# Layered Architecture, Embedded Technology and Security and Privacy Issues in the Web of Things

***Deepak Singh Tomar**
****Kaptan Singh**

## ABSTRACT

The web of Things (WoT) ensures to enhance the efficiency of interconnecting smart and physical device across world wide web as it not only ensure ergonomics along with contribution of IoT, but it gives new variation for device interoperation and information interpretation. It open up new hurdles that cannot be overcomes in an efficient manner with only transport layer protection. Another efficient answer to this problem is needed, in order to protect sensitive data and to provide authentication. This research provides an overview of WoT literature specialized in security issues and privacy and also discuss the important issues raised when securing present Web of Thing Architecture.

**Keywords:-** Internet of Things, Web of Things, Security, Architecture, Embedded Technology.

*Deepak Singh Tomar, Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh, deepaktomar@manit.ac.in
**Kaptan Singh, Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh, Kaptan2007@gmail.com

## I. INTRODUCTION

Figure and statistics of smart objects to World Wide Web is exceeding the population of humans. Since more smart things are capable to communicate on the www, the idea of IoT is being touches to wider area, such as Smart Home, Smart Meter, Remote Healthcare, and Logistics Process Automation [1] - [8]. The IoT is a wide word that points to system where objects work together with one another to produce effective output for user object. Any object, they have computational and communication abilities, known as "smart" that means they are capable to fulfill difficult work using provided intelligence information.

WoT is the Internet of things or everything is also Internet changing idea of multiple object related with smart network and interaction along one another and with humans. In WoT, information transfer with self and cloud is exchanged, hoping about accuracy in gathering, taping along with analyzing currents data [1]. In addition, web-enabled items should be used again and accept established web mechanisms such as search, browsing, linking and caching, as [9].

The Internet of things and web things conceive both idea of conversation being wide, anywhere plus everywhere. The ideas cannot be approved in existence without giving priority to privacy and

Security. Optimizing web technologies provides an intangible complication of low-level protocols.

For example, HTTP and WebSocket is used again through smart things. In addition, developer develop process that communicate via smart things along one another [10, 11]. An open problem in this area, is the smart and allowance of customers to have access to the facilities due to the dangers like:

-Malicious customers and unwanted data sharing

- Anytime and anywhere

- Unexpected work load and availability risk

Unknowingly, the concept are strong for below aspect. Firstly, asymmetry: IOT is composed of infinite dissimilar objects through different platforms, protocols and needs. Secondly, lack of resources: reason being the demand procedure. Third, identity and authentication: Traditionally, identifiers linked to users to examine if someone was permitted to take action on issue. Combination of hardware and technical world where things are smart of working on oneself or someone else's work.

## II. WEB OF THINGS ARCHITECTURE

This section give outline of the WoT architecture and characterize the layers dependent on it: the Accessibility Layer, Findability Layer, Sharing Layer, Composition Layer as appeared in fig 1. The motivation behind this design is to give the capacity of the blend of smart things with existing administrations as the web and furthermore the improvement of new web application by utilizing smart things [12][13].

### A. Accessibility Layer

This layer is answerable for changing any issue to the web issue that may be connected or related to using protocol request similar to the other resource on the web. In other world, a web thing would be REST API which allows to move along with one object within the planet like gap a door or measuring a temperature and looking at its sensing element settled all along the planet.

### B. Findability Layer

This layer answerable for marking things accessible via associate HTTP and WebSocket API is nice however it doesn't implies that application will make a sense that what the thing exactly is what information or the things cannot only be simply used by alternative communications protocol client however can even be findable and automatically can be used by alternative WoT

application. The objective here is to utilize web linguistics standards to clarify things and administrations they gave. This permits finding out things by search engines and alternative net indexes furthermore because the advanced generation of user interfaces to connect with Things.

C. Sharing Layer

This layer shared the information of things over the web an accurate and safe manner however the information created in any smart things. At that point, another set of web protocols helps. First, TLS protocol use for make the transactions on the web secure. Delegated web authentication mechanisms like OAuth which might be integrated to our Things API's. Finally, social networks use for sharing the smart things over the Internet.

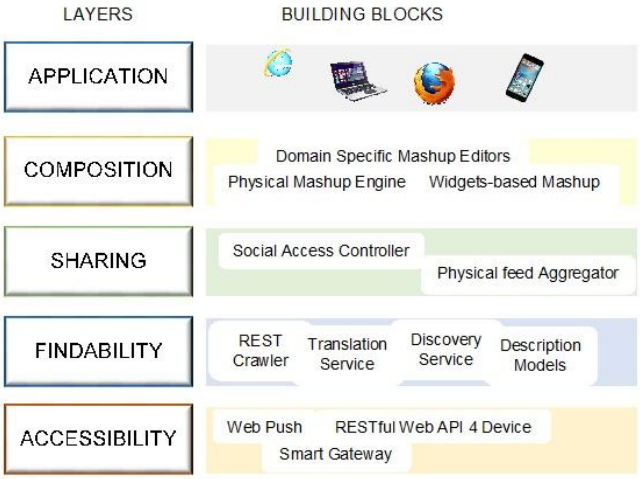


Fig 1 four layers Web of Things architecture

D. Composition Layer

The last layer responsible for developing simple composite web application and its work as go-between developer and end user so that reduce the boundaries between developer and end-users. In other words, want to grasp the combination of information and services from various Things into a massive environment of web tools similar to analytics software package and mashup platforms.

## III. ENABLING TECHNOLOGY

This section describe and analyze consistently capable technologies, in which standard As well as present internet provider technologies, which are very important for WoT, directly or indirectly.

*A. 6LoWPAN*

All the smart device those are enabled with embedded web server, must be first IP Addressable for communication. Various physical Device can be connected in the Internet in the future. Internet Engineering Task Force (IETF) has proposed standards Low Power Wireless Personal Area Network (6LoWPAN) which enable IPv6 based network those are help to connecting the devices to the internet with minimum resource.

It defines the header compression mechanism and encapsulation which is normally allowed to send and receive IPv6 packets between resource devices by taking low-power radio communication protocols. Figure 2 shows the IPv6 protocol stack with 6LoWPANs compared to a normal IP protocol stack.

The main part of 6LoWPAN is the optimization layer because it permit the Ipv6 packet to put in the IEEE802.15.4 frame payload. Following are the function:

***Header Compression***, TCP/IP header data links are oversized for the layer protocol and for the same compression of data is required to be performed.

***Packet Fragmentation and reassembling,*** small size packet are support by the data link layer. For eg. HTTP is used as the transfer protocol for the media web content. The CoAP is resembled as interactive rule set as for devices which understand interoperability. This discrepancy is to be handled in the customization layer by fragmentation and restraint.

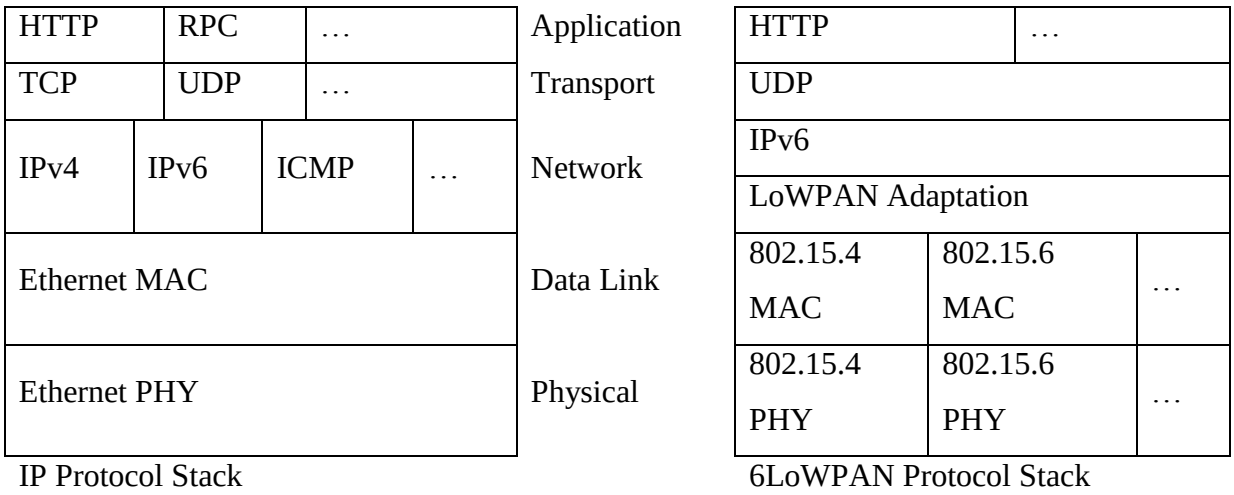


Fig 2 IP and 6LoWPAN Protocol Stack

***Edge routing***, to route the private networks via the WWW, the router, that are located in area through private network and www, holds important part because these root the WWW protocol

package outside & vice versa in the PAN device. Also, the Edge Router has management facilities like IPv6 prefix.

*B. CoAP*

CoAP can be seen as an HTTP target in the form of HTTP supplement, such as Ethernet, where this target resources like wireless sensor networks for network interrupted. Anyhow. This set also work on regular protocols. This is seen in form of compression or redesign of HTTP. The CoAP is resembled as a transfer protocol for devise which understand inter-operability. The CoAP and HTTP protocol piles are painted in Fig. 3

This are characteristics: This uses two layer approach where Transaction layer is utilized for managing UDP and offbeat cooperation. It has four sorts of message clarified on this: Confirmable (CON, requiring a receipt of message), non-confirmable (No, does not retrieve message receipt), acknowledgment (ACK, this CON is accepted), and reset (RST, this define for confirmation message was reached along with little reference missing to function property). The transmission of request and response message is tackle by Rake / Race layer to resource manipulation and interoperability.

GET, PUT, POST and DELETE request methods supported by CoAP protocol. Hypertext transfer Protocol is based on TCP protocol and CoAP is based on UDP whish is connectionless protocol. TCP framework offered high overhead, for example, stream control, isn't appropriate for asset intruded on devices and LAN.

However, CoAP offers an alternative dependable transmission even without the support of TCP. Remember that if the pre-defined retracement timer is out of the time the ACK is not received, then the con message will be transmitted again. To avoid exponential back-up mechanism is used in retransmissions.

Apart from this, there is another advantage in utilizing UDP as well, which enables the best effort of CoAP multicast, while does not support TCP-based HTTP multicast.

| HTTP |
|---|
| TCP |
| IP |

| Req/Res |
|---|
| Transaction |
| UDP |
| IP |

Fig 3 HTTP and CoAP Protocol Stack

The CoAP decrease the resource overhead and complexity of parsing which resources blocking devices. A brief compact-binary header of 4 bytes which has a fixed length is used by CoAP,

which gives a compact binary option. A request contains 10-20 bytes of header overhead continuous fragmentation is prevented by a small header overhead. The average transaction size in the life of byte of CoAP and HTTP has been compared in [34]. All three parameter i.e. life of the bytes, power consumption and expected battery life are given in table I.

**TABLE I**

Comparison between CoAP and HTTP [36]

| | Bytes per-transaction | Power | Lifetime |
|---|---|---|---|
| CoAP | 154 | 0.744 mW | 151 days |
| HTTP | 1451 | 1.333 mW | 84 days |

The CoAP transaction is 10 time smaller than traditional HTTP transaction. Bid deal is resulted by intensive calculation and communication which is the reason for high power consumption that leads to less battery life. Asynchronous transaction, an important requirement for M2M application is supported by CoAP. When server does not answer on time it first accept the response of the message and send the response again and again to the offline fashion without the risk to send request to request again.

Web architecture has the feature of support CoAP URI and built in resource search URI so that resource should have identify and address in to be searchable. Web has a common resource web. Built in resource search format is defined by CoAP in which both search and advertising of resources provided by a device are allowed.

All the end point are inform by CoAP through a built in subscriber/push model. The resource which changes in a pull model is not able to vote for the client in an M2M application. A built push model is supported by CoAP in which customer can request a response when change occurs. Customer complete this push with the sending response message.

## IV. SECURITY ISSUES OF THE WEB OF THINGS

Usually, sharing in a system leads to the end that the system should be secure and there should be no privacy issues. So the concept is same with WoT. During this section, first go through identity management problem than the specialization in information privacy and integrity, and then finally authorization and access management model. The main threats of WoT is specified in following list as follows:

There are various important risks with WoT- the server behaves as a substitute to generate the request for the right target, things or alternative tasks. Associate degree invader may be in advance of the server and pamper itself as a legal server Thus, all the traffic running from this server be adjusted by the attacker, which incorporate the certificate object identification. Additionally, a duplicate object can send malicious content and user open the personal details. Unauthorized permission to access the data and resource. The privacy poling is put at stack by hiding the traffic flow between the different part in the WoT. Denial of service attack i.e. the unavailable of object / resource on the web.

*A. Identity Management in WoT*

Protecting a user identity is a very important part of the any application and system. The identity management is a system that define rules for individual in given system with the help of their identities and depending on the circumstances. Identity management also define the appropriate policy for user or device and identify the entity is authorized on the network or not. The basic design of identity management model inside the WoT, WoT scheme is formed from Associate in Identity Provider (IDP), a Service Provider (SP) and user / object[14].

1) Centralized union model: Identity Provider (IDP) is in charge of gathering clients with personality data. Identity provider share the user identity information with different-different Service Provider (SP). In this model, a problem is arise if any IDP fail than will be fail the all identity management system.
2) Decentralized Union Model**:** This model distribute IDP's features in numerous IDP's in distinct secure domain. This model depends on trust relationship between IDP's and SP. Anyway in this model, the client does not the full control of over identity information because information is stored in the IDP and if the IDP in not trustful then they can be exposed to any of the other party without having the authority.
3) User-centric model: It solves the issue of regulating client's identity, which gives the client complete command over all the offer identified with his identity. In essence, the user needs a true approval to use his identity. Users may have more than one identity issued by more than one identifying providers. Such systems need to guarantee many qualities, some of the basic privacy, integrity and uniqueness. The proper classification of properties of user control is shown in [14]. And an e.g. Of IDM which is user-centric in shown in [15].

*B. Data confidentiality and integrity*

To Save and consume the confidential and integrity of the data, and to prevent the interaction between the various units of the system, it is essential to secure the communication between the various elements of the Thing environment web. In WoT encryption can lead to a problematic situation because cryptographic calculations typically require memory and energy which is unavailable in smart devices. End to end encryption has two types, first deals with the security of transport layer and second deals with security at application layer. CoAP completes the evolution of security at application layer with the help of addition of some new security feature.

The first choice is *Security On* the one that is accurate if the obtained CoAP message is included from an application level security. The application of security fields is indicated by this option. The destination unit recognizes the CoAP URI that the destination should manage, in order to use the traversal of other trust encryption can use this option multiple times in the same CoAP. The proper ciphers and keys are decided when the message are verified.

Enabling the use of authorization and identify mechanism is the second most option *SecurityToken*. In order to achieve an access to a given CoAP useful resource based totally the requester must become identify itself. Request authorization based on per message basis is enabled with the support of this selection also. The authentication process can be used by the requester by using token field or simply by using username or password.

*SecurityEncap* is the last option, security information are transferred by this. If security-on message requires only one encryption this message can be a non-transferable with the options after the data is being encrypted. On the off chance that security-on message requires signature alongside encryption, a MAC, numerous alternatives and encrypted information can be taken with this choice. More data on these new CoAP safety options can be seek in [16].

*C. Authorization in WoT*

Only allowing authorized parties to fined and flexible access control is important for an open environment same as WOT, where the objects are part of the WWW and are easily searchable. Because of disrupted nature of smart object two things i.e. traditional cryptographic algorithms and protocols. Most real solutions goal to establish a discrete authority architecture, where a back-end server is related to complex tasks, for which binding devices need to process resources while handling minimum messages. The smart device and requester are two end point of server. The request from various entities should be separated by device and enforce the correct authorization decision.

An authorization and certification architecture has been proposed specifically for the bound environment, where complex security works will be assigned to any other trusted unit, or assisted by the less affected actors in the system [17]. Each unit will get a bound level ("bound level", "low bound level", etc.) in this architecture. Authority manages also known as less interrupted nodes will execute complex protections from their respective managed nodes such as management keys, enforcement policies, etc. Figure 4 shows the overall authority architecture:

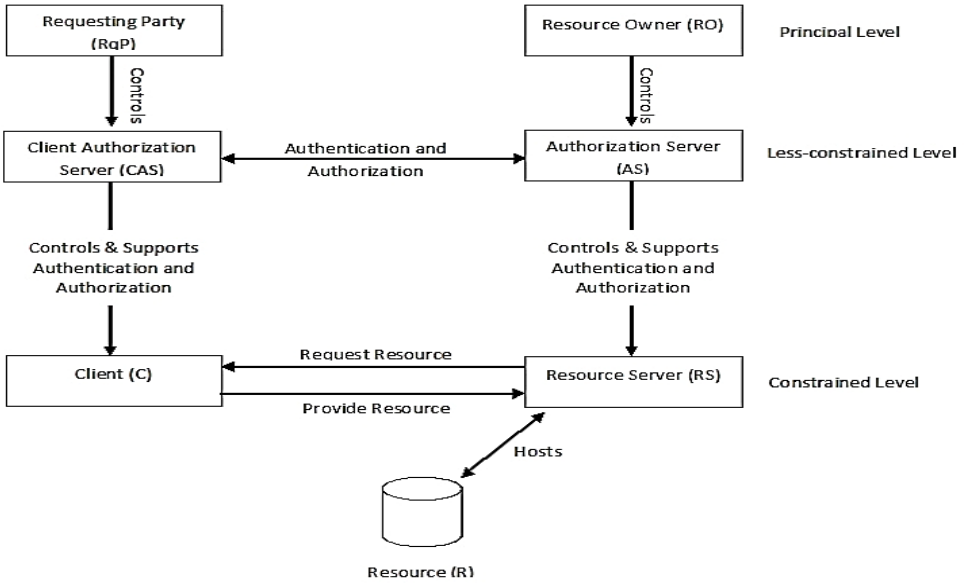


Fig 4 Overall authorization architecture [17]

The Resource Server (RS) is facilitating and speaking to an asset. It very well may be a SO or traditional server (low bound gadget). The client (C) resource server (RS) has an end point requesting resources. These may or may not have trust relationships.

The Authorization Server (AS) In charge of formatting and approving authentication data of Authority Server (AS) authorization and RS, which is low barrier level of architecture. The role of backup of RO and RS is played by this which works to handle access requests. In order to provide further relief to the bound level authorization and authentication mechanisms are deployed. And finally in charge of creating a Client Authority Server (CAS) authorization and approving authentication data for the customer. It additionally has a low resistance level of design and assumes the job of backup for RQP and takes a report at sake of the customer to deal with access request.

Resource owner (RO) is principle unit that is responsible for controlling resources & giving permissions with help of mechanism like Oeth[18] and UMA[19]. It controls and makes decision for RS. Access to resource R is forbidded if any entity remains unauthorized by RO. The in-

charge of costumer is the Request party (RQP), regulated and created by client. Main function of RQP is to govern interaction that customer can work with other intervals and make authorization decisions from client.

The client is forbidden from exchanging information along the asset in authorized way, so the requestor is authorizing the party. Apart from this, RO can provide sufficient information CAS to interact with autonomy of allowance for RS along the AS as the appealing customer.

The Principal it can be either an RQP or a RO.

D. *Protecting the infrastructure*

An important problem in securing IOT come its potential magnitude accompanied with internal technical inequality. Construction off-shelf and creating solutions for every included technical changes into an open protection infrastructure layout, that can be most complementing purpose of the search.

1) Obtaining data privacy and integrity

This means that the data transmitted between different IOT nodes (or stored by them) can be blocked or corrupted by an opponent. Several solutions for storing information have been enforced for almost different architectures and app scenarios [20], [21], [22] while [23], [24] primarily encryption key management problems and distributed unsurprisingly addresses the cancellation of weak connected storage devices, including USB stick.

2) Confidentiality

The aim of the attackers is to impersonate available element of the infrastructure to spread bogus along with missing information instead of preventing, increasing in turn changing function or alarm situation information. Apart from this, the purpose of the attackers may involve blocking the whole or part of the infrastructure (service rejection) by disconnecting some nodes secretly or partially. Intrusion Detection Systems (IDS) [25] is an essential tool for implementing systems / networks to detect and block potential adverse activities. Tailed IDS solutions, which may be suitable for IOT, have been discussed [26], [27]. Trusted computing (TC) is a procedure that is to guarantee that the PC framework screens expected and is having the capacity to demonstrate the stage extends tamper-resistant cryptographic hardware. The maximum mature implementation of this sort of theory is because of the reliable computing group [28], which has issued specification for computer devices along with computer PC platforms. Reliable virtual domains (TVDs) [29], [30] apply leverage to relay reliable computing and virtualization, to deliver alliances of reliable performance environments (coaches): (A) rely on each other, (B) Share a common safety policy

that is being run independently from impartial platform. TVD is considered a solid employer solution for creating efficient cloud based application such as Healthcare Infrastructure [31].

3) Data Secrecy Seeking

Connecting a "smart" device to the network also increases privacy concerns. In the statistics, information in this emerging is unintentionally made “as is” and is provide with concern of “awareness” but has been completed totally thru normal actions, private behaviors, conduct etc (and potentially unconsciousness) for instance inside the smart grid [32], [33]. Since it appeared, RFID technology gave rise to many privacy issues due to statistics that following tools are not capable of efficiently collecting the disclosure or information that is not being carried out. Problems are a common scenarios in almost all RFID application [34].

4) Omnipresent Identity Management

Definition of an identification management system (IDM) device that manages identity residences for both customers and devices / gadgets inside IOT is extensively taken into consideration to be the primary objective. [35] Indeed, anyway at the same time as many multi-tenant, standardized and confidentially-protected mechanisms were proposed to manipulate user identity within the final decade. [36], [37], [38], [39] similar "cheese" identity management. The initiative to define the system is far from reaching its maturity. [40]

5) Access Control Policy Enforcement

Access Control Policy Enforcement is major troubles inside IOT security and confidentiality. Particularly, implementing RBAC policies on the various part of the produced data by the sensor as one of the unavailable interests [41]. However the growth and enlargement of RBAC system, account properties such as asynchronous events [42], nonpermanent rules [43], and geographic data [44] are worth depth.

*E. Web of Things API Vulnerabilities*

Below are some API vulnerabilities in Web of Things:

1) Distributed Denial of Service (DDOS)

Inefficiently designed APIs are often the aim of DDOS attacks. Regularly does not limit the rate on the developer API, or does not slice the harmful requests. There is a complex logic behind API Endpoints here and there is enough to run computationally, it is similar to the confirmation logic for which a hashing algorithm is required. At that time when an opponent searches for such intervals, then they spam the entire structure with requests to bring down. Such intervals should

be served independently from the original API so that the limited performance is affected in the attack

2) Inscribe resource

APIs whose incorporated assets are a gold mine for hacker. Faulty example is spreading customer information through an unapproved open API. It is terrible in itself, though what has increased in this case that the customer ID was numeric - meaning that the attacker does not need to understand the client ID, they can insist on only one limitation and each of the information Can get it.

3) Sharing Resources Using Signed URL's

Regularly gives links to hypermedia resources such as an API picture or video. These resources can then be consumed through customer in any capacity. For instance, to associate through any video, it very well may be played specifically in the browser or in the media player. These kinds of resources, as may be, are interested in hot linking which creates some problems to the provider: on resources Strain, there is not any way to go back to the content provider first. Along these lines, is crucial that a similar resource URLs are fascinating and recognizable. A singed URL can be utilized to execute strategies, for example, rate hurdle, and programmed delays along with check sharing.

4) Weaknesses in third party libraries

These days, many developers use many third party collections, usually for open source or free software license. Benefits make their jobs easier and they are not concerned about adding more features to the library or fixing the bug themselves. It presents the surface of other attack as outcome of an external element and as a result of developers who have been defending the security. Code injection is other security related issues where hacker find out the malicious executable code and inject in to legitimate traffic at the time of end point transfer. Cross-site scripting: same as code injection, written a script from non-desirable sources and put to traffic. Unsafe Direct Object Reference: Unauthorized person getting the file access.

## V. CONCLUSION

This paper firstly give an overview of WoT. It shows multiple benefits of WoT through previous technologies. Some key allowing standard and technologies (e.G. 6LoWPAN, CoAP, mashup, and so on.) associated with WoT also are discussed and examined. The initial things is related to Identity management that ensures authentication of the users. Authentication is very important in any ecosystem so each WoT entity needs to be identifiable. The requester can firstly verify itself and ask for getting permission to access resources. The second phase take the assurance for the

privacy and the reliability of the communication among the entities. They use end to end encryption for secure communication. The third phase is handle the authorization models. In current environment Security and privacy still needs updation. Mainly the problem is trust relationship because different entities communicate each other in the environment. WoT will be necessary in the future lives and some challenging issues arise but this challenging issues will be tackle in the future.

## REFERENCES

1. J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, From Machine-To-Machine to the Internet of Things. Elsevier, pp. 233–235, 2014.
2. Vermesan, O. & Friess, P., Internet of Things: From Research and Innovation to Market Deployment. River, pp. 7–69, 2014.
3. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer System, vol. 29, no. 7, pp. 1645–1660, Feb. 2013.
4. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.
5. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
6. E. Lee, H. Lee, K. Lee, and J. Park, "Automating Configuration System and Protocol for Next-Generation Home Appliances," ETRI Journal, vol. 35, no. 6, pp. 1094-1104, Dec. 2013.
7. G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: From mobile to embedded internet," IEEE Communications Magazine, vol. 49, no. 4, pp. 36–43, 2011.
8. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 1–11, 2014.
9. Framework of the web of things, ITU-T Y.2063, 2012
10. Guinard D, Trifa V, Wilde E. A resource oriented architecture for the web of things. In:Internet of things (IOT), Tokyo, Japan. Nov 2010. p. 1–8.
11. Guinard D, Trifa V. Towards the web of things: web mashups for embedded devices. In: Workshop on mashups, enterprise mashups and lightweight composition on the web. Proceedings of WWW (international world wide web conferences). 2009. p. 15.
12. Dominique Guinard, Christian Floerkemeier, and Sanjay Sarma. Cloud Computing, REST and Mashups to Simplify RFID Application Development and Deployment. In Proc. of the 2nd International Workshop on the Web of Things (WoT 2011), San Fransisco, USA, June 2011. ACM.
13. Dominique Guinard, Iulia Ion, and Simon Mayer. In Search of an Internet of Things Service Architecture: REST or WS-*? A Developers' Perspective. In Proc. Of Mobiquitous 2011 (8th International ICST Conference on Mobile and Ubiquitous Systems)., Copenhagen, Denmark, 2011.
14. Bhargav-Spantzel A, Camenisch J, Gross T, Sommer D. User centricity: a taxonomy and open issues. J Comput Secur 2007;15(5):493–527.
15. van Thuan D, Butkus P, van Thanh D. A user centric identity management for internet of things. In: conference on IT convergence and security (ICITCS). IEEE; Oct 2014.
16. Granjal J, Monteiro E, Silva JS. Application-layer security for the wot: extending coap to support end-to-end message security for internet-integrated sensing applications. In:

Wired/wireless internet communication. Proceedings of 11th international conference. 2013. p. 140–53.
17. Gerdes S, Seitz L, Selander G, Bormann C, et al. An architecture for authorization in constrained environments. In: IETF, Internet-draft. 2015 (Expires: September 2, 2016).
18. Hardt BD. The OAuth 2.0 authorization framework. RFC 6749 (proposed standard), internet engineering task force [Online]. Available: http://www.ietf.org/rfc/rfc6749.txt, Oct. 2012
19. Maler E, Catalano D, Machulak M, Hardjono T. User-managed access (uma) profile of oauth 2.0. In: IETF, Internet-draft. 2015 (Expires: July 29, 2016).
20. G. Cattaneo, L. Catuogno, A. D. Sorbo, and P. Persiano, "The design and implementation of a transparent cryptographic file system for unix," in Proceedings of the FREENIX Track: 2001 USENIX Annual TechnicalConference, June 25-30, 2001, Boston, Massachusetts, USA. USENIX, 2001, pp. 199–212.
21. ] Microsfot Corp., "Bitlocker drive encryption," 2006, http://technet. microsoft.com/en-us/windows/aa905065.aspx.
22. ] A. Castiglione, L. Catuogno, A. Del Sorbo, U. Fiore, and F. Palmieri, "A secure file sharing service for distributed computing environments," Journal of Supercomputing, vol. 67, no. 3, pp. 691–710, 2014.
23. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST '03 Conference on File and Storage Technologies, March 31 - April 2, 2003, Cathedral Hill Hotel, San Francisco, California, USA. USENIX, 2003.
24. L. Catuogno, H. L¨ohr, M. Winandy, and A.-R. Sadeghi, "A trusted versioning file system for passive mobile storage devices," Journal of Network and Computer Applications, vol. 38, no. 1, pp. 65–75, 2014.
25. S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical report, Tech. Rep., 2000.
26. A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wirelesss ad hoc networks," Wireless Communications, IEEE, vol. 11, no. 1, pp. 48–60, 2004.
27. S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," Ad hoc networks, vol. 11, no. 8, pp. 2661–2674, 2013.
28. Trusted Computing Group, "TPM main specification, version 1.2 rev. 103," Jul. 2007, https://www.trustedcomputinggroup.org.
29. J. L. Griffin, T. Jaeger, R. Perez, R. Sailer, L. van Doorn, and R. C´aceres, "Trusted Virtual Domains: Toward secure distributed services," in Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability (HotDep'05), June 2005.
30. L. Catuogno, A. Dmitrienko, K. Eriksson, D. Kuhlmann, G. Ramunno, A.-R. Sadeghi, S. Schulz, M. Schunter, M. Winandy, and J. Zhan, "Trusted virtual domains - design, implementation and lessons learned," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6163 LNCS, pp. 156–179, 2010.
31. H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium (IHI 2010). ACM, 2010, pp. 220–229. [Online]. Available: http://doi.acm.org/10.1145/1882992.1883024
32. H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security & Privacy, no. 1, pp. 81–85, 2010.
33. ] F. G. Marmol, C. Sorge, O. Ugus, and G. M. P´erez, "Do not snoop my habits: preserving privacy in the smart grid," Communications Magazine, IEEE, vol. 50, no. 5, pp. 166–172, 2012.
34. A. Juels, "Rfid security and privacy: A research survey," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 381–394, 2006.

35. A. C. Sarma and J. Gir˜ao, "Identities in the future internet of things," Wireless personal communications, vol. 49, no. 3, pp. 353–363, 2009.
36. [52] Microsoft Coorp., "What is microsoft account?" http://www.microsoft.com/en-us/account/default.aspx, 2012.
37. M. Needleman, "The shibboleth authentication/authorization system," Serials Review, vol. 30, no. 3, pp. 252–253, 2004.
38. [54] OASIS Organization, "Security assertion markup language (SAML) specification," http://saml.xml.org/saml-specifications.
39. The OpenID foundation, "OpenID specification," http://openid.net/developers/specs, 2014.
40. D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.
41. B. Carminati, E. Ferrari, J. Cao, and K. L. Tan, "A framework to enforce access control over data streams," ACM Transactions on Information and System Security (TISSEC), vol. 13, no. 3, p. 28, 2010.
42. P. A. Bonatti, C. Galdi, and D. Torres, "Erbac: event-driven rbac," in 18th ACM Symposium on Access Control Models and Technologies, SACMAT '13, Amsterdam, The Netherlands, June 12-14, 2013, M. Conti, J. Vaidya, and A. Schaad, Eds. ACM, 2013, pp. 125–136.
43. E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal rolebased access control model".

**Dr. Deepak Singh Tomar** received the B.E. and M. Tech degree in Computer Technology from the Government Engineering College Bhopal, India and Ph. d. Degree in Computer Science and Engineering from Maulana Azad National Institute of Technology, Bhopal, India.

He is an Assistant Professor at Department of Computer Science and Engineering in Maulana Azad National Institute of Technology, Bhopal, India. He is the author of more than 50 research paper. His research interests includes Data Mining, Internet Technology, Network Security, and Cyber Security & Cyber Forensics. He is an editorial Board Member of International Journal of Frontier in Technology, MANIT Bhopal.

Dr. Tomar is the member of IEEE, International Association of Computer Science and Information Technology, Computer Science Teachers Association, International Association of Engineers, International Webmasters Association.

**Kaptan Singh** received the B.E. degree in Computer Science and Engineering from University Institute of Technology, Barkatullah University, Bhopal, India, in 2005 and the M.E. degree in Computer Science and Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, in 2012. He is currently pursuing the Ph.D. degree in Computer Science and Engineering from Maulana Azad National Institute of Technology, Bhopal, India.

He is an assistant Professor at department of Computer Science and Engineering in Truba Institute of Engineering and Information Technology, Bhopal, India. He published 06 research paper in various international journal. His research interest includes the cyber forensic, e-mail forensic, Security in Internet of Things, Cyber Security.