EAI Endorsed Transactions
on Smart Cities

Review Article EAI.EU

Secured Authentication Systems for Internet of Things

Gowtham M[1,*], M. K. Banga[2] and Mallanagouda Patil[2]

[1]Research Scholar, Department of Computer Science and Engineering, NIE Institute of Technology, Mysuru & Dayananda Sagar University, Bangalore, Karnataka, India
[2]Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore, Karnataka, India

Abstract

INTRODUCTION: In these days, an enormous extent of contraptions are interconnected with the remote advances which gave the principal light to the front line development of Internet of Things (IoT). Different quick contraptions and machines are by and by watched and controlled using IoT conventions. The developments of IoT are by and by spread to the entire sphere by which there is superb system in the devices related using IoT. From the assessment reports of Statista.com, The closeout of splendid home contraptions raised from 1.2 billion dollars to 4.4 billion dollars from year 2015 to year 2019 in the United States. As indicated by the report from Economics Times, there will connect with more than 2 billion units of ESIM based contraptions by year 2024. With the use of ESIM, the endorsers can use the progressed SIM card for the astute contraptions and the organizations can be activated without need of the physical SIM card. It is one of the progressing and confirmed employments of Internet of Things (IoT).
OBJECTIVES: The presented research manuscript is presenting an outline of the present state of IoT security.
METHODS: Past the standard applications, IoT is under research for the earth watching and prior notification to the coordinating workplaces so the fitting moves can be made. As per the news report by Grand View Research Inc., the overall IoT marketplace size is shown to contact more than 5,000 million dollars by year 2025. The presented IoT suggests the radio advancement standard with LPWAN so the enormous consideration of sharp devices should be conceivable with more significant level of execution in the system.
RESULTS: The key positive of the paper integrates the evaluation of Internet of Things with the assorted dimensions in addition to the cavernous analytics with the implementation aspects towards the security mechanism. The paper is having the focus and goals towards the association of security aware mechanism for the cumulative performance of IoT based environment.
CONCLUSION: With the gigantic utilization of IoT, there is have to incorporate the higher level of security and honesty for the protection mindful system condition.

Keywords: Internet of Things, IoT, Security Mechanisms, Secured IoT Environment

Received on 09 March 2020, accepted on 08 April 2020, published on 21 April 2020

doi: 10.4108/eai.13-7-2018.163998

*Corresponding author. Email: gouthamgouda@gmail.com

1. Introduction

Internet of Things (IoT) is an imaginative worldview moving toward the two businesses and people each day life [1]. It implies the organized interconnection of reliably dissents, which are furnished with inescapable learning. It not simply targets extending the ubiquity of the Internet, yet also at driving towards an especially spread arrangement of contraptions talking with individuals similarly likewise with various devices. Because of snappy advances in fundamental

developments, IoT is opening significant open entryways for innumerable novel applications that assurance to improve the idea of human's lives, empowering the exchanging of organizations. Internet of Things (IoT) [2, 3] is the eventual fate of all the present-day gadgets around the world. Giving them internet network makes IoT the following outskirts of innovation [4, 5]. Conceivable outcomes are boundless as the gadgets convey and connect with one another which make it considerably additionally fascinating for the worldwide markets [6]. For instance, Rolls-Royce declared that it would utilize the Microsoft Azure IoT suite and furthermore the Intelligence suite of Cortana to monitor the fuel use, for execution examination, to streamline the fly courses and so forth which improves the aircraft effectiveness. The gadgets must speak with one another, information from these gadgets must be gathered by the servers, and the information is then dissected or given to the individuals [7, 8, 9].

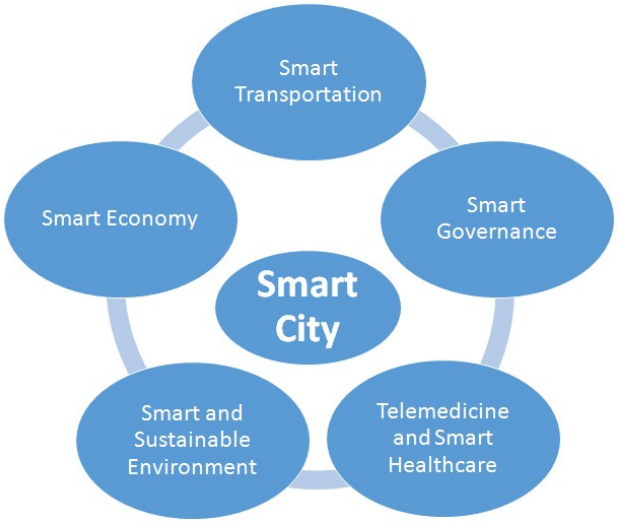

Fig. 1. Smart City as Classical Scenario of IoT

The paper is having key focus on the security mechanisms with the cryptography based approaches in addition to the advanced security aware approaches for IoT environment. The usage patterns and implementations with the blockchain in IoT can elevate the performance and security [10, 11] of IoT environment and it integrated in this work as the goal.

2. Attack Categorization According to IoT Architecture

There exist different types of architectural models of IoT, but predominantly the IoT architecture is considered to have four layers, as shown in Fig. 1. Table 1 depicts a snippet of the different security issues at the different layers of IoT system [12, 13].

Table 1. Security and Layered Aspects

Security Concerns	Application & Interface Layer	Service Support Layer	Network Layer	Device Layer
Insecure web interface	Yes	Yes	Yes	
Insufficient authentication/authorization	Yes	Yes	Yes	Yes
Insecure network services		Yes	Yes	
Lack of transport encryption		Yes	Yes	
Privacy concerns		Yes	Yes	Yes
Insecure cloud interface	Yes			
Insecure mobile interface	Yes		Yes	Yes
Insecure security configuration	Yes	Yes	Yes	
Insecure software/firmware	Yes		Yes	
Poor physical security			Yes	Yes

2.1. Security Threats at the Sensing/Perception Layer

To implement security features with IoT it is recommended to embed security systems onto the device itself and hence the devices should have ability to accommodate and maintain authenticity. The devices must also have the ability to avoid any breach of access to preserve security of the stored data. IoT security systems must ensure strict prevention of the unauthorized access while assuring flexible inter-operability amongst other devices in ad hoc network condition [13, 14].

2.2. Other Threats and Issues

There can be a huge probability that the assailants may need specialized information and in this way decimate gadgets and since the fenced in areas for gadgets are not

carefully designed they can be opened up effectively and their equipment can be gotten to by means of tests and stick headers [15, 16]. Subsequently, to guarantee physical security, it is inescapable that the IoT gadgets be made alter opposition making it hard to get the delicate data, for example, individual information, cryptographic keys or qualifications and so on. There have been accounted for certain situations when the IoT gadgets were not possibly solid to shield their code and information from outside access which in the long run makes the assailant to clone whole gadget or control the product or information. Maybe a couple of the models are the physical security assault when several brilliant traffic light gadgets were harmed by hoodlums who took the SIM cards of gadgets [17, 18]. Those SIM cards were later used to make cell phone brings in South Africa alongside a few vehicle crashes at the area and an extra cost to fix the whole framework. Lately, numerous instances of cloning Debit and Credit card has come into light where absence of physical security came about into colossal money related misfortunes [19, 20, 21].

Node Capture: It has been recently referenced that in spite of the assaults on physical security, an assailant can extricate the data from the gadgets without pulverizing it [22].

Sinkhole Attack: Such assaults are seen in the networks when sensors are left unattended for long lengths. During the sinkhole attack, the traded off hub removes the data from the entire closures by the nodes [23].

Selective Forwarding Attack: In some cases the malicious nodes may pick information packets and drop them out, inevitably performing selective filtering for example sifting the specific packets while conveying the rest, independent of the way that dropped packets [24, 25] may convey some sensitive data.

Witch Attack: The event of this sort of assault is basic if there should be an occurrence of disappointment of a genuine node and a pernicious node exploiting it, since the disappointment of authentic node occupies the accurate connection and enables it to make all its future communications [26, 27] with the malignant hub and hence prompting information misfortune.

Hello Flood Attacks: During such assaults a pernicious node starts a HELLO flood assault by sending HELLO message to all the neighbouring node and after that effects their accessibility. These attacks can cause non accessibility of assets to genuine clients by circulating countless gibberish solicitations to a specific help [27, 28].

Security Threats at the Network and Service Support Layers

The service support layer spoke to in the figure 1 delineates the IoT the executives framework and encourages on boarding gadgets and clients, applying strategies and leads and arranging computerization crosswise over gadgets. The most basic assignments performed at this layer are job based access control to deal with the character of client and gadget and the activities they are approved to perform. Further so as to accomplish non-renouncement, it is of central criticalness to keep up a review trail of changes performed by every client and gadget so it is difficult to invalidate moves made in the framework [29]. This observing could be useful in recognizing the assaulted gadgets in the event of recognition of any anomalous conduct. A piece of the assaults at the network and service support layer has been given in the consequent area.

Man-in-the-Middle (MITM) Attack: Man-in-the-middle assault is a case of the listening stealthily conceivable in the IoT. As gadget confirmation includes trade of gadget personalities, data fraud is conceivable because of man-in-the-middle attack.

Replay Attack: During the trading of character related data or different other credentials in IoT this information can be parody, adjusted or replayed. Replay assault is basically a type of dynamic man-in-the-middle attack.

Denial of Service Attack: As the IoT gadgets in IoT are resource compelled, they are powerless against asset use attack. Attackers can send messages or demands [30] to a particular gadget to expend its resources.

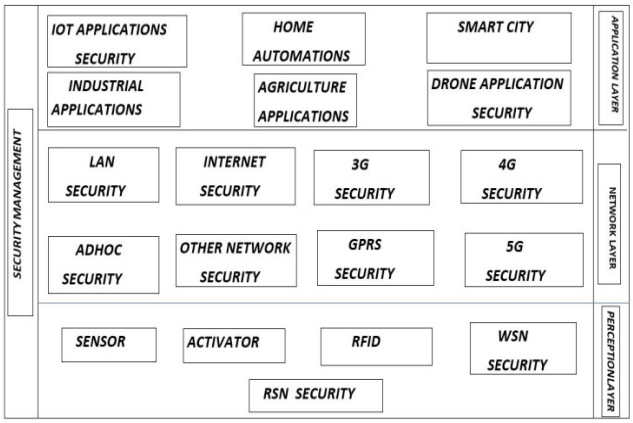

Fig. 2. Different layers of IoT model

Table 2. Possible Attacks

Layers	Types of Attacks
Perception Layer	Jammers, replay attacks, Sybil, selective forwarding, Synchronization attack. Passive interference, active jamming of temporarily disabling the device, replay attacks.
Network Layer	Sinkhole, unfairness, false routing, hello and session flooding, Eavesdropping, cloning, spoofing, impersonation, and network protocol attacks.

Application Layer	Injection, buffer overflows, unauthorized tag reading and modification.

The current manuscript will study the current flow improvement of IoT security inquire about and Table 2 gives the possible attacks in the IoT ecosystems. Troubles in smearing security parts in IoT and its ambush courses will in like manner be discussed. When contrasted with different overviews, this paper discoveries the flow IoT verification security systems in the exploration. Different segments of the displayed original copy are partitioned as pursues. Segment II examines the related work, segment III issues recognized by review, segment IV suggestions for reinforcing the security instruments in IoT and Conclusion of the general research is displayed in segment V, and the references utilized in this paper are given toward the finish of the composition.

3. Attack Categorization According to IoT Architecture

In this segment, we briefly deliberate the current access control, user access control, and intrusion detection and prevention schemes proposed in the literature for WSNs. We at that point underline in detail on the client verification issue in WSNs in light of the fact that it will be the principle dialog of this original copy.

The taxonomy of Security issues at different layers, Table 1 it is noticed that user authentications, access control, user access control, and intrusion detection and prevention are the primary security issues in the IoT ecosystem.

Shin et al. [31] focused on confirmed key understanding plan for secure communication among clients and IoT gadgets, where a two-factor validation model was created. Authors have tried; be that as it may, the key issues like Stolen smart card or Smart Card Loss Attack (SCLA), Offline Password speculating as well as recovery utilizing Brute Force assault which are normal nowadays couldn't be tended to by authors and because of its higher computational and correspondence cost, the suggested approval plan may not relevant to run of the typical sensor nodes.

Wazidet al. [32] built up a Secure User Authenticated Key Management Protocol for Generic IoT Networks. The authors focused on planning another lightweight multifaceted remote client verification conspire for hierarchical IoT network (HIoTN), called the user authenticated key management protocol (UAKMP). Authors proposed to abuse client smart card, password, and individual biometrics to structure authentication model. Certainly the utilization of different factors, for example, smart card, password, and personal biometrics makes generally speaking framework increasingly proficient or secure; be that as it may, a couple of key perspectives, for example, session data, building up a vigorous various parameter based confirmation couldn't be created which could make by and large framework computationally productive and pragmatic. What's more the utilization of non linear or bilinear (bidirectional) hashing method could have made framework progressively effective.

J. Srinivaset al. [33] The proposed plan underpins the adaptability and parts of a WSN without influencing the supportiveness of the enlistment or check arrangement of both the customer and sensor nodes and regular affirmation Dismissing the upsides of the course of action, the proposed Plan has a greater computational overhead than further lightweight validation plans.

Challaet al. [34] built up a Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. Authors focused basically on the security arrangement for Cyber-physical frameworks, for example, smart grids and shrewd transportation,

They built up a signature-based authentication and key agreement scheme essentially centers on signature-based authentication that can't be expressed as strong in current day hacking or breaking situation. Moreover, the old style signature based approaches would have been expanded with certain increasingly successful lightweight cryptosystem.

Porambageet al. [35] Created 2 group key establishment protocols for protected multicast communications among the resource compelled devices in IoT However, Group key establishment can accomplish better security arrangement for a predetermined number of nodes. Anyway under practical IoT applications with an enormous number of nodes and decentralized application condition, these methodologies appear to be limited. In any event, sharing of key data over the nodes may be ruptured accordingly causing unauthenticated information get to. This work, even couldn't address security during channel transmission.

Ninget al. [36] worked on an Aggregated-Proof Based Hierarchical Authentication System for the Internet of Things. Authors focused on a current U2IoT design, to plan an aggregated-proof based hierarchical authentication scheme (APHA) for the layered systems. Solidly, 1) the aggregated-proofs are set up for various focuses to accomplish in reverse and forward unknown information transmission; 2) the coordinated way descriptors, homomorphism capacities, and Chebyshev chaotic maps are together smeared for mutual verification; 3) not the same access authorities are dispersed to achieve hierarchical access control. Could be effective for maintaining node anonymity; however is complicated.

Mick et al. [37] proposed LASER: Lightweight Authentication and Secured Routing for NDN IoT in Smart Towns. (Observably, named information organizing (NDN) project deals highlights usable by IoT applications) It very well may be additionally increased with upgraded ECC making it progressively appropriate. Besides, the incorporation of various security components can be more successful than the old style LASER. As in

smart city there can be diverse application condition or end client equipment and subsequently utilizing various parameters is progressively compelling. It can be called as presenting all the more testing security approach can cause unapproved get to additional to confound and consequently progressively secure for real clients.

He et al. [38] Prescribed ECC based RFID Authentication Schemes for Internet of Things in Healthcare Environment with Elliptic Curve Cryptography. Further enhancement of ECC can be done.

Mohd.et al. [39] worked on a Lightweight Block Ciphers for IoT to augment energy optimization and survivability It requires significant optimization not only for computational cost but also as per environment.

Heung et al. [40] suggested a lightweight privacy-preserving information aggregation system, called Lightweight Privacy-preserving Data Aggregation (LDPA), for fog computing-enhanced IoT. The suggested LPDA is portrayed by utilizing the homomorphism based encryption, Chinese Remainder Theorem, and one-way hash chain techniques to not just total half and half IoT devices' information into one, yet additionally early filter inserted false data at the network edge. It can be effective; however optimization in terms of better cryptosystem, multiple security constraints etc can't be ignored.

Xuet al. [41] worked on network security condition awareness (NSSA). Be that as it may, it is constrained by its capacity to mine and assess security circumstance components from multi-source assorted system security data. To deal with this issue, this manuscript recommends an IoT sort out security condition care model with a situation thinking system reliant on semantic transcendentalism and customer described standards. Mysticism advancement can give a united and formal depiction to deal with the issue of semantic heterogeneity in the IoT security space. In this manuscript, four key sub-zones are suggested to reflect an IoT security situation: setting, assault, powerlessness, and system stream. This paper only focuses on semantic nature exploitation for security provision. It can't be an ideal solution for major IoT ecosystem purposes.

Diroet al. [42] Prescribed utilizing lightweight cryptographic capacities, for example, elliptic curve cryptography to accomplish Fog-to-Things Communication requires optimization to yield a better and robust solution.

Yuan et al. [43] suggested a dependable and lightweight reliance system for IoT edge devices dependent on multi-source criticism data combination. To start with, due to the multi-source input system was utilized for worldwide trust estimation our trust computation component is progressively dependable against sassing assaults brought about by vindictive criticism suppliers. By then, lightweight trust evaluating framework was applied for joint efforts of IoT edge gadgets, which is sensible for huge scale IoT edge figuring since it energizes low-overhead trust preparing counts. Simultaneously, a criticism data combination calculation dependent on target data entropy hypothesis was applied, whereby the trust components are weighted physically or emotionally Feedback appliance can augment computational overhead and bandwidth exhaustion thus making it inappropriate for major mission critical communication over D2D ecosystem.

Zahra et al. [44] concentrated on beating the security disputes experienced during the information redistributing from fog client to fog node and applied Shibboleth otherwise called security and cross area access control convention between fog client and fog node for improved and secure correspondence between the fog client and fog node Use of multiple parameters can make solution more viable and trustworthy, especially when user (node) remains in uncertain use condition.

Diroet al. [45] recommended lightweight cryptographic functions, such as elliptic curve cryptography for IoT Augmentation of ECC can't be ignored. And employing certain enhanced ECC with other security feature can make it a better solution, especially for IoT.

Zhenget al. [46] explained the protection issues in clients' information sharing they use attribute-based encryption to empower information distribution. In like manner, they cleared the property planning limit and use the credit blossom channel to shroud all of the attributes in the passage control structure. In order to progress the adequacy of encryption, an on the web/disconnected encryption advancement was proposed in the encryption arrange. Online-offline encryption approach during encryption could bring down energy consumption however the time delay for users often remains an open question. Removal of attribute matching can make it computational better; however its robustness remains limited for a large scale real-time IoT ecosystem.

Chen et al. [47] Examined secure uplink transmission in a normal Internet of Things (IoT) organization, where various sensors communicate with a controller through the help of a non-trusted hand-off.

Ding et al. [48] Suggested a novel pairing-free data access control system based on Cipher text-policy attribute-based encryption (CP-ABE) with elliptic curve cryptography, abbreviated PF-CP-ABE. Optimization of ECC can be the scope; however inclusion of multiple parameters can make system more effective.

Elhosenyet al. [49] recommends a crossbreed security model for securing the diagnostic text data in medical images. The suggested model is created through coordinating either 2-D discrete wavelet change 1 level (2D-DWT-1L) or 2-D discrete wavelet change 2 level (2D-DWT-2L) strategy with a suggested crossbreed encryption scheme. The proposed hybrid encryption scheme is fabricated utilizing a mix of Advanced Encryption Standard, and Rivest, Shamir, and Adleman calculations. Here, the focus is made on image data security. On the other hand efficacy of RSA often remains dependent on the bit size. ECC can be a better asynchronous cryptosystem solution.

Ruanet al. [50] Conceptualized leakage resilient (LR) security system for password-based authenticated key exchange (PAKE) protocol. Suggest the LR PAKE

convention by utilizing Diffie-Hellman key trade, LR storage (LRS) and LR invigorating of LRS properly and officially suggest security evidence in the standard system. ECC can be a better solution than the classical Diffie Hellman. Its efficacy for a typical next generation IoT system remains a suspicion.

The security, privacy and safety risks related to IoT that was worked in this study were DDoS attacks made with IoT devices, espionage and eavesdropping. Another risk was that personal data can be stolen and used to harm the user in different ways, for example identity theft, hijack mail and social accounts, plan and commit burglary and blackmailing.

The awareness of the risks related to IoT devices correlates with how interested a person is of technology. The more interested a person is of technology, the better awareness the person have regarding the risks associated with IoT devices. Even though many people are aware of the risks related to IoT devices, they do not protect neither their router nor their IoT devices actively. This is because people don't know how they can protect their router or devices.

4. Problems Identified

Considering the significance of a robust and efficient security model for the current IoT ecosystems, though a number of efforts have been made; however realization of the major at hand systems under different attack conditions seems confined to alleviate adversaries. Undeniably, majority of the existing systems are primarily focused on employing single cryptosystem approach to assist transmission security between communicating peer nodes; however in function varied attack events have proved limitations of these all classical cryptosystems. For example, most of the existing security algorithms are found vulnerable to the attacks caused due to:

- Smart Card Loss Attack (SCLA) and several registered in users with the similar credentials attack.
- Offline Password guessing and/or retrieval using Brute Force attack,
- Sensor node spoofing,
- Replay attack and forgery attack
- Privileged-insider and session-specific temporary information attacks.
- User anonymity or non-linking is not addressed in practical IoT specific security systems.
- User impersonation attack or the Session specific temporary information attack (SSTIA) and offline password guessing attack
- Gateway node bypassing and sensor-node key impersonation.

Furthermore, majority of the existing systems don't reserve user's and/or sensor's anonymity, mutual authentication, secrecy of the secret nodes of the sensor node or gateway node and ignore intractability need of the network. Inclusion of such robustness could strengthen IoT communication system, especially sensor assisted M2M communication system to retain seamless communication. It can be considered as the prime driving force for the current research work and allied future proposition. In this research the emphasis is made on exploiting multi-level security provisioning to the WSN assisted M2M communication to serve secure communication across IoT ecosystem.

5. Recommendations

I would recommend doing studies regarding how manufactures can design and create a safer device and maintain it safe for the users. For further studies, it would also be interesting to investigate how companies who sells IoT devices store the data about their users – how well do they protect all the collected data?

When looking at the current solution compared to the CIA-triad, there is definitely benefits when using block chains in an IoT network of this type. The experience and knowledge gained from researching and implementing this solution to create an understanding on how blockchain technology can support the communication and security in an Internet of Things network. Leads us back to the starting problem statement: How do you maintain the information safety in an Internet of Things network based on block chains and user contribution?

The block chain technology offers plenty of solutions to information security problems that can occur in IoT networks, especially within the integrity of the information and the availability of the services since block chains is peer-to-peer. The biggest problem is within confidentiality where all the information on the block chain can be accessed by everyone which makes this not a suitable solution for a system were sensitive or classified information is stored, because even if we encrypt the information with a really secure encryption method the encryption could still be solved in theory.

The existing schemes either require more communication and Calculation costs for the resource constrained sensor nodes or they are vulnerable to several attacks such as malicious node deployment attack, Sybil attack, node replication attack and wormhole attack. Hence, designing of an efficient and more secure access control mechanism is an interesting research problem, which will be based on certificate based analytics.

An important difference between current and future mobile architectures is, indeed the variety of devices for which security solutions must be found. Current mobile phones are vulnerable to many attacks, e.g., malware, Denial-of-Service (DoS), tracking and cryptographic attacks. Future networks will include IoT devices, which are even more attack-prone, and can be used as "tools" in cyber-attacks. The transition to5G networks is expected to not only combine, but to compound risks to all types' of devices.

For 30 years, 3rd and 4th generation mobile networks have allowed users to receive service anywhere, at any

time. The dawning and visionary 5th generation mobile network(5G) aims to create a highly-decentralised architecture, including a massive Internet of Things and a non-federated core network, making telecommunication ubiquitous. The two of the most important cryptographic challenges for future mobile communications, unanswered by current 3G/4G solutions today are designing:

- A versatile secure-channel establishment protocol in 5G networks;
- Secure and privacy-preserving protocols for resource-restricted IoT devices.

6. Conclusion

In conclusion, as per the IoT security engineering, security alleviation includes every one of the layers in the essential IoT design, namely, perception, network, and application, regardless of the way that it is seen that by far furthermost of the present components are smeared to the network layer. It moreover can be assumed that a fitting IoT hazard showing might be worthwhile in manipulating incredible IoT security control. Here this manuscript mainly concentrated on current disadvantages in access control mechanisms. The researchers and IT companies can work on current Authentication drawbacks so that the future IoT environment can be secured with higher performance.

Acknowledgements.

We are thankful to our organization and the research supervisors for their consistent assistance and guidance towards the research perspectives and the dimensions associated with the work inscribed.

References

[1] U. Raza, P. Kulkarni, M. Sooriyabandara, “Low Power Wide Area Networks: An Overview”, IEEE Communications Surveys & Tutorials, Vol. 19, Issue 2, January 2017, pp. 855-873.

[2] C. Gomez, J. Paradells, C. Bormann, J. Crowcroft, "From 6LoWPAN to 6Lo:Expanding the Universe of IPv6-Supported Technologies for the Internet of Things", IEEE Communications Magazine, Vol. 55, Issue 12, pp. 148-155,December 2017.

[3] P. Thubert, A. Pelov, S. Krishnan, "Low-Power Wide-Area Networks at the IETF", IEEE Communications Standards, Vol. 1, Issue 1, March 2017, pp. 76-79.

[4] Minaburo, L. Toutain, C. Gomez, D. Barthel, J.C. Zuniga, “Static Context Header Compression (SCHC) and fragmentation for LPWAN, application to UDP/IPv6”, draft-ietf-lpwan-ipv6-static-context-hc-21, Jul. 2019. (Work in progress, available at https://tools.ietf.org/html/draft-ietf-lpwan-ipv6- static-context-hc-21, accessed on August 22nd 2019.)

[5] J. Haxhibeqiri, E. De Poorter, I. Moerman, J. Hoebeke, “A Survey of LoRaWAN for IoT: From Technology to Application”, Sensors, Vol. 18, 3995, November 2018.

[6] C. Gomez, J.C. Veras, R. Vidal, L. Casals, J. Paradells, “A Sigfox Energy Consumption Model”, Sensors, Vol. 19, 681, February 2019.

[7] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grövlen, Y. Sui, Y. Blankenship, J. Bergman, H.S. Razaghi, “A Primer on 3GPP Narrowband Internet of Things”, IEEE Communications Magazine, Vol. 55, Issue 3, March 2017, pp. 117-123.

[8] L. Feltrin, G. Tsoukaneri, M. Condoluci, C. Buratti, T. Mahmoodi, M. Dohler, R. Verdone, “Narrowband IoT: A Survey on Downlink and Uplink Perspectives”, IEEE Wireless Communications, Vol. 26, Issue 1, February 2019, pp. 78 – 86.

[9] H.-S. Kim, J. Ko. D.E. Culler, J. Paek, “Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey”, IEEE Communications Surveys & Tutorials, Vol. 19, Issue 4, September 2017, pp. 2502 – 2525.

[10] C. Bormann, A.P. Castellani, Z. Shelby, “CoAP: An Application Protocol for Billions of Tiny Internet Nodes”, IEEE Internet Computing, Vol. 16, Issue 2, March 2012, pp. 62-67.

[11] Z. Shelby, C. Bormann, “6LoWPAN: The Wireless Embedded Internet”, Vol. 43. John Wiley & Sons, August 2011.

[12] C. Bormann, S. Lemay, H. Tschofenig, K. Hartke, B. Silverajan, B. Raymor, “CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets”, RFC 8323, February 2018. (Available at https://tools.ietf.org/html/rfc8323, accessed on August 22nd 2019.)

[13] Jacobson, “Compressing TCP/IP Headers for Low-Speed Serial Links”, RFC 1144, February 1990. (Available at https://tools.ietf.org/html/rfc1144, accessed on August 22nd 2019.)

[14] K. Sandlund, G. Pelletier, L-E. Jonsson, “The RObust Header Compression (ROHC) Framework”, RFC 5795, March 2010. (Available at https://tools.ietf.org/html/rfc5795, accessed on August 22nd 2019.)

[15] S. Jeschke, C. Brecher, T. Meisen, D. zdemir, and T. Eschert, Industrial Internet of Things and Cyber Manufacturing Systems, ser. Springer Series in Wireless Technology. Cham: Springer International Publishing, 2016, pp. 3–19.

[16] [Online]. Available: https: //publications.rwth-aachen.de/record/689897

[17] W. G. Hatcher and W. Yu, “A survey of deep learning: Platforms, applications and emerging research trends,” IEEE Access, vol. 6, pp. 24 411–24 432, 2018.

[18] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, “Deep learning for iot big data and streaming analytics: A survey,” IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2923–2960, Fourthquarter 2018.

[19] S. Boschert and R. Rosen, “Digital twinthe simulation aspect,” in Mechatronic Futures. Springer, 2016, pp. 59–74.

[20] Q. Qi and F. Tao, “Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison,” IEEE Access, vol. 6, pp. 3585–3593, 2018.

[21] Canedo, “Industrial iot lifecycle via digital twins,” in 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS). IEEE, 2016, pp. 1–1.

[22] F. Tao, F. Sui, A. Liu, Q. Qi, M. Zhang, B. Song, Z. Guo, S. C.-Y. Lu, and A. Nee, “Digital twin-driven product

design framework," International Journal of Production Research, pp. 1–19, 2018.
[23] K.-D. Thoben, S. Wiesner, and T. Wuest, "industrie 4.0 and smart manufacturing-a review of research issues and application examples," International Journal of Automation Technology, vol. 11, no. 1, pp. 4– 16, 2017.
[24] G. Peralta, M. Iglesias-Urkia, M. Barcelo, R. Gomez, A. Moran, and J. Bilbao, "Fog computing based efficient iot scheme for the industry 4.0," in 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM). IEEE, 2017, pp. 1–6.
[25] X. Li, D. Li, J. Wan, C. Liu, and M. Imran, "Adaptive transmission optimization in sdn-based industrial internet of things with edge computing," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1351–1360, 2018.
[26] X. Xu, "From cloud computing to cloud manufacturing," Robotics and computer-integrated manufacturing, vol. 28, no. 1, pp. 75–86, 2012.
[27] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," IEEE Wireless Communications, vol. 24, no. 2, pp. 98–105, 2017.
[28] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, pp. 372–387.
[29] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: The good, the bad, and the ugly," IEEE Access, vol. 7, pp. 158 126–158 147, 2019.
[30] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.
[31] S. Shin and T. Kwon, "Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G Integrated Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 11229-11241, 2018.
[32] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 269-282, Feb. 2018.
[33] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," Ad Hoc Networks, vol. 54, pp. 147–169, 2017.
[34] S. Challa et al.., "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," in IEEE Access, vol. 5, pp. 3028-3043, 2017.
[35] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila and B. Stiller, "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications," in IEEE Access, vol. 3, pp. 1503-1511, 2015.
[36] H. Ning, H. Liu and L. T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 3, pp. 657-667, March 2015.
[37] T. Mick, R. Tourani and S. Misra, "LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 755-764, April 2018.
[38] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," in IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72-83, Feb. 2015.
[39] B. J. Mohd and T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," in IEEE Access, vol. 6, pp. 35966-35978, 2018.
[40] R. Lu, K. Heung, A. H. Lashkari and A. A. Ghorbani, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," in IEEE Access, vol. 5, pp. 3302-3312, 2017.
[41] G. Xu, Y. Cao, Y. Ren, X. Li and Z. Feng, "Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things," in IEEE Access, vol. 5, pp. 21046-21056, 2017.
[42] A. A. Diro, N. Chilamkurti and Y. Nam, "Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication," in IEEE Access, vol. 6, pp. 26820-26830, 2018.
[43] J. Yuan and X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," in IEEE Access, vol. 6, pp. 23626-23638, 2018.
[44] S. Zahra et al.., "Fog Computing OverIoT: A Secure Deployment and Formal Verification," in IEEE Access, vol. 5, pp. 27132-27144, 2017.
[45] A. A. Diro, N. Chilamkurti and Y. Nam, "Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication," in IEEE Access, vol. 6, pp. 26820-26830, 2018.
[46] D. Zheng, A. Wu, Y. Zhang and Q. Zhao, "Efficient and Privacy-Preserving Medical Data Sharing in Internet of Things With Limited Computing Power," in IEEE Access, vol. 6, pp. 28019-28027, 2018.
[47] D. Chen, W. Yang, J. Hu, Y. Cai and X. Tang, "Energy-Efficient Secure Transmission Design for the Internet of Things With an Untrusted Relay," in IEEE Access, vol. 6, pp. 11862-11870, 2018.
[48] S. Ding, C. Li and H. Li, "A Novel Efficient Pairing-Free CP-ABE Based on Elliptic Curve Cryptography for IoT," in IEEE Access, vol. 6, pp. 27336-27345, 2018.
[49] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, A. N and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018.
[50] O. Ruan, J. Chen and M. Zhang, "Provably Leakage-Resilient Password-Based Authenticated Key Exchange in the Standard Model," in IEEE Access, vol. 5, pp. 26832-26841, 2017.