Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 13, February 2018 – www.caeaccess.org

Review of Research Approaches for Securing Communication in Internet of Things

Shamshekhar S. Patil
AssociateProfessor
Department of Computer Science & Engineering
Dr. AIT, Bengaluru, India

N. R. Sunitha, PhD
Professor
Department of Computer Science Engineering
SIT, Tumkur, Karnataka, India

ABSTRACT
With the advent of Internet-of-Things (IoT), the communication has become very much ubiquitous with a faster response by supporting pervasive application demands. However, its resistivity towards adversary is still flawed with its existing security techniques. Owing to the novel nature of IoT, there have been various initiating attempts to introduce secure communication schemes for offering better security features to a diverse range of applications in IoT. This paper contributes to discuss existing research trend towards secure communication among the devices in IoT. The discussion present in the paper is anticipated to assists a snapshot of existing methods and approaches to research-based techniques in IoT.

Keywords
Authentication, Actuators, Internet-of-Things, Security, Sensors

1. INTRODUCTION
The term IoT is relevant to objects, things and virtually represented internet structures which are uniquely identifiable were first presented in the year 1998. The recent years have shown that the interpretability of IoT has become especially famous via various applications. The four significant components pertained to a system enabling IoT are sensors, access to unrelated information, services and requests and additional parts like privacy and security [1].The physical objects are equipped with the Radio-Frequency Identification (RFID) as tagged identification or as smart sensors identifiable bar-codes. Smart services can be designed in the IoT devices as a combination of sensors [2]. The practical deployment of IoT technique in the development of multiple platforms serving as new programs and technologies involving process, device identification, monitoring actuating, sensing, communicating, sensing the computations, processing the semantic knowledge, distributing the coordinated control and user modeling. Many limitations in the IoT subsystems are energy, lifetime, power, cost effectiveness. Security of IoT is of essential importance as the scope of spreading malicious attacks can be widely spread the world and would be actuated to the physical world from the service of the internet [3]. Technologies of Wireless Sensor Networks, RFID, Machine-To-Machine Interface (M2M) and services accomplished via a cloud computing serve as essential building blocks for IoT to achieve the desired application operation [4]. The infrastructure of IoT is very vulnerable to security issues and also addresses significant privacy drawbacks for the user end interface. With this, the IoT possessing advanced capacities in the area of information exchange is constrained from the security view of perception and appropriate steps need to be initiated to ensure that its development is an active process having a full acceptance overall [5]. Automatic verification of the object presence is improved by processing the image, storage capabilities and different display methods, availability of sensors and the reducing hardware cost would be the foundation for the new era possible by IoT. The interpretability of the perception embedded interaction that would seamlessly unite phenomena into everyday artifacts. It needs sensing in integrated perspective, actuation, and standard networking objectives [6]. Smart connectivity is enabled in IoT with the growing presence of 4G-Long Termed Evolution (LTE) wireless internet access and Wi-Fi, the revolution in the network of communication and information is evident. The embedded intelligence has to be implied beyond everyday scenarios of mobile computing that utilizes portables and smart devices from the environment [7]. The original concept of IoT will also mean sophisticated connectivity of wireless sensor node with a cloud environment. The cloud environment consists of data centers and is highly distribute in its operation, while wireless sensor network works on the local environment. At present, the so-called concept of smart city doesn't use actual logic of wireless sensor networks as all the sensor nodes directly collect the information and forward to the gateway node. Such communication could also be bi-directional where a certain set of instruction could be furnished by a gateway node to its respective sensors. Hence, there is the good feasibility of intrusion from either side.

These paper discuses the survey on the security issues in the IoT realization. The article is categorized as: Section 2 discusses the background of the IoT with the illustration of its origin and the numerous issues faced by it. The existing methodologies giving a solution to the issues and proposed in the various fields are discussed in section 3. The survey of IoT appearing as emerging technology is shown in section 4. Section 5 shows the statistical study of IoT security challenges. Finally, the conclusion and future scope are presented in Section 6 and Section 7 respectively.

2. BACKGROUND
The name Internet of Things wasn't officially so until the year 1999. At the end of the year 2013, it had evolved into a system incorporating various technologies, including the ones ranging from the Internet to communicate in the wireless field and from MEMS to embedded systems. IoT (Fig.1) can be explored to increase the application providing capacity in multiple domains such as control systems, global positioning system, wireless sensor networks and automation.

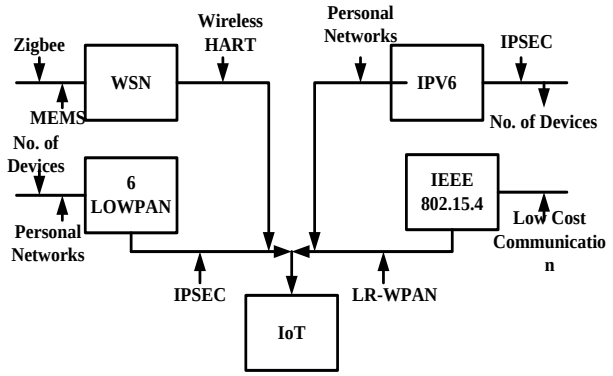

Fig 1: Block Diagram of IoT Background

The wireless connectivity and new techniques of digital identification like RFID got an impact of IoT on our daily lives. Due to the advancements in wireless sensor networks, and little energy, limited resource device have initiated more types of equipment that are internet connectable. To provide more addresses and unite multiple networks in the IoT environment IPv6 and IEEE 802.15.4 have been significant [8]. Here the following shows the number of security problems in IoT. As the focuses on the analysis of real-time extensive data, IoT is proved as an emerging technology. The massive amount of data is transferred to the DCNs; their underlying structures should be able to sustain the IoT data real-time processing necessities. Few open challenges are given as below:

- *Network Scalability***:** The conventional data center has three-tier topology more often to accommodate the networks of larger data centers. The architecture consists of three layers which are the access, core and aggregation layers. As the growth in the complexity and size of the increases, it leads to scalability challenges. The scalability issues arise when furthermore IoT data streams continue to flow into the warehouses. As it is one of the key essentiality to analyze the IoT real-time data, it can be solved by the approach of modular data centers. For the IoT analytics, the challenge of scalability is included with reconfiguration and real-time control of infrastructure for having an agile, routing, access monitor and addressing are a demand.

- *Network Delay:* In the present time analytics, the data flow between the switches and servers causing a delay in the system. Also, it occurs while the data is in the process of being accessed from the database. The tiered architecture of the data centers is the primary reason for a delay.

- *Spectral Efficiency Limitation:* The massive data creates another issue for efficient delivery of data in case of real-time analytics. To avoid this, they should utilize the available range of frequencies in the network. The wireless network should have the potential of taking charge of the controlling deadlines in an analysis of real-time scenario and the data flows. Spectral efficiency as a challenge will be ineffective if the network is performing the required task.

- *Fault Tolerance in the Network*: The functioning of an IoT system is possible only when it continuously operates even when a failure occurs for few of its components. IoT data needs a system to detect the faults and should possess the capacity of resisting it along with reporting a solution for the same.

- *Network Agility*—applying the concept of agility in network analytics, IoT can be met with the demand for scattered sensors shared over a large pool, giving real-time services. At the availability of spare capacities in the network, congestion and computation hotspots have higher priorities. The communication among the different paths of the networks is constrained [9].

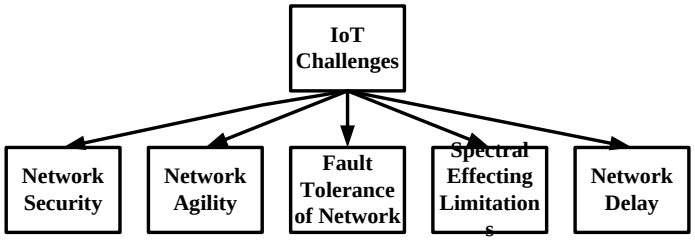

Fig 2: Open Challenges of IoT

Privacy and security challenges of IoT are as mentioned below:-

- *Authentication:* Due to the lack of memory and CPU operational power in IoT it's hard to initiate cryptographic functions needed for the authentication protocol. In a fog detecting device, the resource restricted devices will outsource computations and would further execute the protocol.

- *Privacy:* The IoT devices constrained regarding resource are not able to imply the signcryption or decryption of the data leading to the leakage of private user information in an environment containing usage, locality. The location privacy is another issue to be addressed here used for inferring the place of IoT device. For example- a mobile computing application, the adversary can understand data relevant to IoT device location dependant on the pattern of communication. Also, the reading in the smart meters can disclose IoT clients usage patterns when they are at their residence else when they turn on the television.

- *Detection of Rogue node:* An IoT node found to be malicious can claim to collect and exchange data developed by other IoT devices for malicious services. Since complexities are multiple in numbers for trust management, addressing the problems for the same is a task.

- *Intruder Detection:* Most of the current models in the service of IoT devices have low efficiency in recognizing the intruders. Designing such a system that would adequately identify the intrusion taking place, are complex to design. Ultimately the IT device requires a system that can efficiently work on large scale.

- *Data Protection:* As the number of devices increase, the data generated by them also vary exponentially in volume. The representation of data should take place both at processing and communication level. The limited resources are responsible for the handling of data on the devices which is a difficult job. The data integrity must be preserved throughout the stage analysis.

- *Trust:* No effective mechanism has been proposed to measure how accurate a particular IoT service is. To establish a secure environment, there is a necessity for managing trust between IoT devices to retain reliability and security of the service.

- *Access Control:* It's a technique to ensure that only entities having authorization can gain access to a particular resource like a collection of data or IoT device. Since an enormous

number of things are involved in the challenges of IoT, access control becomes a major issue of concern.

- *Other Challenges:* The mentioned security and privacy issue are not exhaustive and are illustrative. Few other problems faced for implementing an IoT system in a network are the management of key, computational verification and aggregation [10].

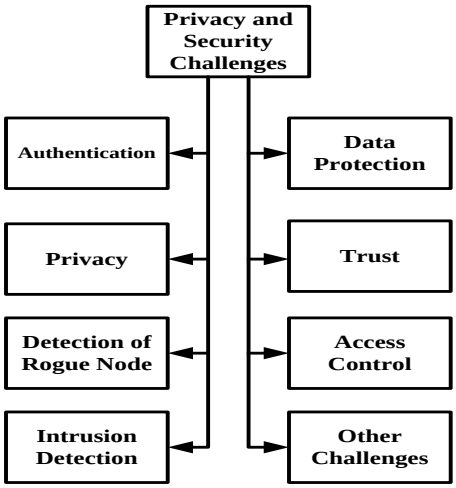

Fig 3: Privacy and Security Challenges in IoT

Fig.3 summarizes the core privacy problems in IoT. The principal issues of concern are:

- *User Authentication:* The operation of a device works on the default password for example- 1234, which everyone is aware of and hence possess a significant risk to the security. Few times theses will be configured to enable default passwords or usernames.
- *Insecure Interface:* The access of IoT –based solutions takes place through a web browser else by a mobile interface for the user level application. The interface having the mobile/web access may be prone to cross-site forgery attacks, cross-site scripting poor session management.
- *Insecure Code Practices:* The middle layer in the network might have problems concerning insecure coding of logical server and business.
- *Personal data Privacy Concerns:* The personal information of the user is usually stored in the IoT device like date of birth, number, name, etc. which is transferred over the network path without the risk of signcryption causing an extreme risk. Unwanted divulgence of the information from the user is accessed in an unauthorized manner.
- *Limited signcryption at the Transport Layer*: The hardware interpretation is very less for IoT devices, making it vulnerable to spoofing as a signcryption algorithm is not implemented [11].

3. EXISTING TECHNIQUES

The emergence of IoT has encouraged the growth in the count of devices in our surrounding and assures the possibility of dealing with a lot of applications. The principal challenge in the IoT is the realization of the interoperability between the devices and their deployments. At present, there are various techniques designed to incorporate IoT security, and therefore this section will only discuss some non-conventional and different from mainstream approaches.

At present, the focus toward IoT security has been emphasized using distributed features. One such unique architecture *Distributed Internet-like Architecture for Things (DIAT)* has been seen in the literature that leads to overcoming all the hindrances towards the progress of IoT expansion. The property of heterogeneity is addressed in the technique discussed for IoT and allows seamless new device addition across various applications. A usage control function method for promising security and privacy in the surrounding would be an advantage in the design. Dealing with the characteristics of IoT such as security, privacy, heterogeneity, scalability and operability in the device components, a level of abstraction is for each is described here.

To incorporate decision making capability, a general use-case is introduced, taking up elements from the domains of multiple applications. The architecture is mended for IoT applications, resembling that of service-oriented model wherein number of services from each service provider has to be united with human intervention being minimum. The different services are created and maintained via analyzing the service request, before executing it as illustrated in the block diagram.

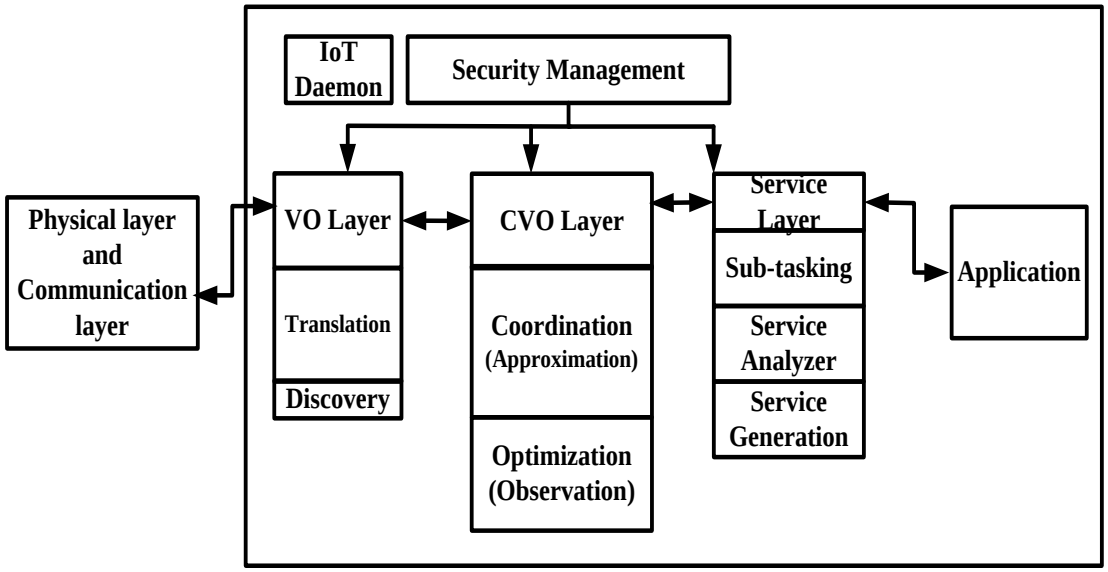

Fig 4: Architecture of DIAT

The three layers in the architecture are virtual object layer, the Composite Virtual Object Layer (CVOL) and Service Layer (SL) respectively. These three layers perform the task of creation and management of services, object virtualization and execution and service composition. Each layer of the architecture has the inbuilt set of cognitive functions to provide automation intelligence in IoT. Combination of all the three layers with their key features contributing to the structure are stacked and called as IoT Daemon. Here, the function of privacy and security maintenance is executed by Security Management cross-layer module.

Table 1: Comparison of Existing Techniques

IoT Parameters	IoT-A	Compose	Butler	DIAT
Layer design	No	Present	No	Present
Scalability	---	No	No	Present
Distributive property	---	No	Partially	Present
Automation	Present	Partially	Present	Partially
Heterogeneity	Present	Present	Partially	Present
Interoperability	Present	Partially	No	Present
Privacy and Security	Present	Partially	Present	Present

Many approaches were enabled to describe the architecture of IoT for smart applications, but a design that is holistic and comprehensive is required as shown in Table 1. The DIAT is compared with existing efforts which are proved to explore the potentiality of the challenges technically and key features of IoT [12].

In the domain of contact-less nature and data throughput from the smart devices such as health care systems employed with body sensor networks along with equipment that can be worn are presented. An IoT based health care management system is designed operating on body sensor networks. The concept of robust crypto-primitives is utilized to establish the communication path to provide particular authenticity feature and confidentiality, enabled in the objects for improving the efficiency of the system. Raspberry Pi model is involved in achieving the practical and feasible implementation of the presented health care system.

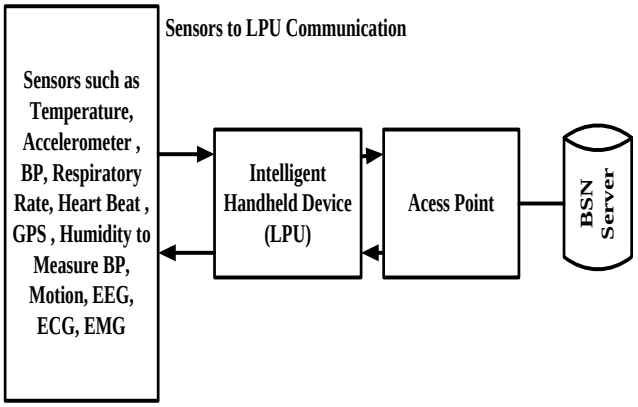

Fig 5: Presented Health Care System

In the above IoT model (Fig.5)for a health care system, three indispensable components used *are Body Sensor Networks server (BSN), Local Processing Unit (LPU)* and the smart objects which are wearable (bio-sensors). The data to be manipulated is taken by the user adopting the edge device for it. The data which is collected is transmitted to the LPU and later on to the BSN server for the purpose of analyzing the data with a provision for user-oriented service. The system will identify and satisfy the needs of the user individually more quickly and have a higher efficiency from the particular bio-data. The presented technique allows the body bio-sensors and LPU to execute the registrations for the BSN server in prior. After the registration is attained, the credentials such as security have to be shared and accumulated in the bio-sensors, BSN server, and the LPU. To have a goal of entity authentication, a path for secure communication and data integrity are guaranteed through the feature of system's interface. Further, to estimate the feasibility of the built scheme implementation in it happens over an IoT test-bed, i.e., a platform of Raspberry Pi model. The computational time of 4.056 ms and 4.965 ms is evaluated to perform two mechanisms of authentication by development platform in IoT. To improvise the system throughput, the replacement of the crypto-hash modules by the conventional SHA-2 method is accomplished [13].

For applications involving concepts of people flow, logistics flow, design interaction and money flow, IoT technology is implied. To maintain these growing device demand and their options in the connectivity, ETSI has to be mentioned too as the solution for the end-to-end M2M system. An Easy Connect system to have better management of the IoT devices is initiated based on the model of ETSI. The categorization of the devices linked via IoT happens based on its features which are display, temperature, and vibration and are altered by network applications.

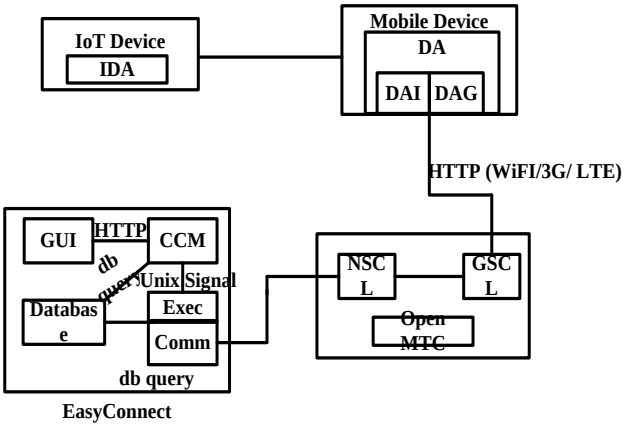

Fig 6: Easy Connect System

The technique of Easy Connect has four modules, the creation, configuration and management module which systematically will divide the characteristics of the IoT devices, balances the functions for automatically configuring the connectivity of the ODFs and IDFs, retains all the essential information in the Database module, i.e., SQL database. The module of Execution and communication is subdivided further into two modules called communication sub-module dealing the interactions of the lower layer M2M device for transferring/reception of the data to the IoT devices from the IDF/ODF. IoT objects are having a connection with Open MTC physically and transparently share resources with one another and through EC in network applications. The sub-module named Execution is held responsible for the requests in the network connected to ODFs and IDFs. The graphical user interface gives the user-friendly interface for the faster establishment of the interactions and connections in the devices of IoT. The operation of the desired task is attained by the graphical user interface which takes the data to be processed from the user to apply the HTTP based REST APIs to start up device functions, mapping roles and configuring the component connection. Employing the signals from the UNIX operating system, the CCM instructs to perform interaction among ODFs and linked IDFs in the IoT devices having the option of preset. The characteristics of the adopted methodology are used to generate the device feature modules which are created with fewer difficulties coding the design in the scripting language Python. Since in this language the execution is permitted without any compilation the ease of implementation is added to system design [14].

4. LITERATURE SURVEY

This section further elaborates the existing research approaches to secure IoT. The study of Shi et al. [15] emphasizes on signcryption as a cryptographic method for the simultaneous performance of signcryption and signatures digitally. It is an effective way as it does not permit the smart device to forget or leak the confidentiality of the communication channel in the system of IoT mostly when the produced cipher texts are converted into a compact form. Implementation of signcryption is very often threatened by the device attacks captured due to the unattended signals from them ensuring that the intruder acquires the cryptographic key from the instrument which is captured. With an obfuscator being accommodated in the signcryption algorithm, is designed by considering the cost of communication and computational speed that should be less to be custom fit in resource-limited embedded tools. The obfuscator can provide the shield for the signcryption programs retrieving the data from key-extraction attacks by transferring them into obfuscator programs. This happens to be the first aggregatable signcryption scheme which is obfuscated. The efficiency positioned for this project is at the middle level having the advantage of being economical when compared to other known-obfuscatable schemes. Also, the feature of enabling security makes the system more beneficial for utilization. In case of IoT, it has broad applications where information has to be forwarded to the sink point from the leaf nodes remained unattended.

In the study of Sajid et al. [16]), the aim is to reduce the operational expense of the industrial systems. Solutions were providing higher-end stability, tolerance in the fault and flexible are required to be designed for the support. The *Cyber-Physical System (CPS)* is one such technique that is the solution for the industrial systems majorly involving IoT along with the services of cloud computing. They are considered as the smart industrial system, with them being readily applicable in the field of eHealth care systems, smart grids, medical, transportation, etc. They mostly run on Supervisory Control and Data Acquisition (SCADA) systems to take charge over and monitor the Critical Infrastructure (CI). Traditional SCADA devices lack appropriate measure in security issues and hence with uniting the new architectures which are complex, the conceptualization of Mobile Sensor Wireless Sensor Networks (MWSN), cloud computing and IoT would face more challenges in security and classical system deployment in them.

Arshad et al. [17] present a methodology of Green IoT idea that intends on reducing the energy consumption of devices using IoT and keeping the environment safe. The different taxonomies that work in favor of the implying the Green Iot in the devices are software based green IoT, hardware-based green IoT, recycling, policy-based, awareness based and the habitat reformation towards green IoT. The influence of IoT on the economy is dominantly applied and is assumed to give an opportunity a revolution in the in the whole of ICT industry. The industry is the cause of 2% of entire CO_2 emission as reported by the IEEE Green ICT report and would double in the upcoming next five years. The Green IoT is highlighted as a function of the policy established, generic architecture and recyclable material for it.

The study of Yasin et al. [18] assures to revolutionize the sector of health care via non-invasive, continuous and remote monitoring of the patients. The two major challenges faced by the medical devices working on the principle of IoT are matter of security and privacy with energy throughput. Solutions such as low power processors of ECG and secure network protocols are the issues elaborated on these bases. Here the proposed system involves ventricular arrhythmia detection through ECG signals in a safe sensing IoT platform having ultra low-power.86% Accuracy rate is achieved when the presented method can analyze the onset of the threshold events in the cardiovascular field up to 3h. The technique is implemented utilizing an application specific integrated circuit as a function

of low-power enhanced technology; the power consumption is noted to be 62.2% lesser than that consumed in the addressed approach of state of the art, having 16% smaller area size. ECG signals are used for fulfilling the requirement of the input to extract the chip-specific ECG key that allows the protection of the communication path. By collaborating the ECG core with the solution of the existing trust design, protection at the level of the hardware is attained. Efficient resource sharing is acquired in the on-chip system providing 9.5% that for the area and 0.7% for the energy with no effect on the computational speed of the IoT device.

The study of Conti et al. [19] deals with the conceptualization of the near-sensor data analytics in the direction of IoT endpoints, since it reduces the energy spent on the network and the communication path, also poses concern towards security due to the valuable data being retained in the various stages of the analytics pipeline network. Incorporating the encryption method, the sensitive data is protected sat the boundary of the engine in the on-chip system to approach security issues. The combined workload is managed by Fulmine, a SoC performing the regular computing task, having a tightly- coupled cluster of multi-core augmented with block specializing in the processing of the intensive computer-data and functions of encryption. The fabrication is done using 65-nm technology, consuming a power range lesser than 20 mW on an average of 0.8V pertaining efficiency of 70pJ/B for encryption, 50pJ/px for convolution and up to 25MIPS/mW in case of software. Three cases are considered security analysis namely, electroencephalogram at 12.7pJ/op for seizure detection of encrypted data collected, face detection along remote recognition based on local *Convolution Neural Network(CNN)*, from the state-of-the-art-device having 3.16pJ.

The study of Cheng et al. [20] discusses the mobility features and technologies in the communication domain with the constraint of the malware propagation, exploiting new challenges in the cyber security of IoT empowered malware. The difficulty arises in the process of patching the end devices under IoT when compared to those in the where nodes have the capability of directly getting repaired. As an alternative, blocking the malware through patch process enables the turning out of the result being more feasible and practical. In particular patch, nodes can in the intermediate of the function prevent the malware propagation proliferation by enabling security links infrastructure and minimizing the malware propagation in the dissemination of the device-to-device communication. A scheme to choose the useful intermediate nodes to patch, which implies to the IoT system with limited patching resources and time of response is limited. As a result, it was demonstrated that the advantage of alleviated malware propagation is obtained with the scheme of presented traffic-aware patching.

The study of Koteshwara and Das [21] show that all the connected device pose a complex challenge for the cryptographic designers by improvised robustness, flexibility, area, and resources. Few authentication schemes named as *Authenticated Encryption (AE)* giving the option of robustness, applicability, and security with the estimation of the lightweight applications are used integrating sensor networks, IoT, implantable wearable and medical devices, IPSec and RFID. Properties such as resistance to noise misuse, the measure of security, parallelizability and few different applications were explored.

The study of Kubler et al. [22] introduces the concept of smart cities as a part of a complex ecosystem that consists of multiple stakeholders such as network operators, logistic centers, service providers who must be united to give the most suitable services and be in a position to unlock the IoT potential. This intending to be one of the major issues in the smart city movement emerges with API Economy. The vertical silos are fed in the market to the objects as they are assumed to handle IoT, thus giving an opportunity to the developers for adding new value across different platforms and various domains. It has the current strategic vision and ambition of the EU to solve the threshold vertical silos problem, introducing the initial building blocks of an open ecosystem generated from IoT as a part of EU project and collaborated with its initiative. Hence the analysis of the performance is accomplished by the proof-of-concept for event management in sporting in the context of upcoming game of FIFA to be held in Qatar in 2022

In the study of Kwon et al. [23], a methodology for the system health industrial application management based on IoT is initiated. A discipline that uses sensors is Prognostics and System Health Management (PHM) to enable the access of health care systems in diagnosing the anomalous behavior and proceeds for the prediction of the remaining useful performance as life asset. The appearance of IoT qualifies PHM for its application to all kinds of assets present in all the sectors and therefore making a scope of the paradigm shift that has to open up new significant opportunities in the business field. The enactment of the IoT based PHM needs the needs in the human capital in abundance, maintenance necessities for the prognostics and communities of engineering, statistics, and machine learning ability to establish. Anomalous pattern recognition for information to detect the node failure that can make a connection to the underlying physics of failure is expected as a characteristic. Big data faces the problem of finding relevant information called spurious correlation. PHM generated based on IoT is supposed to have the notable influence on the execution of the reliable assessment, predicting nature, mitigation for risk and developing new business opportunities.

The study of Hennerbert and Santos [24] shows the application of IoT on the internet to send the data, private information over the web. It is essential to have a security protocol for the transferred data and the unique identities that might be disclosed for them to be made the function with the population of the citizens. Since the mechanism of security employed widely on the internet is large to be integrated on the little-restricted devices. The study involves in the protocols presently required and the solution in the security deployed for the limited resources. The advantages of the easy would be security extension in *Time Synchronization Channel Hopping (TSCH)*, compressed version IPsec and embedded level design in several levels of the OSI model to be implied in the 6LoWPAN attack from DTLS. The issue of privacy as a matter of concern is addressed followed by how successfully the information can be hidden and identity of the device is remained unrevealed. Key is established, and the negotiation in the cipher suite remains a concern, the compressed IPsec would give a source for authentication and confidentiality in the data with an added message overhead cost. Emerging from LoWPAN, Datagram TLS offers tools to secure the application layer. Security schemes are available in the real-time system and the challenges to be dealt in the future such as reducing the size of the packet and bandwidth optimization.

5. STATISTICS OF STUDY OF SECURITY ISSUES IN IOT

Although IoT is a theoretically 5 years old concept, buts it 100% implementation in the form of application cannot be seen today. We carry out a quick check on the existing research trend on IoT security to find that there are very less technical journals to introduce any robust, standard, and novel solution to security threats in IoT. Fig.7, Fig.8, and Fig.9 highlight the existing research trends.

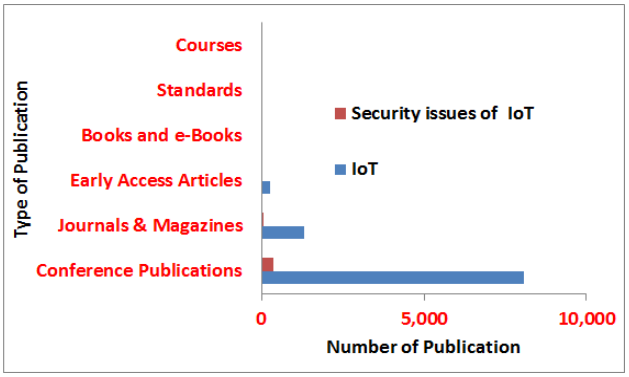

Fig 7: Research Trend (Source: IEEE Xplore)

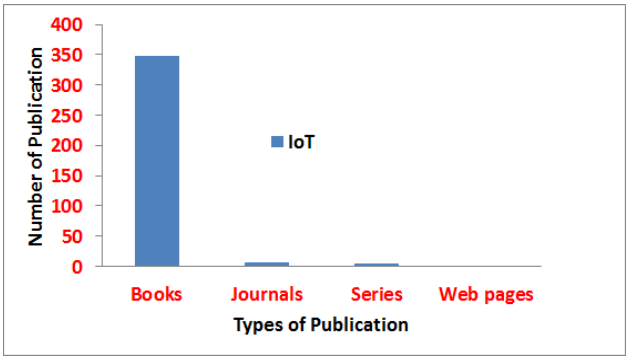

Fig 8: Research Trend (Source: Springer)

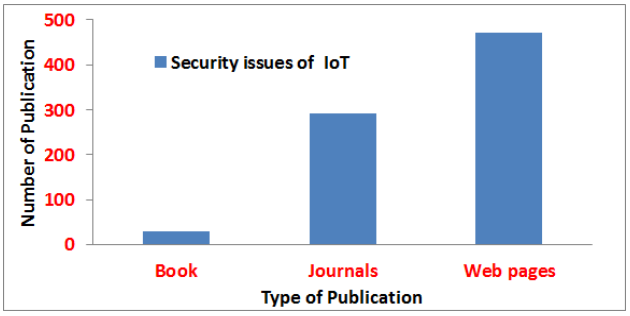

Fig 9: Research Trend (Source: Elsevier)

Therefore after reviewing the existing literature and its trends, we conclude following research gap:

- *Vulnerable usage of Cryptography*: According to the existing research approaches, the cloud environment is more secured using cryptography of complex architecture; however, such forms of encryption is never possible in resource constraint nodes. Hence, good security comes at the cost of communication degradation in the form of latency as well as reduced longevity of network lifetime. In short, existing cryptographic implementation over cloud is not feasible in securing communication from sensor nodes.
- *Error-prone Public Key Encryption*: Existing system also leverages the utilization of public key encryption as it is widely supported by wireless sensor nodes. However, some of the public scheme, e.g., elliptical curve cryptography are not reported much about their limitation. Such schemes although offer reduced key sizes, they cannot offer protection from message forgery attacks which are very frequent in denial of service attack over cloud. In short, it means the most advocated public key encryption will require amendments.
- *Less Emphasis on Sensor's Processing Capability*: Irrespective of deploying homogeneous or heterogeneous forms of the sensor nodes, the networking, and processing capability of each node degrades with progress of time owing to resource depletion. There is no much research work being carried out to emphasize this aspect. The processing capability of sensor matters when it comes to secure routing scheme. Low processing sensors are incapable of processing emergency message update and thereby can invite intrusion. Such intrusion could be avoided by identifying and replacing the low to high processing sensors. However, there is no such work in this direction.

6. CONCLUSION

In an environment of immense growth towards connected and automated gadgets, the entire world can be considered as a vast network of devices having the ability to communicate with each other. The IoT refers to the pervasive environment of computing wherein sensors and actuators are made to work with the Internet and not only computers and smart devices. In the implementation of it, security challenges of the methods and collaborated techniques have a play an original role. In the paper, we discuss the background, challenges concerning open, privacy, security aspects. Further, the existing techniques for the employment of IoT in various disciplines are highlighted. The paper conclusion emphasizes on the different works implemented in the IoT and associated domains.

7. FUTURE SCOPE

As the technology is progressing more and more with the days passing by, the internet access is in every corner of the globe is possibly achievable and so is the future of IoT emerging for the same. The current world requires having better connectivity progress, and hence this gives an opportunity to the IoT as a means of a vital instrument for interconnecting objects. In future, it will be able to bring changes such as reporting, monitoring, access to information, easier commutation and connectivity.

8. REFERENCES

[1] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," *International Conference on Computer Science and Electronics Engineering*, Hangzhou, pp. 648-651, 2012

[2] R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 10th International Conference on Frontiers of Information Technology, Islamabad, pp. 257-260, 2012

[3] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, pp. 417-423, 2014

[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks 57.10, pp.2266-2279, 2013

[5] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of Internet of Things," arXiv preprint arXiv:1501.02211, 2015

[6] M. Kranz, P. Holleis, and A. Schmidt, "Embedded interaction: Interacting with the internet of things," *IEEE internet computing*, vol. 14.2, pp.46-53, 2010

[7] J. Gubbi, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29.7, pp.1645-1660, 2013

[8] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," Telecommunication Systems, pp.1-19, 2017

[9] S. Verma, "A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues," *IEEE Communications Surveys & Tutorials*, 2017

[10] A. Alrawais, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Computing*, vol. 21 (2), pp. 34-42, 2017

[11] A.K. Pathak, "Security Challenges in Internet of Things (IoT)," International Journals of Advanced Research in Computer Science and Software Engineering, 2017

[12] C. Sarkar, "DIAT: A scalable distributed architecture for IoT," *IEEE Internet of Things Journal*, vol. 2(3), pp.230-239, 2015

[13] K-H. Yeh, "A Secure IoT-Based Healthcare System with Body Sensor Networks," *IEEE Access*, vol. 4, pp.10288-10299, 2016

[14] Y-B. Lin, "EasyConnect: A management system for IoT devices and its applications for interactive design and art," *IEEE Internet of Things Journal*, vol. 2(6), pp.551-561, 2015

[15] Y. Shi, "An Obfuscatable Aggregatable Signcryption Scheme for Unattended Devices in IoT Systems," *IEEE Internet of Things Journal*, 2017

[16] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp.1375-1384, 2016

[17] R. Arshad, "Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond", *IEEE Access*, 2017

[18] M. Yasin, "Ultra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases," *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2017

[19] F. Conti, Francesco, "An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics," *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2017

[20] S-M. Cheng, "Traffic-aware Patching for Cyber Security in Mobile IoT," *arXiv preprint arXiv: 1703.05400*, 2017

[21] S. Koteshwara and A. Das, "Comparative study of Authenticated Encryption targeting lightweight IoT applications," *IEEE Design & Test*, 2017

[22] S. Kubler, "Open IoT Ecosystem for Sporting Event Management," *IEEE Access*, vol. 5, pp.7064-7079, 2017

[23] D. Kwon, "IoT-based prognostics and systems health management for industrial applications," *IEEE Access*, vol. 4, pp.3659-3670, 2016.

[24] C. Hennebert and J.D. Santos, "Security protocols and privacy issues into 6LoWPAN stack: a synthesis", *IEEE Internet of Things Journal*, vol.1(5), pp. 384, 2014.