A Survey on Securing IoT Systems

[1]Antara De,[2]Dr H S Guruprasad

[1]Assistant Professor, [2]Professor and Head
[12]Department of Computer Science and Engineering,
[12]BMS College of Engineering, Bangalore,India

***Abstract*—The emerging trend of Internet of Things (IoT) has spread across almost all components of modern life, starting from smart building, smart city, medical care, wearable devices, automobiles or industries. However, physical things getting attached to the Internet poses new challenges of making the entire system more vulnerable, prone to attacks and misuse. Moreover, the heterogeneous nature of all different devices, resource-constrained wireless sensor network nodes make traditional security algorithms inapplicable for IoT scenario. So, IoT systems should consider applying new set of security measures to deal with IoT specific security needs. In this paper, we review the major IoT security approaches, namely authentication & authorization, context aware lightweight protocol design & key management, anonymity, data privacy, trust and standardization. We conclude our discussion by listing the future research direction with respect to securing IoT.**

***IndexTerms*—Internet of Things, Security, Privacy, Trust, Standardization**

I. INTRODUCTION

The emerging trend of Internet of Things (IoT) has spread across almost all components of modern life, starting from smart building, smart city, medical care, wearable devices, automobiles or industries [18, 21, 25, 26]. However, connecting physical things to the Internet poses new challenges of making the entire system more vulnerable, prone to attacks and misuse. In this scenario, communication security and end user privacy may get compromised. Moreover, the heterogeneous nature of all different sensor nodes and traditional Internet hosts makes the security system more difficult.

The most important concern here is how to securely access & transmit the data collected by different sensor nodes. Authentication & authorization strategies have generally been applied to ensure data security [18, 21, 27, 30, 31]. Authentication supports the identity validation of an object, i.e. ensures that the entity is exactly that one what it is claiming to be. Authorization deals with access rights over the resources or the services for different users/subjects. Traditional encryption algorithms are not suitable for IoT scenario because IoT devices are mostly resource-constrained and data would usually get corrupted during data transmission. So, IoT systems should use *lightweight* resource efficient encryption algorithms with error correction capabilities (error tolerance) [1, 28, 34, 44]. IoT architecture consists of heterogeneous resources at different places at different times. However, access right for a particular resource can be different at different places and times. So, any authorization scheme for IoT should be *context aware* i.e. should take into account location & temporal constraint in order to provide robust security [17, 25].

Another concern is user data privacy [11, 13, 35, 41]. IoT is built on the concept that data will be accessed from different physical components (say sensors), stored and processed in Internet and some action will be taken based on the data analysis. So, IoT systems collects a lot of private data (for example: user habits) which must be privately stored and accessed, otherwise IoT can produce security threats however trivial the data seem to be. For example: energy consumption data in smart home can also be analysed to predict home occupancy status (i.e. if the user is present at the residence or not). Trust deals with the reliability of two parties involved in IoT interactions [7, 12, 29, 35, 46, 47]. Trust component provide quantified trust scores which can be used by other security components to make security and privacy decisions. Standardization perspective of IoT security ensures that the heterogeneous IoT devices can securely exchange data among each other in interoperable manner [23, 52].

The rest of the paper is structured as follows: We review the previous surveys related to security systems in Section II. A detailed discussion on the existing security systems is presented in Section III. We present the challenges & future opportunities for research on securing IoT systems and conclude our discussion in Section IV.

II. PREVIOUS SURVEYS

Before delving into our survey of security mechanisms for IoT systems, let us devote some time discussing some of the relevant previous surveys done in this field.

Qi Jing et al. in their 2014 survey paper [19] provide an extensive overview of the security threats in IoT. Here, it is mentioned that IoT comprises of three layers: 1. perception layer, 2. transportation layer & 3. application layer. The security challenges & potential solutions are discussed for each layer separately. Cross-layer communication with many heterogeneous devices attached together and security issues specific to this are also described in this paper. With respect to perception layer, security challenges mentioned are: 1. Security issues of RFID technology (such as Uniform coding, Conflict collision, RFID privacy protection and Trust management) 2. Security challenges & solutions in WSNs (such as Cryptographic algorithms, Key management, Secure routing protocols, Trust management of nodes in WSNs) 3. Security challenges with respect to heterogeneous integration. In transportation layer, security issues are discussed with respect to functional architecture (such as Access network, Ad hoc security issues, 3G network security issues etc.). For Application layer, the security issues described with reference to 1. Application support layer (Security threats, Service interruption and attack issue, Investigate audit issues), 2.Security challenges of IoT applications (such as Intelligent transportation, Smart home). Detailed comparison between security

requirements in IoT and traditional network is also provided here. This paper concludes that IoT applications have to deal with more dangerous security issues with IoT's limited resource capacity. Thus, future research should concentrate on developing lightweight security protocols and computationally efficient strategies to deal with huge amount of heterogeneous data.

S. Sicari et al. in their 2015 survey paper [39] present the published works in literature regarding security, integrity, trust and privacy in IoT scenario. The paper concludes that future research should focus on the development of 1. Platform independent comprehensive security framework for heterogeneous devices. 2. Unification of IoT and data transfer technologies in a secured middleware. 3. Securing mobile devices involved in IoT.

III. SECURITY SYSTEMS

We show different security requirements of IoT in Figure 1

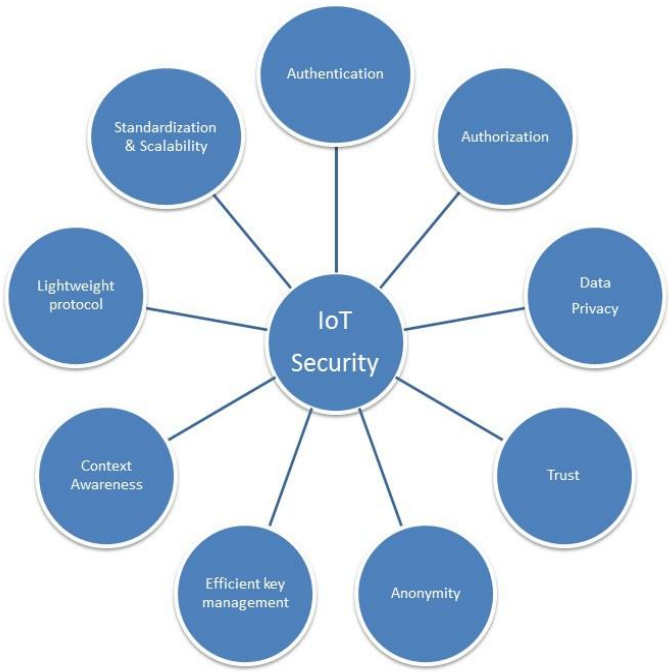

Figure 1: Security Requirements of IoT

The fundamental requirement for any IoT security systems can be summarized as follows: 1. Authentication & Authorization 2. Data Privacy 3. Trust between involved parties 4. Anonymity 5.Efficient key management protocol 6.Context aware security system 7.Lightweight security technique. 8. Forward secrecy 9. Hierarchical Access regulation 10.Standardized, scalable approach. In this section, we will review how previous researches have addresses all these requirements.

A. Authentication and Authorization

The most important part of any security system is undoubtedly authentication & authorization. Authentication supports the identity validation of an object i.e. it ensures that the entity is exactly that one what it is claiming to be. The identity of different users and smart objects is validated by credentials such as digital signature or login id/password [39]. Authorization deals with access rights over the resources or the services for different users/subjects. So, it can be said that authorization policy defines which particular resources/services can be accessed by any given user/subject under what specific conditions (for example: temporal and spatial constraint) [39]. Our discussion in this section reviews general authentication & authorization strategies along with some specific security architectures which focus on either context awareness, reducing the computation complexity or key management or anonymity.

SheetalKalra et al. in [21] categorize the threat model in security systems in the followings ways: *1. Eavesdropping:* Message between device & cloud is travelling via insecure channel and thus any adversary node can access the private data. *2. Traffic Analysis:* It deals with the analysis of eavesdropped message to crack the device's authentication information to the server. *3. Replay Attack:* Adversary node can send eavesdropped message using the server. *4. Man in the Middle Attack:* Adversary node impersonates legitimate device for a server, it accesses the response message from the server, adversary impersonates legitimate server for a device and transmits the previously received messages. *5. Cookie Theft:* Accessing cookies in illegitimate ways & modifying cookies. *6. Offline dictionary attack:* Storing of previous communication messages between device & server so that security parameters can be accessed afterwards. *7. Leak of verifier attack:* Attack & steal information from the server itself. Authentication & data privacy of all the devices connected to cloud is of interest in IoT security system. SheetalKalra et al. [21] propose the use of a secure Elliptic Curve Cryptography (ECC) [16] based authentication protocol for secure data exchanged between embedded devices and cloud servers, which uses Hyper Text Transfer Protocol (HTTP) cookies. ECC has the advantage

of having small key sizes and faster computation over other Public Key Cryptography algorithms. The proposed protocol is verified by AVISPA tool [3]. Authors claim that the proposed protocol is robust against all attackers and also computationally efficient.

A security framework for software defined networking (SDN) is proposed by Flauzac Olivier et al. [31]. Authors claim that this is the first work to integrate current network access control and security methodologies for SDN perspective in IoT. Here, authors present a new security framework with more than one SDN controllers in equal interaction. Next, the architecture is scalable to multiple SDN domains. each controller will have only one domain to control. Inter-domain communications are executed by special controllers, called Border controllers. Another type of controller, named Edge controller, works on distributed interaction in order to ensure the independence of every domain. Here, the security prototype is based on Grid of security paradigm. The developed algorithm can be used in both wired and wireless network and is capable to work in heterogeneous scenario with ad-hoc network consisting of different sensor nodes like smart phones, tablets etc.

HuanshengNing et al. propose an hierarchical, aggregated-proof based authentication framework [30] for unit IoT and ubiquitous IoT architecture (U2IoT) layered networks. Authors mention that the security solution for U2IoT architecture should possess the following properties: 1. CIA (i.e., confidentiality, integrity, and availability) for data, 2. Hierarchical access regulation, 3.Forward security, 4.Mutual authentication, 5.Privacy preservation. The aggregated proof are generated by wrapping numerous targets' information in order to establish forward & backward anonymous information exchange. Here, authentication framework integrates the directional path expressions defined based on homomorphism functions, Chebyshev chaotic maps [14] (utilized to establish the mapping co-relation between the path descriptors and the shared secret keys to achieve mutual authentication). Several access authorities are assigned for achieving hierarchical access regulation.

Yijun Mao et al. [27] mention the use of fuzzy identity-based encryption(FIBE) [33] for secure communication in IoT framework. Traditional FIBE approaches have the following shortcomings: trust random oracle model, prone to attacks in secure selective-ID model etc. In this paper, a new FIBE scheme is proposed. The proposed algorithm is secure in full model without using random oracles. This scheme supports tight security reduction, short key and fixed size public parameters and thus it is quite efficient.

.

1) Context Aware Protocols

IoT architecture consists of heterogeneous resources at different places at different times. However, access right for a particular resource can be different at different places and times. So, any authorization scheme for IoT should take into account location & temporal constraint in order to provide robust security. In this regard, Chao Lee et al. [25] present Location-Temporal Access Control Model (LTAC). Here, lattice approach is used to reduce the size of policy bases. Authors describe how the location data is relevant for determining whether a particular user has appropriate access rights for a particular resource. In the proposed model, access rights for a specific resource is determined by their time and location with reputation, which means the algorithm considers where and when to authorize resource access requests, which particular user is being capable to access the resource and use the concept of access lattice to reduce the size of policy base. Further research may concentrate on taking into account communication instability and therefore delayed access to authorization information.

JosÃ L. Herndez-Ramos et al. [17] focus on developing an Architectural Reference Model(ARM) [36]-based IoT security system for smart homes. Authentication and authorization have been considered here to restrict the access to services. This contextual data as primary component to run the building management and to support home security, in order to enable context aware security for IoT framework. Specifically, authors use localization data as access control mechanism for the services provided by smart homes. This security framework is integrated with City Explorer [6], a smart home service management platform, which deals with the main aspects of security system ensuring the proper execution of user-oriented services, such as user comfort and energy saving.

2) Lightweight Security Architecture & key Management

SomiaSahraoui et al. [34] mention that the heterogeneous nature of all different sensor nodes and traditional Internet hosts makes the security system more challenging in IoT scenario. In IoT, WSN is used where the nodes are generally resource constrained. For this reason, many security algorithms have adapted IP-based algorithms to match with requirements of WSN nodes, by using either message compression or processing load-distribution methodologies. In this paper, authors introduce an robust methodology where 6LoWPAN ("IPv6 over Low power Wireless Personal Area Networks") [37] compression technique is applied on the headers of HIP (Host Identification Protocol) [24] packets. A load distribution scheme is also proposed here for HIP Base EXchange (HIP-BEX) [5]. The load distribution structure focuses on the secured handing over of the computation intensive cryptographic operations in HIP-BEX to a resource-rich remote connected node, ensuring the transparency of the communication for the external Internet user. Both of these compression and load distribution schemes are proposed to achieve energy efficient, lightweight end-to-end security algorithm, named "Compressed and Distributed HIP(CD-HIP)", which is compatible to standard HIP. Authors claim that this the first work to combine load distribution & compression technique in HIP domain.

SanazRahimiMoosavi et al. [28] try to develop a robust and efficient authentication & authorization framework for smart medical systems. For smart medical systems, patients' private data should be protected securely. So, this paper specifically deals with the authentication & authorization of remote medical practitioner who is accessing the data over the Internet. In this approach, authors consider the resource constraints of WSN nodes and delegate the authentication and authorization of remote process by distributed smart e-health gateways. The designed framework makes use of certificate based Datagram Transport Layer Security (DTLS) [33] handshake protocol as primary security algorithm. The prototype implementation of the algorithm is made using a Pandaboard, WiSMotes and a Texus Instrument SmartRF06 board. The experimental results show that this

algorithm can reduce the impact of DoS attacks by its distributed architecture, reduces communication overhead by 26% and speeds up the communication by 16%.

Mohammed Riyadh Abdmeziem et al. [1] propose a secure key management protocol for e-health scenario. Secure key distribution in IoT applications becomes challenging because of having resource-constrained nodes. In order to solve the above mentioned problem, authors develop a lightweight key management protocol which works as follows: First an end-to-end shared secure communication channel is established between a highly low resource node and a remote node (i.e. server), using symmetric cryptography. The constrained node transmits the sensed data to the resource-rich node via secure communication channel, which ensures authentication and confidentiality. Here, a cryptographic primitive, which has high resource requirements, is delegated to third parties, which are not always trusted. Thus, the low resource nodes get assisted by the resource-rich nodes.

Jun Wu et al. [44] focus on security distributed information storage in social Internet of things(SIoT) [4]. SIoT architecture emphasizes on storing the distributed data fragments in different sensor nodes and the storage must possess self-healing capability i.e. regenerate the corrupted data & protect data confidentiality. In order to fulfill the mentioned objectives, a novel Bloom based key management technique is proposed based on regenerating codes as well as symmetric-key encryption. Here, the data blocks, generated from j^{th} nodes & getting stored in i^{th} node, are encrypted by symmetric key Kij. Due to the fact that both Blom's key management [37] and regenerating codes are based on Vandermonde matrix (used to provide space usage reduction & computational efficiency), they can be easily integrated.

3)Anonymity

AlmudenaAlcaide et al. [2] try to develop an anonymous authentication framework for ensuring privacy protection in IoT applications. Here, a fully distributed anonymous, self-adapting authentication protocol has been proposed for target-driven IoT scenarios. The system consists of an ad-hoc network of distributed nodes. However, all these decentralized nodes can interact, take part in cyber physical systems, ensuring complete anonymity. The main advantages of this particular protocol are as follows: 1. No dependence on any central node, not even in the set-up phase. Here, not any central node alone, but all the distributed nodes cooperatively generate the parameters required for the security system. 2. The proposed framework is compatible in the future IoT scenarios. 3. Here, the set of nodes from which data should be collected can be controlled by the data collector node, with the help of attribute-based access restriction strategies which are basically linear Boolean functions whose input parameters are the attributes specific to the Users. 4. Strategy at the data collector node can be easily modified without changing the rest of the system. 5. Any user can communicate with data collector node in fully secured manner, guaranteeing full anonymity.

B. Privacy

The Internet of Things (IoT) supports anywhere, anything, anytime communications. IoT combines a diverse set of devices, sensors, software like mobile app etc. and all these "things" communicate with each other sometimes directly or via Internet. Here, all the devices are autonomous, however, the devices should share/access some of their capabilities or sensed data with the other devices to accomplish one work collectively. So, ensuring data privacy of all those devices becomes one of the prime concerns for the security systems [39].

Sophie Chabridon et al. in his 2014 survey paper [11] provide an intensive overview of the methodologies supporting privacy management in IoT while ensuring quality for context management. Authors identified three major challenges in privacy preservation & quality of context management as: 1. Context data production/consumption decoupling, 2.Quality of Context (QoC)-aware privacy 3. Dynamic interdependency of QoC and privacy. Privacy is considered with respect to confidentiality, anonymity in communication, data minimization and control. Different privacy-enhancing technologies have been used in literature to ensure protection of private contextual information in context management scenario including context data accumulation, context data analysis and dissemination. However, this paper concludes that there is still need for new policy languages capable to deal with heterogeneous anonymity and data protection for the contextual data processing chain. Users also need transparent privacy solutions where the user can feel the control of their own security. Authors envision that future researches should concentrate on the dynamic nature and different spatial-temporal dimension of context management.

Ensuring privacy of collected data from smart homes becomes a big issue of concern for the IoT perspective. In smart home, all the objects under surveillance are going to have unique RFID code attached. So, user profile can be easily created from the smart home queries. Benjamin Fabian et al. [13] propose an innovative peer-to-peer (P2P) framework for systematized sharing and anonymity-preservative retrieval of data, which is designed by various smart devices across several smart homes. Structured P2P frameworks are advantageous to use because these have less computational cost and scalable to future requirements. Authors, here in this approach, use Octopus DHT lookup [43] to collect the either complete product data or else at user-specific data securely as well. Here, authors use SHA-1 hash of the Eigenspace projection clustering (EPC) [10] algorithm as key value.

AfshanSamaniet al. [35] present a privacy ensuring platform based on Cooperative Distributed Systems (CDS) [26], used as computational framework where different devices are autonomous. Here, authors model privacy preservation as "sensitive information" management while different entities are interacting. Here, smart objects contain sensitive data. Here, Privacy Protection Level has been proposed to assess the uncertainty level in privacy preservation methodologies. It utilizes the interaction and protection protocols to establish a privacy supportive interaction scheme. The use of the structure has been verified by extending Contract Net Protocol [40] to provide privacy preservation.

A protection policy, specifically, an attribute based signature Scheme, that preserves data privacy is developed by Jinshu Su et al. in [41]. Emerging attribute based signature (ABS) [15] protocols permit a user making request for a resource to produce a signature with attributes fulfilling the requirement of the protocol without making unnecessary data public. Also, many security policies have been proposed in literature by using Diffie-Hellman assumption [9]. Here, authors present an novel ABS framework where attribute tree is used and also any policy comprising of AND, OR gates can be expressed as Diffie-Hellman problem. Here,

two levels of random values are used to generate user private key specific to a set of attributes, in order to mitigate collision attacks. The policy is modeled as attribute tree, consisting of AND, OR threshold gates over the set of attributes. In order to validate the signature, public key for the tree is utilized, so that signatures produced by attributes meeting the requirement of the tree can be recognized. Another advantage of this scheme is unforgeability of signatures. User cannot forge signature until and unless he possess the correct attributes. In this framework, the attributes of the user are not sent with the signature. So, the verifier has to validate the set of attributes for the tree from the signature only. So, this architecture supports guaranteed attribute privacy for signers.

C. Trust

Trust deals with the reliability of two parties involved in IoT interactions. Trust component provides quantified trust scores which can be used by other security components to make security and privacy decisions [39].

Zheng Yan et al. in their 2014 survey paper [47] provide an exhaustive discussion on trust management in IoT scenarios. Authors mention the trust properties which are important for trust relationships and then classify trust properties into five sub-categories such as 1.“Trustee’s objective properties": trustee’s dependability, security etc., 2. “Trustee’s subjective properties" for example trustee’s goodness, honesty etc., 3. “Trustor’s subjective properties", for example trustor disposition etc. 4. “Trustor’s objective properties": specific criteria, policy etc. 5. Context: temporal and location context etc. Authors conclude that, depending on the context or purpose, either all or part of the mentioned trust properties should be the prime factor(s) for exhaustive trust management. Ten general objectives are presented for complete trust management. The general objectives are: Trust relationship and decision, Data perception trust, Privacy preservation, Data fusion & mining trust, Data transmission & communication trust, Quality of IoT services, System security & robustness, Generality, Human-computer trust interaction, Identity trust. The paper also concludes that the IoT supporting layers, by asserting vertical trust management, can be of prime importance for trust management. The existing works in the literature with reference to trust management, are reviewed under the light of eight taxonomies and open issues (making trust management context aware, complete trust management fulfilling all ten trust properties etc.), challenges (heterogeneous IoT, power efficiency, performance improvement, human privacy & business transaction’s confidentiality preservation, self-supporting trust management, trustworthy data integration etc.) and future research areas are also noted here. A new research model for complete trust management is proposed here. The proposed model considers not only inter layer & cross layer trust properties, but also focuses on providing smart IoT services for trusted relationships.

Bernal Bernabe et al. [7] focus on developing lightweight, flexible, adaptive access control strategies for millions of devices connected all over the world, ensuring reliable interaction among trusted parties. In order to address this challenge, authors develop a trust-aware access control system for IoT (TACIoT), which supports lightweight authorization technique, reliable security framework for the IoT nodes and a new trust model specially customized for IoT applications. Specifically, authors enhance previous access control mechanism by considering trust values which are dependent on four parameters : quality of service, security solutions and devices’ reputation & social relationships. The effectiveness of TACIoT is verified by deploying implemented solution in real deployment scenario for resource-limited and resource rich, powerful devices.

X. Xu et al. [46] propose an automatic agent trust modeling framework for Internet of Things paradigm. The authors focus on addressing security challenges by enhanced reliability as well as credibility while exchanging/processing data. In this architecture, agent & agent frameworks have to be developed on all nodes. An independent, autonomous hardware & software supported system can be termed as agent-based node. The agent technique is also beneficial for regulating the access to the resource also. In this paper, a novel framework, TAEC (Trustworthy Agent Execution Chip) has been presented to develop highly secured, less costly software as well as hardware platform in order to ensure the safety of the Agent. Here, TAEC has to be installed on every sensor node, thereby providing autonomic trusted hardware framework for agents. The following features are supported by Agent Protection model developed on the basis of TAEC: Platform Independence, Multi-function(i.e. more than one agents can run in a single TAEC chip), easy to upgrade with new systems, Flexibility (i.e. supports on-chip programming facility, Compatibility with the international SoC standards &integrable with industry standards, thereby enhancing interoperability between the TAEC and agents.

Kai Kang et al. present an Interactive Trust Model [22] for service distribution area, specifically, for the interaction between application market and the users. Security in application market demands the user data protection by establishing a symmetric methodology where the trustworthiness of an application can be evaluated. In the proposed framework, the resemblance between the current behaviour of the application and behaviour as expected by the user, is taken into account for quantitatively determine application trustworthiness (AT). Specifically, feedback vector & evaluation vector for any particular application in the application market and behaviour of that application on the smart devices can be represented in mathematical formula to form the association between market and users. In smart device, behaviour-based identifying agents can provide proof about the applications having threat potential for the system security/privacy. Data collected from end smart devices is analysed to generate the trustworthiness indicators. This indicator can be displayed in the market along with the application, so that the end user can make a better decision about whether to install one app or not.

The efficiency of any trust evaluation technique is largely dominated by trust parameter calculation, due to the reason that overhead to compute trust parameter largely impacts the resource(bandwidth, power) constrained WSN nodes. In order to address the requirements of WSN, JunqiDuan et al. [12] develop a novel Energy-Aware trustworthiness calculation framework by using Game Theoretic techniques in WSN for IoT Applications. This approach aims to reduce computational overhead and network latency while ensuring robust security for WSN nodes. At first, cooperation between WSN nodes has been modeled by a risk strategy model. This model can be utilized to calculate minimum possible count of recommendations. Next, the trust derivation technique is aided by game theoretic methodologies, specifically trust derivation dilemma game, in order to reduce computational overhead of the entire process. The effectiveness of this approach is verified by extensive simulation experiments.

WU Qiu-xin et al. [45] propose secure trust solution based on trusted cryptography modules (TCM). The paper first analyses the security attributes based on TCM as 1. Trusted sensor node, sensor data confidentiality, sensor data integrity, trusted data source. The algorithm proposed in this paper focuses on enhancing & promoting trusted computing. It covers a broad spectrum of security solutions such as secure boot, storage security, trusted reports, platform metrics, and key functions and suggests a new protocol with all these functionalities. The functionalities supported by secured TCM can be divided in three categories: 1. Platform measurement and report (report can be generated about computing platform's integrity & configuration position and remote verifiers can trust these reports). 2. Safe storage (user data can be protected by secret key generated by TCM and the encrypted data can be decrypted only under trusted platform) 3. Platform authentication.

Ricardo Neisse et al. present a "Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework" [29]. In this work, Event-Condition-Action enforcement regulations are applied for security protocols, which takes into consideration context, role models as well as identity. Here, IoT system structure is viewed as the integration framework of structure, data &behaviour. Authors develop privacy-securing middleware with behaviour-specific services for adjusting to context, privacy-ensuring data collection & transmission according to security & privacy regulations at the device layer, stickyflow rules to annotate data & specify how that data can be utilized.

D. Standardization and Scalability

SyeLoongKeoh et al. [23] focus on standardization perspective so that the heterogeneous IoT devices can securely exchange data among each other in interoperable manner. This paper summarizes the standardization initiative taken up by the Internet Engineering Task Force (IETF) [18]. In this paper, a detailed study on existing security protocols used together with Constrained Application Protocol (CoAP) [38], an application protocol adapted to the resource constraints on WSN nodes, is discussed. Datagram Transport Layer Security (DTLS) [33] is used as the underlying security protocol in CoAP. So, this paper provides a discussion on approaches to standardize the DTLS for IoT scenario. Authors review how raw public key can be used in DTLS, how DTLS record Layer can be extended to secure multicast communication, how DTLS can be profiled to optimize the key size and reduce the computation complexity on embedded platform. Also, a detailed review is provided on the compression schemes proposed in literature to address the message fragmentation issue in DTLS.

Biplob R. Ray et al. [32] mention that many RFID security frameworks have considered anonymity & privacy, but little concern is provided for customization & scalability of IoT applications. Moreover, the existing works mostly have a number of shortfalls such as incompetent identification techniques, latency & non-compatibility. In this paper, authors develop an innovative identification methodology by following a hybrid approach(group approach as well as collaborative) and security check handoff mechanism for mobile RFID systems. The proposed model focuses on customization, adaptability, robust & scalable security deployment. This protocol framework consists of four system modules at the Application Level Event layer of EPCglobal Architecture [42]. An additional level of protection is provided against malwares like SQLIA [20]. The efficacy of this protocol is verified by randomness battery test. Future research in this direction may take in account tag tamper protection and increasing computational efficiency.

IV. CONCLUSION

In this paper, we reviewed different security strategies considered by previous researches for IoT systems. The fundamental requirement for any IoT security systems can be summarized as follows: 1. Authentication & Authorization 2. Data Privacy 3. Trust between involved parties 4. Anonymity 5.Efficient key management protocol 6.Context aware security system 7.Lightweight security technique. 8. Forward secrecy 9. Hierarchical Access regulation 10.Standardized, scalable approach. While a lot of research has focused on authentication, authorization techniques, there is still need of platform-independent, context-aware, resource efficient security protocols for comprehensive IoT security. Security issues specific to RFID systems & mobile applications should also be studiedin depth.

V. ACKNOWLEDGMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] Abdmeziem, Mohammed Riyadh, and DjamelTandjaoui. "An end-to-end secure key management protocol for e-health applications." *Computers & Electrical Engineering* (2015).

[2] Alcaide, Almudena, et al. "Anonymous authentication for privacy-preserving IoT target-driven applications." *Computers & Security* 37 (2013): 111-123.

[3] Armando, Alessandro, David Basin, YohanBoichut, Yannick Chevalier, Luca Compagna, Jorge Cuéllar, P. HankesDrielsma et al. "The AVISPA tool for the automated validation of internet security protocols and applications." In Computer Aided Verification, pp. 281-285. Springer Berlin Heidelberg, 2005.

[4] Atzori, Luigi, et al. "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization." *Computer Networks* 56.16 (2012): 3594-3608.

[5] Aura, Tuomas, AarthiNagarajan, and Andrei Gurtov. "Analysis of the HIP base exchange protocol." In *Information Security and Privacy*, pp. 481-493. Springer Berlin Heidelberg, 2005.

[6] Bauer, Andrea, KlaasKlasing, GeorgiosLidoris, QuirinMühlbauer, Florian Rohrmüller, Stefan Sosnowski, TingtingXu, KoljaKühnlenz, Dirk Wollherr, and Martin Buss. "The autonomous city explorer: Towards natural human-robot interaction in urban environments." *International Journal of Social Robotics* 1, no. 2 (2009): 127-140.

[7] Bernabe, Jorge Bernal, Jose Luis Hernandez Ramos, and Antonio F. Skarmeta Gomez. "TACIoT: multidimensional trust-aware access control system for the Internet of Things." *Soft Computing* (1705): 1-17.

[8] Blundo, Carlo, Alfredo De Santis, Amir Herzberg, Shay Kutten, UgoVaccaro, and Moti Yung. "Perfectly-secure key distribution for dynamic conferences." In *Advances in cryptology—CRYPTO'92*, pp. 471-486. Springer Berlin Heidelberg, 1993.

[9] Boneh, Dan. "The decision diffie-hellman problem." *Algorithmic number theory*. Springer Berlin Heidelberg, 1998. 48-63.

[10] Caelli, Terry, and SerhiyKosinov. "An eigenspace projection clustering method for inexact graph matching." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 26, no. 4 (2004): 515-519.

[11] Chabridon, Sophie, et al. "A survey on addressing privacy together with quality of context for context management in the internet of things." *annals of telecommunications-annales des télécommunications* 69.1-2 (2014): 47-62.

[12] Duan, Junqi, et al. "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications." *Internet of Things Journal, IEEE* 1.1 (2014): 58-69.

[13] Fabian, Benjamin, and Tobias Feldhaus. "Privacy-preserving data infrastructure for smart home appliances based on the Octopus DHT." *Computers in Industry* 65.8 (2014): 1147-1160.

[14] Farash, Mohammad Sabzinejad, and Mahmoud AhmadianAttari. "An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps." *Nonlinear Dynamics* 77.1-2 (2014): 399-411.

[15] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, 2006.

[16] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[17] Hernández-Ramos, José L., et al. "SAFIR: Secure access framework for IoT-enabled services on smart buildings." *Journal of Computer and System Sciences* (2014).

[18] Jacquet, P., and U. Herberg. "Internet Engineering Task Force (IETF) T. Clausen Request for Comments: 7181 LIX, EcolePolytechnique Category: Standards Track C. Dearlove." (2014).

[19] Jing, Qi, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and DechaoQiu. "Security of the Internet of Things: perspectives and challenges." *Wireless Networks* 20, no. 8 (2014): 2481-2501.

[20] Junjin, Mei. "An approach for SQL injection vulnerability detection." Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on. IEEE, 2009.

[21] Kalra, Sheetal, and SandeepSood. "Secure authentication scheme for IoT and cloud servers." *Pervasive and Mobile Computing* (2015).

[22] Kang, Kai, et al. "An interactive trust model for application market of the Internet of Things." *Industrial Informatics, IEEE Transactions on* 10.2 (2014): 1516-1526.

[23] Keoh, SyeLoong, SahooSubhendu Kumar, and HannesTschofenig. "Securing the internet of things: A standardization perspective." *Internet of Things Journal, IEEE* 1.3 (2014): 265-275.

[24] Laganier, Julien, and Lars Eggert. "Host identity protocol (HIP) rendezvous extension." (2008).

[25] Lee, Chao, YunchuanGuo, and Lihua Yin. "A Location Temporal based Access Control Model for IoTs." *AASRI Procedia* 5 (2013): 15-20.

[26] Lesser, V. R., and D. D. Corkill. "Functionally Accurate, Cooperative Distributed Systems: IEEE Trans." *Systems Man And Cybernetics, Vol SMC* 11.

[27] Mao, Yijun, et al. "Fully Secure Fuzzy Identity-Based Encryption for Secure IoT Communications." *Computer Standards & Interfaces* (2015).

[28] Moosavi, SanazRahimi, et al. "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways." *Procedia Computer Science* 52 (2015): 452-459.

[29] Neisse, Ricardo, et al. "Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework." *Chapter in Internet of Things Applications-From Research and Innovation to Market Deployment, IERC Cluster Book* (2014).

[30] Ning, Huansheng, Hong Liu, and Laurence T. Yang. "Aggregated-proof based hierarchical authentication scheme for the Internet of Things." *Parallel and Distributed Systems, IEEE Transactions on* 26.3 (2015): 657-667.

[31] Olivier, Flauzac, Gonzalez Carlos, and NolotFlorent. "New Security Architecture for IoT Network." *Procedia Computer Science* 52 (2015): 1028-1033.

[32] Ray, Biplob R., JemalAbawajy, and MorshedChowdhury. "Scalable RFID security framework and protocol supporting Internet of Things." *Computer Networks* 67 (2014): 89-103.

[33] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." *Advances in Cryptology–EUROCRYPT 2005*. Springer Berlin Heidelberg, 2005. 457-473.

[34] Sahraoui, Somia, and AzeddineBilami. "Efficient HIP-Based approach to ensure lightweight End-to-End security in the internet of things." *Computer Networks* (2015).

[35] Samani, Afshan, Hamada H. Ghenniwa, and AbdulmutalibWahaishi. "Privacy in Internet of Things: A Model and Protection Framework." *Procedia Computer Science* 52 (2015): 606-613.

[36] Seal, David. *ARM architecture reference manual*. Pearson Education, 2001.

[37] Mercado, Gustavo, A. Diedrichs, and M. Aguirre. "The Wireless Embedded Internet." *Annals of CASE* (2011).

[38] Shelby, Zach, Klaus Hartke, and Carsten Bormann. "The constrained application protocol (CoAP)." (2014).

[39] Sicari, S., et al. "Security, privacy and trust in Internet of Things: The road ahead." *Computer Networks* 76 (2015): 146-164.

[40] Smith, Reid G. "The contract net protocol: High-level communication and control in a distributed problem solver." *IEEE Transactions on computers* 12 (1980): 1104-1113.

[41] Su, Jinshu, et al. "ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things." *Future Generation Computer Systems* 33 (2014): 11-18.

[42] Traub, Ken, et al. "The EPCglobal architecture framework." *EPCglobal Ratified specification* (2005).

[43] Wang, Qiyan, and Nikita Borisov. "Octopus: A secure and anonymous dht lookup." *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*. IEEE, 2012.

[44] Wu, Jun, et al. "Securing distributed storage for Social Internet of Things using regenerating code and Blom key agreement." *Peer-to-Peer Networking and Applications* (2014): 1-10.

[45] WU, Qiu-xin, and L. I. Han. "Secure solution of trusted Internet of things base on TCM." *The Journal of China Universities of Posts and Telecommunications* 20 (2013): 47-53.

[46] Xu, X., NikBessis, and J. Cao. "An autonomic agent trust model for IoT systems." *Procedia Computer Science* 21 (2013): 107-113.

[47] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." *Journal of network and computer applications* 42 (2014): 120-134.

[48] Suchetha K N, H S Guruprasad, "Integration of IOT, cloud and Big Data", *Global Journal of Engineering Science and Researches*, Volume 2, Issue 7, July 2015, pp 251-258, ISSN: 2348-8034.

[49] Rachana S C, Dr. H.S. Guruprasad, "Emerging Security Issues and Challenges in Cloud Computing", *International Journal of Engineering Science and Innovative Technology*, Volume: 3, Issue: 2, March 2014, pp 485-490, ISSN: 2319-5967.