shin and M.S. Jun, “Home IoT device certification through Speaker Recognition”, ISBN 978-89-968650-5-6, ICACT2015.

[22] N. M. Vasavada and S. Belhe, “A Power Efficient Scheme for Speech Controlled IoT Applications”,

International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181Vol. 5 Issue 01, January-2016.
[23] Q. Jing J. Lu D. Qiu, "Security of the Internet of Things: perspectives and challenges", Wireless Network, doi : 10.1007/s11276-014-0761-7.
[24] M. A. Crossman and H. Liu, "Two-Factor Authentication through Near Field Communication",doi :978-1-5090-0770-7/16, IEEE, 2016.
[25] Y.S.Dabbagh and W. Saad, "On the Authentication of Devices in the Internet of Things",doi :978-1-5090-2185-7/16, IEEE, 2016.
[26] P. H. Griffin, "Secure Authentication on the Internet of Things",doi :978-1-5386-1539-3/17, 2017 IEEE