ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Security Issues for Cloud Supported IoT

Nikita D. Shingarwade, Sushama C.Suryawanshi, Shashank P. Wankhade

Department of Computer Engineering, Savitribai Phule Pune Univesity, MH, India

ABSTRACT: The internet of things is becoming an attractive system paradigm to realize interconnections through physical, cyber and social spaces. During the interactions among the internet of things, security issues become noteworthy, and it is significant to establish enhanced solutions for security protections. The IoT vision of open data sharing is achieved by using cloud computing concepts. As IoT is built on the basis of the Internet, security problems of internet will also show up in IoT and IoT contain three layers i.e. perception, transportation and application layers. The security issues, technology and solution related to the application layer are discussed in this Paper. The main focus of this Paper on Data Security Protection technique
for application layer and comparison for various techniques.

KEYWORDS*:* Internet of things, security, privacy, cloud computing

I. INTRODUCTION

Nowadays there is rapid development of Internet of Things there is a variety of IoT applications, which uses in our daily life. They cover from traditional equipment to general household equipment, which help make human beings life better. Meanwhile, numbers of challenges are in the way of the IoT.[1] In terms Of scalability, IoT applications that require large number of devices are often difficult to implement because of the restrictions on time, memory and processing and energy constraints. Hackers, malicious software and viruses in the communication process might disturb data and information integrity. Access cards, bus cards and some other small applications also belong to IoT. Application of IoT can bring convenience to people, but if it cannot ensure the security of personal privacy, private information may be leaked at any time.[1][2] The internet of things based on the ever wider connectivity of sensors or actuators based systems, more general data sharing would become possible within the specific applications for which those sensor or actuating systems were developed. Computers would become autonomous, able to collect data and take decisions based on them, without human intervention.Sensors /actuators based system have been developedindependently of the IoT vision of open data sharing. The cloud is an obvious technology for achieving this open sharing. Cloud computing has evolved to manage, process and store big data.[1][3] IoT not only has the same security issues as sensor networks, mobile communications network and the internet,but also has it specialties such as privacy issues, different authentication an daces control network configuration issues, information storage and management and so on. Data and privacy protection is one of the application challenges of IoT. In IoT there are three layers in IoT: perception layer, transportation layer and application layer. Each layer included various security aspects. In mainly application layer having issues of invalid and in secure data and solutions for removing it is data security protection. There are various methods for data security protection.[2][4]

The main objective of these Papers is:

1. Architecture of IoT containing three layers and various techniques for removing issues related to security.
2. Cloud supported security is achieving open sharing of IoT.
3. Comparisons of various methods of data security protection in application layer of IoT.

A. SECURITY ARCHITECTURE AND SECURITY ISSUES ANALYSIS IN IOT

IoT not only has the same not only has the same securityissues as sensor networks, mobile communication networks and the internet, but also has its specialists such as privacy issues, different authentication and access control network configuration issues, information storage and management and so on. Data and privacy protection is one of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

application challenges of IoT.[1] In IoT, RFID systems, WSNs sensors perceive for the end of the information technology, which protect the integrity and confidentiality of information by the password encryption technology. There are many ways to encrypt data and information, such as random hash lock protocol, hash chain protocol, extract key from an infinite channel, encrypted identifier and so on. Identity authentication and access control can determine the communication between both the sides and confirms each other true identity, prevent disguised attacks to ensure the authenticity, validity of the information and so on. There are two major security issues in the transmission process. one risk of the IoT security is from itself, and the other comes from the related technology of construction and implementation of the network functions. IoT itself is the integration of the multiple heterogeneous network, it should deal with compatibility issues between different networks which is prone to security issues. Security issues such as DOS/DDOS attacks, forgery/middle attack, heterogeneous network attacks, application risk of ipv6, WLAN application conflicts also affect the transport security of IoT.[1] IoT divide into three layers: perception layer, transportation layer and application layer. Perception layer includes RFID security, WSNs security, RSN security and any others. Transportation layer includes access network security, core network security and local network security.

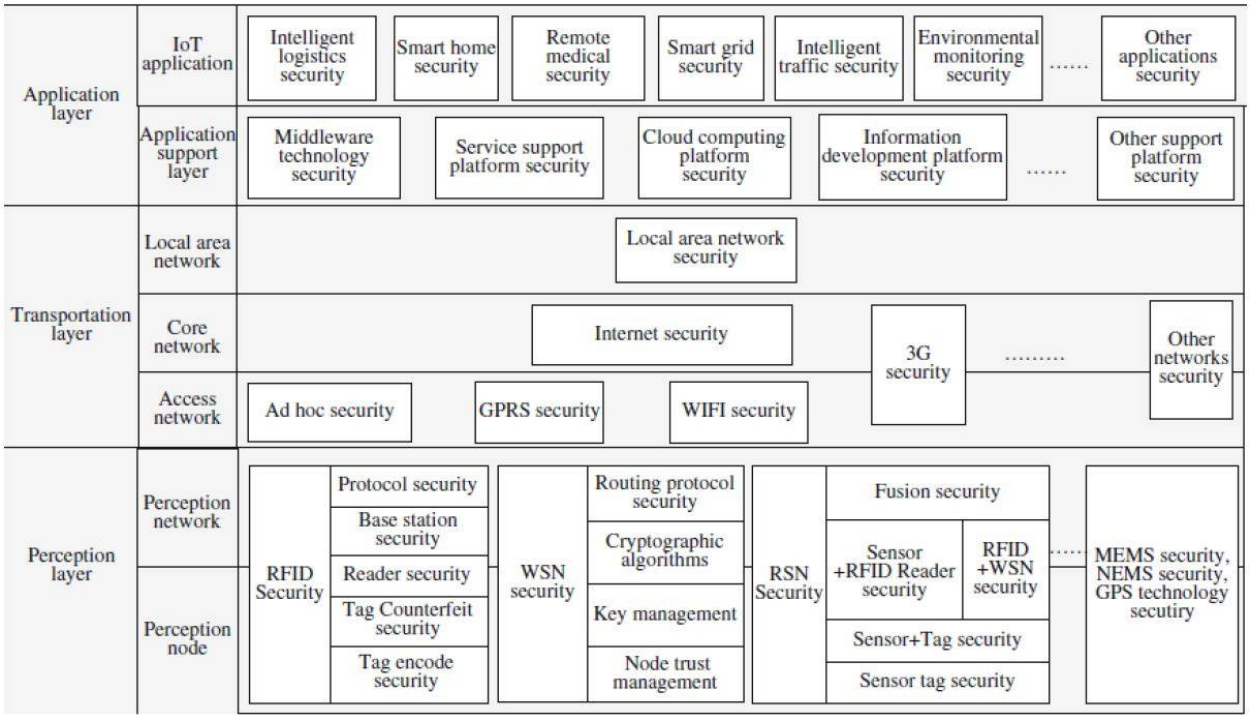

Fig. 1. Security Architecture

Application layer includes support layer and specific IoT applications.

B. CLOUD SUPPORTED IoT

Sensors/actuators-based systems have been developed independently of the IoT vision of open data sharing.[2] It is crucial that the security, privacy and personal safety risks arising from open access to data, across and beyond these systems are evaluated and addressed. The data from a range of different sources are capable of diverse potential application and should be developed with the broad usage and wide availability in mind.The cloud is an obvious technology for achieving this open data sharing.[2] Cloud computing has evolved to manage, process and store big data that, for example, has arisen from services such as search engines. Data analytics became an essential complement to cloud hosted web services. Similar services can be used for large scale data from IoT systems, making them

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

independently shareable and widely available. The cloud is an ideal component in IoT architecture. Firstly, because cloud services can operate across a range of systems, services and devices, it provides the natural point for a) data aggregation and analysis, and b) the management control and coordination of the range of systems and services c) cloud services offer benefits in terms of resource management, as a clouds are always on, can scale to meet demand, and allow the offloading from constrained hardware of data and management specifies. The support for connectivity and open sharing via
cloud services allow. IoT applications are linked to physical world and can directly influence and change it. A cloud system is private and public. Public clouds are the most common, where the cloud provider shares resources between tenants. In a private cloud model, the tenant is offered a dedicated set of resources. This is analogues to in house management, giving the tenant greater control and an increase d sense of security. Hybrid cloud might be processed in private cloud, others on the public cloud. Data and processing may be transferred between two, when and where appropriate.iot subsystems in order to represent aclosed and self contained network of thing. The thing is an entity, physical or virtual, capable of interactionand interacting with cloud services.[2] A subsystem is also.

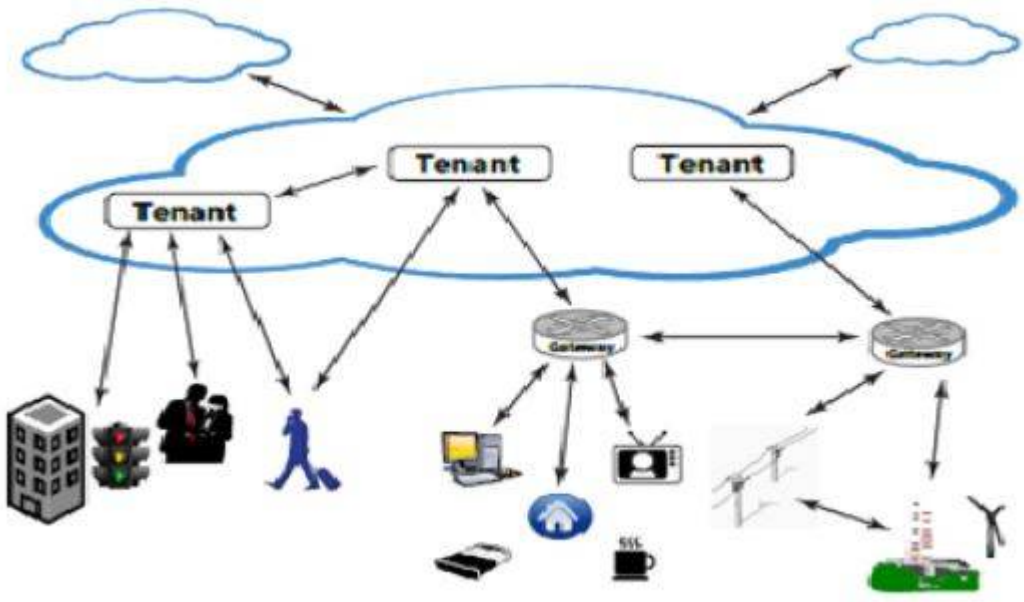

Fig. 2. Interaction with an Iot cloud

considered a thing because the cloud provider sees and interacts with the sub networks gateway component; the gateway represents the end-point of the cloud interaction, mediating between subsystems and the cloud. Early work in such areas often mentioned offloading computing or data onto a server. Moving forward we saw server being replaced by cloud and now see many IoT solutions as tightly integrated with cloud services.Section II presents existing system of cloud supported IoT. Section III presents survey conclusion of all existing system. Section IV presents OSCAR methodology for cloud supported IoT. Section V presents Security consideration i.e. result analysis for OSCAR methodology. Finally, Section VI concludes this paper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

II. EXISTING SYSTEMS

A. AGGREGATED PROOF-BASED HIERARCHICAL AUTHENTICATION SCHEME FOR IOT

The internet of things is becoming an attractive system paradigm to realize interconnections through the physical cyber, and social spaces. During the interactions among the ubiquitous things, security issues become noteworthy, and it is significant to establish enhanced solutions for security protection.[4] U2IoT architecture mankind neural system and social organization framework are introduced to establish the single-application and multi-application IOT frameworks. System security mainly considers a whole IoT system to identify the unique security and privacy challenges, to design systemic security frameworks, and to provide security mainly focuses on wireless communication networks to design key distribution algorithms, authentication protocols, advanced signature algorithms access control mechanisms and secure routing protocols. Application security serves for IoTapplications and resolves practical problems with particular scenario requirements.

The Authentication protocol in the unit IoT:

Towards the homomorphism function. According to FermatsLittle theorem: if q is a prime number, and x is not a multiple of q, thus x q-1=1modq. In the trust model, nDC is an only entity trusted by all the other entities (i.e., Tj, Sb, DCa, iDC). In the unit IoT, DCa is trusted by Tj, Sb and is under iDCs default jurisdiction. In the ubiquitous IoT, iDC and nDC have relatively independent jurisdictions on DCa.
In the U2IoT architecture the unit IoT refers to a

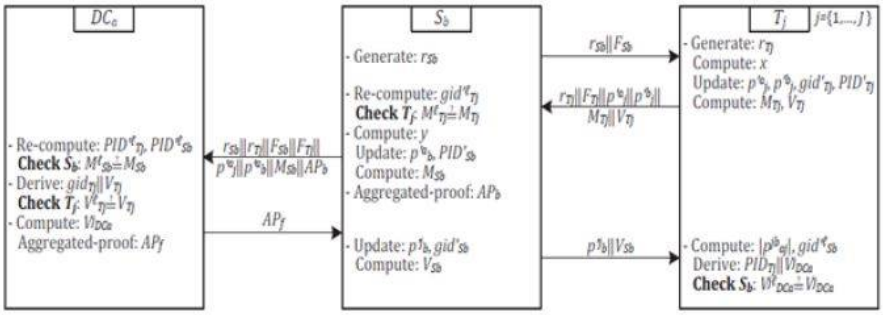

Fig. 3. The Authentication protocol in unit IoT

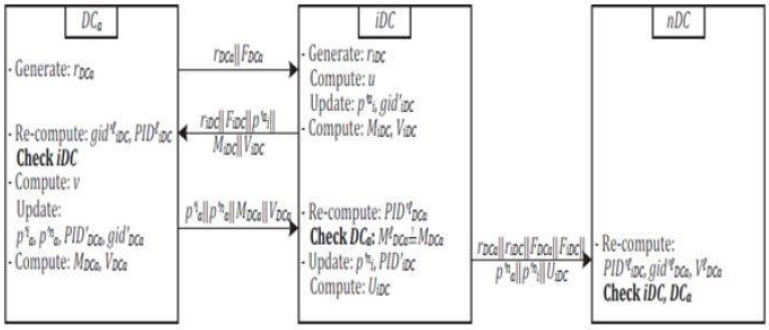

Fig. 4. The Authentication protocol in ubiquitous IoT

basic network unit for a single application, and the ubiquitous IoT includes multiple applications within the centralized national management [4]. Here, we consider an industry oriented scenario, in which multiple industrial IoT manage the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

corresponding unit IoTs in diverse industries. Meanwhile, the industrial IoTs are under the jurisdiction of a national IoT to realize interconnections. In the system model there are heterogeneous sensors (S) and targets (T), which are various according to different scenarios. Multiple unit data centers are under a particular industrial IoT jurisdiction, and industrial data centers have relatively independent authorities on a certain DC. Meanwhile, the trusted national data center (nDC) is introduced to manage multiple iDCs. The APHA is designed based on two main cryptographic primitives: a homomorphism function F (.), and Chebyshev polynomials T*(.).

1. **The authentication protocol in the ubiquitous IoT:**
   An interaction among DCa, iDC, nDC in which DCais under iDCs jurisdiction, and DCa, iDC are within nDCs management range. Dca and iDC have establishedmutual authentication, and nDC has authenticatedDCa, iDC as legal entities. There into, iDCand nDC have different access authorities on DCasgroup identifier and pseudonym to achieve hierarchical access control.

2. **Security properties:**

a. Data confidentiality and data integrity Theonewayvalues apply pseudo-random numbers,which can ensure that attackers cannot derivethe private values for data corruption.

b. Hierarchical access control Two-layered interactions of Tj, Sb, DCa and DCa, iDC, nDC are performed in relatively independent modes,during which DCa acts as a media to connectthe unit IoT and ubiquitous IoT. Accordingto the practical application requirements, Tj,Sb, DCa, iDC, nDC are assigned the differentaccess authorities in the U2IoT.

Forward UnlinkabilityThe pseudo-randomnumbers are generated as session-sensitiveoperators to provide session freshness andrandomization. Additionally, the identityrelated values are dynamically updated duringeach session.

c. Mutual Authentication: In the unit IoT, themutual authentication is established between Tj and Sb and authentication operators areapplied to check the identity correctness andconsistency.

B. PRIVACY-AWARE DISTRIBUTED BAYESIAN DETECTION

The eavesdropping problem in the remotely distributedsensing on privacy-sensible hypothesis fromthe Bayesian detection perspective.[8] We consider aparallel distributed detection network where remotedecision makers independently make local decision sdefined on finite domains and forward them to thefusion center which makes the final decision.An eavesdropper is assumed to intercept a specificset of local decisions to make also a guess onthe hypothesis. Propose a novel Bayesian detectionoperationalprivacy metric given by the minimal achievable Bayesian risk of the eavesdropper. Further,we introduce two privacy-aware distributed Bayesiandetection formulations, namely the privacy-concerneddistributed Bayesian detection problem where the detectionperformance is optimized under a privacy guarantee constraint and a weighted sum objective of thedetection performance and privacy risk is minimizedrespectively. For a optimal decision strategy of employinga deterministic likelihood test or a randomizedstrategy thereof is identified[8].

C. DISTRIBUTED DETECTION SUSCEPTIBLE TO AN EAVESDROPPER:

The eavesdropping problem in the distribute detectionnetwork and develop a concept of privacy- awaredistribute detection design. The parallel model consistsof an m-ary hypothesis H, n remote decisionmakers DMi: iE 1. . ., n, a fusion center FC, andan eavesdropper EVE. The hypothesis H is defined onthe set H= 0. . . m-1 and is generated according to theprior probability pH(h). Each remote decision makerDMi independently makes an mi-ary local decisionUi defined on the set Ui= 0, .m, mi-1 based on ithscontinuous random observation Yi which is defined onthe set Yi. Here, we assume that any likelihood fy—H(yi——h) contains no point masses of probability andall local observations are conditionally independentgiven the hypothesis.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

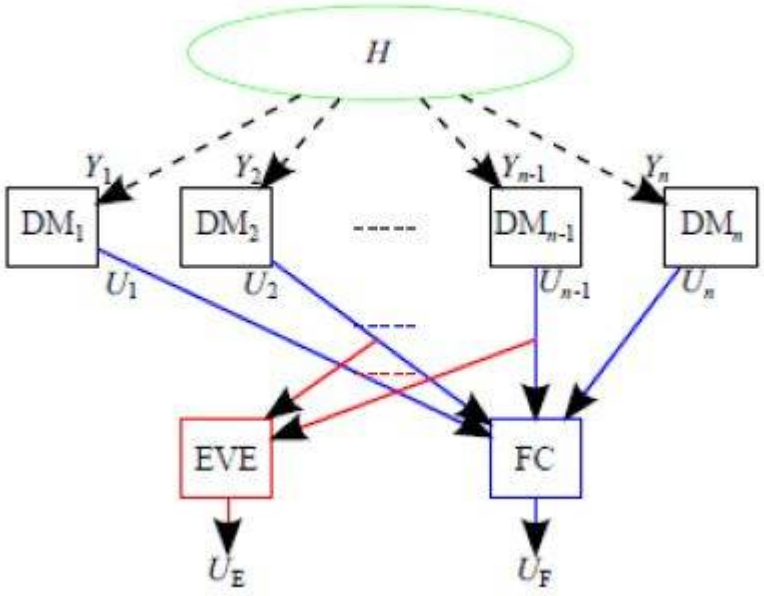

Fig. 5. Model of parallel distributed detection network

D. PRIVACY-AWARE DISTRIBUTED BAYESIAN DETECTIONPROBLEMS:

To develop the Bayesian framework, important resultand concepts of the distributed Bayesian detectionproblem are briefly presented first. Denote the nonnegativedetection cost of the fusion center to make adecision uf when the hypothesis presents h by cf (uf,h). In the Bayesian formulation, it is assumed that thehypothesis proper probability ph (h), likelihoods of the local observation and detection cost assignment of thefusion center are known. If there is no eavesdroppingthreat in figure, the distributed Bayesian detectionproblem is to find the optimal design which minimizesthe Bayesian re=isk of the fusion center rFas.C. JSON Sensor Signatures (JSS): End-to-End integrityProtection from Constrained Device to IoTApplication Integrity of sensor readings or actuator commandsis of paramount importance for a secure operationin the Internet-of-Things (IoT). Data from sensorsmight be stored, forwarded and processed by manydifferent intermediate systems. In this paper we applydigital signatures to achieve end-to-end message levelintegrity for data in JSON.[6] By signing JSON on the constrained device we extend the end-to-end integrityprotection starting from the constrained device to anyentity in the IoT data-processing chain. Just the JSONmessages contents including the enveloped signatureand the data must be preserved. We reached our designgoal to keep the original data accessible by legacyparsers. Hence, signing does not break parsing.Integrity is the property that data has not been alteredor destroyed in an unauthorised manner.[6] It can be achieved on the transport-layer and on the messagelevel. Transport-layer integrity protects the channelbetween two communicating entities, such that insidethe channel integrity cannot be violated without beingdetected by the communication partner. Message-levelintegrity creates an integrity check value, e.g., using

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

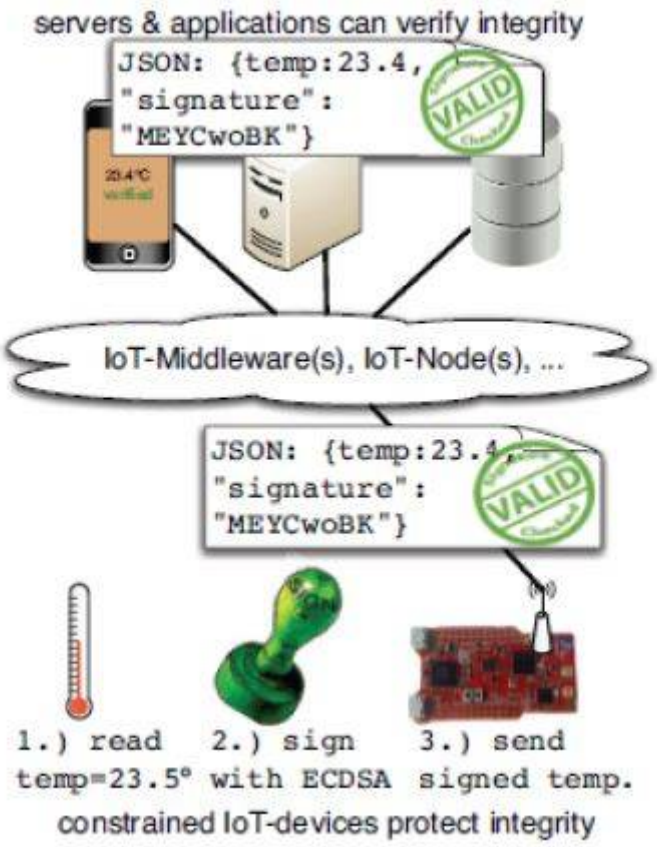

Fig. 6. JSON Sensor Signatures

digital signature, over the message and then send messageand signature over an unsecured communicationchannel. In the Internet-of-Things, sensory informationis gathered by constrained devices and the datais then forwarded to other things or to servers. Currently a cryptographically verifiable proof of integrityand origin is hardly ever seamlessly preserved fromthe sensor-based IoT-world to the world of flexibleinterchangeable services and their applications. Goalis to protect integrity of information in an end-to-endfashion in the IoT data processing chain: starting theearliest, generally already on the device , and extendit seamlessly all the way up to the applications.[6]

E. CRYPTOGRAPHIC PRIMITIVES FOR DIGITAL SIGNATURES ONCONSTRAINED DEVICES:

There are several different approaches to allow cryptoon constrained devices: On the one hand lightweight cryptosuitable for severely resource constrained devicesand on the other hand solutions based ontraditional cryptographic primitives. The need forlightweight cryptography and special schemes. Solutionslike the ultra-lightweight Hummingbird allowbringing crypto to nearly any device in the IoT (8-bitmicrocontroller ATmega128L). These and the ongoing
developments are important to work towards a secureIoT, which is currently not achieved by solutionson the market drastically showed. Especially thosebased on asymmetric keys, which offer strong originauthentication and scalable key distribution, are costly.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

F. MESSAGE-LEVEL INTEGRITY:

Cryptographically digital signatures protect a stringof bits. When facilitated for message-level integrityprocedureon how the messages content is supplied to thecryptographic algorithm. At this point the mechanismsmust be tailored to fit the structure of the data theyprotect.

G. JSON WEB SIGNATURES (JWS):

JavaScript Object Notation (JSON) has become verypopular to represent data in the IoT domain2. It isstandardized, simple, offers structure, and can be self explainingto humans if semantically names are used.JSON formatted temperature value of 23.4 with somemeta-data. One candidate to sign JSON is the so-calledJSON Web Signature (JWS) that is currently discussedin IETFs JOSE working group as an draft.

H. JSON CLEAR TEXT SIGNATURE (JCS):

JCS does not list the accessibility of the content astheir main design goal. Important to note is that JCShas a potential dependency on canonicalization.

III. SURVEY CONCLUSION

In literature survey we studied all existing techniquefor data privacy protection in application layer of anIoT. The technique like JSON provided only end toend protection not for overall system. Another is privacyaware distributed Bayesian technique containinglarge number of calculation. These all technique notprovided privacy and security over application of the IoT i.e. open data sharing of the data. These open datasharing is achieved by the using cloud technology andOSCAR uses cloud.[6][8][4]

TABLE I. COMPARISON OF DATA PRIVACY PROTECTION TECHNIQUE

Technology	Advantages	Disadvantages
JSON Sensor signatures(JSS)	In the prototype, the elliptic curve cryptography, encoding and parsing of the JSON data text only above 2 seconds	It provide only End-to-End integrity protection from constrained device to IoT application
Privacy aware distributed Bayesian Detection	The privacy problem of distributed detection network vulnerable to an inform and greedy eavesdropping	Mathematical model of this technique is hard to perform practically
Aggregate proof based hierarchical authentication scheme for the internet of things	The unit IoT and ubiquitous IoT to provide bottom-up security protection	Application is i.e. Open data sharing is not achieved by this technique

IV. OSCAR

OSCAR relies on secure and authenticated channelsestablished by means of DTLS for key distributionapproach brings together the concepts of connection orientedsecurity with those of content centric networking.Constraints on energy are almost constant.Without breakthrough in chemical engineering, theavailable energy expected to remain the main constraint for IoT devices. Available memory for embeddeddevices slowly increases. However, due tothe economical and energy cost caused by leakagein SoC, expect that memory will remain limited anda determining factor for the unit price. Processingcapabilities constantly increase even for ultra lowpower micro controllers. Apart of sleep mode ofleakages, the energy consumptions is mainly causedby radio communication. Design goal is to minimizethe number

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

of extra frames that need to be transmittedor received for pure security purposes. This goal byleveraging the benefits of public key cryptography,sparse traffic patterns within local constrained networks,
and messages of limited size, trade the radiousage for a higher computation model[7].

A. INTERNET TRUST MODEL AND THE IOT REQUIREMENTS

The host oriented paradigm has a direct consequenceon trust-its transitivity; once a logical connectionbetween the hosts is closed, the trust in the informationis gone. The information is implicitly dependent onthe trust of the communicating entries during theconnection time.DNS is purposely secured with theapplication level extension DNSSEC and not with aconnection-oriented protocol, such as DTLS. Electronicmail, passing multiple application level gatewaysand without clear connection between end pointsis secured with S/MIME or PGP. Application traffic isasynchronous. Servers notify their clients of physicalstate changes as they happen. Clients send commandsto actuating devices asynchronously as the changesin the environment are observed. DNS traffic is agood parallel as it is triggered by asynchronous humanactions. Caching is must. Severe energy constraintslead to servers being asleep more than 99 percentageof the time.As an already supported and intuitive mechanism,caching at untrusted intermediaries is a way to keepapplications running independently. A similar problemis faced with electronic mails, as they are stored atuntrusted servers until delivery. Group communicationis frequent. Commonly, clients instruct a subset of alldevices to perform an action, for example to turn offall lights on the nth floor or to update the firmware.Achieve these, IPv6 multicast and UDP are exploitedbearing no connection state between and points. Webapplications are built around a single logical server andmultiple clients. Access control is often done withinthe server side applications, once the client has beenauthenticated.[7] IoT reverses this paradigm by havingmany devices serving as servers and possibly manyclients, taking part in the same application. Servers aresignificantly resource constrained which results in theminimization of the server side functionality. Accesscontrol become a distributed problem, especially whentaking into account the recent efforts of decouplingthe sensor network infrastructure from applications.Further-more, applications have emerged that use localdatabases to store parts of collected data. Differentsorts of connection time tweaking and keep-alive messagescloud squeeze in connection-oriented securityprotocols and work around the asynchronous trafficrequirements to support caching, need to trust theIntermediate nodes or proxies to store the data. Tosupport group communication, need to open separatesecure connections among group members and addadditional protocols on top of them, which effectivelyprovides redundant security services necessary for theuse cases.

B. PRODUCER-CONSUMER MODEL

Abstract IoT, its sensors and actuators, as an interfaceto the physical world. Decision takers base their reasoning on input data coming from the sensedphysical phenomena. The relation between enforceddecisions and sensed phenomenon is many to manya single measurement often affects multiple decisionsand a single decision may be based on many differentphenomena. The producer-consumer model representswell problem in terms of security. Producers feedconsumers with the required information and mayfurther generate actions. The inspiration for the useof the model comes from cloud and a recent workby Producers in the IoT case are not access controldecision makers content they generate, which is rathera policy of the network operator. Producers should,thus care about generating and securing the content orin the REST terminology, the resource representation,and not about consumers. Consumers with appropriate
access privileges should make sure they can makeuse of the fetched content by decrypting and authenticatingits validity. The extent of security tasksperformed by producers should be minimized producersshould not waste precious resources exchangingsecurity handshake message with each consumer.[7]Resource representations are minimal in size. Thegenerated content that is the resource representationsare typically the measurements of physical quantities or different states of the device with possibly additionalinformation such as location and a timestamp,which very often makes them smaller in size thanindividual messages exchanged during the securityhandshake. As a consequence, responding with an accessprotected resource representation is cheaper thanperforming multiple RTT handshakes. Due to physicalconstraints, the number of supported cryptographicciphers is limited.[7] Indeed, constrained devices often
have a single supported cipher suite. This fact reversesthe paradigm encountered in the internet where oneof the security concerns during the handshake is thedowngrade attack. The motivation behind the attack isthe assumption that the client cipher set is just a subset of those supported by a resource rich server. With thereversed paradigm, as in the IoT case, the motivationfor the attack fades away. Goals are to offload theburden of the authentication from Constrained servers and to place it on more powerfuldevices. Such semi-structured third parties could bephysically secured nodes in the network and hosts inthe cloud.[7][2] Their role would be to authenticateindividual consumers and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

share with them appropriateaccess secrets and necessary certificates an accesssecrets as an access token from which symmetricencryption keys are derived. Consumers can fetch theprotected content either from intermediate proxies or directly from producers.

V. SECURITY CONSIDERATION

A. DENIAL OF SERVICE

OSCAR takes s non-traditional approach to fight Denialof Service. It builds upon the assumption that

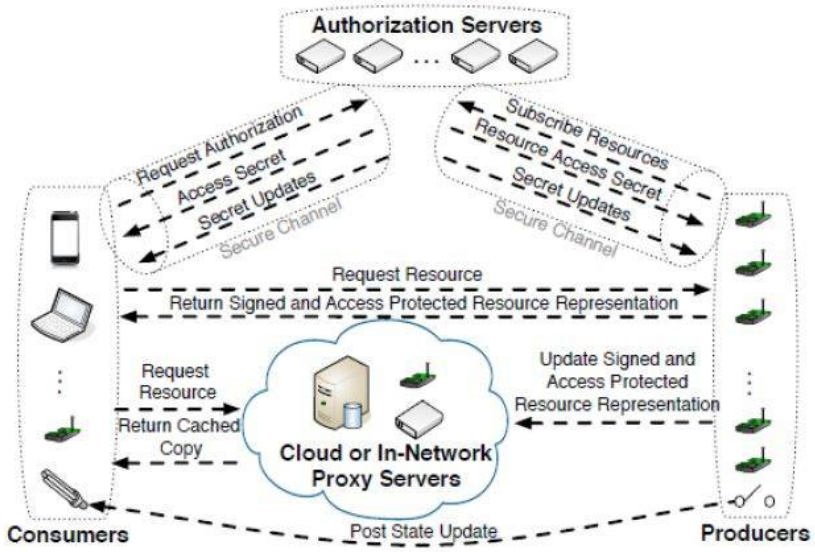

Fig. 7. Producer-Consumer Model For IoT

typical IoT resource representations are small in sizeand directly responds to requests with access protectedresource representations. Moreover, it does not keepany state between communicating entities, which findparticularly important to fight memory exhaustionattacks. Since server-side digital signing operations aredone offline, the intensity of incoming traffic is notcorrelated with asymmetric cryptographic overhead.

Confidentiality:

As content encryption keys are derived from accesssecrets, OSCAR provides confidentiality withinthe resource access right group. Actual securityproperties are dependent on the encryption algorithmused. Note that an adversary able to compromise theAuthorization Servers may only obtain eavesdroppingcapabilities E2E integrity and authenticity propertiesare preserved. If the mutual trust among clientsin terms of confidentiality is not desired, OSCAR
puts the burden on the key management schemerunning on Authorization Servers. One such examplewould be the use of a recently proposed batch-basedgroup key management protocol, where clients wouldbe given cryptographic material corresponding todescendants in the binary tree of the actual accesssecret on a server. However, this would requireadditional signaling of the supported access secret inthe GET request.

Replay Protection:

OSCAR protects from replay at the level of thecontent by using an encryption key that is a functionof the MessageID from the underlying CoAP header.The detection of replay attacks performed at lowernetwork layers depends on the CoAP duplicatedetection mechanism. However, it is important tostress that the current CoAP draft, as is, would

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

notprovide robust protection in security terms. Therefore,successful coupling of OSCAR with CoAP would require additional clarifications and specification tothe duplicate detection mechanism. Another concernwith respect to the replay attack is a maliciousadversary within the resource access tight group incase of asynchronous traffic. Such an adversary is ableto asynchronously inject old resource representationsmaking other members of the group believe they arefresh. Protection against such adversary would requirethe use of a key management scheme that wouldprovide different access secret cryptographic materialon the constrained server and individual clients.

B. SECURING THE IOT

Scalability:

Scalability as a function of the ratio between thetotal number of clients and a maximum number ofopen DTLS sessions at a constrained server (due tomemory limitations, constrained servers have a limitednumber of DTLS session slots). We have followedthe guideline on practical issues with DTLS andextended the Tiny DTLS implementation with theLeast Recently Used (LRU) session closure algorithm.The server immediately releases memory and sends a closing alert to the LRU session as soon as a new clienthas demonstrated good intentions by retransmitting thestateless cookie in the ClientHello message (recall theDTLS handshake). Therefore, the handshake with thenew client proceeds immediately. Clients keep their sessions open as long as possible, i.e. until they receivethe closing alert from the server. The maximum numberof DTLS session slots is dependent on platformmemory capabilities and actual application memoryrequirements.

End-to-End Security at the Network Layer:

Ever since the efforts on integrating Wireless SensorNetworks with the Internet have begun, the so-calledblanket coverage at the network layer has been considereda potential solution to provide end-to-end securityservices. The literature widely discussed the feasibilityof porting the IPsec protocol suite to smart objects.The authors mostly evaluated the processing overhead
and energy requirements of different cryptographicsuites used by IPsec, but also the memory footprintsand system response time. Even though it was initiallyconsidered too heavy for constrained environments,these results led to the common conclusion that alightweight version of IPsec is a feasible option.In the Internet, IPsec mostly secures Virtual PrivateNetworks (VPN).

End-to-End Security at the Transport Layer:

Impracticality of IPSec has been overcome in theInternet by introducing the security services just belowthe application layer, in the form of TLS/SSL. Thewide and successful use of this model in the Web hasalso suggested its use in IoT. The authors evaluatedthe HTTPS stack that leverages assembly optimizedimplementation of ECC as a public key algorithm.SNAIL complemented this work by introducing SSLon all IP architecture, leveraging the 6LoWPAN adaptationefforts done in the meantime. Together withthe introduction of IP to the embedded world camethe dilemma whether TCP is suited or not, due to itsconnection establishment overhead, poor performancein case of lossy networks and short term connections.

Object Security Approaches:

Although the concept of object security, i.e. placingsecurity within the application payload, has been discussedas an option the related work in the literatureleverages its benefits to provide fine grained accesscontrol with an assertion based authorization framework.The problems of E2E security and authorizationfor IoT and use the capability-based access controlsolely as a means to provide communication confidentiality.

Standardization Efforts:

Recent IETF efforts are directed towards profilingDTLS specifically for constrained devices (DICEworking group). Current proposals aim at addingmulticast support to DTLS by reusing the record layerand relying on an independent group key managementprotocol . In essence, the core (D) TLS designassumption (point-to-point communication) is beingrevisited to make it fit better the IoT requirements.Authorization and authentication challenges for constrainedenvironments are being tackled separatelywithin the ACE working group. Requirements that are discussed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

by ACE, however, seem to be contradictorywith the initial choice of DTLS as a security protocol,particularly when it comes to proxies and caching.OSCAR bridges this gap and jointly.

VI. CONCLUSION

The security architecture and security issues of IoT, andhave divided IoT into three layers: perception layer, transportationlayer and application layer. The features and securityissues of each layer, and introduced the corresponding typicalsolutions for these issues. Problem of E2E security in IoT.It is based on the concept of object security that introducessecurity within the application payload. Consider separateconfidentiality and authenticity trust domains. Confidentialityis used as a means to provide capability based access controland a protection against eavesdropping during the communication.The security issues, technology solution related tothe application layer are discussed in this Paper. The mainfocus of this Paper on Data Security Protection technique forapplication layer and comparison for various techniques of Data security protection.

VII. ACKNOWLEDGMENT

It gives us great pleasure on bringing out seminar entitledSecurity Issues For Cloud Supported Internet of Things. Wewould like to thank all who directly or indirectly helped usduring our work.The authors are grateful to the anonymousreviewers for their valuable comments, which helped us toimprove the quality and presentation of this paper.

REFERENCES

[1] Qi Jing, Athanasios V, Vasilakos, Jiafu Wan, Jingwei Lu, DechaoQiu ,Security of the internet of thing : perspectives and challenges, Issue 17thJune 2014 DOI 10.1007/s11276-014-0761-7.
[2] Jatinder Singh, Thomas Pasquier, Jean Bacon, HajoonKo and David Eyers,Twenty security considerations for cloud-supported internet of things,IEEE journal issue on April 2015 DOI 10.1109/JIOT.2015.2460333.
[3] Sandip Ray and ArijitRaychowdhaury,The changing computingparadigm with internet of things: A tutorial introduction, IEEE journalissue on 2015 DOI 10.1109/MDAT.2016.2526612.
[4] HaunshengNing, Hong liu,LaurenceT.Yang , Aggregated proof basedHierarchical Authentication Scheme for Internet Of Things, issue onMarch 2015 DOI 10.1109/TPDS.2014.2311791.
[5] WeizheZhang ,BeoshengQu, Security architecture of the internet ofthings oriented to perceptual layer, IEEE journal issue on 2013.
[6] Henrich C. Pohls, JSON Sensor Architecture:End-to-End integrityProtection from Constrained Device to IoT Application, 2005 DOI10.1109/IMIS.2015.48.
[7] Mali saVucinic, Bernard Tourancheau, Franck Rousseau, AndrzejDuda,Laurent Damon, Roberto Guizzetti, OSCAR: Object Security Architecturefor the Internet of Things.
[8] Zuxing Li, Student Member, IEEE, and Tobias J. Oechtering,Privacy-Aware Distributed Bayesian Detection, IEEE, 2015, DOI10.1109/JSTSP.2015.2429123.
[9] S. Raza, D. Trabalza, and T. Voigt, 6LoWPAN Compressed DTLS forCoAP,in Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE8th International Conference on. IEEE, 2012, pp. 287289.
[10] Z. Shelby, K. Hartke, and C. Bormann, Constrained Application Protocol(CoAP) draft-ietf-core-coap-18,IETF work in progress, 2013