Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC 2020)
DVD Part Number: CFP20J06-DVD; ISBN: 978-1-7281-2812-2

An Intrusion Detection in Internet of Things: A Systematic Study

Harsh Namdev Bhor
Assistant Professor, K.J.Somaiya Institute of Engineering and Information Technology,
Sion, Mumbai, India.
hbhor@somaiya.edu

Mukesh Kalla
Assistant Professor, Sir Padampat Singhania University, Bhatewar, Udaipur,
Rajasthan, India

***Abstract*—IOT (Internet of Things) is another worldview it coordinates web and physical items having a place with various areas, for example, home robotization, mechanical procedure, human wellbeing and ecological checking. It extends the Internet-associated gadgets presence in our day by day exercises, bringing, and numerous advantages, but the challenges leads with safety problems. Intended for over two decades, (IDS) Intrusion Detection Systems take a significant apparatus to the systems shelter and data frameworks. Nonetheless, put on conventional IDS systems to IoT is troublesome because of its specific qualities, for example, compelled asset gadgets, explicit protocol stacks, and principles. In this paper, we present a study of IDS examine endeavors for IoT. Our goal line to distinguish the important patterns, exposed problems, and upcoming investigation potential outcomes. We classify the IDSs proposed in the related works as indicated by the accompanying properties: identification technique, IDS assignment system, safety risk and proof methodology. We additionally talked about the various potential outcomes for each characteristic, enumerating parts of mechanism that either one propose explicit IDS plans for IoT or create occurrence discovery procedures for IoT security dangers that might be inserted in IDSs. The best frameworks recognized old assaults worked in the preparation information, at moderate recognition rates running from 63% to 93% at a bogus caution pace of 10 bogus alerts for every day. Disclosure rates were a lot of more regrettable for new and novel R2L and DoS assaults remembered distinctly for the test information. The best frameworks neglected to distinguish generally a large portion of these new episodes which included harming access to root-level benefits by remote clients.**

Keywords— IoT, Intrusion Detection, security, threat.

I. INTRODUCTION

The IoT accept that items have advanced functionality and can be distinguished and pursued therefore [1]. Programmed object unmistakable evidence, (for instance, Radio Frequency Identification (RFID) or Near Field Communication, and visual markers), abudant organize, improved handling and capacity capacities, distinctive new show progresses, sensor contraption availability, and reducing gear costs all set up the system for another registering period. We would now have the option to manufacture vehicles, devices, items, and normal things to turn into a bit of the IoT. This thinks about correspondence, correspondence, and information get to everywhere and at whatever point to be embedded into anything [2]. IoT is measured as an expansion of the present Internet where Human-to-Human (H2H) joint exertion has ruled the bit by bit arrange correspondence. Human-to Machine (H2M) affiliation has changed into another principal Internet correspondence when machines get progressively clever with AI [3]. In addition with these, Things are getting mechanized, keen, and connected with the web as well and PCs will be everywhere, internet related, and indistinctly living with individuals [4]. IoT is a new idea to get Things related with the network, and Thing-to-Thing or M2M correspondence is the center IoT development. The IoT frames on three sections related to the capacity of insightful things or security, for instance, to convey, for setting awareness, and to coordinate either amongst themselves, building exchanges of interrelated things and objects, or with customers or various substances in the framework [5]. The expanding utilization of smart installed gadgets in business makes new chances to construct an applications that better incorporate ongoing condition of the physical world, and henceforth, gives endeavor benefits that are exceedingly powerful, more various, and effective [6]. The trust interruption recognition and grouping is proposed so as to distinguish the dangerous hubs and communicate the vitality powerful information. In our work, trust-based interruption recognition model is gotten for distinguishing the threatening hubs. Various assortments of trusts were considers, to be specific vitality, information and correspondence trust, which can be created among two sensor hubs [34].

A message correspondence in an IoT device is central starting at an IoT device needs to send a requesting to additional contraption to boss system. Push Protocol (PP) is the most acclaimed message transmission show for IoT since PP is made in uninformed exchange limit routinely [7]. Break down the review information even an assault has happened, for deciding the degree of harm happened, this investigation helps in assault follow back and furthermore in recording the assault designs for future anticipation of such assaults. An interruption identification framework (IDS) can be utilized to investigate review information for such bits of knowledge. This makes IDS an important ongoing recognition and anticipation apparatus just as a measurable investigation instrument [35]. PP is lightweight than other surveying convention and we can utilize various PP for IoT, for example, HTTP, extensible Message and Presence Protocol (XMPP), CoAP and Message Queue Telemetry Transport (MQTT). XMPP is open source

standard PP in context on XML. XMPP utilizes little assets when stimulating data from a server than HTTP convention [8]. Obliged Application Protocol (CoAP) is for sensor gadget with little memory by utilizing Restful structure with URI. CoAP couldn't care less gathering correspondence anyway adjusted correspondence are bolstered by these show. MQTT was proposed to handle low-control gadgets as a light-weight convention and has been utilized as a bit of different IoT and minute informing frameworks [9].The protocol underpins interoperability nature that redesigns the limit of system to exchange and make usage of the normal information [10]. The IoT thought, thus, goes for making the Internet fundamentally increasingly certain. Moreover, by empowering fundamental access and correspondence with a wide arrangement of contraptions, for instance, home mechanical assemblies, surveillance cameras, checking sensors, display, actuators, vehicles, and so on, the IoT will develop the progression of different applications that make use of the potentially tremendous and arrangement of data delivered by such items give new organizations to nationals, associations, and open associations. This structure finds application in a wide scope of areas, for instance, home automation, present day computerization, restorative aides, portable medical coverage, old assistance, shrewd energy organization and smart grids, vehicle, movement organization, and various others [11]. In this paper, review on the IoT applications has been done in order to investigate the execution and limitations of a few approaches. This procedure motivates the specialist's for additionally inquire about work in IoT environment.

This survey is composed as tracks, Sector 2 presents at the basic structure of IoT. Sector 3 describes the key challenges of IoT. Section IV presents the presentation of IDS on detection techniques. Sector 5 survey several recent papers on IoT. The conclusion is made in the sector 6.

II. IoT Architecture

The IoT is fit for interconnecting different heterogeneous items over the Internet, Fundamental necessity for a versatile layered design. The reliably extending amount of proposed structures has not yet united to a situation demonstrate [12]. At that point, there are a couple of tasks like IoT-A [13] which endeavor to design a commonplace structure relies upon the assessment of the necessities of researchers and the business. From the pool of existing techniques, the plain design is Application, Network and Perception Layer.

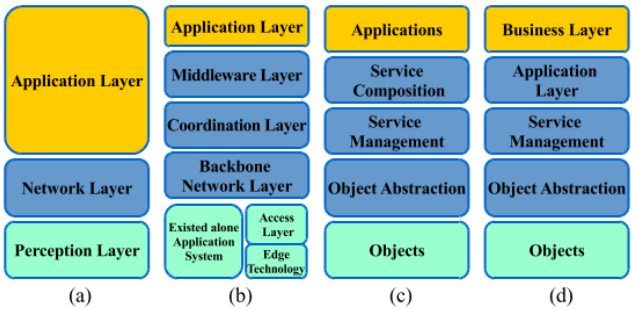

Fig. 1. Figure 1: IoT structure. (a) initial-layer (b) Middle- built (c) SOA built (d) Final-layer

However, a portion of the existing system presents two additional layers in the IoT model. The fundamental model of an IoT structure is exhibited in Figure 1.

A. Object Layer:

The Objects or affirmation layer is the chief layer which shows the physical sensors of the IoT that plan to gather and process data. This layer unites sensors and actuators to perform undeniable functionalities, for example, quering region, temperature, and so forth. Institutionalized attachment and-play instruments should be utilized by the preception layer for orchestrating heterogeneous articles [14-15]. This layer digitizes and exchanges information to the Object Abstraction layer is to the secure channels.

B. Object Abstraction Layer:

This layer moved the data to the Service Management layer which is passed on by the Objects layer through safe channels. Data can be traded through various progressions, for instance, GSM, RFID, Zig-Bee, UMTS, etc. Furthermore, various purposes of constrainment like passed on figuring and data affiliation structures are manage this layer.

C. Service Management Layer:

Middleware (planning) layer or Service Management combines an association with its requester depends upon regions and names. This layer draws in the IoT application programming designers to effort with varied things without thought to a particular equipment organize. Correspondingly, this layer proceeds with the got information, chooses, and passes on the essential associations over the system wire shows [16-17].

D. Application Layer:

It gives the associations to clients which are referenced by them. In IoT the important layer is that it can give great associations to address clients' issues. The application layer covers diverse vertical markets, for example, sharp structure, keen home, present day automation, transportation, and wise human organizations [18].

E. Business Layer:

Its deals with the general IoT structure exercises and associations. The commitments of this layer are to fabricate a business action, flowcharts, diagram subsequently depends upon the information from the Application layer. This layer picks it conceivable to help for settling on choice method according to Big Data assessment. Additionally, watching and association of this layer polished four layers. Similarly, this layer separates the yield of each layer with the respect improve advantages and keeping up the clients' security [16].

In the five-layer technique, the Application Layer is the interface by which end-clients can organize with a gadget and solicitation for hypnotizing information. It gives an interface to the Business Layer where irregular state assessment and reports can be passed on.

III. IoT Challenges

Understanding the vision of the IoT is certainly not a straightforward task on account of the various troubles that ought to be tended to. Instances of key troubles join openness, unwavering quality, movability, trust, execution, security, flexibility, interoperability, and organization. Tending to these challenges engages administration associations and application engineers to execute their organizations beneficially. For example, security and insurance accept an imperative part in all business divisions globally on account of the affectability of clients' assurance. Moreover, assessing the execution of the IoT organizations is a key test [19, 20]. In the below sections, we give a short talk of the key troubles looked in the improvement and deployment times of the IoT and relevant research attempts and exercises.

A. Data Management:

IoT sensors and gadgets are making enormous extents of information that should be organized and set away. The present conduct of the server center isn't set up to arrangement with the heterogeneous nature and sheer volume of individual and endeavor information [21]. The couple of endeavors would be able to put resources into information amassing adequate to house all the IoT information collected from their systems. Finally, they will deal with information for assignments depends upon necessities and respect. Server centers will end up being more appropriated to overhaul managing ability and response time as IoT contraptions ends up being all the more extensively utilized and eat up more move speed.

B. Security:

With respect to the circumstance with sharp success apparatus and brilliant vehicle emergency associations, IoT gadgets can give a gigantic extent of information on IoT clients' region and progressions, thriving conditions, and verifying inclinations all of which can start essential affirmation concerns. Ensuring security is from time to time counter-profitable to suppliers in this situation, as information made by the IoT is fundamental to updating individuals' lives and diminishing suppliers costs by streamlining endeavors. The IoT is in all probability going to update individuals' lives [22]. While the IoT keeps picking up the power through shrewd home structures and wearable gadgets, faith in and insistence of the IoT will rely affirmation of clients' safety.

C. Privacy:

As an increasing amount and variation of related contraptions are brought into IoT frameworks, the possible safekeeping risk elevates. The IoT improves the proficiency of associations and overhauls the idea of people's lives, the IoT will grow the potential assault surfaces for software engineers and other advanced offenders. IoT devices have vulnerabilities as a result of nonattendance of transport encryption, insecure Web interfaces, insufficient software protection, and lacking endorsement. Devices on the IoT generally don't use data encryption methodology. Some IoT applications guides delicate infra-structures and essential organizations, for instance, the keen system and office affirmation. Absence of security and assurance will make protection from determination of the IoT by firms and individuals. Security challenges may be settled by means of training designers to solidify security plans (e.g., firewalls) into things and encouraging customers to utilize IoT security incorporates that are joined with their devices.

D. Chaos

The progression of IoT advances (e.g., chips, sensors, remote advances) is in a hyper stimulated improvement cycle that is impressively speedier than the run of the common consumer thing. There are so far benchmarks, deficient security, insurance issues, complex trades, and duplicating amounts of incapably attempted contraptions. If not illustrated exactly, multi-purpose devices and aggregate applications can change our lives into chaos. In a disengaged world, a little blunder doesn't chop down a structure; regardless, in a hyper-related world, an error in one part of system can cause issue throughout.

E. Networking and Addressing

The IOT will incorporate a fantastically high number of hubs, every one of which will create content that ought to be retrievable by any approved client paying little respect to its position. This requires compelling tending to approaches.

F. Interoperability

In IoT correspondences and tasks will occur among different heterogeneous gadgets, these gadgets ranges from consumer machines to top of the line cloud based server farms. Since the IoT is in advancing stage and different sellers are making shrewd gadgets, mix, information trade and control of these heterogeneous gadgets over the web is a genuine challenge because of absence of interoperability.

IV. Intrusion Detection in IoT

The reason for an interruption detection system (IDS) is to recognize unapproved access. A portion of these frameworks and systems that need get to assurance include: wide region systems and clouds, neighborhood, ad hoc systems, remote neighborhood, and remote individual region systems. In this family the three progressively common systems include: remote sensor systems, cell phones, and radio recurrence recognizable proof. The IDS on these frameworks and systems can comprehensively be classified by the identification procedures used, for example rule base or stateful packet examination, anomalies.

In IoT systems, the IDS be able to be located in the fringe switch, one hosts in at most, or in each physical item. The benefit of putting the IDS in the fringe switch that location of interruption outbreaks from the Internet in contradiction of the objects in area of physical line. But, an IDS at the fringe switch may produce correspondence overhead between the Low power and Lossy Networks (LLN) hubs and the border

switch because of the IDS successive system. Setting the IDS in the LLN hubs may diminish the correspondence overhead connected with system checking, however needs most assets (handling, stockpiling, then vitality). This may be an issue because of resource confinements of LLN hubs. Conveying IDS operators over some devoted hubs may be an answer for see the needs for low checking traffic and most handling limit.

A. Intrusion Detection System Techniques

Interruption recognition procedures are ordered into four classes relying on the discovery instrument utilized in the framework: inconsistency based, signature-based, specification based and hybrid.

- Signature-based approaches

  In Methodologies of signature based IDS recognize detects at framework system and conduct coordinates an attack signature saved in the IDS inner databases. If any framework or system movement equals with kept examples, at that point an alarm will be activated. Signature based IDSs are precise and exceptionally effective at distinguishing known threats, and their system is straightforward. But, this methodology is ineffectual to distinguish fresh assaults and variations of well-known assaults, due to a coordinating name for these assaults is as yet obscure.

- Anomaly-based approaches

  This built IDS ‘s think about the actions of a framework at a moment beside a typical conduct sketch and produces the caution at whatever point a deviation from ordinary conduct surpasses a edge. Methodology is effective to recognize new attacks, specifically, those attacks identified with maltreatment of assets. Nonetheless, anything that doesn't match to an ordinary behaviour is considered as an interruption and learning the whole extent of the typical behaviour is definitely else a straightforward assignment. Consequently, the technique for the most part has high false positive rates.

- Specification-based approaches

  Specification is a lot of standards and limits that characterize the normal behavior for organize segments, for example, hubs, conventions, and routing tables. This methodologies distinguish interruptions when system deviated from determination definition. Subsequently, this detection has a similar purpose of anomaly-based discovery: distinguishing aberrations from ordinary behaviour. But, there is one significant contrast among these techniques: in this methodologies, a human master ought to physically characterize the guidelines of every particular. Physically characterized specifications generally give lesser wrong progressive rates in examination with the difference built identification.

- Hybrid approaches

  Hybrid methodologies use ideas of specification based, signature based and anomaly based detection to expand their advantages and limit the effect of their disadvantages.

V. LITERATURE REVIEW

IoT have lot of methods to suggested by research. In this scenario, short-term evaluations of some main contributions to the present techniques are presented.

Author	Methodology employed	Dataset	Advantage	Limitation	Performance measure
A. Iqbal, et al., [23]	developed an interoperable IoTs podium for a nifty home-based scheme using a Web-of-Objects (WoO)	Cloud Database storage	The method aimed to decrease the humanoid interference, protected admission controller for home-based procedures from anyplace, provide smart homes data for application services as well as for investigation, and improved the use of assets.	The user's home data can be saved into the cloud server, but the safety of the records in cloud is the bottleneck of this method.	Scalability
S. Shokrollahi, and Fereidoon Shams, [24]	(RDS) method to qualify an accessible and active incorporation of varied devices in IoT.	Real world dataset	The proposed methodology misuses the (DDS) middleware for distribute buy in, information driven, constant, and approximately coupled correspondence between device-services. The method provides scalability, elasticity, availability, dynamic, and anonymity for integration of devices in IoT.	1. The method provides maximum-response-time of connector’s needs. 2. The performance of the method was affected by data-latency of a topic, because this idleness relies upon the quantity of its endorsers, the size of its information tests and the distribution pace of its information tests.	Response time of requests

J. V. Espí-Beltran, et al., [25]	Implemented a lightweight Service Oriented Architecture (SOA) model dependent on the utilization of RESTful style for structure and displaying of mechanical procedures.	Real world dataset	The strategy had a preferred position of streamlining the system traffic by presenting the non-concurring model versus synchronous execution dependent on surveying.	The burden of the technique was the reaction time determinism was transformed as the size of the HTTP messages were expanded.	Mean time per GET requests, parallel requests workload.
P. Diogo, et al., [26]	The work concentrated on the M2M/IoT engineering guidelines and conventions, and actualized to tackle the current IoT issues for accomplishing a definitive imagined IoT.	Real world dataset	The strategy gives the significance of structuring explicitly customized for IoT correspondence conventions so as to help continuous applications, in addition, the method offers flexibility and scalability capacity.	There was no ensured protection at the gadget space region, in addition this was an issue for every single compelled gadget and the Arduino was not an exemption.	Traffic comparison such as total number of messages, different factors and total session
A. E. Khaled, and S. Helal, [27]	presented the Atlas IoT communication framework	Real world dataset	The proposed Atlas correspondence system empowers the genuine support of varied things in a cool interplanetary with slightest humanoid mediation and the consistent combination of novel possessions.	The method was lacked in security, reliability and performance.	Scalability, time difference, energy consumption
Hyun Cheon Hwang, et al., [28]	Designed a reliable transmission system using MQTT protocol	Real world dataset	The reliable message transmission framework customer module checked message's succession before handling the messages and demands the past message if there were missed messages to hold the messages requesting	The gadget for home control required precise message transmission to cell phone for sending accurate message to control home hardware.	Message response time, message missing rate, CPU usage per each process.
Augusto Ciuffoletti [29]	defined an OCCI-IoT approach based on the principles of openness and expandability.	Real world dataset	The verification of-idea model portrayed in the technique was effectively reproducible and concentrated on the issues of the strategy.	The method had a bottleneck for security, reliability and performance	Clock drift, round-trip frequency, apparent delay
Z. B. Babovic, et al., [30]	Hypertext Markup Language (HTML5) specifications Web Socket and Canvas graphics	Public database	HTML5 platform is very skilled of running real-time IoT Web applications	The strategy repacking the Protocol Buffer messages into a string, in any case, except if the most brief message sizes are acquired, hence the technique did not enhance the latency, for the most part as a result of the information representation incompatibilities of the utilized systems.	Rendering Time, Decoding Time and Transmit Time
P. Fremantle, and B. Aziz, [31]	Oauthing DidP model	Public database	Every client's information is taken care of by an individual cloud example giving improved security and disconnection, just as giving a believed middle person to the two gadgets and cloud administrations.	The method mainly concentrated on user privacy of data, but the cost per user is too high.	Mean Latency, Time and energy taken to bootstrap, consumption of power
B. Agyemang, et al., [32]	Resource-oriented Device Management and service enablement architecture (IoT DM)	Public database	The methodology handles gadget portrayals as assets which are uncovered and oversaw through uniform APIs notwithstanding gadget specifc network conventions.	The correspondence administration segment of the actualized DM stage and embrace administration ontologies were not streamlined	percentile value of time response and normal median

L. Hou, et al., [33]	blend of the HTTP and MQTT servers to suggestion IoT profits in the design of the IoT cloud	Redis cluster database and SQL and NoSQL databases	The presentation results exhibited the noteworthy effect of the quantity of customers and CPU centers on the CPU use and other paramter assessment for the HTTP and MQTT servers, individually	There is an absence of well-characterized guidelines to bind together fluctuating models and interfaces of the IoT cloud.	Average response time, Throughput, Average CPU utilization, Average transmission latency

VI. CONCLUSION

IoT has made exclusive standards because of its ability of changing basic things of various application areas keen on Internet hosts. But, aggressors can exploit the IoT incredible potential as another approach to compromise clients' protection and safety. The proposed IDS system are very easy to extend. There are various potential assaults against the IoT and all things considered, more assaults will be found. The area data of hubs will likewise alleviate the Sybil and Clone ID assaults and will improve its interruption recognition abilities Thus, security answers for IoT should be made. As in conventional systems, the IDS is most significant security apparatuses for IoT. In our paper, we introduced a study about IDS research efforts for IoT. We proposed a scientific categorization to arrange these papers, which depends on the accompanying traits: recognition technique, difficulties and issues of IoT. We saw that the exploration of IDS schemes for IoT is as yet beginning. The proposed arrangements don't insurance a extensive scope of assaults and IoT advances. In addition, iis not strong which recognition strategies are increasingly sufficient for IoT frameworks. As upcoming research, specialists might concentrate on the accompanying issues: (1) to examine solid and weak purposes of various location strategies; (2) to expand the attack discovery range; (3) to address more IoT advances; (4) to improve security of alert traffic and the executives; and (5) to grow supplementary requests, for example, aware connection then autonomic administration frameworks

REFERENCE

[1] S. N. Han, and N. Crespi, “Semantic service provisioning for smart objects: Integrating IoT applications into the web”, Future Generation Computer Systems, 2017.

[2] T. K. Hui, R. S. Sherratt, and D. D. Sánchez, “Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies”, Future Generation Computer Systems, 2016.

[3] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, “Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes”, Future Generation Computer Systems, 2016.

[4] H. J. Yim, D. Seo, H. Jung, M. K. Back, I. Kim, and K. C. Lee, “Description and classification for facilitating interoperability of heterogeneous data/events/services in the Internet of Things”, Neurocomputing, 2017.

[5] A. G. Kumbhare, Y. Simmhan, M. Frincu, and V. K. Prasanna, “Reactive resource provisioning heuristics for dynamic dataflows on cloud infrastructure”, IEEE Transactions on Cloud Computing, vol. 3, no. 2, pp. 105-118, 2015.

[6] W. Wang, S. De, G. Cassar, and K. Moessner, “An experimental study on geospatial indexing for sensor service discovery”, Expert Systems with Applications, vol. 42, no. 7, pp. 3528-3538, 2015.

[7] N. Sophatsathit, "An IoT Solution for Reliable Internet-Based Services," Journal of Software Engineering and Applications, vol. 11, no. 03, pp. 129, 2018.

[8] J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim, “Secure IoT framework and 2D architecture for End-To-End security,” The Journal of Supercomputing, pp. 1-15, 2016.

[9] G. Gardašević, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović, and M. Radonjić, “The IoT architectural framework, design issues and application domains,” Wireless Personal Communications, vol. 92, no. 1, pp. 127-148, 2017.

[10] Dipa Soni, and Ashwin Makwana, "A SURVEY ON MQTT: A PROTOCOL OF INTERNET OF THINGS (IOT)," Proceedings of the International Congress on Information and Communication Technology. Vol. 6. 2016.

[11] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” IEEE Sens. J., vol. 13, no. 10, pp. 3558–3567, Oct. 2013.

[12] S. Krco, B. Pokric, and F. Carrez, “Designing IoT architecture(s): A European perspective,” in Proc. IEEE WF-IoT, pp. 79–84, 2014.

[13] EU FP7 Internet of Things Architecture Project, Sep. 18, 2014. [Online]. Available: http://www.iot-a.eu/public.

[14] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, “Study and application on the architecture and key technologies for IOT,” in Proc. ICMT, pp. 747–751, 2011.

[15] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, “Research on the architecture of Internet of Things,” in Proc. 3rd ICACTE, vol. 5, pp. 484-487, 2010.

[16] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges,” in Proc. 10th Int. Conf. FIT, pp. 257–260, 2012.

[17] M. A. Chaqfeh and N. Mohamed, “Challenges in middleware solutions for the Internet of Things,” in Proc. Int. Conf. CTS, pp. 21–26, 2012.

[18] L. Tan and N. Wang, “Future Internet: The Internet of Things,” in Proc. 3rd ICACTE, vol. 5, pp. 376-380, 2010.

[19] [19] D. Uckelmann, “Performance measurement and cost benefit analysis for RFID and Internet of Things implementations in logistics,” in Quantifying the Value of RFID and the EPCglobal Architecture Framework in Logistics. New York, NY, USA: Springer-Verlag, pp. 71–100, 2012.

[20] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of IoT: Applications, challenges, and opportunities with china perspective,” IEEE Internet Things J., vol. 1, no. 4, pp. 349–359, 2014.

[21] Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons vol. 58, no. 4, pp. 431-440, 2015.

[22] Chen, Yen-Kuang. "Challenges and opportunities of internet of things." Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific. IEEE, 2012.

[23] A. Iqbal, F. Ullah, H. Anwar, K. S. Kwak, M. Imran, W. Jamal, and A. ur Rahman, “Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud,” Sustainable Cities and Society, vol. 38, pp. 636-646, 2018.

[24] S. Shokrollahi, and Fereidoon Shams, "Rich Device-Services (RDS): A Service-Oriented Approach to the Internet of Things (IoT)," Wireless Personal Communications vol. 97, no. 2, pp. 3183-3201, 2017.

[25] J. V. Espí-Beltrán, V. Gilart-Iglesias, and D. Ruiz-Fernandez, “Enabling distributed manufacturing resources through SOA: The REST approach”, Robotics and Computer-Integrated Manufacturing, vol. 46, pp. 156-165, 2017.

[26] P. Diogo, N. V. Lopes, and L. P. Reis, “An ideal IoT solution for real-time web monitoring,” Cluster Computing, vol. 20, no. 3, pp. 2193-2209, 2017.

[27] A. E. Khaled, and S. Helal, "Interoperable communication framework for bridging RESTful and topic-based communication in IoT," Future Generation Computer Systems, 2018.

[28] Hyun Cheon Hwang, JiSu Park, and Jin Gon Shon, "Design and implementation of a reliable message transmission system based on MQTT protocol in IoT," Wireless Personal Communications, vol. 91, no. 4, pp. 1765-1777, 2016.

[29] A. Ciuffoletti, "OCCI-IOT: an API to deploy and operate an IoT infrastructure", IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1341-1348, 2017.

[30] Z. B. Babovic, Jelica Protic, and Veljko Milutinovic, "Web performance evaluation for internet of things applications." IEEE Access vol. 4, pp. 6974-6992, 2016.

[31] P. Fremantle, and B. Aziz, "Cloud-based federated identity for the Internet of Things." Annals of Telecommunications, pp. 1-13, 2018.

[32] B. Agyemang, Y. Xu, N. Sulemana, and H. Hu, “Resource-oriented architecture toward efficient device management for the Internet of Things,” Journal of Ambient Intelligence and Humanized Computing, pp. 1-13, 2018.

[33] L. Hou, S. Zhao, X. Xiong, K. Zheng, P. Chatzimisios, M. S. Hossain, and W. Xiang, “Internet of things cloud: architecture and implementation,” IEEE Communications Magazine, vol. 54, no. 12, pp. 32-39, 2016.

[34] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." Wireless Personal Communications 104, no. 1 (2019): 1-20

[35] Raj, Jennifer S., S. Smys, G. Josemin Bala, B. Praba, R. Sujath, V. Hilda Christy Gnanam, M. Abdul Rahiman et al. "Editorial Board v-vi A Novel Classification via Clustering Method for Anomaly Based Network Intrusion Detection System 1-6 Mrutyunjaya Panda and Manas Ranjan Patra Performance Improvement in MANETs: A Cross Layer Approach via TCP 7-11.".