DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5258

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

REVIEW ON SECURITY IN THE INTERNET OF THINGS

G. Ambika
Research Scholar
Department of Computer Science,
Marudupandiyar College(Affiliated to Bharathidasan University), Thanjavur - 613 403,Tamilnadu,India

Dr. P. Srivaramangai
Associate Professor
Department of Computer Science,
Marudupandiyar College(Affiliated to Bharathidasan University), Thanjavur - 613 403,Tamilnadu,India

***Abstract*:** Internet of Things (IoT) is a familiar thing (object) in today's world that is a part of our routine life activities. Secures IoT end-to-end, communications of device authentication, and applications from threats. IoT technology using of this technology to improving security and privacy violation. In further analysis of technology that that discomposed lots, together with confidentiality, authenticity, and integrity. To handle these privacy and security issues, in this paper introduce a system that stores IoT data securely within the Cloud information whereas still allowing query processing over the encrypted data. In this research paper, modify this by encrypting IoT data with a group of cryptographic schemes like order-preserving and partially homomorphic encryptions.

Keywords: Security, Internet of Things, Encryption algorithms, Cloud Computing

I. INTRODUCTION

The Internet of Things (IoT) could be a new technology, however at an equivalent time to the previous term. It had been already mentioned by Kevin Ashton in 1999, whereas holding a presentation at Proctor & Gamble. He used the term to link the concept of radio frequency identification (RFID) to the then new topic internet [1]. Since then the use of this term has blossomed and major companies have expected a rise in IoT [2, 3, 4]. One prediction is that the number of connected things within the world can have a thirtyfold increase between 2009 and 2020, so by 2020 there will be 26 billion things that are connected to the internet [5].

Defining the term IoT is somewhat tough as a result of its several definitions looking on who is process the term [6].The essential idea of IoT is to connect things together, thus enabling these "things" to communicate with each other and enabling people to communicate with them [12]. What these things are varies depending on that context the term is used and also the aim of using the thing. During this analysis we have chosen to follow the definition of IoT proposed by ITU's Telecommunication Standardization Sector (a United Nations agency which specializes in ICT): "… a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". Interconnecting the physical world with the virtual world and applying this idea to all things release new possibilities within the sense of having the ability to at any time access anything from anyplace. Providing new possibilities will also generate new threats, security risks, and expose vulnerabilities within the unknown world of interconnected everything. "Things" within the physical world are objects that physically exist and from the perspective of IoT we are able to sense, operate, and connect with these things, whereas within the virtual world "things" are objects which will be stored, accessed, and processed [7]. IoT involves sensors in order to collect data. Sensors are already being employed in standard of living, but most of the people might not are aware of it. Smartphone's contain completely different kind of sensors, like accelerometers, cameras, and GPS receivers. Inherent sensors square measure nothing new in today's society. Kevin Ashton said that IoT is already happening, however we would not see it compared to Smartphone's which can both be seen and touched. RFID is such an IoT-technology that exists however is not essentially seen; so the development of IoT may progress a long method before it is visible for everybody [8].

How does one differentiate an IoT device from any other device? Some basic characteristics for IoT are states below. These characteristics could provide a clearer image of the actual differences between IoTs and alternative devices [10].

- **Interconnectivity:** The whole thing can be connected to the global information and communication infrastructure.
- **Related Services of Things:** Giving related services within the boundary for Things, its only use of security between physical and virtual things.
- **Heterogeneity:** IoT devices use have different hardware, network and platforms.
- **Dynamic changes:** The number of devices can differ when the state of a device can change dynamically. (Device states: connected, disconnected, waking up, and sleeping)[9].
- **Enormous scale:** The number of devices communicating and operating will be bigger than the number of devices in the current Internet. The majority of this communication will be device to device instead of human to device.

The new concept of IoT, it is still mostly unknown and unexplored by many companies and employees in industry.

This limited information might cause them to be afraid of, or as within the previous example, entirely unaware of the potential security and privacy problems connected to their deployment of IoT [11]. This is often why several businesses need to understand additional concerning the potential threats, benefits, disadvantages, and solutions regarding security in conjunction with IoT. In addition, they have to understand what competence in information security is important so as to appreciate value effective security in conjunction with their deployment of IoT. This information and competence should help facilitate their transition from a non-IoT-business to an IoT-business, because it can modify each employees and management to know, address their doubts and issues in terms of their investments and therefore the ensuing security risks. During this method, managers will create a balanced risk-benefit analysis of the adoption of IoT for a particular application or family of applications.

IoT security issues mainly classified into two areas: virtual and physical threats. De-parameterized can be done by increasingthe physical threats.In today IT-environment, the virtual threats are closely coupled with the threats and mainly consist of information (an asset) and obtaining data or taking control of the device itself. Increasing the performance and power of IoT devices use of limited methods for securing an IoT environment.

To support computing on encrypted data, IoT applications need new security architectures. The encrypted data is processed by existing practical systems, such as CryptDB [6] designed for web services.For example, if the users decide the cloud as untrusted then CryptDB selects and performs necessary cryptographic operations on a data flow between the app server and database.An IoT application stores and processes data on gateways as well as the cloud andthis introduces an additional untrusted entity.Smart phones can be root-kitted, which would give an adversary access to personal data. Many untrusted gateways provide to IoT systems.For example, home automation gateways can run arbitrary software.IoT applications need new cryptographic algorithms and protocols. The resources accessible to IoT devices vary by up to six orders of magnitude (i.e., KB to GB of RAM and mhz to ghz of cpu power). Every tier contains a totally different system architecture and communication interface (i.e., BLE and Zig- Bee, to WiFi, LTE, and Ethernet). Gateway and IoT devices are battery powered then want careful power management. One common way to store IoT data is in structured databases, like SQL databases. In an encrypted query processing system, a plaintext SQL query is transformed to an encrypted query, specified the cloud cannot study the values within the query. The question is then executed over encrypted data and also the encrypted result is sent back to the user. Crypt- DB is one among the early systems that used order-preserving encryption schemes and partial homomorphic encryption to make an efficient EDB [13]. Partially Homomorphic encryption (PHE) schemes to enable query processing over encrypted data within the cloud. It offers a new technique for secure sharing of PHE data among users and groups, based on re-encryption techniques. In this research paper, understand how to implement encryption technique in various research papers.

II. LITERATURE REVIEW

Mayuri A. *et al.* [15]summarized read of IOT together with its design has been given. IOT is a future technology of innovation however still at its early stage of analysis and development. IOT cannot be used wide if it is not safe. Therefore, the paper has mentioned security problems with IOT and a few measures for needed security parameters. even though in recent years, an active analysis on IOT goes on, however still some issues will be additional focused on: 1) Use and analysis of Wi-Fi, Ethernet, Bluetooth for networking of IOT or ZigBee protocol; 2) Application oriented study is required for various industrial application in hich IOT will be utilized in order to initiate a new technological revolution; 3) New security challenges and application of light-weight cryptographic protocol need to be studied more.

Hui Suo*, et al.* [16] for a short time reviewed security within the IoT, and security characteristics and four layers including perceptual layer, network layer, support layer and application layer. Encryption mechanism and security, protecting sensor data, and encryption algorithm has discussed.

Tuhin Borgohain , *et al.* [17]surveyed all the security flaws existing within the internet of Things, which will convince to be very detrimental in the development and implementation of IoT in the totally different fields. Therefore adoption of sound security measures countering the above detailed security flaw as well as implementation of various intrusion detection systems ([11], [3]), cryptographic and stenographic security measures within the information exchange process and using efficient methods for communication can lead to a safer and robust IoT infrastructure. In this paper suggest that more effort on development of secured measures for the existing IoT infrastructure before going for further development of latest implementation methods of IoT in lifestyle would convince be a more fruitful and systematic technique.

Rene Hummen,*et al.* [18] analyzed the public-key cryptography on the certificate-based DTLS handshake and known significant Random Access Memory and Read Only Memory needs. Certificate-based handshake provides a limited devices for secure communications. DTLS connection make security for Applications, Servers and Connections.

Taha M. *et al.* [19]presented the security and privacy once using the internet of Things technology, also known as The Internet of Objects, refers to a wireless network between objects; typically the network are wireless and self-configuring, like unit appliances.

Raluca Ada Popa*, et al.* [20]presented CryptDB system for privacy within the two vital threats in database backed(DBA and DBMS) applications. CryptDB meets Encrypted Data and SQL -aware cryptography strategy. Onion of encryption to untrusted DBMS Servers and user passwords.

Alexandra Boldyreva, *et al*[21].surveyed the cryptographic study of Order-preserving symmetric cryptography (OPE) Curiously, in this paper initial show that straightforward

relaxations of standard security notion for encryption similar to distinguish ability against chosen-plain text attack (IND-CPA) is unrealizable by a practical OPE scheme. Then design an efficient OPE scheme and prove its security under our notion based on pseudo randomness of an underlying block cipher. Explained random order-preserving function and hyper geometric probability distribution.

Florian Kerschbaum, *et al.* [22] presented a novel, strictly safer order-preserving encryption. In this paper compress the data on the client by a ratio of almost 15, but are able to do much higher ratios (of up to several thousands) with a number of repeated cipher-texts and unauthorized leaking some frequency information. User Selection allowed security of order preserving and storage cost.

John Kolb, *et al.* [23] proposed for a new distributed run-time system to facilitate fast application development for the IoT, informed by the belief that an intermediate tier of resources lying between edge devices and the cloud, is an integral however underutilized element of the IoT landscape. in this paper the proposed system includes a set of services to orchestrate the execution of IoT applications, a programming model to modify the construction of application components, and a configuration engine that permits developers to stipulate wherever their application's components may run as well as who will access them. in this study believe that this is able to represent a vital step forward in enabling developers to unleash the potential of the internet of Things. The paper aim is not only to assist developers a lot of simply construct applications however additionally to function a platform that provides precise and simply controlled execution semantics for distributed IoT software.

Liam Morris,et al. [24]proposeda homomorphic cryptosystems provide identical level of privacy as the other cryptosystem, whereas additionally allowing operations to be performed on the data while not the requirement to examine the particular data. If a computationally efficient fully homomorphic cryptosystem were to be developed, the implications are extraordinary. Complete privacy between client and server would be possible without any decreased functionality.Such systems might be applied to almost anything that needs computation, like voting, banking, cloud computing, and many others. Whereas the theoretical applications of homomorphic encryption are very useful and exciting, it is still the case that these systems have not however matured to the point of being practical. However, these systems are extremely young and there is still an excellent amount of analysis that must be done in this area. Additional installments in this area should prove interesting, and eventually it's going to be possible that such systems be widely adopted.

Ms.Parin, et al. [25]analyzed the survey on various homomorphic cryptography schemes. In a cloud computing fully homomorphic primarily based security is new idea. In this idea client encrypt the data using client's private key and that encrypted data is received by the server. Without decrypting that data server performs the operation and sends result back to the client. Now client decrypt that data and obtain the result. So, security drawback is overcome through this Homomorphic algorithm. Data confidentiality is managed by this algorithm.

Caroline Fontaine, *et al.* [27] presented in this paper a state of the art on homomorphic encryption schemes discussing their parameters, performances and security problems are given. In this paper saw, these schemes are not compatible for every use, and their characteristics should be taken into account. Their utilization in the signal processing community is kind of innovative and this paper will serve as a guide for understanding their specificity advantages and limits.

Mirza Abdur Razzaq, et al. [28]discussed IoT security needs to focus on major security problems with IoT particularly, focusing the security attacks and their countermeasures.As a result of lack of security mechanism in IoT devices, several IoT devices become soft targets and even this is often not in the victim's knowledge of being infected. In this paper, the security needs are discussed like confidentiality, integrity, and authentication, etc.In this survey, twelve differing kinds of attacks are classified as low-level attacks, medium-level attacks, high-level attacks, and extremely high-level attacks together with their nature/behavior yet as suggested solutions to encounter these attacks are mentioned. Considering the importance of security in IoT applications, it is extremely important to install security mechanism in IoT devices and communication networks.Moreover, to protect from any intruders or security threat, it is additionally suggested to not use default passwords for the devices and read the security needs for the devices before using it for the first time.Disabling the options that donot seem to be used might decrease the possibilities of security attacks.Moreover, it is necessary to review completely different security protocols utilized in IoT devices and networks.

Muhammad Usman, et al. [29] proposed IoT are going to be an important part of our daily lives.Various energy constrained devices and sensors will continuously be communicating with one another the security of that should not be compromised. For this purpose a light-weight security algorithm is proposed in this paper named as SIT. The implementation show promising results creating the algorithm for a suitable candidate to be adopted in IoT applications.

Hossein Shafagh, et al. [30] presented Pilatus, a replacement practical system tailored for the IoT ecosystem. In this paper empower the user with full management over their data, despite it being hold on in third-party clouds. In Pilatus, the cloud does not have access to any secret keys and stores only encrypted data. It can though process queries on encrypted data and re-encrypt it for sharing. In this paper the sharing scheme comes with cryptographic guarantees and the possibility of revocation. In this paper optimized the underlying cryptographic operations towards mobile platforms. The implementation and case studies on fit bit and Ava show that Pilatus has reasonable overhead in processing time and end-to-end latency. In this paper anticipate the presented cryptosystem and open-source platform to be useful for the design of secure mobile applications and to enable more analysis in this field.

III. CONCLUSION

Internet of Things (IoT) is a concept that encompasses various objects and strategies of communication to exchange data. Nowadays IoT is a lot of a descriptive term of a vision that everything should be connected to the internet. Finally, we would prefer to recommend that a lot of effort on development of secured measures for the existing IoT infrastructure before going for further development of recent implementation methods of IoT in daily life would prove to be a lot of fruitful and systematic method.

IV.REFERENCES

[1]. Andrew C. Yao. Protocols for Secure Computations.In Annual Symposium on Foundations of ComputerScience (SFCS), 1982.

[2]. D. F. Aranha and C. P. L. Gouvˆea. RELIC is anEfficient Library for Cryptography. Online:https://github.com/relic-toolkit/relic.

[3]. A. Arasu, S. Blanas, K. Eguro, R. Kaushik,D. Kossmann, R. Ramamurthy, and R. Venkatesan.Orthogonal Security with Cipherbase. In Conferenceon Innovative Data Systems Research (CIDR), 2013.

[4]. J. Benaloh. Verifiable Secret-Ballot Elections. PhDthesis, 1988. Yale University, Department of ComputerScience.

[5]. D. Boneh and M. Franklin. Identity-based Encryptionfrom the Weil Pairing. In Advances in Cryptology(CRYPTO), 2001.

[6]. D. Boneh, C. Gentry, S. Halevi, F. Wang, and D. J.Wu. Private Database Queries Using SomewhatHomomorphic Encryption. In Applied Cryptographyand Network Security (ACNS), 2013.

[7]. D. Boneh, E.-J. Goh, and K. Nissim. Evaluating2-DNF Formulas on Ciphertexts. In Theory ofCryptography (TCC), 2005.

[8]. D. Boneh, K. Lewi, M. Raykova, A. Sahai,M. Zhandry, and J. Zimmerman. Semantically SecureOrder-Revealing Encryption: Multi-Input FunctionalEncryption Without Obfuscation. In EUROCRYPT,2015.

[9]. S. Bajaj and R. Sion. TrustedDB: A TrustedHardware Based Database with Privacy and DataConfidentiality. In ACM Special Interest Group onManagement of Data (SIGMOD), 2011.

[10]. M. Bellare, A. Boldyreva, and A. O'Neill.Deterministic and Efficiently Searchable Encryption.In Advances in Cryptology (CRYPTO), 2007

[11]. D. Boneh, G. Segev, and B. Waters. TargetedMalleability: Homomorphic Encryption for RestrictedComputations. In Theoretical Computer ScienceConference (ITCS), 2012.

[12]. R. Bost, R. A. Popa, S. Tu, and S. Goldwasser.Machine Learning Classification over Encrypted Data.In Network and Distributed System SecuritySymposium (NDSS), 2015.

[13]. H. Chan, A. Perrig, and D. Song. Secure HierarchicalIn-network Aggregation in Sensor Networks. In ACMComputer and Communications Security (CCS), 2006.

[14]. D. X. Song, D. Wagner, and A. Perrig. PracticalTechniques for Searches on Encrypted Data. In IEEESymposium on Security and Privacy, 2000.

[15]. Mayuri A. Bhabad Sudhir T. Bagade "Internet of Things: Architecture, Security Issues and CountermeasuresInternational Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015

[16]. Hui Suo, Jiafu Wan,Caifeng Zou, Jianqi Liu"Security in the Internet of Things: A Review",International Conference on Computer Science and Electronics Engineering,2012.

[17]. Tuhin Borgohain, Uday Kumar, Sugata Sanyal "Survey of Security and Privacy Issues of Internet of Things", Department of Instrumentation Engineering, Assam Engineering College, Guwahati-13.

[18]. Rene Hummen, Hossein Shafagh, Shahid Raza, Thiemo Voigt, Klaus Wehrle, "Delegation-based Authentication and Authorizationfor the IP-based Internet of Things" Communication and Distributed Systems, RWTH Aachen University, Germany

[19]. Taha M. Alfaqih, Jalal Al-Muhtadi, "Internet of Things Security based on Devices Architecture", International Journal of Computer Applications (0975 – 8887) Volume 133 – No.15, January 2016.

[20]. Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan," CryptDB: Protecting Confidentiality withEncrypted Query Processing", MIT CSAIL.

[21]. Alexandra Boldyreva, Nathan Chenette, Younho Lee and Adam O'Neill,"Order-Preserving Symmetric Encryption",Georgia Institute of Technology, Atlanta, GA, USA.

[22]. Florian Kerschbaum, "Frequency-Hiding Order-Preserving Encryption", Karlsruhe, Germany, DOI: http://dx.doi.org/10.1145/2810103.2813629.

[23]. John Kolb, Kaifei Chen, Randy H. Katz, "The Case for a Local Tier in the Internet of Things Computer Science Division University of California", Berkeley, December 30, 2016.

[24]. Liam Morris, "Analysis of Partially and Fully Homomorphic Encryption", Rochester Institute of Technology, Rochester, New York May 10, 2013.

[25]. Ms.Parin.V.Patel, Mr Hitesh D Patel, "A Survey Of The Homomorphic Encryption Approach For Data Security In Cloud Computing", International Journal Of Engineering Development And Research, 2013.

[26]. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, "Internet of Things (IoT): A Literature ReviewJournal of Computer and Communications", 2015, 3, 164-173

[27]. Caroline Fontaine and Fabien Galand, A Survey of Homomorphic Encryption for Nonspecialists, Journal of Information Security, 2009, 1, 41-50

[28]. Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, Saleem Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[29]. Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan and Usman Ali Shahy, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017

[30]. Hossein Shafagh, Anwar Hithnawi, Lukas Burkhalter, Pascal Fischli, Simon Duquennoy, "Secure Sharing of Partially Homomorphic Encrypted IoT Data", In Proceedings of SenSys '17, Delft, Netherlands, November 6–8, 2017,14 pages. https://doi.org/10.1145/3131672.3131697