A REVIEW ON AUTHENTICATION AND SECURITY PROCEDURES FOR IOE SYSTEMS.

[1]Mr. Amit Jaykumar Chinchawade, [2] Dr. O.S. Lamba,
[1] Research Scholar, [2] Professor, H.O.D,
[1,2] Department of Electronics & Communication Engineering
Suresh Gyan Vihar University, Jaipur, Rajasthan, India.

Abstract : Internet of Everything (IoE) is bringing together people, process, data, and things to make networked connections more relevant for exchanging the information , controlling the devices and getting data from various wireless sensor networks to monitor and study the various parameters for controlling and managing the various dependant things connected with IOE. IOE provides unprecedented economic opportunity for businesses, individuals, and countries. Security and privacy in Internet of Everything (IoE) is a major challenge, mainly due to the massive scale and distributed nature of IoE networks. Robust authentication and security procedures in IoE is need of time and we propose to achieve such procedures in our research work.

IndexTerms - Internet of Everything (IoE) , IOT (Internet Of Things), Attribute-Based Encryption (ABE), differential power analysis (DPA), ZigBee Light Link (ZLL), low-power wireless personal area networks (LoWPANs), HomeKit Accessory Protocol (HAP).

I. INTRODUCTION

CISCO defines the Internet of Everything (IoE) is the intelligent connection of people, process, data and things .The Internet of Everything (IoE) describes a world where billions of objects have sensors to detect measure and assess their status; all connected over public or private networks using standard and proprietary protocols.

Moreover, even if Cisco tends to depict the Internet of Everything as a next stage in the Internet of Things, it is as much related with the Internet of Things

. In addition, IoE further advances the power of the Internet to improve business and industry outcomes, and ultimately make people's lives better by adding to the progress of IoT.

Internet of Everything (IoE) is a latest technology which has good number of benefits to its users. It's an emerging technology where we connect daily objects to the internet for sending and receiving data. In recent years, the Internet of Everything (IoE) has received considerable research attention. The IoE is considered as future of the internet. In future, IoE will play a vital role and will change our living styles, standards, as well as business.

There is need of a dynamic authentication mechanism for mobile users are needed to protect against unauthorized access. To securely exchange information with fast computing speed, symmetric encryption scheme can be used. Although it uses only one secret key for two communicating parties, key agreement protocol to agree on a shared key or key distribution protocol is required. These protocols introduce security requirements such as authentication of parties in key agreement protocol or secure and integrity-assured key distribution to prevent man-in-the-middle attacks and other attacks. Without the use of public-key cryptography, symmetric key scheme is not sufficient to get secure communication features such as confidentiality, integrity, authentication, and non-repudiation.

II. LITERATURE SURVEY

In [1] author have addressed Built upon the Internet of Everything (IoE) acknowledges the importance of data quality within sensor-based systems, alongside with people, processes and Things. Nevertheless, the impact of many technologies and paradigms that pertain to the IoE is still unknown regarding Quality of Observation (QoO). This paper proposes to study experimental results from three IoE-related deployment scenarios in order to promote the QoO notion and raise awareness about the need for characterizing observation quality within sensor-based systems.

In [2] author have addressed Internet of Everything (IoE) trend especially in homes. Marketing forces towards smart homes are also accelerating the spread of IoE devices in households. An obvious danger of rapid adoption of these gadgets is that many of them lack controls for protecting the privacy and security of end users from attacks designed to disrupt lives and incur financial losses. Goal for this paper is to develop an IoE threat model geared specifically for home users who are often unaware of the privacy and security threats which the IoE appliances pose. Goal of this paper is to propose an effective solution to alerting users of imminent IoE security threats and offering actionable steps to mitigate them through an intuitive and friendly user interface design.

In [3] author have presented a energy consumption accounting for around one-third of the total primary energy in the world. A building energy management system (BEMs) is an efficient method used for monitoring and controlling a building's energy needs. To solve these existing issues of the current building energy management system such as the large amounts of BEMs energy data, energy data loss and energy overload problems, a BEMs based on Internet of Energy (IoE) has been proposed. In this paper, we will give the potential of IoE-based BEMs for enhancing the performance of building energy utilization in the future.

In [4] author have addressed the investment on Internet of Everything is increasing exponentially. This new global technological approach opens the doors for connecting everything and anything. Such massive propagation of Big Data generated from a wide variety of sensors requires consolidated efforts to put forward solutions to address specific related business problems and needs. The aim of this paper is to provide a systematic review of the state-of-the-art scientific research on the Internet of Everything and Big Data.

In [5] author have describes how in a very short time, the Internet has dramatically changed how we work, live, play, and learn. Yet, we have barely scratched the surface. Using existing and new technologies, we are connecting the physical world to the Internet. It is by connecting the unconnected that we transition from the Internet to the Internet of Everything (IoE). Internet of Everything has top five applications; Traffic monitoring, Healthcare, Security, Transport and logistics, and Daily life. Therefore, in this paper, we proposed an architectural framework to monitor the health of a patient with a diabetic illness in proactive and reactive monitoring behavior. This type of patients have difficulty maintaining healthy glucose levels which can be lead to a diabetic coma, where a patient becomes unconscious, and can die if left untreated. In the proposed system a patient has registries in the health monitoring company (HMC) to help him avoid diabetic comas and emergency visits to the hospital. He wears a continuous glucose monitoring (CGM) device and a fitness tracker to monitor his exercise level and respiration. Based on the type of data transmission; proactive or reactive, these devices will process and provide the data for the health monitoring company to take the correct action when patient's state of health moves outside normal range. Finally, the proposed model was simulated by using Packet tracer 7.

In [6] author have describes, the networked connection of people, things, processes, and data is called the Internet of Everything (IoE). It is projected to provide high revenues to many companies due to the increase of work efficiency, as well as the increase of security and comfort of workers. The sector-specific infrastructures where the IoE is successfully implemented are smart grid, critical infrastructure management, smart homes, smart manufacturing, and smart meters, among others. IoE is based on near Internet ubiquity and includes three types of connections: machine-to-machine, person-to-machine, and person-to-person. Machine-to-machine is closely related to security, including civil security (e.g., security on the road, disaster alert) and military security. Person-to-machine communication brings an unquestionable increase of well being in home automation systems but is also fundamental for intelligent parking, patient monitoring, and disaster response, among others. Person-to-person connection is already changing interpersonal relations, which are becoming more multimedia- centric and located in social networks. IoE will increase the scenarios of person-to-person networked communication; for example, telework, networked learning, and telemedicine.

In [7] author worked on an The current prominence and future promises of the Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT) are extensively reviewed and a summary survey report is presented. The analysis clearly distinguishes between IoT and IoE which are wrongly considered to be the same by many people. Upon examining the current advancement in the fields of IoT, IoE and IoNT, the paper presents scenarios for the possible future expansion of their applications.

In [8] author have addressed Identification, Authentication and device diversity are the real security and protection concern in IoT. This paper discusses critical issues related to safety and privacy of IoT.

In [9] author have presented an end-to-end view of IoT security and privacy and a case study. Our contribution is twofold. Firstend-to-end view of an IoT system and this view can guide risk assessment and design of an IoT system. Have identified various attacks that can fully control all the cameras from the manufacturer. Real- world experiments demonstrate the effectiveness of the discovered attacks and raise the alarms again for the IoT manufacturers.

In [10] author have addressed the proposed and existing methods and are reviewed. Based on this survey, the research gap in the security issues is identified.

In [11] author have proposed a robust, lightweight and energy-efficient security protocol for the WSN systems. The real tests we made and a performance evaluation of our security protocol are provided.

In [12] author have addressed new directions and ideas for research in the ever vibrant fields of telecom and IoT security. It attempts by no means to present a complete set of security solutions; this would be by definition impossible. It rather serves as a short but comprehensive introduction to various technologies and cryptographic techniques in the area of lightweight cryptography in our quest to address the security challenges in the IoT and 5G-connectivity era. We use the term lightweight cryptography interchangeably both for symmetric and suitable asymmetric ciphers, thus covering all aspects of traditional cryptography namely encryption/decryption, authentication, identification, nonrepudiation, integrity protection, and key exchange. Possible use cases that challenge the applicability of lightweight cryptography as well future projections for further discussions are also offered.

In [13] author have presented a prototype for a lightweight, secure application level protocol wrapper that ensures communication consistency, secrecy and integrity for low cost IoT devices like the ESP8266 and Photon particle.

In [14] author have discussed countermeasures of the security attacks on different layers of IoT and highlight the future research directions within the IoT architecture. Internet of Things (IoT) has been a massive advancement in the Information and Communication Technology (ICT). It is projected that over 50 billion devices will become part of the IoT in the next few years. Security of the IoT network should be the foremost priority. In this paper, we evaluate the security challenges in the four layers of the IoT architecture and their solutions proposed from 2010 to 2016. Furthermore, important security technologies like encryption are also analyzed in the IoT context.

In [15] author have discussed overview of the architecture of IoT with the help of Smart World. In the second phase of this paper, the security challenges in IoT followed by the security measures in IoT are discussed. Finally, these challenges, which are discussed in the paper, can be research direction for future work in security for IoT.

In [16] author have discussed a true random number generator using write speed variation of oxide-based RRAM is proposed for the first time. The signal of this physical unclonable function (PUF) is strong with long duration to be easily and accurately

captured by simple circuit, of which the advantage is attributed to the mechanism that the speed variation amplifies the fluctuation of oxygen vacancy trap and de-trap. Some function parts of normal RRAM IP can be reused as entropy source cells and implementation circuit. The variation of write end point is monitored by a self-adaptive write drive circuit to trig a counter, and then serialized into a bit stream. The test chips, which are AlOx/WOx bilayer back-end RRAM fabricated in 0.18 Um logic process, passed all NIST tests with advantages of small area, low power, and not using post-processor corrector. Enough bits can be generated within the endurance limitation to ensure usual Internet of Things (IoT) security application.

In [17] author have proposed protecting physical devices from illegal access by intruders and give basic analysis for fundamental gaps between physical devices and embedded IoT software's. Also the IoT Agent Platform mechanism to separate IoT functions from physical devices and to run isolated IoT functions on cloud environment. The mechanism is based on the Drip cast which is a transparent programming framework for IoT devices where we don't care about communication, server-side programming nor database, at all. The Drip cast provides a very simple and easy development model which is a key for device vendors to develop physical devices to use IoT functions.

In [18] author have proposed EdgeSec, the design of a novel security service which is deployed at the Edge layer to enhance the security of IoT systems. EdgeSec consists of seven major components that work together to systematically handle specific security challenges in IoT systems. Finally, the effectiveness of EdgeSec is demonstrated in the context of a typical IoT application, Smart Home.

In [19] author have provided a novel IoT protocol architecture and examines security tools and techniques that can be leveraged as part of the deployment of IoT, these mechanisms are particularly important in e-health and assisted living applications.

In [20] author have discussed a multi-factors security key generation mechanism for self-organizing Internet of Things (IoT) network and nodes. The mechanism enables users to generate unique set of security keys to enhance IoT security while meeting various business needs. The multi-factor security keys presents an additional security layer to existing security standards and practices currently being adopted by the IoT community. The proposed security key generation mechanism enables user to define and choose any physical and logical parameters he/she prefers, in generating a set of security keys to be encrypted and distributed to registered IoT nodes. IoT applications and services will only be activated after verifying that all security keys are present. Multiple levels of authorization for different user groups can be easily created through the mix and match of the generated multi-factors security keys. A use case, covering indoor and outdoor field tests was conducted. The results of the tests showed that the mechanism is easily adaptable to meet diverse multivendor IoT devices and is scalable for various applications.

In [21] author have addressed some of the challenges, the current industrial practice to address them, some gaping holes in the state of the practice, and potential research directions to address them. Security is a critical component for computing devices targeted towards Internet-of-Things applications. Unfortunately, IoT security assurance is a challenging enterprise, involving cooperation and conflicts among a variety of stakeholders working in concert with a variety of architecture and design collateral generated across various points in a complex design life-cycle. Furthermore, the long life and aggressive energy/performance needs of IoT applications bring in new challenges to security designs.

In [22] author have presented the design and implementation of a middleware featuring "intermittent" and "flexible" end-to-end security for cloud-fog communications. Intermittent security copes with unreliable network connections, and flexibility is achieved through security configurations that are tailored to application needs. Our experiment results show how middleware that leverages static pre-shared keys forms a promising solution for delivering light-weight, fast and resource-aware security for a variety of IoT-based applications.

In [23] author have proposed two designs of a reconfigurable PUF, a speed optimized reconfigurable hybrid oscillator arbiter PUF and its power optimized counterpart. Both designs can be introduced into two different categories of IoT devices, one where high performance is needed and one with low power consumption. The Hamming distance of the speed optimized and power optimized designs is 47 % and 48 % with power consumption of 167.5 µW and 143.3 µW, respectively.

In [24] author have presented some of the challenges related to the deployment of the Internet Of Things (IoT), specifically to ascertain that security becomes an integral part of the technology rather than a bolted-on wrapper of limited efficacy. IoT security (IoTSec) is needed at all `layers' of the IoT environment and may be specific to the IoT `layer' in question.

In [25] author have addressed diverse IoT platforms such as oneM2M, FIWARE and IoTivity have been developing. In this context, security must be discussed as a main consideration. Vulnerability of IoT platform will affects IoT device directly, and it will also cause a critical influence in all connected IoT platforms during their interworking process.OAuth 2.0-based oneM2M security component is shown to provide authentication and authorization, which are essential security goals in IoT security and secure interworking between IoT platforms. Finally, the examples regarding the oneM2M security component are presented.

In [26] author have addressed IoT applications in houses are equipped with variety of appliances like personal computer, switches, doorbells, Ovens, Televisions, LED lighting, Water heaters, HVAC (Heating, Ventilation, & Air Conditioning)etc. It becomes difficult to monitor all the appliances at a time. Sometimes if no one present at home & some appliances remains on, it will consume large amount of power and result's more electricity bill. This could be achieved by using modern technology like an IoT. In this two sensors motion and temperature sensor are used. The PIR (Pyro-electric passive infrared) is used for authentication purpose, and temperature sensor LM35 is used for detecting current temperature of the room and accordingly operate the appliances present in the home.

In [27] author has addressed on 5G network features for machine-type communication and security challenges for mobile cloud robots. A distributed security platform based on machine learning algorithms that would detect and mitigate malicious robots or drones in an IoT network.

In [28] author have proposed a conceptual Holistic Security Architecture for addressing the trust, confidentiality and privacy issues in Internet of Things (IoT). A novel design with a configurable policy-based architecture that can scale proportionately in solving trust, confidentiality and privacy concerns simultaneously in distributed security domains. The architecture shows a mechanism for negotiated release of provable attributes and resources, especially when devices have the capabilities and requirements to share data as well as collaborate in solving problems.

In [29] author introduces a smart system developed with sensors that is useful for internal and external security. The system is useful for people living in houses, apartments, high officials, bank, and offices. The system is developed in two phases one for internal security like home another is external security like open areas, streets. The system is consist of a mobile application,

capacitive sensing, smart routing these valuable features to ensure safety of life and wealth. This security system is wireless sensor based which is an effective alternative of cctv cameras and other available security systems. Efficiency of this system is developed after going through practical studies and prototyping.

In [30] author propose a vehicle door latch with tracking and alert system. Lock with tracking device integrates GPS module, microcontroller, pneumatic lock and a battery for power supply. A microcontroller is used to control the GPS and the pneumatic lock. The tracking system uses the GPS module to get geographic coordinates. The alert system will activate when the lock is closed but the door is not in its position, which only means the door is not intact with the latch. A unique website is built for accessing location data and control to lock and unlock.

In [31] author have discussed about an IoT authentication service for smart-home devices using a smart-phone as security anchor, QR codes and attribute based cryptography (ABC). Regarding the fact that in an IoT ecosystem some of the IoT devices and the cloud components may be considered un-trusted, A privacy preserving attribute based access control protocol to handle the device authentication to the cloud service. For the smart-phone centric authentication to the cloud component, employ the FIDO UAF protocol and extend it, by adding an attributed based privacy preserving component.

In [32] author have addressed the challenges and possible solutions for IoT security that needs to be addressed at IoT perception layer/Edge node. The inevitable component of the IoT edge node is microcontroller/System on Chip (SoC). The microcontroller/SoC used in sensitive applications consists of Trusted Execution Environment (TEE), a hardware support for security. TEE's are not sufficient to address all the security issues in IoT systems. Hardware security issues like hardware Trojans, counterfeiting and debug security are tightly interlinked with the IoT perception layer security. There can be common solution to the hardware security issues and IoT perception layer security. In this paper, we briefly discuss the challenges in IoT design, IoT security, vulnerabilities of edge device, existing solutions and need for new security architecture for IoT edge nodes. And finally we present what security features, the next generation SoC/microcontrollers should incorporate to solve both hardware intrinsic security and IoT perception layer security more holistically.

In [33] author have addressed IoT applications include smart infrastructure, smart healthcare, smart governance, smart mobility, smart technology, etc. Also needs in security in IoT services. Technologies like Bluetooth, ZigBee and Radio Frequency Identification Technology (RFID) enable security in IoT are discussed.

In [34] author have addressed requirement analysis of IoT security in distributed systems, particularly looking at trust, confidentiality and privacy issues. A novel requirement specification for addressing trust, confidentiality and privacy concerns simultaneously, after security requirements analysis is presented. The requirements among others prescribe the need for negotiated release of provable attributes and resources, especially when devices have the Capabilities and Requirements to share data as well as collaborate in solving business problems.

In [35] Author introduces IoT security items and how to achieve the requirements of these items in a constrained environment to guarantee security in every stage (Device, transmission of data, data on reset, service, and user). Also, it combines these items in one stack to deal with different IoT platforms, this made integration between items to assure the continuity of security from one stage to another stage and helps to have a full tracing of data from IoT device through the middleware to the user and vice versa.

In [36] author have addressed IoT Top Security Concerns: Device Cloning, Sensitive Data Exposure, Denial of Service, Unauthorized Device Access and Control, Tampering Data. This research work accomplishes the need to mitigate IoT security challenges Device Cloning and Sensitive Data Exposure.

In [37] author have explored the existing studies on IoT security issues and the mixture of two main technologies of IoT in context of their threats, corresponding security requirements and their solutions while moving toward synthesizing a model for the security and data piracy issues from various viewpoints. This generic model for implementing security comprises of, combination of security standards and corresponding security requirements heading on the functional architecture of IoT.

In [38] author have reviewed the vulnerabilities in point of security threat/attacks associated with both of the key technologies. The exchange of data in two or more devices can be made through different communication methods but the two main traditional methods are Wireless Sensor Network (WSN) and Radio Frequency Identification (RFID). WSN is consisting of sensor nodes and on other side RFID technology uses passive and active RFID tags (Transponders). IoT is the most rapidly increasing technology spreading all over the world but there are some security concerns regarding its expansion. Security, Privacy and trust must not be neglected by the independent communication of the objects. There are definite network security issues in IoT technologies by the growing trend. The hackers can easily attack the IoT system which can be a great risk for the end user in daily life. By fulfilling various security requirements, it will not be cumbersome to embed security in the remote devices. Emerging nonvolatile memory (NVM) devices are not limited to build nonvolatile memory macros. They can also be used in developing nonvolatile logics (nvLogics) for nonvolatile processors, security circuits for the internet of things (IoT), and computing-in-memory (CIM) for artificial intelligence (AI) chips. This paper explores the challenges in circuit designs of emerging memory devices for application in nonvolatile logics, security circuits, and CIM for deep neural networks (DNN). Several silicon-verified examples of these circuits are reviewed in this paper.

In [39] author have proposed to detect malicious nodes that manipulate the link quality estimator of the routing protocol. In order to accomplish this task, MINTROUTE and CTP routing protocols are selected and updated with intrusion detection schemes (IDSs) for further investigations with other factors. It is proved that these two routing protocols under scrutiny possess inherent susceptibilities, that are capable of interrupting the link quality calculations. Malicious nodes that abuse such vulnerabilities can be registered through operational detection mechanisms. The overall performance of the new LQR protocol with IDSs features is experimented, validated and represented via the detection rates and false alarm rates.

In [40] author have proposed a novel framework aiming to exploit SDN/NFV-based security features and devise new efficient integration with existing IoT security approaches. The potential benefits of the proposed framework is validated in two case studies. Finally, a feasibility study is presented, accounting for potential interactions with open-source SDN/NFV projects and relevant standardization activities.

In [41] author have proposed security architecture for IoT smart services environment. The proposed security architecture is supported with a set of algorithms for different levels of security. The performance of the simulated environment of the proposed architecture is tested and the results are furnished in this paper which are satisfactory.

In [42] author have shown survey on Internet of things (IoT) continues to the draw attention of academics and researchers across the globe, since it represents the future of ubiquitous Computing. This is triggered by number of both digital and physical objects connecting to each other using ICT technologies, platforms and the internet to facilitate the whole processes of connectivity and services provision. With this massive connectivity of objects and devices forming the IoT, comes a great responsibility in terms of confronting new sets of challenges ranging from IoT security threats, ethics and privacy.

In [43] author have shown an IoT security roadmap overview is presented in this work based on a novel cognitive and systemic vision. The role of each component of the approach will be explained and relations with the other elements and their impact on the overall system will be detailed. According to the novel taxonomy of IoT vision, a case study of military live simulation is presented to highlight components and interactions of the systemic and cognitive approach. Then, a discussion of security questions about privacy, trust, identification and access control will be provided, and different research challenges are highlighted.

In [44] author have proposed protocol uses the unique Device ID of the sensors to generate key pair to establish mutual authentication between Devices and Services. Finally, the Mutual authentication mechanism is implemented in the gateway.

In [45] author have discussed the needs for input to public policy discourse by communications professionals who have some insights as to how IoT advances may impact their clients and society as a whole. In the near future, education and communications professionals may also empower households by designing instructional materials for use in establishing cyber hygiene routines and resolving IoT-related concerns.

In [46] author have presented implementation of IoT Sentinel, which is a system aimed at protecting the user's network from vulnerable IoT devices. IoT Sentinel automatically identifies vulnerable devices when they are first introduced to the network and enforces appropriate traffic filtering rules to protect other devices from the threats originating from the vulnerable devices.

In [47] author have presented IoT Sentinel, a system capable of automatically identifying the types of devices being connected to an IoT network and enabling enforcement of rules for constraining the communications of vulnerable devices so as to minimize damage resulting from their compromise. We show that IoT Sentinel is effective in identifying device types and has minimal performance overhead.

In [48] author have presented a software tool for security analysis of IoT systems is presented. The tool, named ASTo (Apparatus Software Tool) enables the visualization of IoT systems using a domain-specific modeling language. The modeling language provides constructs to express the hardware, software and social concepts of an IoT system along with security concepts. Security issues of IoT systems are identified based on the attributes of the constructs and their relationships. Security analysis is facilitated using the visualization mechanisms of the tool to recognize the secure posture of an IoT system.

In [49] author have provided an experimental result showing learning effectiveness of experiential learning for cyber security education by comparing with non-experiential learning. The experiential learning, the experimental group in this research, took two lecture styles. One was a classroom-styled lecture that a lecturer teaches basic knowledge of cyber security to learners. The other one was practical exercises that learners made groups and experientially implemented their products with security protection. The non-experiential learning, the control group in this research, took an e-learning-styled lecture using a video educational material containing the same contents of the classroom-styled lecture in the experimental group but the contents about any practical exercise were removed. The learning effectiveness of the two learning groups were evaluated by comparing several metrics of pre-/post-test scores and delayed-test scores. The evaluation result indicates that learners who took the experiential learning could keep retaining knowledge they learned than learner who took the non-experiential learning.

In [50] author have proposed a method to bring order on the IoT security panorama providing a taxonomic analysis from the perspective of the three main key layers of the IoT system model: Perception, Transportation and Application levels. As a result of the analysis, the most critical issues with the aim of guiding future research directions are highlighted.

III. FORMULATION OF RESEARCH HYPOTHESIS WITH EXPECTED OUTCOMES:

There is need of robust user authentication and secure device access strategy in IoE. IOE will be widely used in our lives a huge impact on social life and business environments at home, work, and in intelligent transport and healthcare thus in these crucial areas the security risks will be higher. IOE security could be compromised by several types of attacks. These attacks could be on physical level or on software level. To narration in this section, we will draw a few key challenge areas:

- Access control, Security, Privacy, Management of identity.
- Standardization and Interoperability.
- Data deluge.

Using open source simulation as well as working libraries in Linux platform environment can be best applicable platforms for the implementation. The testing environment can be consist of open source based simulation tools and libraries for authentication and encryption purpose.

The developed technique can provide efficient way for IoE system authentication and security in terms of used identity and access.

IV. SIGNIFICANCE OF RESEARCH:-

The Internet of Everything (IoE) is one of the so-called disruptive technologies. It has diverse impact margins that can influence our lives, the business world and even the global economy. In utmost synthesis, IoE can be considered a family of technologies whose goal is to enable anything that can be connected to the Internet even things which do not have any electronic purpose to be monitored and controlled from afar and thus to provide a service to its users. That thing can perform as a sensor, or be enabled to produce information about itself or its surroundings. And that thing can be programmed from a distance, without any specific technologies, but rather through Internet connections. With optimum authentication and security IoE can prove itself as boon to mankind.

We have identified the gap in IoE security techniques which addresses variety of security concerns. Our proposed mechanism should withstand against speed, security and trust for authenticated users utilization.

REFERENCES

[1] Auger, E. Exposito and E. Lochin, "Towards the internet of everything: Deployment scenarios for a QoO-aware integration platform," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 499-504. doi: 10.1109/WF-IoT.2018.8355113

[2] J. Ryoo, S. Kim, J. Cho, H. Kim, S. Tjoa and C. Derobertis, "IoE Security Threats and You," 2017 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, 2017, pp. 13-19.doi: 10.1109/ICSSA.2017.28

[3] T. Nguyen, T. Luan Vu, N. T. Le and Y. Min Jang, "An Overview of Internet of Energy (IoE) Based Building Energy Management System," 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju,2018,pp.852-855.doi: 10.1109/ICTC.2018.8539513

[4] J. Kaur, P. Wongthongtham, B. Abu-Salih and S. Fathy, "Analysis of Scientific Production of IoE Big Data Research," 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, 2018,pp.715-720.doi: 10.1109/WAINA.2018.00173

[5] S. F. Ismail, "IOE solution for a diabetic patient monitoring," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 244-248. doi: 10.1109/ICITECH.2017.8080007

[6] L. Daza and S. Misra, "Beyond the internet of things: everything interconnected: technology, communications and computing [book review]," in IEEE Wireless Communications, vol. 24, no. 6, pp. 10-11, Dec. 2017. doi: 10.1109/MWC.2017.8246819

[7] M. H. Miraz, M. Ali, P. S. Excell and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technologies and Applications (ITA), Wrexham, 2015, pp. 219-224. doi: 10.1109/ITechA.2015.7317398

[8] S. Naik and V. Maral, "Cyber security — IoT," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 764-767.

[9] Punia, D. Gupta and S. Jaiswal, "A perspective on available security techniques in IoT," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 1553-1559.

[10] Dou et al., "Challenges of emerging memory and memristor based circuits: Nonvolatile logics, IoT security, deep learning and neuromorphic computing," 2017 IEEE 12th International Conference on ASIC (ASICON), Guiyang, 2017, pp. 140-143.

[11] Schinianakis, "Alternative Security Options in the 5G and IoT Era," in IEEE Circuits and Systems Magazine, vol. 17, no. 4, pp. 6-28, Fourthquarter 2017.

[12] Farris et al., "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 169-174.

[13] O. Mavropoulos, H. Mouratidis, A. Fish and E. Panaousis, "ASTo: A tool for security analysis of IoT systems," 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), London, 2017, pp. 395-400.

[14] J. Yang, Y. Lin, Y. Fu, X. Xue and B. A. Chen, "A small area and low power true random number generator using write speed variation of oxidebased RRAM for IoT security application," 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, 2017, pp. 1-4.

[15] Nakagawa and S. Shimojo, "IoT Agent Platform Mechanism with Transparent Cloud Computing Framework for Improving IoT Security," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, 2017, pp. 684-689.

[16] K. Sha, R. Errabelly, W. Wei, T. A. Yang and Z. Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), Madrid, 2017, pp. 81-88.

[17] J. A. Oravec, "Emerging “cyber hygiene” practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security," 2017 IEEE International Professional Communication Conference (ProComm), Madison, WI, 2017, pp. 1-5.

[18] Minoli, K. Sohraby and B. Occhiogrosso, "IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications," 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, 2017, pp. 13-18.

[19] S. Ray, "System-on-chip security assurance for IoT devices: Cooperations and conflicts," *2017 IEEE Custom Integrated Circuits Conference (CICC)*, Austin, TX, 2017, pp. 1-4.

[20] B. Mukherjee, R. L. Neupane and P. Calyam, "End-to-End IoT Security Middleware for Cloud-Fog Communication," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 151-156.

[21] P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel and J. Singh, "Reconfigurable Robust Hybrid Oscillator Arbiter PUF for IoT Security Based on DL-FET," 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, 2017, pp. 665-670.

[22] D. Minoli, K. Sohraby and J. Kouns, "IoT security (IoTSec) considerations, requirements, and architectures," 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2017, pp. 1006-1007.

[23] M. Miettinenet al., "IoT Sentinel Demo: Automated Device-Type Identification for Security Enforcement in IoT," 2017 IEEE 37th International Conference on Distributed Computing Systems

[24] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. R. Sadeghi and S. Tarkoma, "IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, 2017, pp. 2177-2184.

[25] Oh and Y. G. Kim, "Development of IoT security component for interoperability," 2017 13th International Computer Engineering Conference (ICENCO), Cairo, 2017, pp. 41-44.

[26] D. S. Namdeo and V. R. Pawar, "IoT based smart home for power & security management," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 477-481.

[27] Madhusanka Liyanage; Ijaz Ahmad; Ahmed Bux Abro; Andrei Gurtov; Mika Ylianttila, "IoT Security," in A Comprehensive Guide to 5G Security , 1, Wiley Telecom,2017,pp.480.

[28] U. M. Mbanaso, G. A. Chukwudebe and B. Adebisi, "Holistic security architecture for IoT technologies," 2017 13th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, 2017, pp. 11-16.

[29] F. H. Chowdhury et al., "Design, control & performance analysis of secure you IoT based smart security system," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017, pp. 1-6.

[30] M. Togan, B. C. Chifor, I. Florea and G. Gugulea, "A smart-phone based privacy-preserving security framework for IoT devices," 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, 2017, pp. 1-7.

[31] S. R. Oh and Y. G. Kim, "Development of IoT security component for interoperability," 2017 13th International Computer Engineering Conference (ICENCO), Cairo, 2017, pp. 41-44.

[32] *P. Datta and B. Sharma, " IoT architectures, protocols, security and smart city based applications," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017, pp. 1-5.*

[33] R. Waz, M. A. Sobh and A. M. Bahaa-Eldin, "Internet of Things (IoT) security platforms," 2017 12th International Conference on Computer Engineering and Systems (ICCES),Cairo,2017,pp.500-507.

[34] Ahmed, A. P. Saleel, B. Beheshti, Z. A. Khan and I. Ahmad, "Security in the Internet of Things (IoT)," 2017 Fourth HCT Information Technology Trends (ITT), Al Ain, 2017, pp. 84-90.

[35] Z. Ling, K. Liu, Y. Xu, Y. Jin and X. Fu, "An End-to-End View of IoT Security and Privacy," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-7.

[36] M. Daud, Q. Khan and Y. Saleem, "A study of key technologies for IoT and associated security challenges," 2017 International Symposium on Wireless Systems and Networks (ISWSN), Lahore, 2017, pp. 1-6.

[37] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni and P. Minet, "A lightweight IoT security protocol," 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, 2017, pp. 1-8.

[38] J. Jiang, Z. Chaczko, F. Al-Doghman and W. Narantaka, "New LQR Protocols with Intrusion Detection Schemes for IOT Security," 2017 25th International Conference on Systems Engineering (ICSEng), Las Vegas, NV, 2017, pp. 466-474.

[39] Y. Ban, K. Okamura and K. Kaneko, "Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education," 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), Hamamatsu, 2017, pp. 699-704.

[40] V. Jerald, S. A. Rabara and D. P. Bai, "Algorithmic Approach to Security Architecture for Integrated IoT Smart Services Environment," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 24-29.

[41] R. Sfar, Z. Chtourou and Y. Challal, "A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges," 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), Sfax, 2017, pp. 101-105.

[42] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2017, pp. 1-5.

[43] M. M. Ahemd, M. A. Shah and A. Wahid, "IoT security: A layered approach for attacks & defenses," 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, 2017, pp. 104-110.

[44] *S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 492-496.*

[45] Kan-Siew-Leong, P. L. R. Chze, A. K. Wee, E. Sim and K. E. May, "A multi-factors security key generation mechanism for IoT," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, 2017, pp. 1019-1021.

[46] D. Andročec, B. Tomaš and T. Kišasondi, "Interoperability and lightweight security for simple IoT devices," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017, pp. 1285-1291.

[47] M. Radovan and B. Golub, "Trends in IoT security," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017, pp. 1302-1308.

[48] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. R. Sadeghi and S. Tarkoma, "IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT," *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, 2017, pp. 2177-2184.

[49] M. FRUSTACI, P. PACE, G. ALOI and G. FORTINO, "Evaluating critical security issues of the IoT world: Present and Future challenges," in IEEE Internet of Things Journal.. 2017, pp 1-1.

[50] E. Tabane and T. Zuva, "Is there a room for security and privacy in IoT?," 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban, 2016, pp. 260-264.