SPIC: A Survey on Security and Privacy Issues, Challenges of Internet of Things

Abdul Razzak Khan Qureshi[1], **Dr. Jitendra Sheetlani**[2]

Research Scholar, Department of Computer Applications, SSSUTMS, Sehore, Madhya Pradesh, India[1]

Associate Professor, Department of Computer Applications, SSSUTMS, Sehore, Madhya Pradesh, India[2]

ABSTRACT: IoT act as a system that uses the infrastructure of the Internet to establish a connection to and between our electronic devices which can be connected from anywhere, anytime and from any devices. Nowadays this system is used in various sectors such as health, home automation, agriculture, smart city and telecommunication etc. This provides an efficient and effective solution to these sectors but it faces the security and privacy issues and challenges because of its ad hoc behaviour. In this paper, we mainly emphasis the survey on privacy and security issues and challenges of IoT. We also discuss the layered architecture of internet of things, security principles with related security threats and their solutions to combat from these threats. We also discuss some future aspects of the IoT securityconjuncture in the various fields.

KEYWORDS: Internet of Things, Security and Privacy, Threats, IoT Applications.

I. INTRODUCTION

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established.[1] Over 9 billion 'Things' (physical objects) are currently connected to the Internet, as of now. In the near future, this number is expected to rise to a whopping 20 billion. For making physical or virtual connections, it uses objects like sensors, actuators, etc. The success of IoT infrastructure and applications depends on IoT security. The IoT collects the data from a vast geographical region using sensors [3]. IoT is a very good and intelligent technique which reduces human effort as well as easy access to physical devices. This technique also has autonomous control feature by which any device can control without any human interaction. The below figure 1 shows the connectivity of various devices of different fields with Internet and exchange data between them. So above figure represent the connectivity of world through various existing technologies. "Things" in the IoT sense, is the mixture of hardware, software, data, and services. "Things" can refer to a wide variety of devices such as DNA analysis devices for environmental monitoring, electric clamps in coastal waters, Arduino chips in home automation and many others. These devices gather useful data

with the help of various existing technologies and share that data between other devices. Examples include Home Automation System which uses Wi-Fi or Bluetooth for exchange data between various devices of home.

Fig.1 : Connectivity of devices with various fields [2]

There are four main components used in IoT:

- Low-power embedded systems
  Less battery consumption, high performances are the inverse factors play a significant role during the design of electronic systems.
- Cloud computing
  Data collected through IoT devices is massive and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
- Availability of big data
  We know that IoT relies heavily on sensors, especially real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
- Networking connection
  In order to communicate, internet connectivity is a must where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

1.1 Characteristic of IoT

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that does not use IP, so IoT is made possible.
- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- A device that is connected to another device right now may not be connected in another instant of time.
- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

1.2 Advantages of IoT

Internet of things poses various advantages in different area of sectors like:

- Communication
- Automation
- Remote Control
- Better Decision
- Money control
- Time Saving
- Continuous Monitoring
- Efficient handling

1.3 Disadvantages of IoT

- Lagging of standard compatibility
- More opportunities for failure
- Loss of privacy or security
- More dependent on technology

The internet of things is more vulnerable to various types of security threats due to their ad hoc nature so it becomes the challenging task for us and to mitigate or combat various techniques has been developed. In this paper, we present the survey of the security and privacy issues and their measures solution. The rest of the paper is organized in such manner: Section II presents the security goals of the internet of things. Section III presents the layered architecture and the security threat related to each layers. Section IV presents the Privacy challenges of Internet of Things. Section V presents the some solutions from the security threats. And last section gives overall conclusion of the whole research paper.

II. SECURITY GOALS OF INTERNET OF THINGS

In the literature, traditional security goals are divided into three major groups: (i) confidentiality, (ii) integrity, and (iii) availability, known as a CIA-triad. Confidentiality: It ensures that sensitive information can only be accessed by authorized objects or users. With the advent of IoT, it is essential to guarantee the confidentiality of IoT objects, as they may deal with sensitive information like credit cards and medical records. For example, the authors in [5] illustrate the impacts of an authorized access to medical objects which may expose personal information or result in life-threatening cases. In an IoT context, integrity is also essential for providing reliable solutions in which only valid commands and data are received. Integrity compromise can result in harmful consequences. For instance, the authors in [6] describe successful attacks against an Insulin Pump which can reveal patients' privacy. IoT availability [24] is crucial to assure that IoT services are available and cannot be interrupted. Despite the popularity of the CIA-triad, the authors in [7] prove its insufficiency of addressing novel threats, emerging in a collaborative environment. To cope with this issue, they offer a thorough set of security goals called information, assurance, and security (IAS) octave, referred to as the IAS-octave, by examining a huge number of information in literature in terms of security. Table 1 highlights the security goals suggested by the IAS-octave, along with their definitions.

Table 1. Security goals of IoT [4]

Security Requirements	Definition
Confidentiality	The process in which only authorized objects or users can get access to the data
Integrity	The process in which data completeness, and accuracy is preserved
Non-repudiation	The process in which an IoT system can validate the incident or non-incident of an event
Availability	An ability of an IoT system to make sure its services are accessible, when demanded by authorized objects or users
Privacy	The process in which an IoT system follows privacy rules or policies and allowing users to control their sensitive data
Audibility	Ensuring the ability of an IoT system to perform firm monitoring on its actions
Accountability	The process in which an IoT system holds users taking charge of their actions
Trustworthiness	Ensuring the ability of an IoT system to prove identity and confirm trust in third party

III. LAYERED ARCHITECTURE OF IOT

The architecture of IoT should be flexible in nature, because it has to interconnect heterogeneous objects in billions and trillions. There are many proposed architectures for IoT but all of them are not yet converged to form a unique reference model yet. Many projects are available that have helped to create a common architecture of IoT based on technological changes and researches. We will be discussing two architectures which are used generally by many researchers and in industry from pool of architectures available [8].

3.1 Three Layer Architecture

The most basic architecture is three-layer architecture [9–11] as shown in figure 2. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

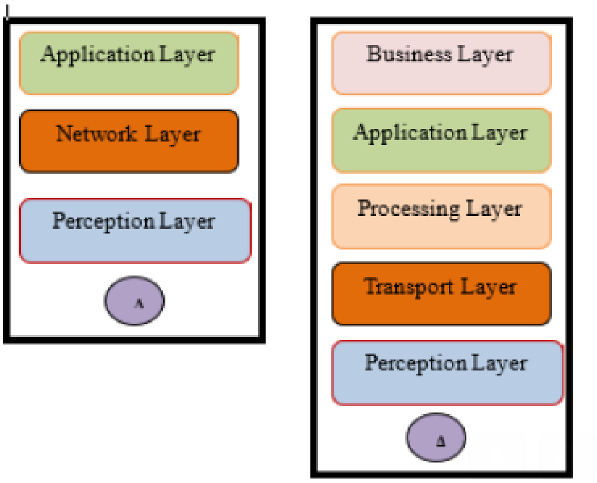

Fig. 2: Three and Five layer architecture of IOT

(i) The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment. The lowest layer of the IoT architecture and also the brain of the three layered architecture. This layer also affected by the various types of attack such as eavesdropping, node capture, fake node, replay attack etc. The brief description about the perception layer attack is discussed in table 2.

Table 2: Security Threats at Perception Layer

Threats	Definition
Eavesdropping	It is an unauthorized real time attack where private communications, such as phone calls, text messages, fax transmissions or video conferences are intercepted by an attacker.
Node Capture	Where attacker gains full control over a key node, such as a gateway node. It may also leak all information including communication between sender and receiver, a key used to make secure communication and information stored in memory
Fake Node and Malicious	In this type of attack an attacker adds a node to the system and inputs fake data. It main purpose is to stop transmitting real information.
Replay Attack	It is also called as a play back attack. Where an intruder eavesdrops on the conservation between sender and receiver and takes authentic information from the sender
Timing Attack	It permits an attacker to discover vulnerabilities and extract secrets maintained in the security of a system by observing how long it takes the system to respond to different queries, input or cryptographic algorithms

(ii) The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data. It transfers the information through wireless technology such as Wi-Fi, Bluetooth, and Infrared etc. [17] Hence, this layer is mainly responsible for transferring the information from perception layer to upper layer. There are some common security problems in LAN, Wi-Fi, and Internet. They are: illegal access network, eavesdropping information, confidentiality and integrity damage, DoS attack, Man-in-the-middle attack etc. Here, in table 3 descriptions about the security threats at network layer is described below:

Table 3: Security Threats at Network Layer

Threats	Definition
Denial of Service (DoS) Attack	A DoS attack is an attack to prevent authentic users from accessing devices or other network resources
Main-in-The-Middle Attack	This attack is an attack where the attacker secretly intercepts and alters the communication between sender and receiver who are under assumption that they are directly communicating with each other
Storage Attack	The user store information either on storage devices or the cloud. The attacker will try to attack both storage devices and cloud to retrieve user's information and try to change into incorrect details
Exploit Attack	An exploit is any immoral or illegal attack in a form of software, chunks of data or a sequence of commands

(ii) The application layer is responsible for delivering application specific services to the user. This layer is the topmost layer of the IoT architecture that provides the delivery of all services in various fields. It includes cloud computing, intelligent transportation, environmental monitoring etc. Application layer has some security problems such as data security, cloud platform security, data protection and recovery etc. To solve the security problems of this layer, authentication and privacy protection are needed. Particularly, password management is very important for data security [1]. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health. Here table 4 give brief detail about the security threats at application layer.

Table 4: Security Threats at Application Layer

Threats	Definition
Cross Site Scripting	It is also known as an injection attack. It permits an attacker to insert a client-side script, such as java script in a trusted site viewed other users
Malicious Code Attack	It is intended to cause undesired effects and damage the system with the help of a code in any part of software. It is not be blocked or controlled by anti-virus tools
The ability of dealing with Mass Data	It has no ability to deal with data processing according to the requirements due to a large number of devices and a massive amount of data transmission between users, As a result, it leads to network disturbance and data loss.

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five layer architecture, which additionally includes the processing and business layers [9–12]. The five layers are perception, transport, processing, application, and business layers (see Figure 4). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

(i) The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC. This layer also get compromised with different types of security threats which is described in table 5.

Table 5: Security Threats at Transport Layer

Threats	Definition
DoS Attack	It is related to the network layer. Where an attacker sends a large amount of data to make network traffic inundated. Therefore, the massive consumption of system resources exhausts the IoT and makes the user not capable of accessing the system
Malicious Insider Attack	It happens from the inside of an IoT environment to access the personal information of users. Where an authorized user access the information of other users

(ii) The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big d
ata processing modules. In this layer, exhaustion and malware threat is found whose description is done in table 6.

Table 6: Security Threats at Processing Layer

Threats	Definition
Exhaustion	The aim is to exhaust the system resources, such as battery and memory resources. As IoT has a distributed nature; therefore, it does not have a high amount of hazards. It is comparatively easier to implement protecting procedures against it
Malwares	Its main focus is on an attack on the confidentiality of the information of users. In the form of executable codes, scripts and contents to affect the confidentiality

(iii) The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further. In this layer zero-day attack and business logic attack is found and it is described in table 7.

Table 7: Security Threats at Business Layer

Threats	Definition
Business Logic Attack	It takes advantage of faults in a programming. The exchange of information between a user and a supporting database of an application can be managed by this layer
Zero-Day Attack	It uses a security hole or a problem in an application that is unfamiliar to a vendor. Where the security hole is exploited by the attacker to take control without user's consent and without their knowledge.

Another architecture proposed by Ning and Wang [12] is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

3.2 Cloud Based Architecture

As described in the figure 3, cloud-based architecture of IoT contains mainly physical layer, process layer, gateway layer and cloud services.[13]

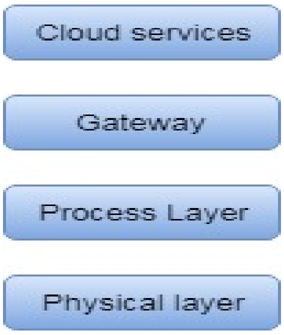

Fig. 3: Cloud based architecture of IoT

- Physical layer contains technologies used like RFID, to collect the information from the devices connected in the network.
- As the name indicates the process layer tries to analyze the information received.
- Gateway layer contains the network information like LAN or WAN etc. It performs data transformations and makes the received raw data suitable for cloud services. It establishes path for end to end communication.
- The main and important part of cloud-based architecture is cloud services. It is responsible for executing the data (collected from industries or user etc.) by using data analytic algorithms. The main components of cloud services are : 1) Broker and message queue , 2) Data base, 3) Server and 4) Event managers.
- Broker and message queue, are responsible for managing incoming messages. It streamlines the messages from various clients and processes them. It helps in increasing the scalability of the network (i.e., number of devices can be increased.)
- Database is used for the storage purpose.
- Server helps in visualizing the data, reporting. It helps user to understand data. It also provides recommendations to the user.
- Event managers, performs event handling. It executes high priority interrupts like fire alarm. In case of emergency, it triggers certain actions [15].

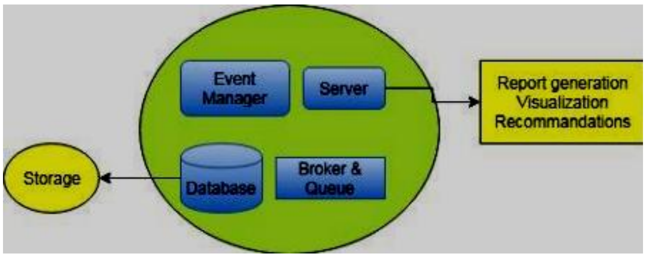

Fig. 4: Cloud services

3.3 Fog based architecture

Fog computing is latest technology. It extends the features of cloud computing. Fog computing offers processing the data (computing), takes care of storage and provides the network information between client and the cloud services. Computing (processing the data) occurs in decentralized manner. Here the data computing, storage and resource management are distributed in an efficient manner between client and cloud. [13,14]

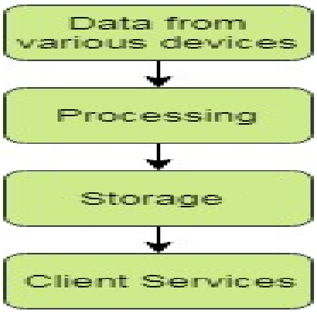

Fig.7: Fog based architecture

Both cloud computing architecture and fog computing architecture is more or less same [13]. The only difference in this architecture is the computing of data takes place at devices, which are connected at the edge of the network. So, the other name of fog computing is edge computing. As discussed in cloud-based architecture, the scalability is more in this architecture.

3.4 SoA-based Architecture

In service-oriented architecture a service layer is introduced between network and application layer to make the architecture more flexible and to provide the data services in IoT. It is model used to connect different services using interfaces and protocols. SoA is capable of reusing the software and hardware components, which improves feasibility of using SoA in IoT. There are four layers in this architecture perception layer, network layer, service layer, application layer. Here, the service layer is divided into 2 sublayers known as service composition, service management sublayer. The perception layer present at the bottom of the architecture collects data from sensors, as in the previous architecture. Network layer also performs the same function as the basic architecture, i.e. determining the routes, providing data transmission via the same integrated network. [16]

Service layer acts as a middle layer provides all the services for supporting application layer. This layer consists of all the functionalities like discovery of service which is used to discover the service request which is desired , composition of services to connect or interact with the connected object in the architectures and also it performs integration of various services to meet the requirements of service request , management of services is also done to manage the service requests and along with that service interfaces are present which are used to support the various interactions that are present among all the services that are provided. The upper layer is the application layer that performs same functions as that of application layer of the basic architecture. It supports all the applications like smart homes, smart cities etc.

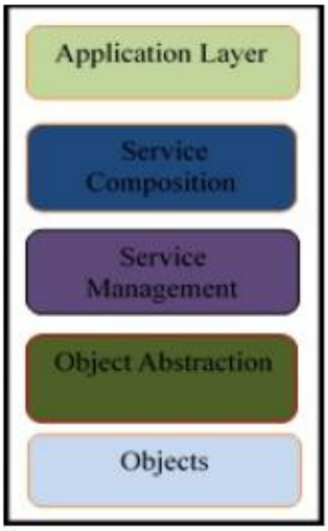

Fig. 8. SoA-Based Architecture

IV. INTERNET OF THINGS PRIVACY ISSUES

Privacy in IoT defined by the Internet security glossary [18]as"the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others".

In IoT, the network of devices tries to gain data from the environment, and then broadcast it with some events to the server that has applications. During all that steps, privacy must be managed, in the device, storage, communication and while processing. The privacy with the protection of sensitive information in IoT was identified as one of the critical issues that need to be addressed [19].

A. During Communication Privacy

Data confidentiality when data being transmitted through network channels commonly achieved using encryption techniques. Encryption in some cases adds data to packets to provide tracing property. Communication Protocol for security can provide some solutions for privacy. Pseudonyms can be used during communication for encryption that may help to decrease the vulnerability. Devices should communicate only if it is necessary, to reduce privacy exposing during communication. Also, devices must be able to disconnect from the network if it is inactivity to minimize tracking of location information. The authorized device only allowed to communicate and if it is turned on, it must re-authenticate itself to the network before start dealing with any information [19].

B. Device Privacy

Sensitive information in IoT could be targeted when unauthorized access happens in hardware or software. For example, an invader able to re-program a camera to make it sends information not to the authorized server only, but to invaders too. To provide the privacy in devices, there are many issues must be addressed, like device location privacy which can be achieved by Multi-Routing Random Walk Algorithm for Wireless Sensor Network (WSN), protecting the identification of device nature that can be achieved by adding noise and protecting the sensitive information even in case of device theft by using Quick Response Code technique [19].

C. Privacy at Processing

Personal and sensitive data must be processed in a suitable manner and for the processing aim only. The acceptance and the data owner authentication are necessary gained before exposing personal information to third parties. Digital Rights Management (DRM) system is a good method that can be used to control exchanged data rights and defend against illegally processing. DRM works on the base of devices trusted and secure to be effective. The permission and awareness of data owner must be obtained before processing or even dealing with personal data. User notification helps to avoid improper use of private data and sensitive information [19].

D. Privacy in Storage

To protect information privacy, store only the needed and important information to keep the least possible amount of stored information. Information is transported only in case of "need-to-know". Anonymization could be used to disguise the identity of the stored information. A database must limit access to statistical data only. To ensure independency of the output on other database records, differential privacy can be used or adding noise technique [19].

V. INTERNET OF THINGS SECURITY SOLUTIONS

For the security concern of internet of things various solutions has been given by the researchers/ authors. Here we are representing the problems and their solutions which is shown in table 8.

Table 8: Security solutions of Internet of Things

Year	Author	Problem	Solution
2014	Porambage et al. [20]	Resource-constrained	(i) PAuth Key protocol, (ii) An authentication schemes (iii) keying mechanism
2010	C. Thompson [21]	Digital Forgetting and Data Summarization	(i) Delete encrypted data when decryption key is deleted (ii) Acquire only the strictly needed data rather than all data (iii) Apply knowledge discovery in databases and data miningtechnologies
2016	Salman et al. [22]	Authentication and Authorization	(i) Lightweight authentication and key establishment mechanisms (ii) Frameworks based on device fingerprinting techniques (iii) Context-aware access control models and enforcing mechanisms
2016	Davies et al. [23]	Edge Computing and plug in architecture	(i) Software modules on the edge to overcome privacy concerns (ii) Privacy aware systems to allow user control over data (iii) Decentralized architectures based on Personal-Cloud Butlers

2011	Zhou et al. [25]	Multimedia traffic security	(i) Media-mindful Traffic Security Architecture (MTSA) was proposed (ii) MTSA is empowered with apparent mixed media mutilation methods. (iii) The MTSA lessens the multifaceted nature of sight and sound calculations and diminishes the size of the offers MTSA is acquired from a setting mindful media administration-based security structure.
2016	Morchon et al.[26]	Light wight security	HIMMO is highlighted by full arrangement opposition, gadget and back-end confirmation and check, pair-wise key understanding, support for numerous TTPs and key escrow, or security against DoS assaults
2008	B. Zhou et al. [27]	Data Anonymizing and denaturing	(i) Data brokers and separation algorithms to offer flexibility toservice providers, yet respect user-predefined access rules (ii) Generalization to mask personal data (iii) Frameworks that provide emotion analytics lifecycle to allow denaturing

VI. CONCLUSION

Security and privacy are the major issue of the internet of things as it is the emerging technology nowadays. Because of its ad hoc nature it can be access from anywhere but at the same time the nodes of the network may compromise from the threats or opponents which degrade the performance in case of efficiency and accuracy of the IoT and it also does not maintain the integrity of the data. In this paper, we present the survey of the security and privacy issues of the IoT. We also present the layered architecture of IoT and also discuss the threats found at each layer of the IoT. Together with the security threats we also discuss some privacy issues and their solutions. In future work, need to develop such security technique which the integrity of the system and improves the performance of the IoT which also help to thwart the security of the network.

REFERENCES

[1] https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/
[2]https://www.gkmit.co/blog/internet-of-things-iot-introduction-applications-and-future-scope.
[3] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[4] Akram Abdul-Ghani, H.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey Based on a Building-Blocked Reference Model. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 2018, 9.
[5] Zhang, M.; Raghunathan, A.; Jha, N.K. Trustworthiness of medical devices and body area networks. Proc. IEEE 2014, 102, 1174–1188.
[6] Li, C.; Raghunathan, A.; Jha, N.K. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011, Columbia, MO, USA, 13–15 June 2011; pp. 150–156.
[7] Cherdantseva, Y.; Hilton, J. A Reference Model of Information Assurance & Security. In Proceedings of the 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany, 2–6 September 2013.
[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.
[9] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68– 90, 2015.
[10] O. Said and M. Masud, "Towards internet of things: survey and future vision," International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.
[11] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.
[12] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp. 257–260, December 2012.
[13] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization

framework?” IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.

[14] Harika Devi Kotha, V Mnssvkr Gupta, “IoT Application, A Survey”, International Journal of Engineering & Technology, 7 (2.7) (2018) 891-896

[15] Ademir F. da Silva, Ricardo L. Ohta, Marcelo N. dos Santos, Alecio P.D. Binotto, "A Cloud-based Architecture for the Internet of Things targeting Industrial Devices Remote Monitoring and Control," IFAC-PapersOnLine, Volume 49, Issue 30, 2016, Pages 108-113.

[16] Karandeep Kaur, “Survey on Internet of Things – Architecture, Applications, and Future Trends”, First International Conference on Secure Cyber Computing and Communication (ICSCCC)-2018. In proceeding of IEEExplore digital library 978-1-5386-6373-8/18.

[17] Gurpreet Singh Mathuru, Priyanka Upadhyay and Lalita Chaudhary, “The Internet of Things: Challenges & Security Issues”, IEEE International Conference on Emerging Technologies (ICET), 2014, pp. 54-59.

[18] "RFC 2828, Internet Security Glossary," May 2000. [Online]. Available: https://www.ietf.org/rfc/rfc2828.txt.

[19] J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.

[20] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, “Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications,” International Journal of Distributed Sensor Networks, vol. 2014, Article ID 357430, 14 pages, 2014.

[21] C. Thompson, “25 Ideas for 2010: Digital Forgetting,” 25 Ideas for 2010: Digital Forgetting, November 2009.

[22] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, “Identity-based authentication scheme for the Internet of Things,” in Proceedings of the 2016 IEEE Symposium on Computers and Communication, ISCC 2016, pp. 1109–1111, Italy, July 2016.

[23] N.Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, “Privacy mediators: Helping IoT cross the chasm,” in Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, HotMobile 2016, pp. 39–44, USA, February 2016.

[24] Harsh Pratap Singh, R. P. Singh, Rashmi Singh, and Bhaskar Singh, “Internet of Things (IoT) Based on User Command Analysis and Regulator Systems”, International Conference on Recent Trends in IoT and Blockchain, 2019

[25] Liang Zhou, Nanjng University of Posts and Telecommunications Han-Chieh Chao, “Multimedia Traffic Security Architecture for the Internet of Things” in IEEE Network, May/June 2011, 35-40.

[26] Oscar Garcia Morchon, Domingo Gomez Perez, Jaime Gutierrez, Ronald Rietman, Berry Schoenmakers, and Ludo Tolhuizen, “HIMMO: A Lightweight Collusion-Resistant Key Pre-distribution Scheme” in ACM 2016.

[27] B. Zhou, J. Pei, andW. Luk, “A brief survey on anonymization techniques for privacy preserving publishing of social networkdata,” ACM SIGKDD Explorations Newsletter, vol. 10, no. 2, p. 12, 2008.

[28] Jitendra Sheetlani, Anil Kumar, Harsh Kumar Gupta, “Analysis of IOT Technology Based Cattle Fitness Monitor System”, Journal Current Science, 2019, Vol-20 issue-06.