International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

A Study on Security in the Internet of Things

G. Ambika[1], Dr. P. Srivaramangai[2]
[1]Research Scholar, Department of Computer Science, Marudupandiyar College(Affiliated to Bharathidasan University), Thanjavur,Tamilnadu,India
[2]Associate Professor, Department of Computer Science, Marudupandiyar College(Affiliated to Bharathidasan University), Thanjavur,Tamilnadu,India

ABSTRACT

The technology of computing introduce a new enter called the Internet of Things (IoT). Machine to machine, machine to infrastructure, machine to environment, the Internet of Everything, the Internet of Intelligent Things, intelligent systems—term it what you desire but its occurrence, and its potential is huge. Security and privacy issues for IoT are challenges to prove targets of great importance. IoT networks extremely required to ensure confidentiality, authentication, access control, and integrity on the deployment of efficient security and privacy protocols. Therefore, the requirements of a secure environment are very important so as to secure the transmitting data from it devices over the network. In this paper will discuss about basics of IoT and also briefly understand the cryptographic schemes like order-preserving and partially homomorphic encryption.

Keywords : Security, Internet of things, Crypt DB, Order-preserving encryption, Partial Homomorphic Encryption

I. INTRODUCTION

Without Internet, how would be the world communicate easily? It is complicate to imagine like scenario we have never seen. Today, the internet becomes more important for everyone in both personal life and professional life. Completely different devices like smart phones, sensors, mobile computers, and more other smart objects are samples of things every day we have a tendency to addressing. The enterprise system technologies [1] and new ICT affects on the IoT related technologies. In the early evolution, it's called “Internet of Computers”; then modified to “Internet of People”; and recently, with the fast development within the ICT, it is recognized as the “Internet of Things”. It become simply to identify uniquely and accessible by increasing the use of internet with the help of various devices and smart objects. The connectivity is improved from “any-time, any-place” for “any-one” into “anytime, any-place” for “any-thing” [2]. In the economy developments of IoT technologies together with ICT innovations helps to develop the infrastructures of their promotion and future strategies. The main aim is to allow interaction and integration of the physical world and the cyber space [3].

As to the security, the IoT will be faced with more challenging issues [4]. There are the following reasons: 1) the IoT extends the ‘internet’ through the traditional internet, mobile network and sensor network and so on, 2) every ‘thing’ will be connected to this ‘internet’ and 3) these ‘things’ will communicate with each other. As a result, the new security and privacy problems will occur. We should give more awareness to the research issues for confidentiality, authenticity, and integrity of data in the IOT. Current cryptographic models and security schemes are based on extensively adopted encryption algorithms, and privacy standards. Confidentiality is ensured with the help of Advanced Encryption Standard (AES). The asymmetric algorithm RSA serves for asymmetric encryption, digital signatures and also performs key management. Secure hash functions can be done by SHA standards. On the other hand, Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC) supplement the privacy schemes, fundamentally in asymmetric cryptography. Really, the applied suites have been designed for general purpose uses, and their functionality is based on significant processing power, good memory resources, and power availability. Since the applicability of these cryptographic models and security schemes are confused, detailed analysis is needed for implemention

of specified resources of the IoT [5]. Especially, minimized capabilities requirments of the hand-held and portable devices [6] becomes of the above case study. Additionally, other security services, like key management, are growing up and have to be applied successfully, in future designs [7]. In order to enhance better results, there is an ongoing research for more flexible cryptographic suites. Special interest has been concerned by the security schemes of combined mode that supports probably encryption and authentication [8]. About the security terms of devices, a baseline security level is oriented each time, for the applied cryptographic techniques, in order, at least, to assume an unbreakable strength. Even though, more complicated security systems with special services are estimated to be needed in the near future, in order to satisfy advance needs for security, and serve for special cryptographic purposes [9].

CryptDB [10] is one of the first practical systems which are integrated efficient encrypted query processing into the database management system. The checking of traditional database queries in the CryptDB encrypted data; finally the encrypted results will be generated. To achieve this, CryptDB relies on a trusted proxy who intercepts the communication and applies encryption/decryption process transparent to the user. The major barrier of cryptographic primitives is resource constraints. IoT devices are naturally limited with regards to energy, memory, CPU and bandwidth. These challenges are exacerbated with computationally significant public-key-based cryptographic schemes, like order-preserving and additive homomorphic encryption. Order-preserving symmetric encryption (OPE) is a deterministic encryption scheme (aka. cipher) which encrypt funtion is totally different and ordering the plaintext by numerical. OPE has a briefy history within the kind of one-part codes, which are lists of plaintexts and therefore the related cipher texts, both ordered in alphabetical or numerical order therefore only one copy is needed for efficient encryption and decryption. Partially Homomorphic encryption (PHE) is especially additive homomorphic schemes. These are practical solutions that enable a very important set of queries [11], like the sum query on encrypted data – a standard operation in IoT applications when history data needs summing or averaging. Additionally note that with limited involvement of the client side, a lot of complicated computations (e.g., linear regression) may also be achieved [11].

II. OVERVIEW OF INTERNET OF THINGS

The IoT is a paradigm wherever each entity is connected to the internet and is ready to uniquely identify itself to other devices. Such physical objects are referred to as smart, which means that they contain embedded electronics that exhibits some style of intelligence. The term IoT was first utilized by Kevin Sir Frederick Ashton in 1999 [9], to explain a supply chain system using Radio-Frequency Identification (RFID) [3] to a potential client. Today, we have a tendency to envision the IoT to cover a good vary of applications, like smart Grids [13], sensible Cities [11], Industrial Automation [10], Home Automation [13] and Building Automation [12,10]. The history of the IoT is often derived within the area of ubiquitous computing. Mark Weiser proposed the thought of a smart environment: *"a physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network"* [99]. The integration task of this idea is explored within the area of Wireless sensor Networks (WSNs), wherever the goal is to build a system of the many low cost computational parts, referred to as *sensor nodes*, wirelessly connected and together with working towards a typical goal.

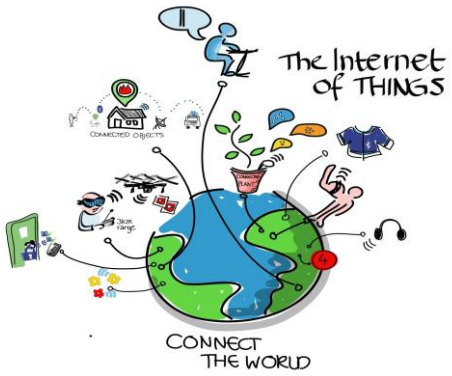

Figure 1: Internet of Things

The main concept behind the IoT to supports convergence process, where IoT is established end-to-end connectivity between any two devices as possible. The devices can be of disproportionate nature, as as an example, a powerful server reads out a temperature sensor, or a user controlling light-weight bulbs via a smart phone. The existence of a standard communication infrastructure, using standardized protocols, makes this communication possible. This

integration at a large scale is expected to enhance several current systems, as transport logistics and various automation systems. However, it will also enable for developing new applications, as smart cities and smart grids (Figure 1) [10,13]. The IoT is the whole thing other than a complete project. In fact, its realization faces several issues. Sociological challenges to faces issues differ as making people conscious and knowledgeable of technological challenges in the system design, data usability, security, and privacy for technolgy development as the main concept.

A) Internet of Things Communications Models

From an operational perspective, it is useful to understand about how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452), [17] which describes outline of four common communication models used by IoT devices. The discussion below presents these key characteristics of each communication model in the framework.

- **Device-to-Device Communications:** In the device-to-device communication model represents two or more devices to directly connect and communicate between each other network, rather than intermediary application server. These devices connect and communicate over various types of networks, together with IP networks or the internet. Often, but these devices use protocols like Bluetooth [14] Z-Wave [15] or ZigBee [16] to set up direct device-to-device communication.
- **Device-to-Cloud Communications:** In the device-to-cloud communication model, the IoT device connects and communicates directly to an Internet cloud service such as an application service provider to control message traffic and exchange data. This approach often takes advantage of existing communications mechanisms such as traditional wired Ethernet or Wi-Fi connections to set up a connection between the device and the IP network, which ultimately connects to the cloud service.
- **Device-to-Gateway Model:** In the device-to-application-layer gateway (ALG) model or the device-to-gateway model further typically, the IoT device connects and communicates through an ALG service as a conduit to arrive at a cloud service. This means there is application software operating on a local gateway device, which acts as an intermediary connection between the device and the cloud service and provides security and additional functionality such as data or protocol translation in simpler terms.
- **Back-End Data-Sharing Model:** In this concept, back-end data-sharing model refers to a communication architecture that enables users to analyze and export smart object data from a cloud service in combination with data from additional sources. This architecture supports "the [user's] desire for granting access to the upload sensor data to third party access" [18]. This approach is established between single device-to-cloud communication model, which can guide to data silos where "IoT devices upload data only to a single application service provider'' [19]. Single IoT device data streams to be aggregated and analyzed through a back-end sharing architecture that allows the collected data.

B) IoT Challenges

The IoT technical challenges can be identified in several areas to improve security level. They are as follows,

- **Connectivity**. Connecting trillions of devices in virtually the similar network is not a simple task. The heterogeneity of the concerned devices makes it even harder, since many different physical interconnections will be expected. These differences can fully break certain communications. As an example, city wide ad-hoc wireless networks generally have large latencies, which break timing perspectives of current internet protocols. IoT solutions need to address this heterogeneity within the design phase.
- **Power consumption**. All electronic devices have need of power to operate. On the one side, mains powered devices, as servers and light bulbs, make help of the power grid. On the other side, sensors deployed within the wild either consider on batteries, or use some form of energy harvesting. In both cases, the devices should be built and so they use as little energy as possible due to the scale of the IoT. Moreover, they open up new challenges, like the design of sustainable energy gathering technologies, and also the improvement of energy consumption within the local (e.g. information

centre, building) or global energy distribution system (e.g. city-wide grid).

- **System Architecture**. The multi-domain nature of the IoT makes it complicated to build a single, killer architecture and application. Basically put, solutions for a certain domain are inapplicable to others, either due to functional requirements, or due to hardware differences. IoT challengeses construct such architectures, with portability, auto-configuration, integration and connectivity in mind.
- **Interoperability and integration**. The IoT is built by many distinct vendors and also using different technologies. Their seamless integration can only be achievable if IoT systems are built on top of open standards. There are many standards for the same areas (e.g. different wireless networking standards), but interoperability between them has to be established (e.g. gateways between different physical networks).
- **Computational and storage complexity**. The IoT devices will generate massive amounts of data. These data can be continuous or bursty, and be in structured or unstructured form. In order to extract data, they have to be transported, stored and analyzed. These operations have enormous pressure on networking, storage and computational infrastructure. The IoT challengeses develop and maintain such difficult infrastructures.
- **Security, Trust and Privacy**. The IoT penetration in every day lives emphasizes the need of suitable secure solutions. On the one hand, the large number of devices involved and makes the design of a completely difficult secure system, as there are many points of potential attack. Then, any solutions have to be portable to a wide set of devices, despite their intrinsic differences. On the other hand, the potentially collectable data and its impact are enormous.

III. Crypt DB

CryptDB is working as a proxy between database and application. An application may be websites, mobile device application called “app” or classic desktop application, principally anything that connects to a database.

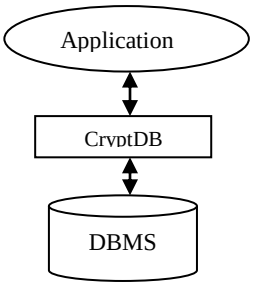

Figure 2: Communication scheme of an application with CryptDB

- **Onion Layers**

While CryptDB comes to SQL responsive encryption there are different features of computation that are based on different essential principles.

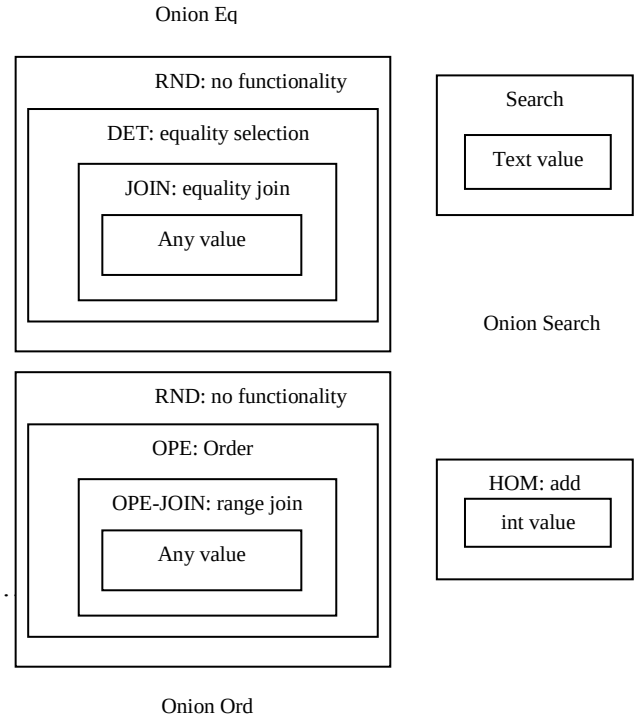

Figure 3: Diagrams of the onions construct with various layers that is used in CryptDB

For sample the operator GROUP BY depend on on equality checks concerning the encrypted data, other functions similar SUM depend on on the capability to perform additions of the encrypted data. CryptDB deals with these different computational features by clustering functions by their fundamental operations.Around these different aspects or clusters CryptDB build a construct that the developers have called onion: An onion features different layers of encryption from least revealing on the outside to most revealing on the inside, shown in Figure 3. At the same time the outmost layer is the one with the least functionality while the innermost one offers the

greatest functionality. The transformation from one layer into anotherhappens automatically when the need arises. In this situation CryptDB automatically re-encrypts the entire column and remembers its state. While technically it is possibly to re-encrypt everything to a higher layer of security again it is not suggested by the developers in case of common queries as it would demand a considerable amount of computationpower, besides that the information might have already been exposed.

- **Encryption Types**

Each type uses a different algorithm that meets the detailed requirements for a certain type and can be exchanged for another algorithm should the need get up, e.g. when a used cipher is damaged. In such an incident existing encrypted data would have to be decrypted with the old algorithm and re-encrypted using the new one. The different layers area listed from most to least secure. However least secure means that this particular layer does reveal the most information about its encrypted content, please notice that this is sometimes necessary in order to perform certain operations and is not automatically insecure. CryptDB [7] is a recent system which extends this line of work and tries to address some of the shortcomings of [5]. CryptDB's main insight is to use specialized cryptosystems designed to perform common database operations entirely on the server. The properties of various cryptosystems are discussed below.

- **Randomized encryption (RND**). This is usually what people think of when they think of encryption. A randomized encryption scheme has the following property (usually known as semantic security or IND-CPA): if a = $EncRand_k(x)$ and b = $EncRand_k(x)$, then with high probability a 6 not equal to b. IND-CPA is achieved in practice by using a secure block cipher (e.g. AES-CBC) coupled with a randomly chosen initialization vector.
- **Deterministic encryption (DET).** This is a weaker form of encryption than randomized. Specifically, for all x ↔ y in the plaintext space
$$x = y \leftrightarrow EncDet_k(x) = EncDet_k(y)$$
- **Order preserving encryption (OPE).** This is an even weaker form of encryption than deterministic (OPE implies deterministic). Specifically, for all x,y have
$$x < y \leftrightarrow EncOPE_k(x) < EncOPE_k(y)$$
- **Additive homomorphic encryption (HOM).** An additive homomorphic encryption scheme has the following property: given any two ciphertexts $EncHOM_k(x)$ and $EncHOM_k(y)$, there existsome computable function f such that f($EncHOM_k(x)$; $EncHOM_k(y)$) = $EncHOM_k(x + y)$.

IV. SECURITY IN IOT

Security in IoT is a need to provide integrity, confidentiality, non-repudiation and authentication of the information flows. Security of IoT communications can be addressed with the help of communication protocol, or on the other end by external mechanisms. Other security requirements should be considered for the IoT which helps to communications with sensing devices. Moreover, mechanisms are also needed to implement protection against threats to the normal functioning of IoT communication protocols. For example, fragmentation attacks should be take place at the 6LoWPAN adaptation layer. The related security requirements are anonymity, privacy, trust and liability which will be essential for the social acceptance of the future IoT applications employing Internet integrated sensing devices.

A. Security Parameters

Based on the IoT security issues, the need of security is required for IoT system.

The parameters of security demand needs a safe internet system of things. They are as follows,

- **Authenticity:** Received information by a reader should be noticeable and check whether is sent from authenticated electronic tag or not.
- **Confidentiality:** Using an RFID electronic tag to protect Sensitive information from unauthorized reader.
- **Integrality:** While transmitting the information to IoT, data integrity can ensure the originality of information. IOT should ensure that the information transmitting is not fabricated whether it is not rewritten, copied or replaced by the attacker.
- **Privacy:** The secure IOT system is protected privacy such as identity or commercial interest of an individual user.
- **Availability:** IoT provide various services to an authorized user and also prevent DOS attack for the availability of the services.

- DOS attack is main reason for threat to the availability.

B. Secure Architecture

Generally the IoT can be separated into four key levels [18].Figure 4.Shows that the IoT level architecture.

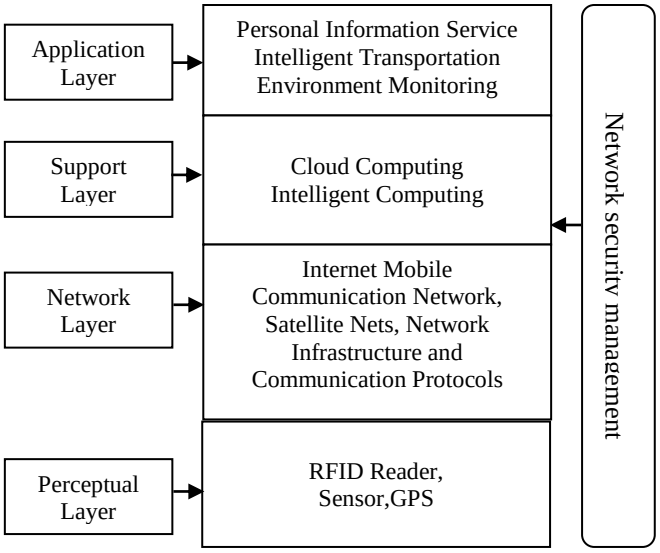

Figure 4: Security architecture

- ***Application Layer****:* In this level security needs for different application environment and data sharing is the one of the main characteristics of application layer, which creating issues of data privacy, access control and disclosure of information [18,19]. To solve the security problem of application layerwith the help of two aspects. On the one hand, authentication and key agreement across the heterogeneous network and on the other hand, user's privacy protection. In addition that, education and management are very vital role to information security, especially password management [18,19].
- ***Support Layer*****:** In the layer, data processing and intelligent decision of network behavior can be done. Intelligent processing is limited for malicious information, so it is a challenge to enhance the ability to recognize the malicious information. Support layer requires a lot of the application security architecture such as cloud computing and secure multiparty computation, use strong encryption algorithm and encryption protocol, stronger system security technology and anti-virus.
- ***Network Layer:*** Even though, the core network has relatively absolute safety protection ability, but Man-in-the-Middle Attack and counterfeit attack still be present, in the meantime junk mail and computer virus cannot be ignored, a large number of data sending cause congestion. Therefore security mechanism in this level is very essential to the IoT. In this layer existing communication and security mechanisms are complicated to apply. Identity authentication is a one of mechanism to avoid the illegal nodes, and it is the principle of the security mechanism, confidentiality and integrality are of equal importance, thus we also need to establish data confidentiality and integrality mechanism. Further distributed denial of service attack (DDoS) is a general attack method in the network and is mostly severe in the internet of thing, so to avoid the DDOS attack for the vulnerable node is another issue to be solved in this layer.
- ***Perceptual Layer:*** Generally perceptual nodes are less computer power and storage capacity because they are simple and with less power. Therefore it is unable to use frequency hopping communication and public key encryption algorithm to security protection. And it is very complicated to set up security protection system. Meanwhile attacks from the external network such as deny of service also carry new security issues. In the other hand of sensor data still necessary to protect secure communication for integrity, authenticity and confidentiality. At initial node authentication is necessary to prevent protection from illegal node access, and before the data encryption key agreement is an important process in advance technology. Resources consumption is stronger and more secure for the safety measures to solve this issues, lightweight encryption technology becomes very important, which includes Lightweight cryptographic algorithm and lightweight cryptographic protocol.

V. CRYPTOGRAPHIC

Generally the symmetric encryption algorithm is used to encrypt data for authenticity and confidentiality such as the advanced encryption standard (AES) block cipher. The asymmetric algorithm is frequently used to key transport and digital signatures, frequently-used algorithm is the rivest shamir adelman (RSA). The diffie-hellman (DH) asymmetric key agreement algorithm is used to secure data encryption key agreement. The SHA-1 and SHA-256 secure hash

algorithms will be useful to integrality process. Another significant asymmetric algorithm is called as elliptic curve cryptography (ECC), ECC can provide equal safety protection by using shorter length key encryption, the adoption of ECC has slow down and maybe encouraged recently [20]. To implement these cryptographic algorithms available resources are necessary to improve processor speed and memory. In order to solve, whether it is located in IoT devices, Talos relies on optimize algorithms that accelerate partially homomorphic encryption and order-preserving technique by 1 to 2 orders of magnitude. In this paper review an achievability of Talos on low-power consumption devices, it is check whether the device with and without cryptographic accelerators and measure its overhead within terms of latency, energy and computation.

A) Order-preserving encryption

Order-preserving encryption is a special important case of property preserving encryption [21, 22]. This encryption performs sorting and searching the order and it is useful property to preserve. Using other cryptographic schemes, searches on encrypted data can also be performed, usually encryption scheme specific search algorithms.Cryptographic schemes like searchable encryption, functional encryption and homomorphic encryption. Searchable encryption [24] accomplishes a stronger notion of security after perform order-preserving encryption. Searchable encryption has been presented [22, 23, 25] for range queries.Token of range boundaries is generated by using the secret key to match with ciphertexts which are within the range boundaries of this token. Searchable encryption schemes require data which is performed by a linear scan, unless additional indexing information is provided. Searchable encryption is a special important case of functional encryption. Functional encryption allows any function on a set of ciphertexts, such that the result of the function is revealed. Recently, functional encryption has been designed for general functions [14]. Specific functions, like the inner product, have been proposed before [21]. Functional encryption can also reveal only the order while else remaining semantically secure [11]. Homomorphic encryption can also be implemented by using searching encryption where the search result remains unknown to the service provider. Theis involves if the result size is unbounded, the entire database necessary to be transferred for several query. Completely homomorphic encryption [13] enables arbitrary search functions.

An order-preserving symmetric encryption (OPE) scheme with plaintext-space [M] and ciphertext space [N] is a tuple of algorithms OPE = (Kg, Enc, Dec) where:

- The randomized key-generation algorithm Kg outputs a key K.
- The deterministic encryption algorithm Enc on inputs a key K and a plaintext m outputs a ciphertext c.
- The deterministic decryption algorithm Dec on inputs a key K and a ciphertext c outputs a plaintext m.

In addition to the usual correctness requirement that

$$Dec(Enc(K, m)) = m$$

for every plaintext m and key K, require that

$$m1 \leq m2 \text{ if and only if } Enc(K, m1) \leq Enc(K, m2)$$

for all plaintexts m1, m2 and every key K. For notational convenience, extend encryption notation to sets. That is, if X is a set then Enc(K, X) denotes the set $\{Enc(K, x) \mid x \in X\}$.

B) Partial Homomorphic Encryption

Partial Homomorphic Encryption (PHE) schemes allow to the computation over encrypted data of certain mathematical operations. For example, additive homomorphic schemes, such as the Paillier cryptosystem [14], support the addition of ciphertexts, such that the result is equivalent to the addition of the plaintext values (i.e.,$ENC(m_1)$ o $ENC(m_2) = ENC(m_1 + m_2)$).

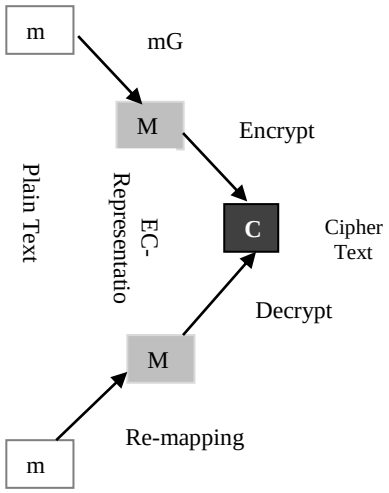

Figure 5: Plaintext to EC point mapping (before encryption and after decryption).

The Elliptic Curve (EC) version of the ElGamal cryptosystem is an alternate additive homomorphic scheme, utilized in Talos and Pilatus.EC-ElGamal's security is established on the EC Discrete Logarithm Problem (ECDLP) [26]. The ECDLP provides semantic security (i.e., IND-CPA under the assumption of decisional Diffie-Hellman). A challenge in making realistic use of EC-ElGamal operates over EC points rather than arbitrary messages. Hence, a scheme maps an integer to an EC point (and back), whereas preserving the homomorphic property of EC-ElGamal. Talos, which focuses on IoT data, utilize a theoretical method [27] that becomes realistic for small integer data, e.g., 32-bit (frequent in IoT scenarios, to represent an integer or fixed point number) [28]. The process as follows to map an integer m to an EC point M, m is multiplied by a widely known point G on the curve: M = m G. After decryption, M must be mapped back to m. This needs to solve an ECDLP. Even though this is computationally infeasible for large numbers, solving it for smaller than 32-bit integers can be analyzed in a reasonable specific time with, e.g., the Baby-Step-Giant-Step(BSGS) algorithm (this is equivalent to breaking 32-bit security).As the result, this mapping procedure, as shown in Figure 3, does not affect the overall security: the ECDLP is solved to obtain from M, therefore M itself is secured with strong cryptography, in this case,80-bit or 128-bit security.

VI. CONCLUSION

IoT systems have the ability to make huge changes to our professional life and personal life. In this concept, the IoT has the capability to reduce waste, improve efficiency, and create new markets through better opportunities and newly gathered data. A practical secure system provides secure communication between readers and it is provide data security features for privacy-preserving IoT applications. Talos allows computation on encrypted data only without disclosing decryption keys to the Cloud. To achieve this process, the system utilizes optimized encryption schemes, specifically for the expensive additive homomorphic and order-preserving encryptions, accelerating them by 1 to 2 orders of magnitude.

VII. REFERENCES

[1]. L. D. Xu et al., "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, Nov 2014.

[2]. L. Coetzee and J. Eksteen, "The internet of things - promise for the future? An introduction," in Proceedings of IST-Africa Conference, 2011.

[3]. H.-D. Ma, "Internet of things: Objectives and scientific challenges," Computer Science and Technology, Springer, vol. 26, no. 6, Nov 2011.

[4]. M. Botterman, Internet of Things: an early reality of the Future Internet. a Workshop Report, European Commission, May 2009.

[5]. S. Gusmeroli, S. Piccione, D. Rotondi, "A capability-based security approach to manage access control in the internet of things", Mathematical and Computer Modelling 58 (5) (2013) 1189.

[6]. Kiev Gama, Lionel Touseau, Didier Donsez, "Combining heterogeneous service technologies for building an Internet of Things middleware", Computer Communications, Volume 35, Issue 4, 15 February 2012, Pages 405-417, ISSN 0140-3664.

[7]. R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Computer Networks 57 (10) (2013).

[8]. N. Sklavos, R. Chaves, F. Regazzoni, Wireless-SoC-Security: "FPGA Based System-On-A-Chip Security Schemes for 4G & 5G", Tutorial, 11th HiPEAC Conference 2016 (HiPEAC'16), Prague, Czech Republic, January 18-20, 2016.

[9]. N. Sklavos, "Securing Communication Devices via Physical Unclonable Functions (PUFs)", Information Security Solutions Europe (isse'13), Brussels, 22-23 October, Belgium, 2013, pp. 253-261, Springer, ISBN: 978-3-658-03370-5.

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

[11]. Stephen Tu, M. Frans Kaashoek, Samuel Madden, and Nickolai Zeldovich. 2013. Processing Analytical Queries Over Encrypted Data. In Proceedings of the Conference on Very Large Data Bases (VLDB).

[12]. Vlado Altmann, Jan Skodzik, Frank Golatowski, and Dirk Timmermann. "Investigation of the use

of embedded Web Services in smart metering applications". In: Conference on IEEE Industrial Electronics Society. IECON. Oct. 2012, pp. 6172–6177. DOI: 10.1109/IECON.2012.6389071.

[13]. Sven Bendel et al. "A service infrastructure for the Internet of Things based on XMPP". In: Int. Conference on Pervasive Computing and Communications Workshops. PERCOM Workshops. Mar. 2013, pp. 385–388. DOI: 10.1109/PerComW.2013.6529522.

[14]. SHEN changxiang, ZHANG Huanguo and FENG Dengguo, "Literature Review of Information Security" Science in China (Series E: Information Sciences), vol.37, no.2, 2007, pp.129-150

[15]. WU chuankun, "A Preliminary Investigation on the Security Architecture of the Internet of Things," Bulletin of Chinese Academy of Sciences, vol 25, no. 4, 2010, pp 411-419.

[16]. Anne James and Joshua Cooper, "Database Architecture for the Internet of Things," IETE Technical Review, vol.26, 2009, pp.311-312.

[17]. Abdemalek Amine, Otmane Ait Mohamed, Boualem Benatellah "Network Security Technologies: Design and Applications"

[18]. G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[19]. C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

[20]. T. Polk, and S. Turner. "Security challenges for the internet of things," http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[21]. Agrawal, S., Agrawal, S., Badrinarayanan, S., Kumarasubramanian, A., Prabhakaran, M., and Sahai, A. Function private functional encryption and property preserving encryption: new definitions and positive results. Tech. Rep. 744, IACR Cryptology ePrint Archive, 2013.

[22]. Boneh, D., and Waters, B. Conjunctive, subset, and range queries on encrypted data. In Proceedings of the 4th Theory of Cryptography Conference (2007), TCC.

[23]. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the Symposium on Theory of Computing (2009), STOC.

[24]. Goldwasser, S., Kalai, Y. T., Popa, R. A., Vaikuntanathan, V., and Zeldovich, N. Reusable garbled circuits and succinct functional encryption. In Proceedings of the Symposium on Theory of Computing (2013), STOC.

[25]. Hacig¨um¨us, H., Iyer, B. R., Li, C., and Mehrotra, S. Executing sql over encrypted data in the database-service-provider model. In Proceedings of the ACM International Conference on Management of Data (2002), SIGMOD.

[26]. Katz, J., Sahai, A., and Waters, B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Advances in Cryptology (2008), EUROCRYPT.

[27]. Lu, Y. Privacy-preserving logarithmic-time search on encrypted data in cloud. In Proceedings of the 19th Network and Distributed System Security Symposium (2012), NDSS.

[28]. Pandey, O., and Rouselakis, Y. Property preserving symmetric encryption. In Proceedings of the 31th International Conference on Advances in Cryptology (2012), EUROCRYPT.

[29]. Shi, E., Bethencourt, J., Chan, H. T.-H., Song, D. X., and Perrig, A. Multi-dimensional range query over encrypted data. In Proceedings of the 2007 Symposium on Security and Privacy (2007), S&P.

[30]. Song, D. X., Wagner, D., and Perrig, A. Practical techniques for searches on encrypted data. In Proceedings of the 21st IEEE Symposium on Security and Privacy (2000), S&P.